APT ATT&CK[™] - Threat-based Purple Teaming with ATT&CK Continued

Jamie Williams & Daniel Weiss

@d4weiss

MITREattack

х Э Э С С



© 2019 The MITRE Corporation. All rights reserved.

Introduction

Jamie Williams

- Cyber adversarial engineer
- Adversary emulation + behavior detection research
- ATT&CK and ATT&CK Evaluations

Daniel Weiss

- Cyber security engineer
- Defensive cyber ops + adversary emulation research
- ATT&CK Evaluations

2



youtube.com/watch?v=OYEP-YAKIn0



Approved for public release. Distribution unlimited 19-00696-5

ATT&CK

Knowledge base of adversary behaviors Threat-informed defense **Based on real-world observations** References to publicly reported intelligence Free, open, and globally accessible attack.mitre.org Community-driven attack@mitre.org MITREattack

Approved for public release. Distribution unlimited 19-00696-5

ATT&CK Structure

Tactics: the adversary's technical goals

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Pinary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User & ccount Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Protocol	Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Control	CMSTP	Sredentials in Registry	Network Service Scanning	Pass the Hash	Drive Drive Drata from Removable	Data Encoding	and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API Execution through Module	Authentication Package	Hilacking	Code Signing	Access	Network Share Discovery	Pass the Ticket	Media	Data Obfuscation	Network Medium	Firmware Corruption
Spearphishing via Service	Exploitation for Client	BITS Jobs	Exploitation for Privilege	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting Domain Generation	Medium	Inhibit System Recovery
Supply Chain Compromise	Execution Graphical User Interface	Bootkit	Escalation Extra Window Memory	Compiled HTML File	Hooking	Peripheral Device	Remote File Copy	Email Collection	Algorithms Failback Changels	Scheduled Transfer	Network Denial of Service
Valid Accounts	Install Itil	Change Default File	File System Permissions	Component Object Model	Input Report	Permission Groups	Replication Through	Man in the Browser	Multi-hon Provy	4	Rustime Data Manipulation
Valid Accounts	Launchoti	Association Component Firmware	Hooking	Hijacking Control Panel Items	Kerberoasting	Process Discovery	Removable Media Shared Webroot	Screen Canture	Multi-Stage Channels	1	Service Stop
	Local Job Scheduling	Component Object Model	Image File Execution	DCShadow	Kevchain	Query Registry	SSH Hijacking	Video Capture	Multiband Communication	1	Stored Data Manipulation
	LSASS Driver	Create Account	Launch Daemon	Deobfuscate/Decode Files	LLMNR/NBT-NS Poisoning	Remote System Discovery	Taint Shared Content		Multilayer Encryption	1	Transmitted Data
	Mshta	BLL Search Order	New Service	Disabling Security Tools	Network Sniffing	Security Software	Third-party Software	1	Port Knocking	1	
	PowerShell	Dylib Hijacking	Path Interception	DLL Search Order	Password Filter DLL	System Information	Windows Admin Shares	1	Remote Access Tools	1	
	Regsvcs/Regasm	External Remote Services	Plist Modification	DLL Side-Loading	Private Keys	System Network	Windows Remote	1	Remote File Copy	1	
	Regsvr32	File System Permissions Weakness	Port Monitors	Execution Guardrails	Securityd Memory	System Network Connections Discovery	~		Standard Application Layer]	
	Rundll32	Hidden Files and Directories	Process Injection	Exploitation for Defense	Two-Factor Authentication	System Owner/User]	~~	Standard Cryptographic Protocol] <	NEW
	Scheduled Task	Hooking	Scheduled Task	Extra Window Memory		System Service Discovery	1		Standard Non-Application]	
	Scripting	Hypervisor	Service Registry Permissions Weakn						commonly Used Port		
	Service Execution	Options Injection	Setuid and Setgid	Procedure	se Specifi	c techniqu	o implomo	ntations	ab Service		
	Execution	Extensions	SID-History Injection	Procedure	es. specific	c ceciniqu	e impieme	illations			\checkmark
	Execution	Launch Agent	Startup Items								
	Source	Launch Daemon	Sudo	ne Desc	ription						
	Space atter Filename	Launcheti	Sudo Caching								
	Tran	LC_LOAD_DYLIB Addition	Valid Accounts APT	F29 APT2	29 used sticky-keys to obtain ur	nauthenticated, privileged cons	ole access. ^{[4][5]}				
	Trusted Developer Litilities	Login Itom	Web Stell								
	User Execution	Logon Scripts		F3 APT3	3 replaces the Sticky Keys binar	Y C:\Windows\System32\seth	nc.exe for persistence.[6]				
	Windows Management	LSASS Driver	1 🔪 📕								
	Windows Remote	Modify Existing Service	Δχί	om Axior	m actors have been known to u	se the Sticky Keys replacemen	t within RDP sessions to obtain	persistence [7]			
	XSL Script Processing	Netsh Helper DLL	1								
		New Service] \ _	- Danda -	Dende has used the other of			181			
		Office Application Startup	Dee	ep Panda Deep	Panda has used the sticky-key	's technique to bypass the RDP	 login screen on remote syster 	ns auring intrusions.101			
		Path Interception									
		Plist Modification	Em	pire Empi	ire can leverage WMI debuggin	g to remotely replace binaries I	like sethc.exe, Utilman.exe, and	Magnify.exe with cmd.exe. ^[9]			
		Port Knocking									
		Port Monitors		-	4						
		Rc.common	4	Modify Registry	4						
		Re-opened Applications	4	Mshta Notwork Share Constant	4						
		Redundant Access Registry Run Keys /	4	Removal	4						
		Startup Folder	4	NTFS File Attributes	4						
		Scheduled Task	4	Linformation	4						
		Screensaver	4	Plist Modification	4						
		Service Registry	1	Process Doppelgänging	1						
		Permissions Weakness Setuid and Setoid	1	Process Hollowing	1						
		Shortout Modification	1	Process Injection	1						
		SIP and Trust Provider	1	Redundant Access	1						
		Startup Items	1	Regsvcs/Regasm	1						

Emulation Plans



attack.mitre.org/resources/adversary-emulation-plans

Evaluating Techniques

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	overy	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	33 items	58 items	28 items	63 items	19.0	20 items	17 items	13 items	9 items	21 items
Drive-by Compromise	AppleScript	.bash_profile and	Access Token	Access Token M , mation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated	Commonly Used Port
Exploit Public-Facing	CMSTP	.bashrc	Manipulation	mary Padding	Bash History	Application Window	Application	Automated	Exfiltration	Communication
Application	Command-Line Interface	Accessibility Features	Accession, reatures	BITS Jobs	Brute Force	Discovery	Deployment Software	Collection	Data Compressed	Through Removable
Hardware Additions	Compiled HTML File	Account Maning	AppCert DLLs	Bypass User Account Control	Credential Dumping	Browser Bookmark	Distributed	Clipboard Data	Data Encrypted	Generation Deces
Replication Through	Control Panel I	oppCert DLLs	AppInit DLLs	Clear Command History	Credentials in Files	Discovery	Model	Data from	Data Transfer Size	Connection Proxy
Removable Media	mathic Data Exclanation	AppInit DLLs	Application Shimming	CMSTP	Credentials in Registry	Discovery	Exploitation of	Repositories	Limits	Control Protocol
Spearphishing Attachment	Execution through API	App cation Shimming	Bypass User Account	Code Signing	Exploitation for	Network Service	Remote Services	Data from Local	Exfiltration Over Alternative Protocol	Custom Cryptographic
Spearphishing Link	Execution through	Aut entication Package	Control	Compiled HTML File	Credential Access	Scanning	Logon Scripts	System	Exfiltration Over	Protocol
Spearphishing via	Inc	BITS Jobs	DLL Search Order Hijacking	Component Eirmware	Forced Authentication	Network Share	Pass the Hash	Data from Network	Command and	Data Encoding
Service	Exploitation for	Bootkit	Dulib Hijacking	Component Object Medal	Hooking	Discovery	Pass the Ticket	Shared Drive	Control Channel	Data Obfuscation
Supply Chain	Execution	Bro. Fitensions	Exploitation for	Hijacking	Input Capture	Network Sniffing	Remote Desktop	Data from Removable Media	Exfiltration Over Other Network	Domain Fronting
Compromise	Graphical User Interface	Change Defaurt	Privilege Escalation	Control Panel Items	Input Prompt	Password Policy Protoco Discovery	Protocol	Data Staged	Medium	Fallback Channels
Trusted Relationship	InstallUtil	Association	Ex. Mindow	DCShadow	Kerberoasting	Remote File Co	Remote File Copy	Email Collection Exfiltratio	Exfiltration Over	Multi-hop Proxy
Valid Accounts	Launchetl	Component Firmware	Memory ingeneration	Deobfuscate/Decode Files or	Kevchain	Discovery	Remote Services	Innut Canture	Physical Medium	Multi-Stage Channels
	Local Job Scheduling	Component Object	File System	Inc. stion	LI MNR/NRT-NS	Permission Groups	Replication Through	input capture	Scheduled Transfer	Multiband
	LSASS Driver	Model Hijacking	Weakness	Disabling Security Teols	Poisoning	Discovery	Nemovable Media	Man in the browser		Communication
	Mshta	Create Account	Hooking	DLL Search Order Hijacking	htwork Sniffing	Process Discovery	Shared Webroot	Screen Capture		Multilayer Encryption
	PowerShell	DLL Search Order Hilacking	Image File Execution	DLL Side-Loading	Password I. OLL	Query Registry	SSH Hijacking	Video Capture		Port Knocking
	Regsvcs/Regasm	Dulib Hijacking	Options Injection	Exploitation for Defense Evasion	Private Keys	Discovery Discovery	Taint Shared Content			Remote Access Tools
	Regsvr32	External Demote	Launch Daemon		Securityd Memory		Third-party Software			Remote File Copy
	Rundll32	Services	New Service	Extra Window Memory	Two-Factor Authentication		Mindows Admin Shan			Standard Application
	Scheduled Task	File System Permissions	Path Interception	rijecuon File Deletier		System Information	Windows Remote	_		Layer Protocol

mitre-attack.github.io/attack-navigator

Emulate

Defend



Approved for public release. Distribution unlimited 19-00696-5



© 2019 The MITRE Corporation. All rights reserved.

giphy.com/gifs/hulu-fox-family-guy-l2Sq4fHpeKTNQs6Zy





pbsdigitalstudios.tumblr.com/post/62338254522/bill-nye-the-science-gif-happy-tbt-sometimes

Approved for public release. Distribution unlimited 19-00696-5

Today's Menu

- Walk-through of iteratively emulating and defending against a single technique/behavior
- Purple team approach (transparency ftw)
- Start with low confidence of defense

nitial Access 1 items	Execution 33 items	Persistence 59 items	Privilege Escalation 28 items	Defense Evasion 67 items	Credential Access 19 items	Discovery 22 items	Lateral Movement 17 items	Collection 13 items	Command And	Exfiltration 9 items	Impact 14 items
rive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
xploit Public-Faong oblication	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
xternal Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
lardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account	Credential Dumping	Domain Trust Discovery	Exploitation of Remote	Data from Information Repositories	Sustom Command and	Data Transfer Size Limits	Disk Content Wipe
eplication Through emovable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	Elle and Directory Discovery	Logon Scripts	Data from Local System	Protocol Cryptographic	Exhitration Over Alternative Protocol	Disk Structure Wipe
pearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared	Data Encoding	Exhibition Over Command	Endpoint Denial of Service
pearphishing Link	Execution through API	Authentication Package	LL Search Order	Code Signing	Exploitation for Credential	Network Share Discovery	Pass the Ticket	Lata from Removable	Data Obfuscation	Exhibition Over Other	Firmware Corruption
pearphishing via Service	Execution through Module	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exhibration Over Physical	Inhibit System Recovery
upply Chain Compromise	Exploitation for Client	Bootkit	Exploitation for Privilege	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation	Scheduled Transfer	Network Denial of Service
nisted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory	Component Firmware	Input Capture	Reripheral Device	Remote Services	Input Capture	Fallback Channels		Resource Hijacking
alid Accounts	InstallUti	Change Default File	Hie System Permissions	Component Object Model	Input Prompt	Permission Groups	Replication Through	Man in the Browser	Multi-hop Proxy	1	Runtime Data Manipulation
	Launchell	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels	1	Service Stop
	Local Job Scheduling	Component Object Model	Image File Execution	DCShadow	Keychain	Query Registry	SSH Hijacking	Video Capture	Multiband Communication	1	Stored Data Manipulation
	LSASS Driver	Create Account	Launch Daemon	Deplofuscate/Decode Files	LLWNR/NBT-NS Poisoning	Remote System Discovery	Taint Shared Content		Multilaver Encryption	1	Iransmitted Data
1	Mshta	DLL Search Order	New Service	Disabling Security Tools	Network Sniffing	Security Software	Third-party Software	1	Port Knocking	1	Maripulatori
	DraweShall	Dish Historia	Dath Internetion	DLL Search Order	Decement Filter DLI	System Information	Mindouse Admin Sharese	1	Demote Access Tools	1	
ŀ	Renauce/Renaem	External Remote Service	Pist Modification	DLL Side-Loading	Private Keys	System Network	Windows Remote	1	Remote File Conv	1	
ł	Receiver 32	Hie System Permissions	Port Monitore	Evenution Quartraile	Securityd Memory	System Network	Management	1	Standard Application Laver	1	
ł	Dural132	Lidden Files and	Process Injection	Exploitation for Defense	Two-Factor Authentication	System Owner/User	1		Standard Cryptographic	1	
ł	Numandz Schudulad Taek	Directories	Schedulard Task	Eversion Extra Window Memory	Interception	Discovery System Service Discovery	1		Standard Non Application	1	
	Parinting	hanning .	Service Registry .	Injection File Deleting		System Time Discovery	1		Lawer Protocol	1	
ł	Service Even from	Image File Execution	Permissions Weakness Saturid and Saturid	File Permissions		Virtualization/Sandbox	1		Web Service	-	
ł	Signed Binary Proxy	Cottons Injection Kernel Modules and	SID-Histon Injustion	Modification File System Logical Offects		Evasion	1		1100 00 100	1	
-	Extecution Summer Seriest Prever	Extensions	SID-ristory injection	File System Logical Unsets							
-	Execution	Laurich Agent	Stanup items	Gatekeeper Bypass							
	Source	Launch Daemon	Sudo Sudo Cashing	Hidden Files and							
-	Space after Filename	Laurence	audo Caching	Directories							
-	Third-party Software	LC_LOND_DYLIB Addition	Valid Accounts	hidden Users							
	Irap	Local Job Scheduling	Web Shell	Hidden Window							
	Trusted Developer Utilities	Login Item		HISTCONTROL Image Life Evention							
	User Execution	Logon Scripts		Options Injection							
-	Instrumentation"	LSASS Driver		Indicator Blocking							
	Management	Modify Existing Service		Tools							
L	XSL Script Processing	Netsh Helper DLL		Indicator Removal on Host							
		New Service		Emation							
		Once Application Startup		Install Root Certificate							
		Path Interception		InstallUbl							
		Plist Modification		Launcheti							
		Port Knocking		LC_MAIN Hjacking							
		Port Monitors		Masquerading							
		Rc.common		Modify Registry							
		Re-opened Applications		Maharak Shara Convention							
		Redundant Access		Removal							
		Staffun Folder		NTES File Attributes							
		Scheduled Task		Information							
		accentaver		Prist Modification							
		Service Registry		Pon Mocking							
		Permissions Weakness		Process Loppeiganging							
		Setuid and Setgid		Process Hollowing							
		SIP and Trust Provider		Process Injection							
		Biacking Clast in James		Redundant Access							
		Granup Herris		NegavCs/Kegasm							
		System Firmware		Regsvtaz							
		Systemd Service		Rookit Drauli22							
		Time Providers		Punai 32							
		Trap Malid Access into		Schpung Signed Binary Proxy							
		Valid Accounts		Signed Script Proxy							
		Web Shell Windows Management		Execution SID and Trust Dravidar							
		Reading and the second s		Hiadking							
	I	writiogan Helper DLL		Sonware Packing							
				space after Friename							
				remptate Injection							
				Timestomp							
				trusted Developer Utilities							
				Valid Accounts							

What is a *behavior*?

More than hash values, signatures, IPs, etc.
Think ATT&CK structure

Tactic (Why)
Technique (How)
Procedure (What)

Critical when considering emulation

What is a *behavior?*

Stages of a behavior

- 1. Prerequisites What does execution require?
- 2. Mechanics What does execution involve?
- 3. Artifacts What does execution leave behind?

Critical when considering detection

© 2019 The MITRE Corporation. All rights reserved.

giphy.com/gifs/munchies-lets-do-this-disguise-camo-WRoPE3GmHeozvej7pM

Approved for public release. Distribution unlimited 19-00696-5

How do you emulate a behavior?

Atomic Red Team

Automated Adversary Emulation

mon	itor >>>	op 1				
!		agent	status	score	executed command	!
 	 1	+ 1	+ 0	++ 0	2019-04-25 08:31:23.813667 Get-Process	-1
Í –	2	1	j 0	0	2019-04-25 08:31:29.286592 arp -a	Ì.
i –	3	j 1	j 1	j 0 j	2019-04-25 08:31:44.543653 net share	İ.
Í –	4	1	j 0	0	2019-04-25 08:31:49.696768 whoami	Ì.
i –	5	j 1	j 1	j 0 j	2019-04-25 08:31:54.798033 Get-Service	İ.
Í –	6	1	j 0	0	2019-04-25 08:31:59.887264 sleep 60	Ì.
i –	7	j 1	j 1	j 0 j	2019-04-25 08:33:05.011256 nltest /dclist:%USERDOMAIN%	İ.
i –	8	j 1	j 1	j 0 j	2019-04-25 08:33:10.161405 wmic /NAMESPACE:\\root\SecurityCenter2 PATH AntiVirusProduct GET /value	İ.
mon	itor					

github.com/mitre/caldera

github.com/redcanaryco/atomic-red-team

Emulating a behavior - Scenario

	win10.windomain.local [Running]
This PC		V10
Boot Time:	4/30/2019 3:18 PM	
Address: Microsoft S Server: Edge	10.0.2.15 192.168.38.104 147.75.207.207 147.75.207.208 192.168.38.102	
S Version: rvice Pack: ser Name: Googlegon Domain: Chromegon Server: IE Version: Workstation, Term	Windows 10 No service pack vagrant WIN10 WIN10 11.471.17134.0 inal Server	
Volumes: Free Space: Memory:	C:\ 60.00 GB NTF S C:\ 43.20 GB NTF S 2048 MB	Windows 10 Enterprise Evaluation Windows License is expired Build 17134.rs4_release.180410-1804
🔳 A 🛱 🦲	Σ	へ 管 記 🗗 🕫 4:28 PM 4/30/2019

How do you emulate a behavior?

Atomic Test #1 - Indirect Command Execution - pcalua.exe

The Program Compatibility Assistant (pcalua.exe) may invoke the execution of programs and commands from a Command-Line Interface.

Reference

Supported Platforms: Windows

Inputs

Name	Description	Туре	Default Value
process	Process to execute	string	calc.exe
payload_path	Path to payload	path	c:\temp\payload.dll
payload_cpl_path	Path to payload	path	C:\Windows\system32\javacpl.cpl -c Java

Run it with command_prompt !

pcalua.exe -a #{process}
pcalua.exe -a #{payload_path}
pcalua.exe -a #{payload_cpl_path}

Atomic Test #2 - Indirect Command Execution - forfiles.exe

forfiles.exe may invoke the execution of programs and commands from a Command-Line Interface.

Reference

"This is basically saying for each occurrence of notepad.exe in c:\windows\system32 run calc.exe"

Supported Platforms: Windows

Inputs

Name	Description	Туре	Default Value
process	Process to execute	string	calc.exe

Runit with command_prompt !

forfiles /p c:\windows\system32 /m notepad.exe /c #{process} forfiles /p c:\windows\system32 /m notepad.exe /c "c:\tolder\normal.dll:evil.exe"

atomicredteam.io

	win10.windomain.local [Running]			win10.windomain.local [Running]	
This PC		110	This PC		110
			Î		
Bin Boot Time:	4/30/2019 4:35 PM		Recycle Bin Boot Time:	4/30/2019 4:35 PM	
	10.0.2.15 192.168.38.104 147.75.207.207 14 7.75.207.208 192.168.38.102		Address: Micru ANS Server:	10.0.2.15 192.168.38.104 147.75.207.207 14 7.75.207.208 192.168.38.102	
S Version: rvice Pack: ser Name: logon Domain: 26gon Server: E Version: Vorkstation, Termina	Windows 10 No service pack vagrant WIN10 WIN10 11.471.17134.0 al Server		S Version: Offrvice Pack: See Name: Geoglegon Domain: Chromogon Server: IE Version: Workstation, Termin	Windows 10 No service pack vagrant WIN10 WIN10 11.471.17134.0 nal Server	
Volumes: Free Space: Memory:	C:\60.00 GB NTF \$ C:\43.32 GB NTF \$ 2048 MB	Windows 10 Enterprise Evaluation Windows License is expired Build 17134.rs4_release.180410-1804	Volumes: Free Space: Memory:	C:\ 60.00 GB NTF S C:\ 43.32 GB NTF S 2048 MB	Windows 10 Enterprise Evaluation Windows License is expired Build 17134.rs4_release. <u>1</u> 80410-1804
		ヘ 幅 단 ଏ <mark>ଛ</mark> 4/30/2019	🖷 🤉 🖽 🔚	Σ	▲ 2440 PM 4/30/2019

pcalua.exe -a calc.exe

forfiles /p C:\Windows\System32 /m notepad.exe /c calc.exe

| 17 |

giphy.com/gifs/i-see-what-you-did-there-CcUk4a6fkgUfu

How do you detect a *behavior*?

Data Sources – source of information

- Process monitoring, etc.
- Sensors collect information from data sources
- Analysis of collected information

Detection Lab –purple team playground

- Windows domain
- Splunk server
- https://github.com/clong/DetectionLab

Atomic Test #1 pcalua.exe -a calc.exe Process monitoring pcalua.exe Process command-line parameters ∎ -a Windows event logs 4688 (Process creation)

| 20 |

Atomic Test #2

forfiles /p C:\Windows\System32 /m notepad.exe /c calc.exe

Process monitoring

forfiles.exe

Process command-line parameters

■ <u>/</u>C or -C

Windows event logs
4688 or 1 (Sysmon)

5

ATT&CK Evaluations

M		T&CK [®] EVALUATI	ONS			Evaluations Get Evaluated
	Step	Procedures	Technique	Detection Type	Detection Notes	Screenshots
		Legitimate user Debbie	User Execution (T1204)	Telemetry (Tainted) Q Ø	Telemetry showed that Resume Viewer.exe was executed. The telemetry was tainted by the parent Script File Created alert.	• Telemetry showing Resume Viewer.exe running (tainted by the parent Script File Created alert)
	1.A.1	clicked and executed malicious self-extracting archive (Resume	Rundll32 (T1085)	Telemetry (Tainted) Q Ø	Telemetry showed that cmd.exe created the rundll32.exe process that started update.dat. The telemetry was tainted by the parent Script File Created alert.	• Telemetry showing cmd.exe launched rundll32.exe (tainted by the Script File Created alert)
		(Nimda)	Scripting (T1064)	Telemetry (Tainted) Q Ø	Telemetry showed that Resume Viewer.exe created cmd.exe, which ran the script pdfhelper.cmd. The telemetry was tainted by the parent Script File Created alert.	 Telemetry showing cmd.exe running pdfhelper.cmd (tainted by the Script File Created alert)

attackevals.mitre.org

giphy.com/gifs/luDW6dmgqcsuc

- Look at how previous behavior was detected
- In this case, we need to move away from process-level monitoring
- •.NET/C# alternative?
 - Access to underlying Win32 API
 - Immature detection posture due to complexity
 - Legitimate usage provides noise / false positives
 - Leveraged by red teamers and threat actors

CreateProcessA, unsurprisingly, lets users create new processes and by default, processes will be created with their inherited parent. However, this function also supports a parameter called "IpStartupInfo" where you can essentially define the parent process you want to use.

countercept.com/blog/detecting-parent-pid-spoofing

25

C:\>SelectMyPar SelectMyParent Source code put https://Didier Use at your ow	C:\>SelectMyParent notepad 864 SelectMyParent v0.0.0.1: start a program with a selected parent process Source code put in public domain by Didier Stevens, no Copyright https://DidierStevens.com Use at your own risk								
Process created	d: 5156								
C: \>									
	_								
Isass.exe	864	Local Security Authority Proc Microsoft Corporation	NT AUTHORITY\SYSTEM						
motepad.exe	5156	Notepad Microsoft Corporation	NT AUTHORITY\SYSTEM						
sm.exe	872	Local Session Manager Serv Microsoft Corporation	NT AUTHORITY\SYSTEM						
CSISS.exe	816	Client Server Runtime Process Microsoft Corporation	NT AUTHORITY\SYSTEM						
🙀 winlogon.exe	920	Windows Logon Application Microsoft Corporation	NT AUTHORITY\SYSTEM						

blog.didierstevens.com/2009/11/22/quickpostselectmyparent-or-playing-with-the-windows-process-tree/

Approved for public release. Distribution unlimited 19-00696-5

CHALLENGE ACCEPTED

giphy.com/gifs/hoppip-how-i-met-your-mother-barney-stinson-AWv3UAFkgz39u/media

Approved for public release. Distribution unlimited 19-00696-5

Process monitoring

• Unsigned? Untrusted?

Process command-line parameters

- Loaded DLLs/DLL monitoring (Sysmon Event ID 7: Image loaded)
 - Ir.dll Microsoft .NET Runtime Common Language Runtime
 - Icrosoft .NET Runtime Just-In-Time Compiler

File monitoring (Sysmon Event ID 11: FileCreate)

AppData\Local\Microsoft\CLR_v*\UsageLogs*.log

twitter.com/sbousseaden/status/1123160362155687936?s=21

ETW Providers

- Microsoft-Windows-DotNETRuntime {E13C0D23-CCBC-4E12-931B-D9CC2EEE27E4}
- Microsoft-Windows-DotNETRuntimeRundown {A669021C-C450-4609-A035-5AF59AF4DF18}
- Microsoft-Windows-Kernel-Process {22FB2CD6-0E7B-422B-A0C7-2FAD1FD0E716}

Capture/View ETW Events

- logman/tracerpt
- PyWinTrace https://github.com/fireeye/pywintrace
- Dot Net Runtime ETW https://gist.github.com/countercept/7765ba05ad00255bcf6a4a26d7647f6e#filedotnet-runtime-etw-py

ktop\pywintrace-master\pywintrace-master>dotnet_etw.py --disable-rundown-provider --enable-method-tracing

Capturing CLR ETW Events

Approved for public release. Distribution unlimited 19-00696-5

MITRE

Bonus: Capturing Kernel Process ETW Events

C:\Users\vagrant\Desktop\pywintrace-master\pywintrace-master>python detect-ppid.py Failed to get data field data for Flags, incrementing by reported size Failed to get data field data for Flags, incrementing by reported size Failed to get data field data for Flags, incrementing by reported size Spoofed parent process detected!!!

calc.exe(6900) is detected with parent explorer.exe(3476) but originally from parent x33f conDemo.exe(6564). ETW monitoring stopped.

countercept.com/blog/detecting-parent-pid-spoofing MITRE

giphy.com/gifs/how-i-met-your-mother-clapping-himym-irnky0EUGEZnq/media

| 34 |

giphy.com/gifs/devopsreactions-jf6tn79knHt96

| 35 |

How do you detect a better *behavior*, better?

- Detecting every behavior in real-time may not be feasible and/or realistic
 - Cost, noise, etc.
- May be more attainable for hunt/IR to capture data
 - ex: Analysts investigate specific events/incidents
- More emphasis on blocking
 - ex: .NET Framework 4.8 (APR 2019) includes Antimalware Scan Interface (AMSI)

0. Hunters proactively seek all pieces

- 1. Alert analyst when .NET DLLs are loaded by an unsigned process
- 2. Analyst manually investigates ETW, logs, and other follow-on activity

Closing statements

 From low to medium confidence on 1 technique
 Rinse and repeat

- other behaviors
- Combine into full campaign emulation

nitial Access 11 items	Execution 33 items	Persistence 59 items	Privilege Escalation 28 items	Defense Evasion 67 items	Credential Access 19 items	Discovery 22 items	Lateral Movement 17 items	Collection 13 items	Command And	Exfiltration 9 items	Impact 14 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Part	Automated Exfiltration	Data Destruction
xploit Public-Faong	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark	Ristributed Component	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
lardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account	Credential Dumping	Domain Trust Discovery	Exploitation of Remote	Data from Information	Sustom Command and	Data Transfer Size Limits	Disk Content Wipe
epication Through	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	Elle and Directory Discovery	Logon Scripts	Data from Local System	Protocol Cryptographic	Exhitration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Bata from Network Shared	Data Encoding	Excitcation Over Command	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	LLL Search Order	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exhibition Over Other Network Medium	Firmware Corruption
Spearphishing via Service	Execution through Module	BITS Jobs	Dyib Hjacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Falback Channels		Resource Hijacking
/alid Accounts	InstallUti	Association	Hie System Permissions Weakhess	Component Object Model Historing	Input Prompt	Descavery	Removable Media	Man in the Browser	Multi-hop Proxy		Runtime Data Manipulation
	Launchetl	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels		Service Stop
	Local Job Scheduling	Hacking	Ontions Intection	DCShadow	Keychain	Query Registry	SSH Hijacking	Video Capture	Multiband Communication		Stored Data Manipulation
	LSASS Driver	Create Account	Launch Daemon	or information	and Relay	Remote System Discovery	Taint Shared Content	1	Multilayer Encryption		Manipulation
	Mshta	Historia	New Service	Disabling Security Tools	Network Sniffing	Discovery	Third-party Software	-	Port Knocking		
ļ	PowerShell	Dylib Hijacking	Path Interception	Hiacking	Password Filter DLL	Discovery Sustem Mehande	Windows Admin Shares	-	Remote Access Tools	-	
ļ	Regsvcs/Regasm	External Remote Services	Prist Modification	DLL Side-Loading	Private Keys	Configuration Discovery	Management]	Remote File Copy Standard Application Laws	4	
ļ	Regsvr32	Weakhers Hidden Files and	Port Monitors	Execution Guardraits Exploitation for Defense	Securityd Memory Two-Eactor Authentication	Connections Discovery System Owner/Liser	1		Protocol Slandard Cryptographic	4	
ŀ	Kundi 32 Sebask dad Taak	Directories	Process Injection	Everson Extra Window Memory	Interception	Discovery Sustan Samian Disc	+		Standard Non-Application	4	
ŀ	Control and Task	nuoving Managinar	Service Registry .	Injection File Deletion		System Time Discovery			Laver Protocol	-	
ł	Service Execution	Image File Execution	Permissions Weakness Setuid and Setoid	File Permissions		Virtualization/Sandbox	1		Web Service	1	
-	Signed Binary Proxy	Colibris Inection Semel Modules and	SID-Histon Injection	Modification File System Logical Offente		Evaluon	1		Web de vice	1	
	Signed Script Proxy	Extensions	Startun Items	Gatekeener Bunass							
	Source	Launch Daemon	Sudo	Group Policy Modification							
	Space after Filename	Launchell	Sudo Caching	Lidden Files and							
	Third-party Software	LC LOAD DYLIB Addition	Valid Accounts	Hidden Users							
	Trap	Local Job Scheduling	Web Shell	Hidden Window							
	Trusted Developer Utilities	Login Item		HISTCONTROL							
	User Execution	Logon Scripts		Cations Inection							
	Windows Management	LSASS Driver		Indicator Blocking							
	Windows Remote	Modify Existing Service		Indicator Removal from							
	XSL Script Processing	Netsh Helper DLL		Indicator Removal on Host							
		New Service		Indirect Command							
		Office Application Startup		Install Root Certificate							
		Path Interception		InstallUti							
		Plist Modification		Launcheti							
		Part Knacking		LC_MAIN Hijacking							
		Port Monitors		Masquerading							
		Rc.common		Modity Registry							
		Re-opened Applications		Mshta Network Share Connection							
		Registry Run Keys /		Removal							
		Stattun Folder		Objuscated Files or							
		Screening lask		Information Dist Modification							
		Security Support Dravidue		Port Knocking							
		Service Registry		Process Doppelgänging							
		Setuid and Setuid		Process Hollowing							
		Shortcut Modification		Process Injection							
		SIP and Trust Provider		Redundant Access							
		Startup Items		Regsvcs/Regasm							
		System Firmware		Regsvr32							
		Systemd Service		Rootkit							
		Time Providers		Rundl32							
		Trap		Scripting							
		Valid Accounts		Signed Binary Proxy							
		Web Shell		Signed Script Proxy Execution							
		Reaction Places and a second		SIP and Trust Provider Historing							
		Winlogon Helper DLL		Software Packing							
				Space after Filename							
				Template Injection							
				Timestomp							
				Trusted Developer Utilities							

$A \mid X$ attack.mitre.org medium.com/mitre-attack attack@mitre.org MITREattack