CrowdStrike Products

CROWDSTRIKE

OBSERVATIONS FROM THE FRONT LINES OF THREAT HUNTING

A 2018 Mid-Year Review From Falcon OverWatch

INTRODUCTION

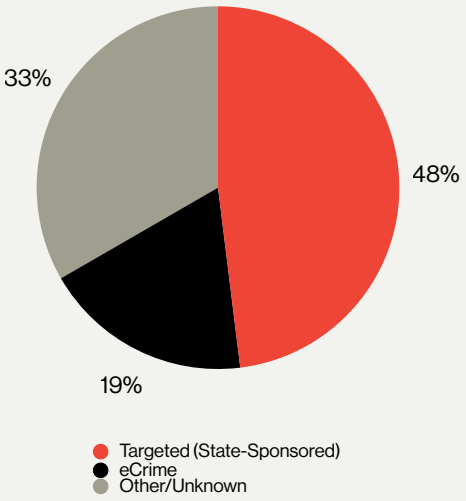
CrowdStrike® Falcon® OverWatch™ is the CrowdStrike managed threat hunting service (MDR). OverWatch's mission includes using the market-leading CrowdStrike Falcon endpoint security platform to detect intrusions by sophisticated or persistent adversaries that might otherwise go unnoticed, and then providing timely, actionable and relevant notifications to customers [1].

This report provides a summary of OverWatch's findings from intrusion hunting during the first half (January through June) of 2018. It reviews intrusion trends during that time frame, provides insights into the current landscape of adversary tactics and delivers highlights of notable intrusions OverWatch identified. OverWatch specifically hunts for targeted adversaries. Therefore, this report's findings cover state-sponsored and targeted eCrime intrusion activity, not all forms of attacks.

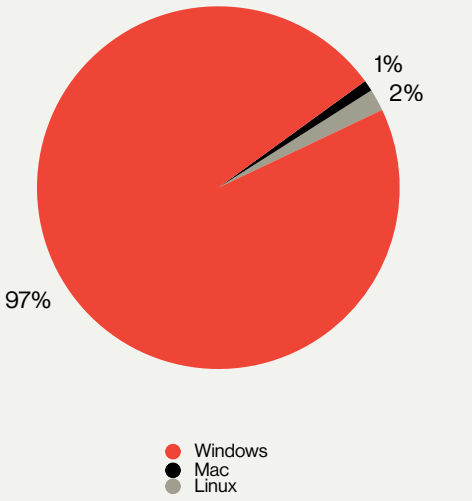
INTRUSIONS SUMMARY

OverWatch observed and analyzed numerous intrusion events during this time period.

INTRUSION CASES* BY THREAT TYPE



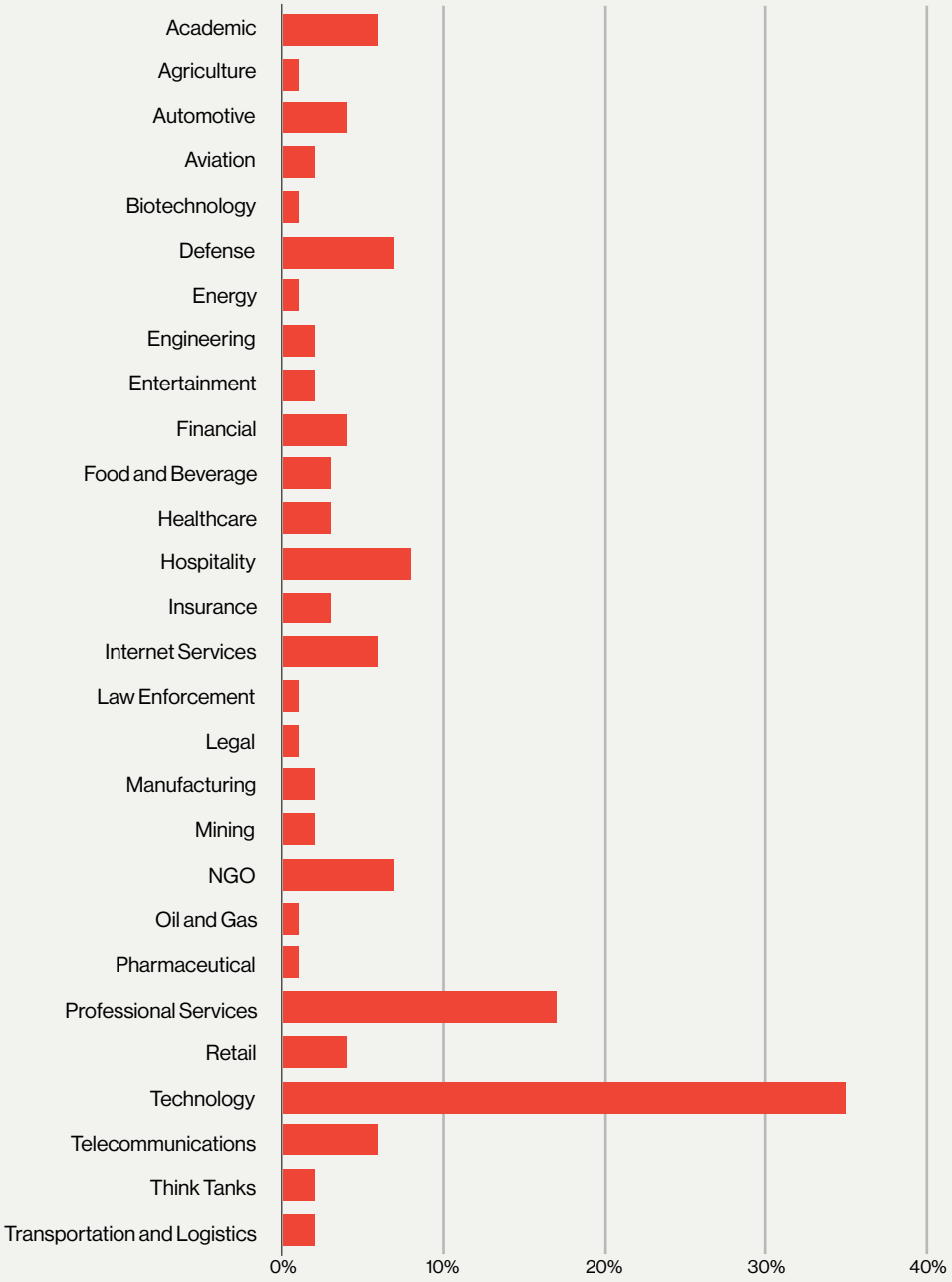
INTRUSION CASES* BY OPERATING SYSTEM



*Percentages in these graphs reflect only those intrusion cases involving notable sophisticated and/or persistent adversaries.

[1] For more information on how Falcon OverWatch performs its mission, please see the Falcon OverWatch product page: https://www.crowdstrike.com/products/falcon-overwatch/

PERCENTAGE OF INTRUSION CASES BY VERTICAL



Note: Combined percentages add up to more than 100% because some victims belong to more than one vertical.

While OverWatch analyzed numerous intrusions during this period, only some could be attributed to an adversary at this time. CrowdStrike Falcon Intelligence™ has tracked over 110 specific adversary groups, as well as many unidentified actors. The following chart shows the number of intrusion cases attributed to an adversary by industry vertical.

Vertical	VENOMOUS BEAR	Suspected BEAR	AURORA PANDA	JUDGEMENT PANDA	LOTUS PANDA	PIRATE PANDA	WICKED PANDA	Suspected PANDA	HELIX KITTEN	OCEAN BUFFALO	CARBON SPIDER	Suspected SPIDER
Academic												3
Agriculture												1
Biotechnology				1								
Defense								5				
Energy					1							
Entertainment								1				
Financial	2											
Food & Beverage											1	1
Hospitality						1				1		4
Insurance												2
Internet Services							2					
Legal												1
Mining							2					
NGO		1						5				
Pharmaceutical				1					2			
Professional Services		2					2	5				
Retail											2	2
Technology		1	1				2	9				1
Telecommuni-cations								1				2
Think Tanks		1										
Transportation & Logistics								1				1

When the Falcon OverWatch team analyzes an intrusion, it uses the MITRE ATT&CK™ matrix[2] as a framework to categorize adversary behavior. A heat map of observable tactics, techniques and procedures (TTPs) that were tracked across sophisticated and/or persistent intrusions through the first half of 2018 is available in the Appendix at the end of this report.

[2] More information about Mitre's ATT&CK matrix is available online at: https://attack.mitre.org/wiki/ATT%26CK_Matrix

E-CRIME ACTORS SHOW INCREASING INTEREST IN CRYPTOCURRENCY MINING

During the first quarter of 2018, Falcon OverWatch identified multiple intrusions against victims in the legal and insurance industries where criminal perpetrators gained privileged access to internal networks. Historically, the OverWatch team has seen such actors take advantage of their access to steal sensitive information that could be used for financial gain. However, in these cases, adversaries pursued post-exploitation financial gain by deploying cryptocurrency miners. They employed techniques that allowed them to perform extensive lateral movement, creating as large a foothold as they could to commandeer mining resources. It appears that the rise in the value of cryptocurrencies during the winter of 2017 led eCrime actors to shift their preferred objectives in several cases. Two examples of these intrusions are the following:

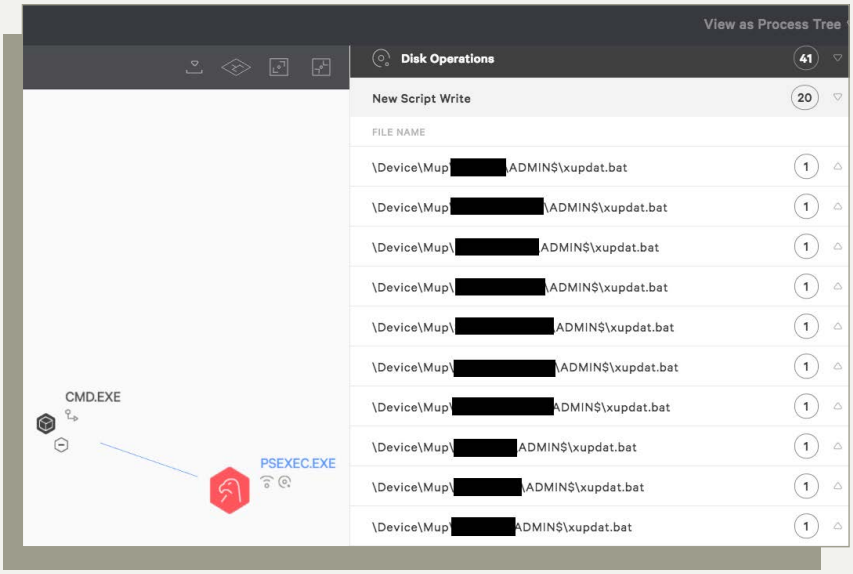
- In January, OverWatch observed an unidentified criminal actor installing a number of malicious tools on compromised hosts belonging to an organization in the legal vertical. These tools included the xDedic[3] RDPPatch tool, the Monero cryptocurrency mining tool XMRig and a disk usage tool used for reconnaissance purposes.
  - RDPPatch allows threat actors to patch the Windows RDP substitution system, which then supports multiple user logins to the compromised host. The RDPPatch binary used in the attack was:
    FILE: C:\Temp\3\Temp1_xrdp.zip\xRdp.v2.1.exe
    HASH: daddc833bffcade36b432b21046487b29dcd2a162d91b503334a52caee9c1fd2
  - XMRig is an open-source Monero cryptocurrency mining software distributed via a public code repository. During this intrusion, the actor attempted to download and install XMRig with the likely intent to passively generate revenue while the host was not otherwise in use:
    FILE: XMRig 64bit version 2.4.3
    HASH: 08b55f9b7dafc53dfc43f7f70cdd7048d231767745b76dc4474370fb323d7ae7
    NOTE: Installed from minergate[.]com/download/win-srv
  - The disk usage tool observed was the otherwise legitimate tool, TreeSize[4]. TreeSize provides an operator with the ability to easily view disk space usage, which could facilitate actions on objectives.
- In late January, Falcon OverWatch assisted CrowdStrike Services in responding to an engagement on the network of an organization in the insurance vertical. OverWatch uncovered widespread malicious activity involving WMI and PowerShell on multiple hosts. Among the extensive telemetry collected during the intrusion were several notable TTPs, including:
  - Attempts to download Pupy RAT[5] files from **https://54.183.214[.]137:8080/eiloShaegae1** and **https://54.183.214[.]137:8080/IMo8oosieVai**
  - Accessing the Domain Controller via RDP using valid credentials
  - Use of PowerShell for host reconnaissance and credential theft
  - Creation of malicious scheduled tasks via Microsoft Management Console

Beyond these behaviors, the adversary also used PsExec to execute a batch file on numerous hosts.

[3] xDedic is a criminal Russian underground marketplace that brings together affiliates who want to either buy or sell access to compromised dedicated RDP servers. The compromised servers are used for activities such as spam email or as VPN endpoints.

[4] https://www.jam-software.com/treesize_free/

[5] https://github.com/n1nj4sec/pupy



Adversary use of PsExec to deploy xpudate.bat to various hosts in an attempt to install Monero miners across the victim network.

The batch script, named xupdate.bat, used PowerShell to download and install a Monero miner:
FILE: C:\Program Files\MSUtil\x.exe
HASH: 85623bf5df6e1ad047bc1b8e94e1db91b922907357251cb7451e1507a38c6426
NOTE: Downloaded from https://bread.rumpus[.]press/zwxjwy

The rise in the value of cryptocurrencies during the winter of 2017 led eCrime actors to shift their preferred objectives in several cases.

BLURRED LINES CONTINUE

A key theme noted in the CrowdStrike 2018 Global Threat Report was the blurring of lines between the TTPs of highly skilled nation-state adversaries and their criminally motivated counterparts. That trend has continued as CrowdStrike saw less skilled criminal actors adopt more advanced TTPs used by well known nation-state actors. One specific manner in which this recurring trend was observed was with the malicious use of TeamViewer software. TeamViewer is a legitimate, publicly available remote control software tool[6]. Malicious use of TeamViewer came to light in 2013 when the adversary that CrowdStrike first tracked as TEAM BEAR was found using the software maliciously to facilitate remote access to targets. Malicious versions of TeamViewer ensured persistence on victim machines, hid their locations and were configured to report to command and control (C2) servers. Since 2013 when TEAM BEAR's tactics were publicly reported, multiple adversaries possessing varying levels of capability and intent, including criminal, have adopted the malicious use of TeamViewer in their operations. Despite extensive public exposure of this known threat, even recently[7], OverWatch continues to see the malicious use of TeamViewer plague organizations across the spectrum of industry verticals.

[6] https://github.com/n1nj4sec/pupy

[7] https://blog.avast.com/update-ccleaner-attackers-entered-via-teamviewer

- In the first quarter of 2018, OverWatch uncovered malicious activity leveraging TeamViewer specifically targeting the hospitality sector. At the time of this writing, at least four global hospitality organizations were victimized during the quarter. In each case, TeamViewer binaries were masquerading as otherwise expected file names, including **msoobe.exe** (Microsoft Out-of-Box Experience) and **jusched.exe** (Java Update Scheduler). Victims' TeamViewer config files had also been modified so that TeamViewer network communications would connect to actor-controlled C2 nodes.

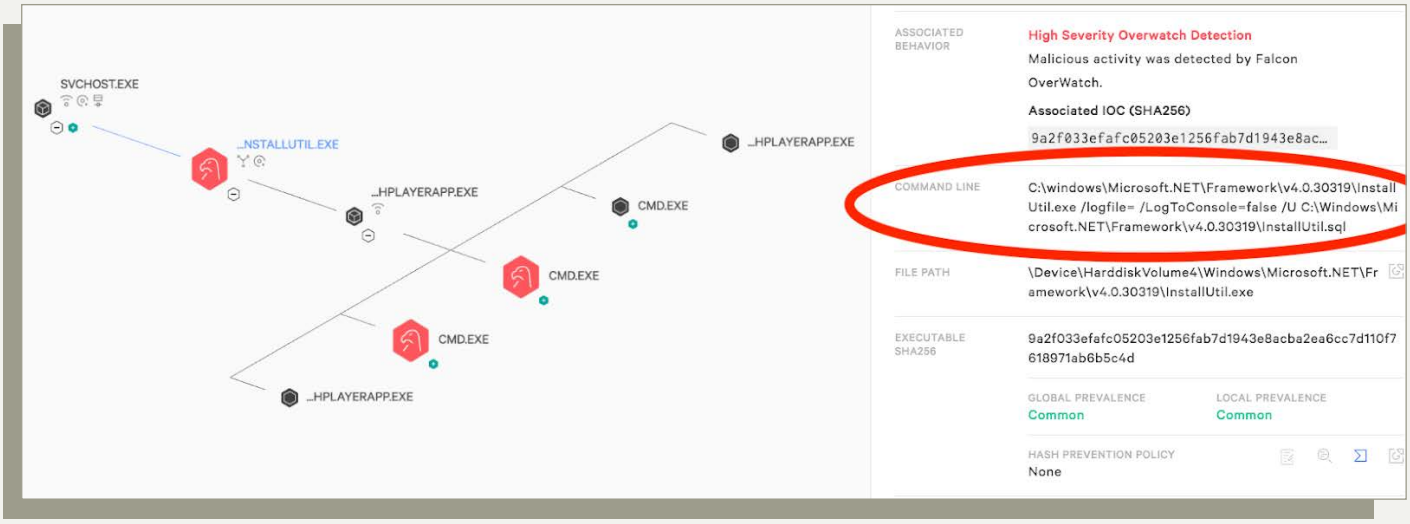
  The malicious TeamViewer activity at each hospitality victim shared overlapping C2 infrastructure, indicating a common adversary was responsible. C2 domains observed in this campaign were:

  - **teravisore[.]ru**
  - **votonafo[.]ru**
  - **sistemappruve[.]ru**
  - **lirubhdk1753[.]ru**

- In January, an unknown actor gained remote access to the network of an entertainment organization. Among the behaviors observed were WebDAV scans, enumerating SMB shares, lateral movement and creating malicious scheduled tasks via schtasks.exe and at.exe. The initial entry, however, was via TeamViewer. The adversary used valid credentials to log into TeamViewer remotely, and then dropped various malicious tools that facilitated the extensive follow-on activity.

Despite extensive public exposure of this known threat, even recently, OverWatch continues to see the malicious use of TeamViewer plague organizations across the spectrum of industry verticals.

After gaining initial access to the network via TeamViewer, the actors moved laterally to another host and deployed PlugX using a method that leverages InstallUtil.exe[8] to bypass whitelisting. InstallUtil.exe is a Microsoft signed binary that can run any .NET executables, bypassing AppLocker restrictions while doing so. OverWatch has observed actors exploiting that capability by recompiling malicious payloads as .NET executables and running them with InstallUtil. The command line in the Falcon console detection of this event demonstrates the tactic:



Adversary use of InstallUtil.exe to deploy PlugX implant.

As noted in the image above, InstallUtil.exe executes with a command line employing the following format:
InstallUtil.exe "/logfile= /LogToConsole=false /u" {path to implant}

In this case, the path to the implant points to a previously unknown InstallUtil.sql file. This binary was dropped by the adversary and further analysis identified it as a variant of the PlugX RAT, which is malware commonly associated with PANDA threat actors. PlugX has been designed to leverage Dynamic-Link Library (DLL) side-loading[9] to successfully obtain execution, typically via a legitimate and signed host binary. During this event, PlugX was side-loaded by the otherwise legitimate FlashPlayerApp.exe process spawned by IntallUtil.exe as shown in the process tree above. The adversary then was able to leverage PlugX to initiate the the interactive cmd.exe shells.

IT CAN HAPPEN TO ANYONE

In March, a business technology solutions organization began deploying the Falcon platform across its network. OverWatch quickly identified evidence of an ongoing, legacy intrusion. An adversary was actively targeting the web-hosting branch of the victim company, resulting in successful exploitation of numerous servers. C2 infrastructure included domains and IP addresses attributed to WICKED PANDA. Malicious network activity in this campaign was seen connecting to the following:

- **backup.aolonline[.]cc**
- **tiwwter[.]net**
- **bot.googlecustomservice[.]com**
- **mall.googlebills[.]net**
- **login.googlebills[.]net**
- **43.239.159[.]41**
- **45.32.9[.]211**
- **103.84.91[.]78**
- **103.84.91[.]146**

During the time of observation, the actor performed limited actions on objectives beyond staging their custom tools, which included PlugX[10]. In this case, OverWatch assesses with moderate confidence that the victim was not the primary target. Rather, the actor was likely taking advantage of this target of opportunity to build their malicious infrastructure to facilitate future operations. An important take-away from this event is the reminder that sophisticated, nation-state adversaries could target anyone as part of a larger operation. OverWatch has observed similar activity across several industry verticals. As a result, customers in any sector could find themselves in the cross-hairs of targeted adversaries.

An important take-away from this event is the reminder that sophisticated, nation-state adversaries could target anyone as part of a larger operation.

[8] https://docs.microsoft.com/en-us/dotnet/framework/tools/installutil-exe-installer-tool

[9] https://attack.mitre.org/wiki/Technique/T1073

[10] https://attack.mitre.org/wiki/Software/S0013

POLICY NGOs A PRIME TARGET

During the last several months, OverWatch has observed multiple adversary campaigns against policy NGOs (nongovernmental organizations) operating overseas. In the first case, threat actors exploited an external server prior to Falcon endpoint protection deployment. Once Falcon was installed, OverWatch was able to identify active use of China Chopper[11] on the victimized server when the adversary connected to the web shell. It appeared the actor had long had a foothold in the environment and was returning to perform access maintenance. Over the course of an hour, they performed host, account and network discovery operations. Specifically, they tested previously compromised credentials by attempting to connect to remote network shares with several valid accounts.

Before leaving, the adversary wrote files associated with the open-source HTran reverse proxy tool[12] in a likely attempt to redirect C2 traffic from additional targets. HTran files were written to the following locations:

- **C:\ProgramData\htran.exe**
- **C:\HR\htran.exe**
- **C:\[REDACTED]\Template\htran.exe**

Falcon endpoint protection customers should be aware that they can turn on Falcon's prevention policy setting to block the Chopper web shell.

A separate and distinct set of adversary activity was also observed against another policy NGO. OverWatch discovered artifacts and active beaconing associated with malicious implants following installation of the Falcon platform across the victim's network. The backdoor of choice in this case was PlugX. As noted before, PlugX remains a prevalent choice for targeted adversaries and historically has been popular among those groups associated with China.

In this case, the legitimate binary used by PlugX for DLL side-loading was a signed BitDefender Crash Handler file:

FILE: C:\ProgramData\DSSM\log.exe
HASH: 386eb7aa33c76ce671d6685f79512597f1fab28ea46c8ec7d89e58340081e2bd

Once running, the malicious process was observed making network connections to the following nodes:

- **46.101.119[.]159:80**
- **46.101.119[.]159:443**

No further actions on objections were observed. While both of these campaigns against policy NGOs involve tactics bearing hallmarks of previously observed Chinese targeted intrusions, CrowdStrike has not yet attributed this activity to a specific adversary.

[11] https://attack.mitre.org/wiki/Software/S0020

[12] https://github.com/zcnhonkerHTran

FURTHER TARGETING OF THE BIOTECHNOLOGY INDUSTRY

OverWatch has observed continued targeted adversary interest in the biotechnology industry vertical in recent months. Industrial espionage is the likely motive behind these attacks. During the rollout of the Falcon platform to one such customer in the first quarter of 2018, OverWatch was able to quickly identify an existing breach.

An unknown adversary had established persistence on an infected host belonging to a senior executive in the organization. The Windows Registry had been modified to execute the following PowerShell commands upon execution of Explorer:

- **powershell.exe -noprofile Invoke-Command -scriptblock{$path='C:\Users\[REDACTED]\Application Data\Microsoft\Network\log\inf32.dat';$data=Get-Content $path;foreach($cmd in $data){iex $cmd;}}**

- **powershell.exe -noprofile Invoke-Command -scriptblock{$path='C:\Users\[REDACTED]\Application Data\Microsoft\Network\log\imeins32.dat';$data=Get-Content $path;foreach($cmd in $data){iex $cmd;}}**

These commands leveraged script blocks to read and execute each line in **inf32.dat** and **imeins32.dat**. Analysis of the .dat files revealed them to be keylogger and file extraction utilities, respectively.

In addition to the key logging and file copying performed by the two malicious .dat files, the adversary also connected to the host to actively perform additional exfiltration. Over the course of 44 minutes, the actor employed the compression utility WinRAR (renamed as **winrs**) to create archives of targeted files from within the active user's home Desktop and Documents directories. The files they targeted were very specific to the highly specialized research and intellectual property of the victim company.

Adversary use of WinRAR to prepare specific files of interest for exfiltration.

The archives created were subsequently deleted after exfiltration. As visible in the Falcon UI detection displayed above, the operator used WinRAR's **-ta** flag to select files by a date range. This is a tactic often observed with nation-state or sophisticated adversaries who are maintaining an ongoing collection effort against an organization.

TECHNOLOGY SECTOR INTRUSION EXHIBITS CREATIVE EVASION TECHNIQUES

In March, a persistent and embedded nation-state adversary returned to a victim network in the technology sector to perform further intrusion operations. The actors gained access via RDP by leveraging valid credentials. They then demonstrated defensive evasion creativity by using the legitimate Microsoft certutil.exe and expand.exe tools to decode binaries masquerading as Windows Update log files. The decoded files turned out to be the following:

FILE: C:\[REDACTED]\psping.exe
HASH: c8453110682d999223a84146462b0b4fc6979f40a01b60a7b925783b71b2d6ff
NOTE: Legitimate SysInternals PsPing[13] tool

FILE: C:\Users\[REDACTED]\Documents\pie.exe
HASH: b072e3a32aea8ba555614ad573364c8469da7023efec984185168733230a45d0
NOTE: Spetnik TCPing[14] utility

These legitimate scanning tools were executed thousands of times to identify open 3389 ports. Results of their enumeration activity were written to the following file:

FILE: C:\[REDACTED]\a.txt

In the course of scanning wide swaths of internal network IP ranges, the adversary potentially revealed part of their C2 infrastructure by pinging the external IP address **45.77.233[.]19**.

The adversary was intent on covering their tracks beyond disguising the tools they dropped and executed. They also removed numerous entries in the Windows Remote Desktop Connection Client listing within the victim machines' registries. They performed further measures to hide evidence of their presence by clearing a wide array of log files using wevtutil.exe. A summary of the defense evasion techniques employed by this committed adversary is provided in the following table:

Defense Evasion Technique(s)	Specific Activity Observed	Commands Observed
Masquerading and Deobfuscate/Decode Files or Information	Used certutil.exe and expand .exe tools to decode malicious binaries masquerading as Windows Update log files	**certutil.exe -decode KB285032.log KB273171.log** **expand KB273171.log pie.exe**
Indicator Removal on Host	Cleared RDP connections history	**reg delete "HKCU\Software\ Microsoft\Terminal Server Client\Default" /va /f** **reg delete "HKCU\Software\ Microsoft\Terminal Server Client\Servers" /va /f**
Indicator Removal on Host	Viewed and cleared event logs	**wevtutil el** **wevtutil cl "Application"**

[13] https://docs.microsoft.com/en-us/sysinternals/downloads/psping

[14] https://tcping.soft32.com/

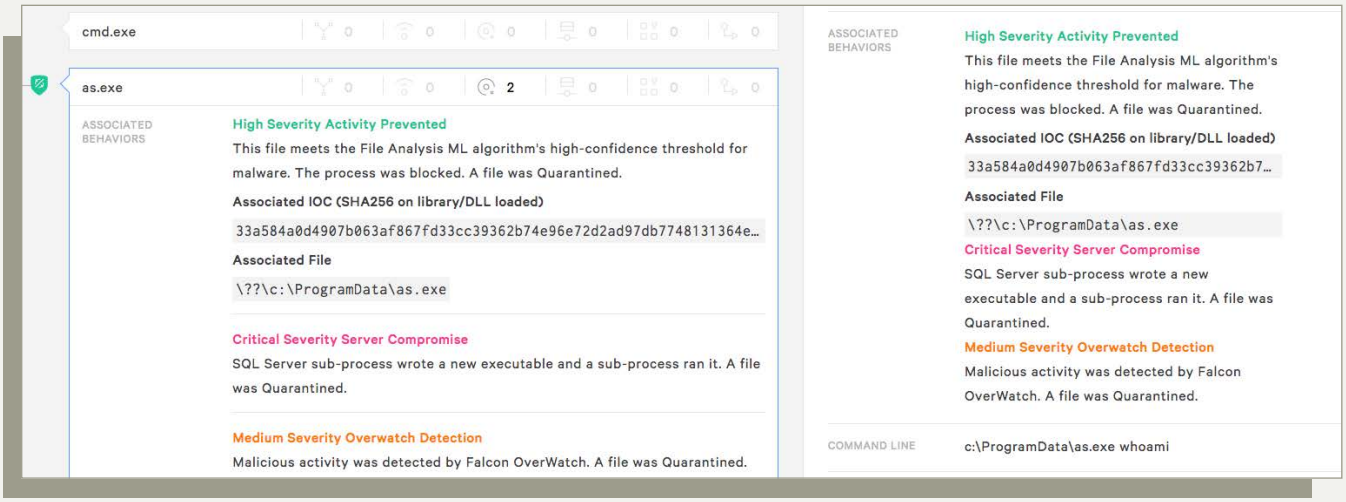
CROWDSTRIKE FALCON STOPS ANOTHER BREACH IN ITS TRACKS

A recent intrusion against the hospitality sector again proved the effectiveness of the Falcon platform in stopping breaches. The victim organization had an externally facing SQL server that was unknowingly exploited prior to the victim moving it to the internal network. After the customer placed it inside their DMZ and installed the Falcon sensor on it, OverWatch was able to identify the intrusion. An unknown, likely criminal adversary was observed returning to the victimized server to perform access maintenance.

The actors initially performed taskkill.exe commands in attempts to kill an array of potentially existing security products. However, their attempts to disable Falcon were unsuccessful. (Current versions of Falcon for Windows and Mac include the ability for an organization to set additional safeguards that will help to prevent the sensor from being uninstalled even by users with administrative privileges.) In conjunction with the taskkill.exe commands, the operators also ran cacls.exe to determine permissions for disabling the security tools.

Later, the adversary attempted to deploy a large number of tools to further build on their beachhead within the network. However, Falcon blocked their attempted expansion and exposed their use of external IP address **222.186.58[.]186** for C2.

Among the tools they attempted to use was a privilege escalation tool[15] that exploits CVE-2016-0099 (MS16-032):
FILE: C:\ProgramData\as.exe
HASH: 33a584a0d4907b063af867fd33cc39362b74e96e72d2ad97db7748131364eab1



CrowdStrike Falcon endpoint protection blocking execution of privilege escalation tool.

Other tools the operator attempted to employ included:

- **Cryptocurrency miner**
- **SQLCrack**[16]
- **Packed version of SysInternals PsKill**[17]
- **TCP scan utility**
- **iSQL query tool**

Thanks to Falcon, the impact of this pre-existing intrusion was mitigated and the attackers were finally thwarted.

[15] https://github.com/zcgonvh/MS16-032/blob/master/ms16-032/ms16-032.cpp

[16] https://www.nccgroup.trust/uk/our-services/cyber-security/products-and-cloud-services/information-security-software/

[17] https://docs.microsoft.com/en-us/sysinternals/downloads/psping

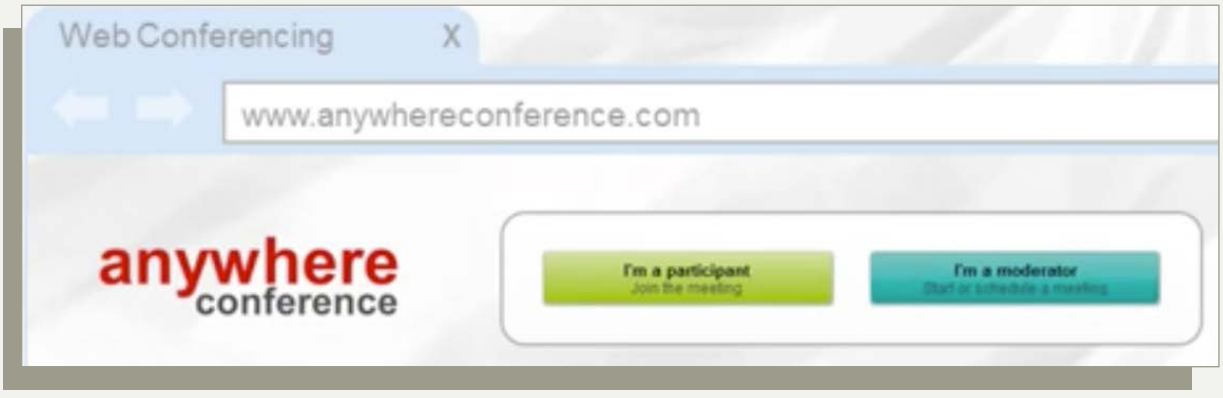
ADVERSARY ATTACKS THINK TANK WITH COMPROMISED TELECONFERENCING SOFTWARE

In April 2018, Falcon OverWatch detected targeted activity on the network of a think tank organization utilizing a set of relatively rare TTPs. The attack began when a user received a spear-phishing message. The sender, claiming to be a university professor hosting a series of webinars for students, asked the targeted victim to join one of the webinars as an expert in the class topic of global politics and economics. The victim user proceeded to follow the sender's instructions to install a teleconferencing application in order to join the webinar. Unbeknownst to the victim, the teleconferencing application was actually a trojanized version of the legitimate Arcadin Vision Desktop App program. As part of the installation, the victim downloaded and extracted the following malicious files:

FILE: C:\Users\[REDACTED]\AppData\Local\Temp\Temp1_VisionDesktopApp.zip\VisionDesktopApp.exe
HASH: 9cbcfb735db96abf9b0774f5311a69bd8bec45beaddae8adb38cae085275d3e6

FILE: C:\Users\[REDACTED]\AppData\Local\VisionDesktopApp\VisionDesktopApp.exe
HASH: c76fbf957b158aa78239e3a3bd8f478fe7a35f1237c6f730b57b6b318fc9ddad

During subsequent installation, these binaries fetched and executed second stage payloads from the adversary's C2 domain anywhereconferencelic[.]com, which the attacker had created to spoof the legitimate domain of Arcadin's teleconferencing service "Anywhere Conference."



Snapshot of the legitimate "Anywhere Conference" website, spoofed in this attack as anywhereconferencelic[.]com to disguise malicious C2 communications.

Following the C2 connections, the actors performed hands-on-keyboard activity. Initially, they carried out brief host reconnaissance, enumerating the local user account and network interfaces. They returned shortly thereafter to drop additional second stage tools, including the following implant:

FILE: C:\Users\[REDACTED]\AppData\Roaming\aylnlfdx.exe
HASH: 1c02630c75d85a3ae59de0a22d3bb82411957ad2cb93626d54f48138c9b0e9e2
C2 : 89.34.111[.]113

The adversary then attempted to establish persistence via a scheduled task by executing the following command:

schtasks.exe /Create /Sc MINUTE /MO 2 /TN "Microsoft Windows DataBase Components" /TR "C:\Windows\TEMP\wdusrv.exe

Minutes later, OverWatch identified the use of a Meterpreter reverse shell attempting to run Mimikatz, but the operation was blocked by the Falcon sensor. The attacker then downloaded an OpenSSL certificate, presumably to secure C2 communications. During this phase, C2 traffic to **asbisua[.]com** was identified, which represents another possible attempt to hide the malicious nature of this activity because the domain closely resembles the website for the legitimate Ukraine-based communications technology distributor, ASBIS. Another defense evasion technique OverWatch uncovered was the actor's use of the Windows "extract" command to uncompress a malicious .dat file containing malicious files, followed by use of the "attrib" command to manipulate the visibility of those files.

The host targeted in this intrusion belonged to an employee of the think tank who was responsible for event coordination. While there is no evidence to confirm that the affected host was specifically targeted by the actor, OverWatch has observed targeted intrusion adversaries focusing on personnel involved in event coordination for think tank organizations in the past. These individuals are of interest to nation-state actors because they may possess information that could facilitate targeting of events involving key individuals involved in global affairs.

This campaign bears similarities to another that also used a fake university professor persona to facilitate targeting of bitcoin exchanges[18]. Social engineering tactics were used to convince victims to install fake GoToMeeting software. If the victim proceeded to join a staged call, the attackers would claim technical difficulties while carrying out actions on objectives.

EXTENSIVE DEFENSE EVASION TECHNIQUES OBSERVED IN INTRUSION AGAINST A UNIVERSITY NETWORK

The Falcon OverWatch team often sees attempts to breach universities, likely due to the potentially valuable research, financial and personal data resources available on those networks. Academic institutions also have reputations for somewhat relaxed IT security postures, providing adversaries with potential opportunities to easily build malicious network infrastructures to facilitate additional attacks elsewhere.

During Q2, OverWatch observed an unknown adversary conducting operations against American universities. In one case, the attacker employed smbexec[19], an open source tool that leverages Samba tools, to provide a PsExec-style shell. Under smbexec, the operator created a new user account, "SQLDebugger," and added it to the local administrators group. They also performed reconnaissance and deployed additional tools to dump credentials, including the following binary:

FILE: C:\Users\SQLDebugger\Desktop\gp2.exe
HASH: 25f236981c13620575967d4e0521539920c6b8eb9140f0fc15d000a36ed157e8

NOTE: This file was also seen with a filename of 'IODPS.exe' in a similar attack at another university.

[18] https://www.slideshare.net/JISC/parallel-session-security

[19] https://github.com/brav0hax/smbexec

After using these dropped tools, the actors immediately overwrote their malicious files with a copy of a legitimate Windows DLL:
copy c:\windows\system32\crypt32.dll gp2.exe /y

They then proceeded to delete their executable files from the filesystem. The actors also deleted the user account they had created (SQLDebugger). These efforts at removing artifacts from the host make recovery and investigation more difficult, and demonstrate a high level of operational security (OPSEC).

About fifteen minutes later, the attackers accessed a second machine using recently stolen credentials. Once again, they employed a remote shell but this time they used a different open-source shell known as CACTUSTORCH[20]. The actors changed shells, possibly, because they were concerned their previous one was detected.

CACTUSTORCH was spawned as a scheduled task in the following manner:
schtasks /create /ru system /sc daily /tr "cmd /c cscript c:\windows\temp\osww.js" /tn osww /f

The adversary then deleted the **osww.js file** from disk, leaving only the copy running in memory via the cscript.exe process. This again demonstrates the remarkable lengths taken to cover their tracks and inhibit response efforts.

The Falcon OverWatch team often sees attempts to breach universities, likely due to the potentially valuable research, financial and personal data resources available on those networks.

WICKED PANDA TARGETS MULTINATIONAL RESOURCES COMPANY

OverWatch identified a targeted intrusion in May 2018 impacting a multinational resources company. The first signs of malicious activity began when a suspicious TeamViewer process on a victim machine wrote the following DLL, which was then loaded into an Explorer process:

FILE: C:\Windows\winmm.dll
HASH: 32998d564425bb796ad55dc464cb0dbf983c1acd200bfd75a8329b7aeed2e2a3

This DLL spoofs a legitimate Windows component of the same name by copying its filename as well as a large number of exported function names. This allows it to be installed on a target system in a location chosen so that it will be loaded by legitimate software via a DLL search-order hijacking technique. When loaded, the DLL acts as a flexible loader for a shellcode payload.

After its installation, the implant connected to the following adversary-controlled infrastructure:

C2 : newspic.x24hr[.]com
C2 : 150.109.37[.]160
NOTE: Registered to Tencent Cloud Computing Co. Ltd., Beijing, China.

The actors used their implant to perform reconnaissance and deploy a number of tools and scripts, including the legitimate "dsquery" tool, likely to perform account and permission groups discovery while attempting to blend in with the native Windows environment. They also dropped the legitimate WinRAR utility and used it to package output from the dsquery tool for exfiltration.

[20] https://github.com/mdsecactivebreach/CACTUSTORCH/blob/master/CACTUSTORCH.js

Another malicious file installed during this phase of the attack was the following implant:

FILE: C:\ProgramData\DatacardService\version.dll
HASH: 54cb25a1d7c71e01920929e834b9376e50636a83ac12f2135730e59c56de72df
C2 : newspic.x24hr[.]com

In addition, the adversary installed the following legitimate service file, which was then executed as service, and sideloaded the malicious version.dll implant:

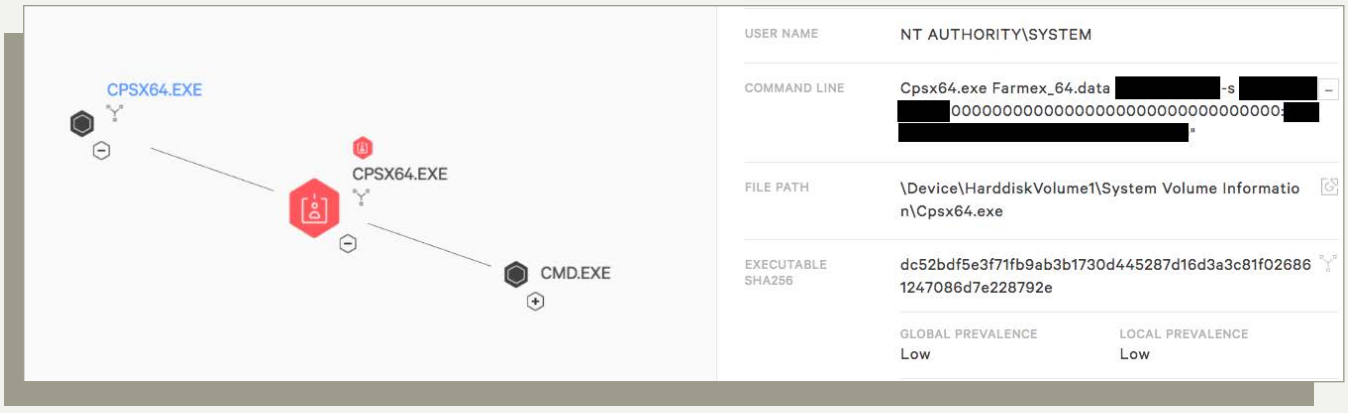
FILE: C:\Users\[REDACTED]\HWDeviceService64.exe
HASH: bb18c63c1982f5cb99c9b65d2b801e8c1909ad7cd0171326dc0015d6b781b451
NOTE: Legitimate service file

Under the newly installed implant, the attacker attempted to dump credentials using a variant of AceHash[21] as well as the Nishang "Get-PassHashes" function[22], but the Falcon endpoint protection platform blocked these operations.

The following day, the actor returned to perform network scanning and then employ the following binary:

FILE: C:\System Volume Information\Cpsx64.exe
HASH: dc52bdf5e3f71fb9ab3b1730d445287d16d3a3c81f026861247086d7e228792e

This tool was executed with the following command line as part of a pass-the-hash attack to facilitate lateral movement to three further hosts in the network, as shown in the Falcon UI here:



Falcon UI display of the pass-the-hash attack

A credential-dumping utility was deployed on the additional victim machines and further reconnaissance was performed. Once the victim organization responded by using the Falcon platform to contain the exploited systems, adversary activity ceased.

Based on the tool, infrastructure, and TTP overlap, CrowdStrike Falcon Intelligence has attributed this activity to WICKED PANDA with medium confidence.

A credential-dumping utility was deployed on the additional victim machines and further reconnaissance was performed. Once the victim organization responded by using the Falcon platform to contain the exploited systems, adversary activity ceased.

[21] https://jpcertcc.github.io ToolAnalysisResultSheet/details/AceHash.htm

[22] https://github.com/samratashok/nishang/blob/master/Gather/Get-PassHashes.ps1

THREAT ACTOR EMPLOYS SEVERAL CREDENTIAL THEFT TECHNIQUES AGAINST A SINGLE VICTIM

Another intrusion OverWatch analyzed this year involved an unidentified adversary targeting the network of a policy research organization. The attacker gained initial access to a domain controller using valid credentials over an RDP session. The malicious activity included lateral movement attempts to other systems over RDP and SMB shares, as well as reconnaissance of the types of research carried out by various staff.

Throughout the attack, the operator placed a high priority on stealing more credentials, employing several TTPs[23] to do so:

- **Credentials in Files**[24]
- **Credential Dumping**[25]
- **Kerberoasting**[26]

CREDENTIALS IN FILES

The actor employed the "Credentials in Files" technique by using xcopy to gather the domain Group Policy Preference (GPP) files from the domain controller's SYSVOL folder with the following command:

```
xcopy /S /E /C /Q /H \\[REDACTED]\sysvol\[REDACTED]\policies\*.*
```

The purpose of copying GPP files is that they can be mined for credentials and other information, facilitating a deeper foothold in the network.

CREDENTIAL DUMPING

The adversary returned later to perform credential dumping by deploying and executing the legitimate Windows Sysinternals tool "AD Explorer"[27] with the following command:

```
adexplorer -snapshot "" c:\users\[REDACTED]\downloads\adexplorer\\snapshot1.snp
```

This utility provides the ability to save snapshots of the Active Directory database for offline viewing. Later, the actor accessed a SQL server over RDP using valid credentials and deployed the ProcDump utility to dump memory from the LSASS process, providing the attacker with additional credentials.[28] OverWatch also identified that the adversary connected to a third host over a network logon session and attempted to harvest the Ntds.dit file and SYSTEM registry archive from a Volume Shadow Copy. The SYSTEM registry archive contains the key required to decrypt the Ntds.dit file as well as other sensitive information.

KERBEROASTING

The Falcon platform also captured the malicious operator downloading and running the legitimate Windows Setspn[29] tool, which searches for service principal names (SPNs) over the network's domain. This information was used in an attempt to compromise credentials via Kerberoasting. Kerberoasting occurs when an attacker, using a valid Kerberos ticket-granting ticket, requests one or more ticket-granting service tickets for SPNs from the domain controller.

[23] These credential access TTPs are part of the MITRE ATT&CK model, which provides an industry standard for understanding and categorizing adversary post-exploitation behavior. More information available at https://attack.mitre.org/wiki/Main_Page.

[24] https://attack.mitre.org/wiki/Technique/T1081

[25] https://attack.mitre.org/wiki/Technique/T1003

[26] https://attack.mitre.org/wiki/Technique/T1208

[27] https://docs.microsoft.com/en-us/sysinternals/downloads/adexplorer

[28] https://docs.microsoft.com/en-us/sysinternals/downloads/procdump

[29] https://technet.microsoft.com/pt-pt/library/cc773257(v=ws.10).aspx

These tickets may be vulnerable to offline brute force attacks that can expose plaintext credentials. In this case, OverWatch identified the adversary retrieving and executing a PowerShell script that employed PowerSploit's Invoke-Kerberoast module, which requests service tickets and returns crackable ticket hashes.

While the Falcon OverWatch team commonly sees attempts to harvest credentials during targeted intrusions, this case was unique in the number of techniques observed. The attackers clearly placed credential theft as a top priority for their operation, likely with the intention of maintaining access to a network they consider a high-value target.

CONCLUSION

During the first half of 2018, Falcon OverWatch continued to identify and analyze a growing number of sophisticated and/or persistent intrusions. The technology, professional services and hospitality sectors were targeted most often, but government-sponsored and criminal adversaries attacked victims across a wide range of industries. The actors used a variety of techniques, demonstrating particular creativity and perseverance in defense-evasion and credential-access TTPs. OverWatch sees no evidence suggesting these trends will EDR change significantly over the next several months.

Threat hunting across detailed endpoint data, such as that collected by EDR (endpoint detection and response) tools like CrowdStrike Falcon, is invaluable in identifying stealthy adversaries using these types of TTPs and evasions. All organizations that are at risk from these threats should deploy threat hunting teams — internal or MDR services like Falcon OverWatch — to rapidly detect, investigate and remediate intrusions before adversaries can accomplish their objective and cause a data breach.

One of the key metrics that CrowdStrike OverWatch tracks for all intrusions it identifies is breakout time, the time it takes for an intruder to begin moving laterally outside of the initial beachhead to other systems in the network. The current average breakout time is 1 hour and 58 minutes, which means that if defenders are able to detect, investigate and remediate the intrusion within 2 hours, they can stop the adversary before they can cause serious damage. CrowdStrike recommends that all organizations adopt the "1-10-60" rule:

- **Strive to detect a threat in 1 minute on average**
- **Investigate the detection in 10 minutes**
- **Remediate and contain the attack in 1 hour**

APPENDIX

CROWDSTRIKE FALCON OVERWATCH INTRUSIONS MAPPED TO MITRE ATT&CK FRAMEWORK (H1 2018)

INITIAL ACCESS 10 items	EXECUTION 31 items	PERSISTENCE 56 items	PRIVILEGE ESCALATION 28 items	DEFENSE EVASION 59 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	BITS Jobs
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	Clear Command History
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	CMSTP
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Code Signing
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Dylib Hijacking	Component Firmware
Trusted Relationship	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking
Valid Accounts	Install	Change Default File Association	Extra Window Memory Injection	Control Panel Items
	UtilLaunchctl	Component Firmware	File System Permissions Weakness	DCShadow
	Local Job Scheduling	Component Object Model Hijacking	Hooking	Deobfuscate/Decode Files or Information
	LSASS Driver	Create Account	Image File Execution Options Injection	Disabling Security Tools
	Mshta	DLL Search Order Hijacking	Launch Daemon	DLL Search Order Hijacking
	PowerShell	Dylib Hijacking	New Service	DLL Side-Loading
	Regsvcs/Regasm	External Remote Services	Path Interception	Exploitation for Defense Evasion
	Regsvr32	File System Permissions Weakness	Plist Modification	Extra Window Memory Injection
	Rundll32	Hidden Files and Directories	Port Monitors	File Deletion
	Scheduled Task	Hooking	Process Injection	File System Logical Offsets
	Scripting	Hypervisor	Scheduled Task	Gatekeeper Bypass
	Service Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	Hidden Files and Directories
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Setuid and Setgid	Hidden Users
	Signed Script Proxy Execution	Launch Agent	SID-History Injection	Hidden Window
	SourceSpace after Filename	Launch Daemon	Startup Items	HISTCONTROL
	Third-party Software	Launchctl	Sudo	Image File Execution Options Injection
	Trap	LC_LOAD_DYLIB Addition	Sudo Caching	Indicator Blocking
	Trusted Developer Utilities	Local Job Scheduling	Valid Accounts	Indicator Removal from Tools
	User Execution	Login Item	Web Shell	Indicator Removal on Host
	Windows Management Instrumentation	Logon Scripts		Indirect Command Execution
	Windows Remote Management	LSASS Driver		Install Root Certificate
		Modify Existing Service		InstallUtil
		Netsh Helper DLL		Launchctl
		New Service		LC_MAIN Hijacking
		Office Application Startup		Masquerading
		Path Interception		Modify Registry
		Plist Modification		Mshta
		Port Knocking		Network Share Connection Removal
		Port Monitors		NTFS File Attributes
		Rc.common		Obfuscated Files or Information
		Re-opened Applications		Plist Modification
		Redundant Access		Port Knocking
		Registry Run Keys / Start Folder		Process Doppelgänging
		Scheduled Task		Process Hollowing
		Screensaver		Process Injection
		Security Support Provider		Redundant Access
		Service Registry Permissions Weakness		Regsvcs/Regasm
		Shortcut Modification		Regsvr32
		SIP and Trust Provider Hijacking		Rootkit
		Startup Items		Rundll32
		System Firmware		Scripting
		Time Providers		Signed Binary Proxy Execution
		Trap		Signed Script Proxy Execution
		Valid Accounts		SIP and Trust Provider Hijacking
		Web Shell		Software Packing
		Windows Management Instrumentation Event Subscription		Space after Filename
		Winlogon Helper DLL		Timestomp
				Trusted Developer Utilities
				Valid Accounts
				Web Service

Number of Intrusions Where Technique Was Observed

1 52

CREDENTIAL ACCESS 20 items	DISCOVERY 19 items	LATERAL MOVEMENT 17 items	COLLECTION 13 items	EXFILTRATION 9 items	COMMAND & CONTROL 21 items
Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Brute Force			Clipboard Data	Data Encrypted	
Credential Dumping	Browser Bookmark Discovery	Distributed Component Object Model	Data from Information Repositories	Data Transfer Size Limits	Connection Proxy
Credentials in Files				Exfiltration Over Alternative Protocol	Custom Command and Control Protocol
Credentials in Registry	File and Directory Discovery	Exploitation of Remote Services	Data from Local System		
Exploitation for Credential Access	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Custom Cryptographic Protocol
Forced Authentication	Network Share Discovery	Pass the Hash	Data from Removable Media	Exfiltration Over Other Network Medium	Data Encoding
Hooking	Password Policy Discovery	Pass the Ticket			Data Obfuscation
Input Capture	Peripheral Device Discovery	Remote Desktop Protocol	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Input Prompt		Remote File Copy	Email Collection		Fallback Channels
Kerberoasting	Permission Groups Discovery	Remote Services	Input Capture	Scheduled Transfer	Multi-Hop Proxy
Keychain		Replication Through Removable Media	Man in the Browser		Multi-Stage Channels
LLMNR/NBT-NS Poisoning	Process Discovery		Screen Capture		Multiband Communication
Network Sniffing	Query Registry	Shared Webroot	Video Capture		Multilayer Encryption
Password Filter DLL	Remote System Discovery	SSH Hijacking			Port Knocking
Private Keys	Security Software Discovery	Taint Shared Content			Remote Access Tools
Replication Through Removable Media		Third-party Software			Remote File Copy
Securityd Memory	System Information Discovery	Windows Admin Shares			Standard Application Layer Protocol
Two-Factor Authentication Interception	System Network Configuration Discovery	Windows Remote Management			Standard Cryptographic Protocol
	System Network Connections Discovery				Standard Non-Application Layer Protocol
	System Owner/User Discovery				Uncommonly Used Port
	System Service Discovery				Web Service
	System Time Discovery				

Number of Intrusions Where Technique Was Observed

1 52

ABOUT CROWDSTRIKE

CrowdStrike is the leader in cloud-delivered endpoint protection. The CrowdStrike Falcon® platform offers instant visibility and protection across the enterprise and prevents attacks on endpoints on or off the network. The lightweight Falcon agent deploys in minutes to deliver actionable intelligence and real-time protection from Day One. The Falcon platform seamlessly unifies next-generation AV with best-in-class endpoint detection and response, backed by a 24/7 managed hunting. Its cloud infrastructure and single-agent architecture take away complexity and add scalability, manageability, and speed. The Falcon platform protects customers against all cyberattack types, using sophisticated signatureless artificial intelligence/machine learning and indicator-of-attack-based (IOA) threat prevention to stop known and unknown threats in real time. Powered by the CrowdStrike Threat Graph™ database, the Falcon platform instantly correlates over 1 trillion security events per week from across the globe to immediately prevent and detect threats.

Learn more at

www.crowdstrike.com