FireEye Cyber Defense SUMMIT

ATT&CKing FIN7 The Value of Using Frameworks for Threat Intelligence

Regina Elwell, FireEye Katie Nickels, MITRE

OCTOBER 1 - 4, 2018 | WASHINGTON, D.C.

Agenda

- Why Should We Use Frameworks for Threat Intelligence?
 - Introduction to MITRE ATT&CK™
 - Introduction to the Attack Lifecycle
 - How ATT&CK and the Attack Lifecycle Complement Each Other
- Introduction to FIN7
- FIN7 Targeted Lifecycle Overview
- FIN7 Deep Dive

Why Use a Framework to Organize Threat Intel? Regardless of which one you choose, it can help you...

- Identify where you have gaps in knowledge
- Compare adversaries to each other
- Compare adversary behavior to defenses

Introduction to MITRE ATT&CK™

A knowledge base of adversary behavior

- Based on real-world observations
- Free, open, globally accessible, and community-driven
- A common language





Breaking Down Enterprise ATT&CK

Tactics: the adversary's technical goals

are	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	У	Lateral Movement	Col	lection	Exfiltration	Command & Control
O	Hardware Additions	Scheduled Task		Binary Padding 🗕 🗕		Credentials in Registry	Browser Bookmark		Exploitation of Remote	Data fi	rom Information	Exfiltration Over	Remote Access Tools
e goals	Trusted Relationship	LSASS	Drive	Extra Window M	Nemory Injection	Exploitation for	Discovery		Services	R	epositories	Physical Medium	Port Knocking
	Supply Chain Compromise	Local Job Scheduling		Access Token Manipulation		Credential Access	Network Share	Distributed Component Vi			deo Capture	e Exfiltration Over	Multi-hop Proxy
		Тгар			Scheduled Task						Command and	Domain Fronting	
	Spearphishing Attachment	Launchetl		Main page	ted Collection Control Cha					Control Channel	Data Encoding		
		Signed Binary	Im	ig Help Contribute	Utilities such as at and schtasks, along with the Windows Task Scheduler, can be				Schodulod Task		board Data	Data Encrypted	Remote File Copy
	Exploit Public-Facing Application	Proxy Execution		References	used to schedule programs or scripts to be executed at a date and time. A task can also be scheduled on a remote system, provided the proper authentication is met to use RPC and file and printer sharing is turned on. Scheduling a task on a remote system typically required being a member of the Administrators group on the the remote system. ^[1] An adversary may use task scheduling to execute programs at system startup or on a scheduled basis for persistence, to conduct remote Execution as part of Lateral) ID T Tactic E Platform V Permissions L Required	T1053 Execution, Persistence, Privilege Escalation		il Collection	Automated Exfiltration	Multi-Stage Channels
		User Execution		Data Drilldown							en Capture	Exfiltration Over Other	Web Service
Ψ	Replication Through Removable Media	Exploitation for		Using the API						Privilege	ta Staged Network Medium	Network Medium	Standard
		Client Execution	АррСе	rt I Initial Access							ut Capture Exfil rom Network	Exfiltration Over	Non-Application Layer Protocol
+-	Spearphishing via Service	CMSTP	Ноо	kir Execution					ions User Administrator SYS	s User Administrator SYSTEM		Alternative Protocol	
>		Dynamic Data Exchange	Startup	Persistence Privilege Escalation					d	ared Drive	Data Transfer	Connection Proxy	
>	Spearphishing Link	Mshta 🔪	Launch	Dat Defense Evasion	Movement, to gain SYSTE	M privileges, or to run a process	under the context of a Effect	Effective	User, Administrator, SYSTEM	TEM	m Local System	Size Limits	Multilayer Encryption
$\overline{\mathbf{O}}$	Drive-by Compromise	AppleScript	Dylib H	ijac Credential Access	specified account.	Pe Da So	Data File mo Sources Proces Vindou	File monitoring, Process command-line parameters,		h the Browser	Data Compressed	Standard Application	
ž	Valid Accounts	Source	Application	Lateral Movement	Contents [hide]				arameters,	pm Removable	Scheduled Transfer	Layer Protocol	
		Space after Filename	AppIni	C Collection	1 Examples			Process monitoring, Windows event logs	Process monitoring, Windows event logs	Media		Commonly Used Port	
S:		Execution through Module Load	Web	Sh Exfiltration Command and Control	2 Mitigation	o :::	· · · ·	Supports	rte Ves				Standard Cryptographic Protocol
() _		Regsvcs/Regasm	New S	en	Procedures – Specific fechnique implementation						Custom Cryptographic		
	Ο	InstallUtil	File System Perm	iss All Techniques	Examples Leo			Leo Leoback @leolacha	Leo Loobeek, @leoloobeek, Alain Homewood, Insomnia Security			Protocol	
	(1)	Regsvr32	N Path Inte	erce Windows				Alain Homewood, Insc				Data Obfuscation	
O	\checkmark	Execution through API	Accessibilit	Linux	APT18 actors used the	native at Windows task schedul	ler tool to use scheduled					Custom Command	
	PowerShell Port Mo		on Add a Technique	tasks for execution on a victim network. ^[2]							and Control Protocol		
	Rundll32 Kernel Modules and Extensions			Groups	AP 1 29 used named and mjacked scheduled tasks to establish persistence.							Communication	
$\overline{}$.				All Groups	C:\Users\Public\t	st.exe /sc ONLOGON /ru "System" [4]							Through
() -		Scripting	Port Knocking 👌	Add a Group	 APT32 has used scheduled tasks to persist on victim systems.^[5] BRONZE BUTLER has used at and schtasks to register a scheduled task to execute malware during lateral movement.^[6] Dragonfly 2.0 used scheduled tasks to automatically log out of created accounts every 8 hours as well as to execute tools to 							Removable Media	
$\check{\Phi}$	\underline{O}	Graphical User Interface	SIP and Trust Provider Hijacking	All Software								Multiband Communication	
	0	Command-Line Interface	Screensaver	Exploitation for Privilege Escalation	Hidden Window								Fallback Channels

©2018 FireEye ©2018 The MITRE Corporation. ALL RIGHTS RESERVED. Approved for public release. Distribution unlimited 18-1528-22.

Uncommonly Used Port

The Targeted Attack Lifecycle



How ATT&CK and the Attack Lifecycle are Complementary



FireEye Cyber Defense Summit

FIN7

Introduction

- Active since late 2015
- Financially motivated
- Primary objective: point of sale compromise
- Mainly use spearphishing for malware distribution
- Limited use of exploits, and no known use of zeroday exploits
- Blend of publicly available and unique or altered tools



FIN7 Targeted Attack Lifecycle



Spearphishing



- Targeted spearphishing with customized lures
 ATT&CK T1193: Spearphishing with attachment
 - Weaponized Word documents with malicious VBA macros T1064: Scripting
 - LNK files used to launch VBA code embedded within document contents
 - Embedded OLE objects containing malware T1173: Dynamic Data Exchange
- Use social engineering to encourage response
 T1204: User execution

Spearphishing: Mitigation and Detection

- User training
 - Even if they click, will they report?
 - Don't rely just on this
- Tools: email filtering and application whitelisting
- Use GPO to block execution of macros in documents from the Internet
- Create analytics on suspicious execution chains to detect macros
 - Example: winword.exe spawning cmd.exe, wscript.exe, or powershell.exe

HALFBAKED

- The HALFBAKED malware has several components:
 - A dropper contained in a VBA Macro which writes out the installer and backdoor to the infected system
 T1064: Scripting
 - A VBScript installer which installs the backdoor as a persistent service
 - A VBScript backdoor possessing typical capabilities:
 - Reverse shell

T1059: Command-Line Interface

- Execute shell commands
- Upload and download files T1105: Remote File Copy
- Uses Windows Management Instrumentation (WMI) to collect reconnaissance details

T1047: WMI

INITIAL COMPROMISE ESTABLISH FOOTHOLD ESCALATE PRIVILEGES INTERNAL RECONNAISSANCE MISSION

T1050: New Service

HALFBAKED: Detection and Mitigation

- Implement least-privilege model for domain users
 - Ensure domain users are not in local admins group
- Monitor service creation through command-line invocation and look for low frequency services in your environment
- Monitor network traffic for WMI connections and capture command-line arguments of "wmic"
 - Look for anomalies in systems using WMI

BELLHOP



 BELLHOP is a javascript-based backdoor interpreted using the native Windows Scripting Host (WSH)

T1082: System Information Discovery

- The BELLHOP dropper gathers basic host information and downloads a base64encoded blob of javascript to disk and sets up persistence in three ways:
 - Creating a Run key in the Registry **T1060: Registry Run Keys**
 - Creating a RunOnce key in the Registry
 - Creating a persistent named scheduled task T1053: Scheduled Task
- BELLHOP communicates using HTTP and HTTPS with primarily benign sites such as Google documents and Pastebin T1071: Standard Application Layer Protocol T1102: Web Service

BELLHOP: Mitigation and Detection

- Monitor for ver, systeminfo, and dir executed from the command line
 - Create a detection that chain these with other discovery commands
- Monitor for Registry run keys that do not correlate with known software
- Limit privileges of user accounts so only authorized admins can create scheduled tasks on remote systems
- Configure event logging for scheduled task creation and changes by enabling "Microsoft-Windows-TaskScheduler/Operational" in event logging
 - Example BELLHOP Scheduled Task: SysChecks

POWERSOURCE & TEXTMATE



T1043: Commonly Used Port

- POWERSOURCE is a heavily obfuscated and modified version of the publicly available tool DNS_TXT_Pwnage T1027: Obfuscated Files or Information
 - Installed in the registry or Alternate Data Streams
 T1060: Registry Run Keys T1096: NTFS File Attributes
 - Uses DNS TXT requests (port 53) for command and control T1071: Standard App Layer Protocol T1043: Commonly Used Port
- TEXTMATE has been observed being downloaded via POWERSOURCE
 - Second-stage "file-less" payload, runs in memory via PowerShell T1086: PowerShell
 - Implements reverse shell via DNS TXT (port 53) commands
 T1059: Command-Line Interface T1071: Standard Application Layer Protocol

POWERSOURCE & TEXTMATE: Mitigation and Detection

- Force web traffic through a proxy
 - Including DNS traffic do not allow Internet DNS resolution
- Flag and analyze commands containing indicators of obfuscation and known suspicious syntax such as uninterpreted escape characters like A and "
- Restrict PowerShell execution policy to administrators and to only execute signed scripts

PowerAdmin Exec (PAExec)



- PowerAdmin Exec (PAExec)
 - Functionally similar to SysInternals PsExec, PAExec supports execution of remote commands
 T1035: Service Execution
 - Most forensic artifacts are created on the source and not the target

PAExec: Mitigation and Detection

- Look for unusual file names such as "logsXXX.exe" (unique to FIN7)
- Monitor for unusual executables running from "C:\Windows\Temp\"
- If you have technology capable of it, look at binaries for:
 - CompanyName Power Admin LLC
 - FileDescription PAExec Application
 - InternalName PAExec
 - OriginalFilename PAExec.exe

PILLOWMINT



- PILLOWMINT is a Point-of-Sale malware tool used to scrape track 1 and track 2 payment card data from memory
 - Scraped payment card data is encrypted and stored in the registry and as plaintext in a file
 T1074: Data Staged
 - Contains additional backdoor capabilities including:
 - Running processes
 - Downloading and executing files T1105: Remote File Copy
 - Downloading and injecting DLLs T1055: Process Injection
 - Communicates with a command and control (C2) server over HTTP using AES encrypted messages
 T1071: Standard Application Layer Protocol

T1032: Standard Cryptographic Protocol

PILLOWMINT: Mitigation and Detection

- Implement point-to-point encryption and tokenization
- Use data loss prevention software
- Look for registry keys:
 - HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\server
 - HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\com man
 - HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\PDSK 21_<random>
- Look for output files in the directory: %WINDIR%\system32\sysvols\

Using Structured Threat Intelligence

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control	
Drive-by Compromise	AppleScript	bash_profile and bashrc	Access Token Manipulation	Access Token Manipulation	AccountManipulation	AccountDiscovery	AppleScript	AudioCapture	Automated Extitination	Commonly Used Part	
ExploitPublic-Facing Application	CMSTP	A cossibility Features	Accessibility Features	Binary Padding	BashHistory	Application Window Discovery	Application Deployment Software	AutomatedCollection	DataCompressed	CommunicationThrough	
HardwareAdditions	Command-Line Interface	AppCer DLLs	AppCertDLLs	BITSJobs	Destruct	Browser Bookmark Discovery	Distributed Component ObjectModel	ClipboardData	DataEncrypted	ConnectionPraxy	
Replication Through Removable Media	Content	ApphitDLLs	AppInitDLLs	Bypass User Account Control	Credential Dumping	Filean: Directory Discovery	Exploitation of Remote Services	DatafromInformation Repositories	DataTransfer Size Limits	CustomCommand and Control Protocol	
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	Clear Command History	Credentials in Files	Nework Service Scanning	Logon Scripts	Data from Local System	Extitration Over Alternative Protocol	Custom Cryptographic Protocol	
SpearphishingLink	ExecutionthroughAPI	Authentication Package	Bypass User Account Control	CMSTP	Credentials in Registry	Network Share Discovery	PasstheHash	Data from Network Shared Drive	Exfitration Over Command and Control Channel	DataEncoding	
Spearphishing via Service	Execution through Module	BITSJabs	DLL Search Order Hijacking	CodeSigning	Exploitation for Credential Access	Password Policy Discovery	PasstheTicket	DatafromRemovableMedia	Exfiltration Over Other Network Medium	DataObluscation	
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	DylibHijacking	ComponentFirmware	ForcedAuthentication	Peripheral Device Discovery	Remote Desktop Protocol	DataStaged	Exfiltration Over Physical Medium	DomainFronting	
TrustedRelationship	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	ComponentObjectModel Hilacking	Hooking	Permission Groups Discovery	RemoteFileCopy	Email Collection	ScheduledTransfer	Fallback Channels	
Valid Accounts	InstallUtil	ChangeDefaultFile Association	Extra Window Memory Injection	Control Panel items	hputCapture	Process Discovery	Remote Services	hputCapture		Multi-hopProxy	
	Laurchol	ComponentFirmware	File System Permissions Weakness	DCShadow	InputPrompt	QueryRegistry	Replication Through Removable Media	ManintheBrowser		Multi-Stage Channels	
	Local Job Scheduling	ComponentObjectModel Hilacking	Hooking	DeobluscaleDecode Files or Information	Kerbercasting	Remote System Discovery	SharedWebroot	ScreenCapture		MultibandCommunication	
	LSASS Driver	CreateAccount	ImageFileExecutionOptions	Disabling Security Tools	Keychain	Security Software Discovery	SSH Hijacking	VideoCapture		Multilayer Encryption	
	Martin	DLL Search Order Hijacking	LaunchDaemon	DLL Search Order Hijacking	LLMNR/NBT-NS Paisoning	System Information Discovery	TaintSharedContent		-	PartKnacking	
\mathcal{C}	PowerShell	Dylib Huncking	New Service	DLL Side-Loading	Network Sniffing	SystemNetwork ConfigurationDiscovery	Third-party Software	1		Remote Access Tools	
	ReceivesRegasm	Exemal Remote Services	PathInterception	Exploitation for Defense Evasion	Password Filter DLL	SystemNetwork Connections	Windows Admin Shares	1		RemoteFileCopy	
	Regsvr32	File System Permissions Weekness	PlistModification	Exrawindow Memory	PrivetoKeys	SystemOwner/User Discovery	Windows Remote Management	1		Standard Application Layer Protocol	
	Rundli32	Hidden Files and Directories	PortMonitors	FileDeletion	Replicat in Through Rem vable Media	SystemServiceDiscovery		-		Standard Cryptographic Protocol	
	ScheduledTask	Hooking	Process Injection	FileSystemasgearcieus	SecuritydMemory	System Time Discovery	1			Standard Non-Application Laver Protocol	
	Scripting	Hypervisor	ScheduledTask	Gatekeeper Bypass	Two-Factor Authentication Interception		-			Uncommonly Used Part	
	Service Execution	ImageFileExecutionOptions	Service Registry Permissions Weakness	Hidden Files and Directories						WebService	
	Signed Binary Proxy Execution	Kernel Modules and Extensions	SetuidandSetgid	HiddenUsers]				-		
	Signed ScriptPraxy Execution	LaunchAgent	SID-History Injection	HiddenWindow	1						
	Source	LaunchDaemon	Startupliems	HISTCONTROL	1			Overlay			
	Space after Filename	Launchot	Sudo	Image File Execution Options Injection	1	FIN/					
	Third-party Software	LC_LOAD_DYLIBAddition	SudoCaching	Indicator Blocking							
	Trap	Local Job Scheduling	Valid Accounts	Indicator Removal from Tools	1						
	Trusted Developer Utilities	Loginitem	Web Shell	Indicator Removal on Host	1	FIN8					
	User Execution	Logon Scripts		IndirectCommandExecution]			aerensive gaps			
	Windows Management Instrumentation	LSASSDriver		Install Root Certificate	1 🗖						
	Windows Remote Management	Modify Existing Service	1	InstallUti	1	Roth arou	nc	(notional)			
	Contraction of the second s	NetshHelperDLL		Laurchof	1 🗖	boin giot	, ps				
		New Service		LC_MAIN Hijacking	1 🗖						
		Office Application Startup		Masquerading							
		Pathinterception	1	Mcdify Registry							

Conclusion

- Frameworks are useful for organizing threat intel regardless of which one
- Consider which framework based on your use case, and consider combining them for analysis
- FIN7 has been successful because they use social engineering and well-disguised lures
- FIN7 continues to be successful because they are constantly adapting and evolving to prevent detection
- For the best chance of detecting FIN7, look across their attack lifecycle and ATT&CK techniques they use

Additional Resources

- Visit <u>https://attack.mitre.org</u> for more information on ATT&CK
 - FIN7: <u>https://attack.mitre.org/wiki/Group/G0046</u>
 - Contact us: attack@mitre.org
- More information on FIN7:
 - On the Hunt for FIN7: Pursuing an Enigmatic and Evasive Global Criminal Operation <u>https://www.fireeye.com/blog/threat-research/2018/08/fin7-</u> <u>pursuing-an-enigmatic-and-evasive-global-criminal-operation.html</u>
 - Tracking a Cyber Crime Group: FIN7 at a Glance <u>https://www.fireeye.com/blog/executive-perspective/2018/08/tracking-a-</u> <u>cyber-crime-group-fin7-at-a-glance.html</u>



Questions?