



Windows Defender ATP customer engagement

Ransomware response playbook

January 2017

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

This document is provided "as-is." Information and views expressed in this document, including URL and other Internet website references, may change without notice. You bear the risk of using it.

Copyright © 2017 Microsoft Corporation. All rights reserved.

Please refer to <u>Microsoft Trademarks</u> (https://aka.ms/MSTrademarks) for a list of trademarked products.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners

Contents

Overview	4
1. Discover ransomware and mitigate	5
1.1. Threats that evade email filters and endpoint antimalware	5
1.2 Mitigating the threat	6
2. Investigate delivery and arrival	7
2.1. Investigating Windows Defender ATP alerts	8
2.2. Checking for other artifacts	10
2.3. Investigating with no alerts raised	11
3. Scope the incident	12
3.1. Searching for the executable file using the process SHA-1	12
3.2. Searching for the executable file by name	13
3.3. Searching for URLs or IP addresses	13
4. Protect against the ransomware	14
4.1. Protecting from email-borne ransomware	14
4.2. Protecting from ransomware that arrive through web browsers	14
4.3. Enhancing other endpoint defenses	15
4.4. Blocking malicious IPs, URLs, and domains	15
5. Recover from infection	16
6. Summary of the response process	17
6.1 Responding with Windows Defender ATP	17
7 References	10

Overview

Ransomware is a menace that affects both home users and large enterprises, including organizations in various industries. If left unabated, ransomware attacks can result in significant losses for its victims. Ransomware attacks have also provided a revenue stream for cybercriminals, who are likely to leverage these resources as well as the experience of running malicious campaigns to pursue other criminal activities, particularly cyberespionage.

This document provides an overview of how enterprise customers can leverage Windows Defender Advanced Threat Protection (Windows Defender ATP) to detect, investigate, and mitigate ransomware threats in their networks. It walks through different stages of incident response and shows how Windows Defender ATP can serve as an invaluable tool during each of these stages.

To illustrate how ransomware can be addressed, we use a real-world infection involving Cerber ransomware, the most active ransomware family for close to a year now. We show how Windows Defender ATP can help catch this specific Cerber variant and, at the same time, catch ransomware behavior generically.

1. Discover ransomware and mitigate

There are several ways ransomware can be discovered:

- Antispam and other email filters
- Detections by Windows Defender Antivirus (Windows Defender AV) or other endpoint antimalware
- Reports from end-users
- Windows Defender ATP alerts

1.1. Threats that evade email filters and endpoint antimalware

In cases where ransomware manages to evade email filters and endpoint antimalware, it would be reasonable to expect end-users to report cases of ransomware infection. However, employees might hesitate to report a ransomware attack or might delay reporting. Thus, the threat could remain active, leaving the network vulnerable.

Windows Defender ATP detects all kinds of threat and breach activity, including ransomware activity. It automatically raises alerts to help ensure that SecOps personnel are aware of ransomware infections and can respond accordingly. In our real-world Cerber case, Windows Defender ATP raised several alerts, indicating how each alert maps to an infection stage shown in the red boxes below.

11.28.2016 01:04:52	File backups have been deleted.	Pre-encryption steps	Medium	Suspicious Activity	In progress
11.28.2016 01:04:40	A process exhibiting suspicious behaviors was observed	Installation	Low	Suspicious Activity	In progress
11.28.2016 01:01:19	A network request to a hidden service has been made.	C2 communication	Low	Suspicious Network Traffic	In progress
11.28.2016 01:00:57	Suspicious Powershell commandline	Part of distribution	Medium	Suspicious Activity	In progress

Figure 1. Windows Defender ATP alerts for Cerber infection activity

1.2 Mitigating the threat

Although most ransomware are not known to move laterally, it is good practice to isolate affected machines from the network as soon as a ransomware infection or the presence of any other threat is suspected. Isolating affected machines also helps prevent ransomware from encrypting data on shared folders and mapped drives.

2. Investigate delivery and arrival

The two most common ransomware delivery vectors observed by Microsoft security researchers are malicious emails and drive-by downloads. A very common infection pattern unfolds as follows:

- 1. An employee gets an email from a spoofed address that appears trustworthy, such as addresses of online retailers, banks, or insurance providers.
- 2. The email has a *.zip* attachment, and the text inside the email body encourages the user to open the attachment.
- 3. Once the user extracts the contents of the .zip archive —typically a .docm, .js, .vbs, .lnk or .swf file is extracted—and opens the extracted file, the file downloads and runs an .exe or .dll file containing the ransomware payload.

There are also other ways machines get infected:

- User downloads malicious files from the internet
- User visits a website, triggering an exploit that downloads and runs the ransomware payload. Many of these exploits target outdated browser versions typically active in older versions of Windows.

Once a machine is found affected by ransomware, it is critical to understand how the machine became infected. When notified of an infection by a user, an antimalware detection, or a Windows Defender ATP alert, check the timeline of the affected machine in the Windows Defender ATP console and look for related events in the timeline. Windows Defender AV detections also trigger alerts in the Windows Defender ATP console and are visible in the timeline.

2.1. Investigating Windows Defender ATP alerts

Most advanced threats are polymorphic and actively modify themselves during infection to bypass antimalware and other protection layers deployed in enterprises. By focusing on generic behavioral patterns across a threat's lifecycle and across machines within organizations, Windows Defender ATP can help identify threats that are otherwise able to avoid traditional security solutions.

Our Cerber sample uses *cmd.exe* to run malicious commands using *Powershell.exe*. Behavioral detection in Windows Defender ATP recognizes this PowerShell activity as malicious and triggers an alert.

When we check the Windows Defender ATP console to investigate the network connection made by our Cerber ransomware sample, we clearly see how the ransomware used PowerShell to communicate with a command and control (C&C) address through a TOR anonymization service.



Figure 2. Cerber C&C connection via TOR

The timeline in the Windows Defender ATP console shows that the PowerShell command originated from Microsoft Word, which is unexpected behavior for most documents.

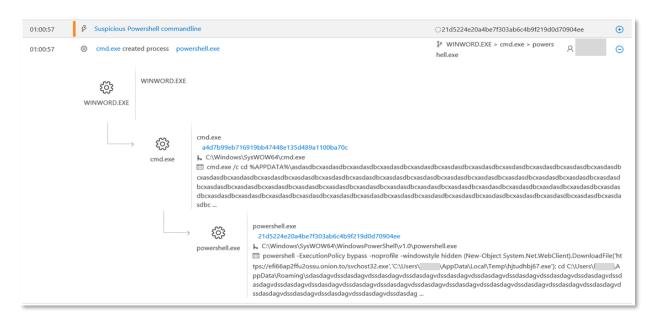


Figure 3. Document causes Microsoft Word to launch PowerShell

Now that it is known that the ransomware came from a Word document—most likely macros were enabled since the document was able to run a process—the next steps would be to look for a file creation event wherein a .doc or .docm file was created and to check which process created the file.

Again, most likely this event could be traced back to:

- An email client
- A web browser

Identifying the infection source can be done in the Windows Defender ATP console by investigating the alert process tree.

Apart from arriving via a macro-enabled Word (.docm) or Excel file (.xlsm), ransomware can also be downloaded by link (.lnk), JavaScript (.js) or VB script (.vbs) files. Locating any of these files and tracing how they reached the infected machine can help uncover the ransomware delivery mechanism.

2.2. Checking for other artifacts

With the payload file apparent from the alerts, the next thing to look for would be any network connections made *before* the payload file appeared on the machine.

To introduce the payload file to the victim's machine—in this context, the second stage payload is an .exe or .dll file—our Cerber sample opened a suspicious network connection through TOR and downloaded the payload file.

Using the process tree view on Windows Defender ATP, you can spot the connection between the suspicious PowerShell command line alert and the TOR communication alert. You can also see invaluable information about other artifacts, such as the IP address, domain, or URL involved in the communication.

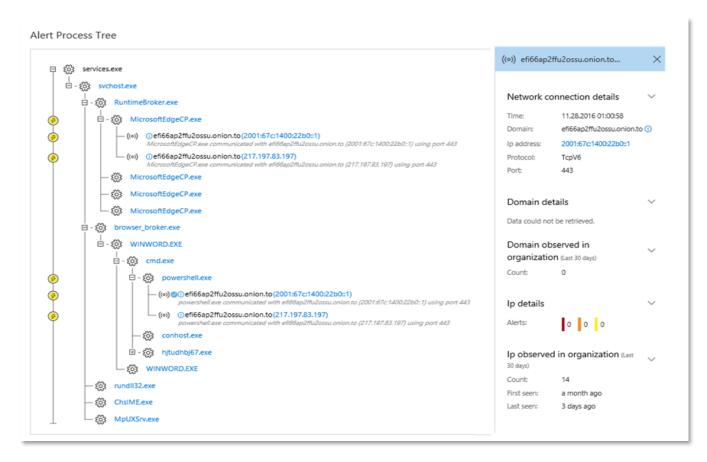


Figure 4. Full process tree showing the PowerShell command, the TOR connection, and the IP address

2.3. Investigating with no alerts raised

If you have been notified about the ransomware infection by a user or another solution, you can still go in the Windows Defender ATP console to check the timeline of the affected machine for:

- Any suspicious executables that have run on the affected machine; consider all available information to identify suspicious files, including prevalence and signer information, which are provided by Windows Defender ATP. To better understand file behavior, submit files for deep analysis.
- The process that triggered the creation of the suspicious executable
- The file associated with the process that triggered the creation of the suspicious executable

In general, if no alerts have been triggered on Windows Defender ATP for a verified infection, notify Microsoft immediately through Premier Support, which is accessible via the Windows Defender ATP help (?) menu. Notifying Microsoft helps us enhance detection of verified threats and their variants.

3. Scope the incident

With the known affected machine already isolated during the mitigation phase, you can proceed to investigate if the threat has affected other machines on the network. This will allow you to check whether the threat can spread laterally and how widespread the attack is.

NOTE: Spreading laterally is not a common ransomware technique. However, it is important to make sure no other machines on the network are impacted by the same threat.

To perform the techniques described below, you can leverage Windows Defender ATP search. In the search bar, specify the type of artifact you want to locate: file, IP address, URL, machine name, or user.



Figure 5. Windows Defender ATP search

3.1. Searching for the executable file using the process SHA-1

By searching for the SHA-1 of the suspect process, you can identify all other machines that have the same file and are likely also affected by the threat.

For our Cerber case, the file SHA-1 is quite rare, not being known to VirusTotal and having a global prevalence score of *one*. This rarity strongly indicates that the file is indeed malicious and very likely polymorphic.

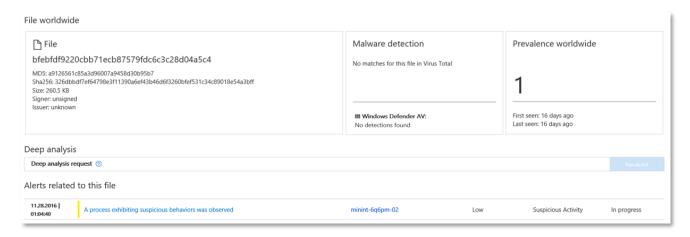


Figure 6. Windows Defender ATP showing SHA-1 prevalence and VirusTotal detections

3.2. Searching for the executable file by name

If the payload file is polymorphic, its SHA-1 will not be the same across its copies. By searching for the file by name instead of SHA-1, you may be able to find other affected machines. In the screenshot below, the Cerber payload file was found on multiple machines with the same filename but different SHA-1s.

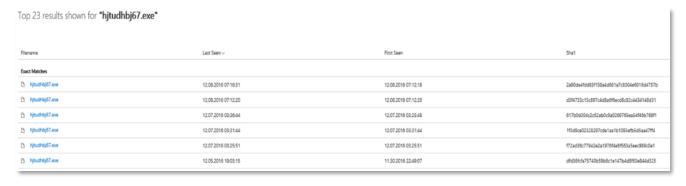


Figure 7. Searching for the polymorphic ransomware file by name

3.3. Searching for URLs or IP addresses

If you have identified a network address that the ransomware has connected to, search for the URL or IP address to identify similar connections from other machines on the network. Machines that have connected to the same address are likely affected by the same threat.

4. Protect against the ransomware

Now that we understand how the threat arrives and the extent of its impact, we can consider steps that can be taken to protect the network from further attacks.

4.1. Protecting from email-borne ransomware

If the threat arrived by email, consider the following preventive actions on your mail product. Office 365 provides powerful features that allow you to:

- Block the sender and message by marking it as spam
- Check the email header for a unique X-Mailer or sender IP address information and add message transport rules
- Remind end-users to move the attack email to the "junk" folder and report spam or malicious emails in Microsoft Office Outlook or Outlook on the web

Protect your email in real time against unknown and sophisticated attacks with Office 365 Advanced Threat Protection (Office 365 ATP). Office 365 ATP helps stop attacks by removing unsafe attachments and replacing unsafe links. It also provides message tracing, so you can investigate attack messages and track clicks on malicious links.

4.2. Protecting from ransomware that arrive through web browsers

If the threat arrived from a malicious or compromised website, consider the following preventive actions:

- Block the website:
 - o Block the site at the perimeter using a web proxy.
 - o Sinkhole the domain on internal DNS servers.
 - o Block the site IP address using Windows Firewall or the network firewall.

- Ensure that web browsers used in the enterprise have the latest security updates.
- Switch to newer browsers. Microsoft recommends Microsoft Edge for secure browsing.
- Report malicious sites to SmartScreen using Microsoft Edge (click Send feedback) or Internet Explorer (click Safety > Report unsafe website)

4.3. Enhancing other endpoint defenses

In addition to improving user awareness and requiring the use of secure browsers, the following actions can help enhance protection on individual machines:

- Apply the latest updates to all software.
- Update antimalware definitions.
- Configure Microsoft Office settings to disable macros.
- Set up backups to cover critical data.

4.4. Blocking malicious IPs, URLs, and domains

In addition to connections to a website hosting ransomware, you might have identified other malicious connections. Look for attempts to download additional malware components as well as attempts to report back to a command-and-control (C&C) server. Blocking the network addresses involved in these connections can help prevent the ransomware payload from being downloaded and eventually detonated. It can also prevent attackers from communicating with the malware.

5. Recover from infection

Machines that have been infected with ransomware should be reimaged to ensure that all threat components are removed and that the threat is prevented from spreading to other machines on the network. If you have active backups of files from the machine, do not restore backups until the machine is reimaged. Ensure that any system or data backups that you restore are from before the arrival of the ransomware.

After the affected machine has been rebuilt, ensure that the machine is well-protected. Refer to the recommendations in 4.3. Enhancing other endpoint defenses.

6. Summary of the response process

The response process for a ransomware infection can be summarized in the following steps:

- 1. Take the machine fully off the network. Do not allow the machine to be used unless for investigation.
- 2. Check if files on the affected machine were encrypted by ransomware.
- 3. Check for other suspicious events in the machine timeline.
- 4. Look for other affected machines on the network by checking for the same file names or SHA-1s. Check for connections to the same malicious network addresses.
- 5. Find any infection vectors, whether email, IP address, or URL, and block these infection sources.
- 6. Strengthen defenses at the endpoint by using newer browsers, deploying latest updates to software, and running endpoint antimalware. Configure Microsoft Office to disable macros by default.
- 7. Rebuild the affected machine. Recover data from backups generated before the infection.

6.1 Responding with Windows Defender ATP

By detecting ransomware behavior, Windows Defender ATP can help security responders quickly find ransomware, including those missed by email filters and endpoint antimalware. Windows Defender ATP helps trigger a timely response

process and enables responders to perform critical investigative and response tasks efficiently from a central console.

7. References

For more information about how you can defend against ransomware, see the following resources:

- Ransomware protection in Windows 10 Anniversary Update
- Defending against ransomware with Windows 10 Anniversary Update
- Ransomware facts on Microsoft Malware Protection Center
- Microsoft Malware Protection Center blog posts about active ransomware campaigns, prominent families, and the latest variants