Threat Research

Cerber: Analyzing a Ransomware Attack Methodology To Enable Protection

July 18, 2016 | by Ankit Anubhav , Raghav Ellur | Advanced Malware

RANSOMWARE CYBER ATTACK MICROSOFT ADVANCED MALWARE CYBER THREATS CYBER

CYBER SECURITY RANSOM

Ransomware is a common method of cyber extortion for financial gain that typically involves users being unable to interact with their files, applications or systems until a ransom is paid. Accessibility of cryptocurrency such as Bitcoin has directly contributed to this ransomware model. Based on data from FireEye Dynamic Threat Intelligence (DTI), ransomware activities have been rising fairly steadily since mid-2015.

On June 10, 2016, FireEye's HX detected a Cerber ransomware campaign involving the distribution of emails with a malicious Microsoft Word document attached. If a recipient were to open the document a malicious macro would contact an attacker-controlled website to download and install the Cerber family of ransomware.

Exploit Guard, a major new feature of FireEye Endpoint Security (HX), detected the threat and alerted HX customers on infections in the field so that organizations could inhibit the deployment of Cerber ransomware. After investigating further, the FireEye research team worked with security agency CERT-Netherlands, as well as web hosting providers who unknowingly hosted the Cerber installer, and were able to shut down that instance of the Cerber command and control (C2) within hours of detecting the activity. With the attacker-controlled servers offline, macros and other malicious payloads configured to download are incapable of infecting users with ransomware.

FireEye hasn't seen any additional infections from this attacker since shutting down the C2 server, although the attacker could configure one or more additional C2 servers and resume the campaign at any time. This particular campaign was observed on six unique endpoints from three different FireEye endpoint security customers. HX has proven effective at detecting and inhibiting the success of Cerber malware.

Attack Process

The Cerber ransomware attack cycle we observed can be broadly broken down into eight steps:

1. Target receives and opens a Word document.

2. Macro in document is invoked to run PowerShell in hidden mode.

4. On successful connection, the ransomware is written to the disk of the victim.
5. PowerShell executes the ransomware.
6. The malware configures multiple concurrent persistence mechanisms by creating command processor, screensaver, startup.run and runonce registry entries.
7. The executable uses native Windows utilities such as WMIC and/or VSSAdmin to delete backups and shadow copies.
8. Files are encrypted and messages are presented to the user requesting payment.

Rather than waiting for the payload to be downloaded or started around stage four or five of the aforementioned attack cycle, Exploit Guard provides coverage for most steps of the attack cycle – beginning in this case at the second step.

The most common way to deliver ransomware is via Word documents with embedded macros or a Microsoft Office exploit. FireEye Exploit Guard detects both of these attacks at the initial stage of the attack cycle.

PowerShell Abuse

When the victim opens the attached Word document, the malicious macro writes a small piece of VBScript into memory and executes it. This VBScript executes PowerShell to connect to an

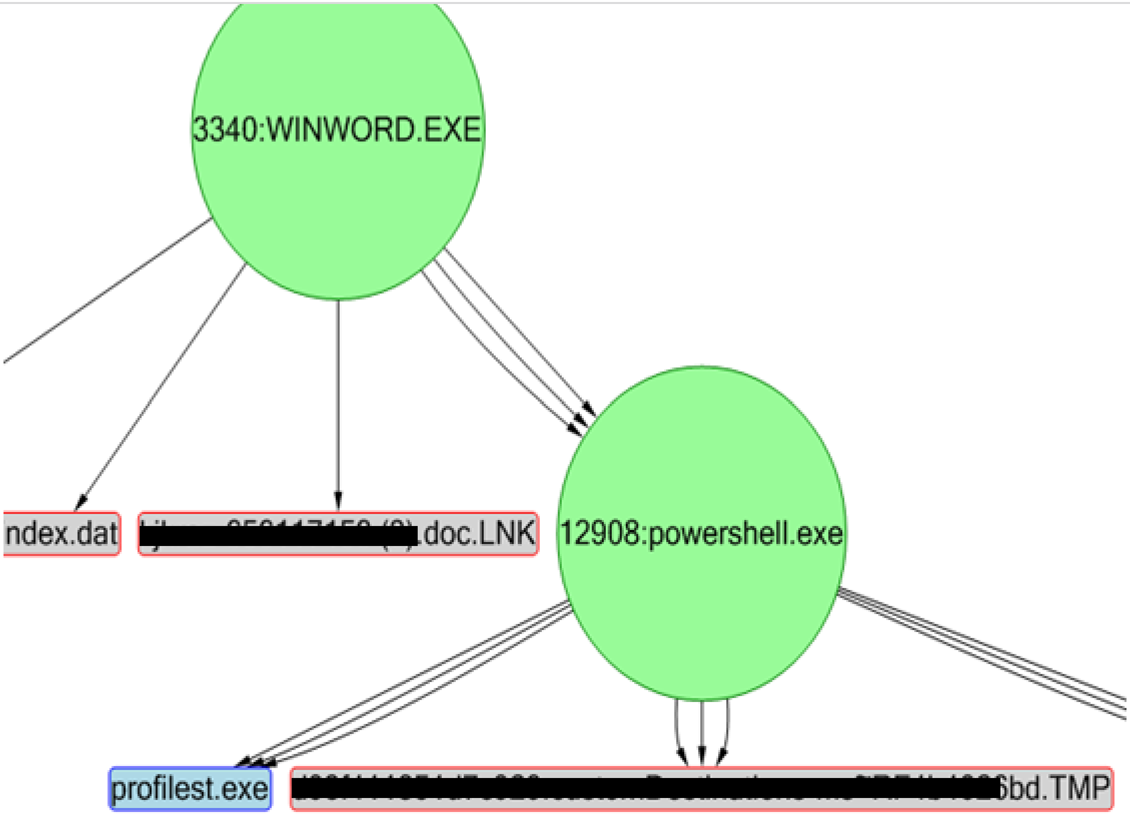


Figure 1. Launch sequence of Cerber – the macro is responsible for invoking PowerShell and PowerShell downloads and runs the malware

It has been increasingly common for threat actors to use malicious macros to infect users because the majority of organizations permit macros to run from Internet-sourced office documents.

In this case we observed the macrocode calling PowerShell to bypass execution policies – and run in hidden as well as encrypted mode – with the intention that PowerShell would download the ransomware and execute it without the knowledge of the victim.

Further investigation of the link and executable showed that every few seconds the malware hash changed with a more current compilation timestamp and different appended data bytes – a technique often used to evade hash-based detection.

Cerber in Action

Initial payload behavior

Upon execution, the Cerber malware will check to see where it is being launched from. Unless it is being launched from a specific location (%APPDATA%\&#60GUID&#62), it creates a copy of itself in the victim's %APPDATA% folder under a filename chosen randomly and obtained from the %WINDIR%\system32 folder.

"%APPDATA%\&#60GUID&#62" using a pseudo-randomly selected name from the "system32" directory. The malware executes the malware from the new location and then cleans up after itself.

Shadow deletion

As with many other ransomware families, Cerber will bypass UAC checks, delete any volume shadow copies and disable safe boot options. Cerber accomplished this by launching the following processes using respective arguments:

□□Vssadmin.exe "delete shadows /all /quiet"

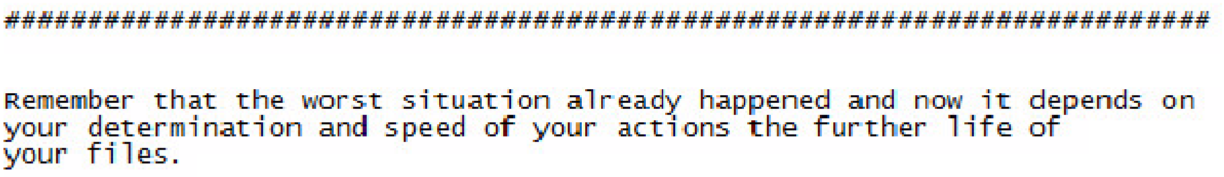
□□WMIC.exe "shadowcopy delete"

□□Bcdedit.exe "/set {default} recoveryenabled no"

□□Bcdedit.exe "/set {default} bootstatuspolicy ignoreallfailures

Coercion

People may wonder why victims pay the ransom to the threat actors. In some cases it is as simple as needing to get files back, but in other instances a victim may feel coerced or even intimidated. We noticed these tactics being used in this campaign, where the victim is shown the message in Figure 2 upon being infected with Cerber.

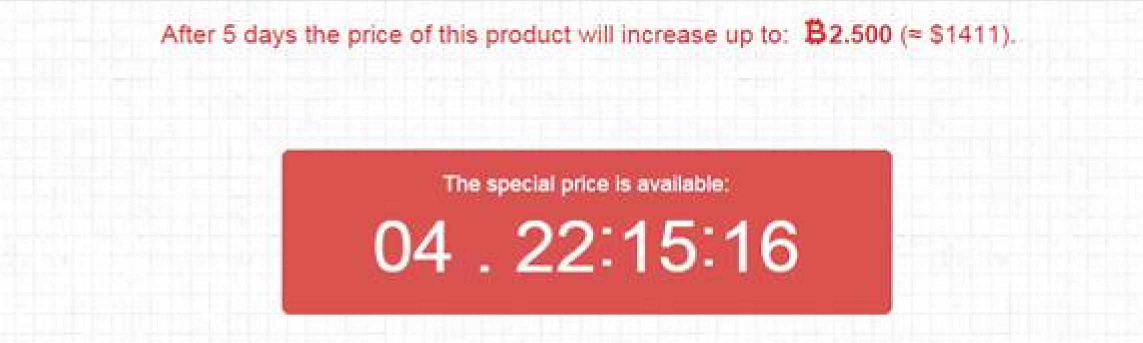


```
#########################################################################


Remember that the worst situation already happened and now it depends on
your determination and speed of your actions the further life of
your files.
```

Figure 2. A message to the victim after encryption

The ransomware authors attempt to incentivize the victim into paying quickly by providing a 50 percent discount if the ransom is paid within a certain timeframe, as seen in Figure 3.



After 5 days the price of this product will increase up to: Ƀ2.500 (≈ $1411).

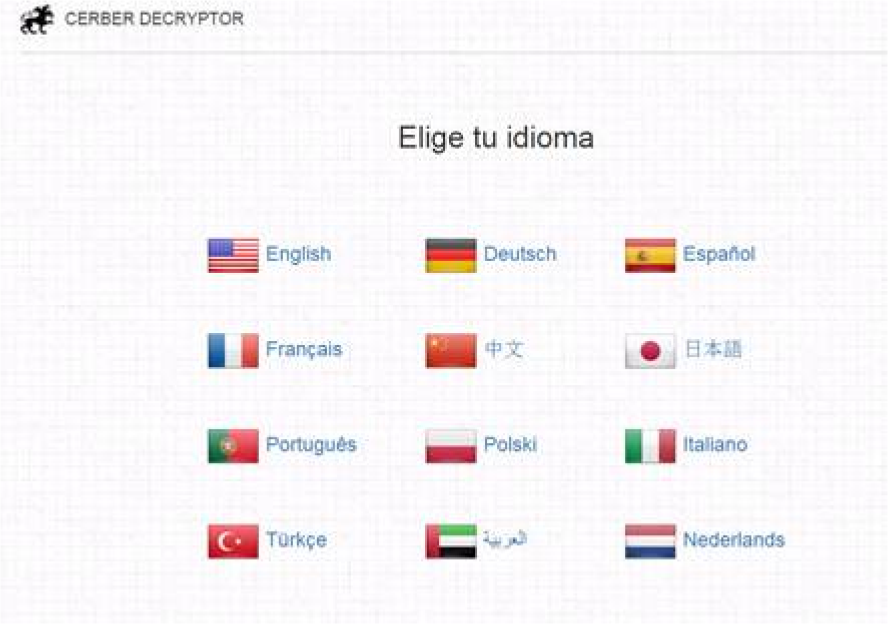
The special price is available:

04 . 22:15:16

Figure 3. Ransom offered to victim, which is discounted for five days

Multilingual Support

As seen in Figure 4, the Cerber ransomware presented its message and instructions in 12 different languages, indicating this attack was on a global scale.



CERBER DECRYPTOR

Elige tu idioma

English Deutsch Español

Français 中文 日本語

Português Polski Italiano

Türkçe العربية Nederlands

Figure 4. Interface provided to the victim to pay ransom supports 12 languages

Encryption

Cerber targets 294 different file extensions for encryption, including .doc (typically Microsoft Word documents), .ppt (generally Microsoft PowerPoint slideshows), .jpg and other images. It also targets financial file formats such as. ibank (used with certain personal finance management software) and .wallet (used for Bitcoin).

configuration, utilizing online services such as ipinfo.io to verify the information. Blacklisted (protected) countries include: *Armenia, Azerbaijan, Belarus, Georgia, Kyrgyzstan, Kazakhstan, Moldova, Russia, Turkmenistan, Tajikistan, Ukraine, and Uzbekistan*.

The attack also checked a system's keyboard layout to further ensure it avoided infecting machines in the attackers geography: *1049—Russian, ¨ 1058—Ukrainian, 1059—Belarusian, 1064—Tajik, 1067—Armenian, 1068—Azeri, (Latin), 1079—Georgian, 1087—Kazakh, 1088—Kyrgyz (Cyrillic), 1090—Turkmen, 1091—Uzbek (Latin), 2072—Romanian (Moldova), 2073—Russian (Moldova), 2092—Azeri (Cyrillic), 2115—Uzbek (Cyrillic).*

Selective targeting has historically been used to keep malware from infecting endpoints within the author’s geographical region, thus protecting them from the wrath of local authorities. The actor also controls their exposure using this technique. In this case, there is reason to suspect the attackers are based in Russia or the surrounding region.

Anti VM Checks

The malware searches for a series of hooked modules, specific filenames and paths, and known sandbox volume serial numbers, including: sbiedll.dll, dir_watch.dll, api_log.dll, dbghelp.dll, Frz_State, C:\popupkiller.exe, C:\stimulator.exe, C:\TOOLS\execute.exe, \sand-box\, \cwsandbox\, \sandbox\, 0CD1A40, 6CBBC508, 774E1682, 837F873E, 8B6F64BC.

Aside from the aforementioned checks and blacklisting, there is also a wait option built in where the payload will delay execution on an infected machine before it launches an encryption routine. This technique was likely implemented to further avoid detection within sandbox environments.

Persistence

Once executed, Cerber deploys the following persistence techniques to make sure a system remains infected:

- A registry key is added to launch the malware instead of the screensaver when the system becomes idle.
- The “CommandProcessor” Autorun keyvalue is changed to point to the Cerber payload so that the malware will be launched each time the Windows terminal, “cmd.exe”, is launched.
- A shortcut (.lnk) file is added to the startup folder. This file references the ransomware and Windows will execute the file immediately after the infected user logs in.
- Common persistence methods such as run and runonce key are also used.

A Solid Defense

Mitigating ransomware malware has become a high priority for affected organizations because passive security technologies such as signature-based containment have proven ineffective.

Malware authors have demonstrated an ability to outpace most endpoint controls by compiling multiple variations of their malware with minor binary differences. By using alternative packers

Disabling support for macros in documents from the internet and increasing user awareness are two ways to reduce the likelihood of infection. If you can, consider blocking connections to websites you haven't explicitly whitelisted. However, these controls may not be sufficient to prevent all infections or they may not be possible based on your organization.

FireEye Endpoint Security with Exploit Guard helps to detect exploits and techniques used by ransomware attacks (and other threat activity) during execution and provides analysts with greater visibility. This helps your security team conduct more detailed investigations of broader categories of threats. This information enables your organization to quickly stop threats and adapt defenses as needed.

Conclusion

Ransomware has become an increasingly common and effective attack affecting enterprises, impacting productivity and preventing users from accessing files and data.

Mitigating the threat of ransomware requires strong endpoint controls, and may include technologies that allow security personnel to quickly analyze multiple systems and correlate events to identify and respond to threats.

HX with Exploit Guard uses behavioral intelligence to accelerate this process, quickly analyzing endpoints within your enterprise and alerting your team so they can conduct an investigation and scope the compromise in real-time.

Traditional defenses don't have the granular view required to do this, nor can they connect the dots of discreet individual processes that may be steps in an attack. This takes behavioral intelligence that is able to quickly analyze a wide array of processes and alert on them so analysts and security teams can conduct a complete investigation into what has, or is, transpiring. This can only be done if those professionals have the right tools and the visibility into all endpoint activity to effectively find every aspect of a threat and deal with it, all in real-time. Also, at FireEye, we go one step ahead and contact relevant authorities to bring down these types of campaigns.

Click here for more information about Exploit Guard technology.

□ PREVIOUS POST

NEXT POST □

Investor Relations
Supplier Documents

News and Events
Newsroom
Press Releases
Webinars
Events
Awards and Honors
Email Preferences

Technical Support
Incident?
Report Security Issue
Contact Support
Customer Portal
Communities
Documentation Portal

Threat Map
View the Latest Threats

Contact Us
+1 877-347-3393

Stay Connected

□ □ □ □ □

Privacy & Cookies Policy | Privacy Shield | Legal Documentation

Site Language
English □

□ Promotion □ Subscribe □ Share □ Recent □ RSS