Cerber Starts Evading Machine Learning

blog.trendmicro.com/trendlabs-security-intelligence/cerber-starts-evading-machine-learning/

March 28, 2017

Ransomware

CERBER is a ransomware family which has adopted a new technique to make itself harder to detect: it is now using a new loader which appears to be designed to evade detection by machine learning solutions.

By: Trend Micro March 28, 2017 Read time: (words)

The CERBER family of ransomware has been found to have adopted a new technique to make itself harder to detect: it is now using a new loader that appears to be designed to evade detection by machine learning solutions. This loader is designed to hollow out a normal process where the code of CERBER is instead run.

Behavior and Analysis

Ransomware typically arrives via email, and these new CERBER variants are no exception. Emails that claim to be from various utilities may have been used. The emails contain a link to a self-extracting archive, which has been uploaded to a Dropbox account controlled by the attackers. The target then downloads and opens it to infect a system. The following flow chart shows what happens next.

Figure 1. Cerber behavior flowchart

The downloaded file is a self-extracting archive that contains three files: a Visual Basic script, a DLL file, and a binary file that looks like a configuration file. In one sample we saw, these files are named *38oDr5.vbs*, *8ivq.dll*, and *x,* respectively. Other cases with the same behavior may have different file names, however.

Figure 2. Contents of self-extracting archive

First, the script is run using the Windows Script Host. The script, in turn, loads the DLL file using *rundll32.exe* with the DLL's filename and exports as the arguments.

The DLL file itself is simple and straightforward. All it does is read the configuration file (file *x*), decrypts part of it, and execute whatever it decrypts. The DLL file is not packed or encrypted; however, the code that it decrypted from file x is definitely malicious.

Figure 3. Start of binary file in X

X contains the loader, as well as various configuration settings. The loader has features that check if it is running in a virtual machine (VM), if it is running in a sandbox, if certain analysis tools are running on the machine, or if certain AV products are present. If any of these checks fail, the malware stops running. The lists below highlight the specific tools and products this software checks for:

Analysis Tools

- Msconfig
- Sandboxes
- Regedit
- Task Manager
- Virtual Machines
- Wireshark

Security vendors

- 360
- AVG
- Bitdefender
- Dr. Web
- Kaspersky
- Norton
- Trend Micro

The main payload of the loader is the injection of code in another process. In this case, the injected code is the whole Cerber binary, and it can be injected into any of the following processes:

- C:\Windows\Microsoft.NET\Framework\v2.0.50727\csc.exe
- C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe
- C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
- C:\Windows\SysWow64\WerFault.exe
- C:\Windows\System32\WerFault.exe

Please note that we have provided a list of the Dropbox URLs to their security team. The URLs in question are no longer functional, and the accounts involved have been banned from the service.

Machine Learning and Evasion

As a threat, Cerber has already been blocked by earlier advances in security solutions. Running Cerber in a normal process (as done by the loader) can help evade behavioral monitoring, but why go to the trouble of repackaging Cerber and using a separate loader? Earlier versions of Cerber already had a code injection routine which could mimic that particular behavior, so why was the separate loader necessary?

The answer lies in the adoption of the security industry of machine learning solutions. The industry has created features to proactively detect malicious files based on features instead of signatures. The new packaging and loading mechanism employed by Cerber can cause problems for static machine learning approaches–i.e, methods that analyze a file without any execution or emulation.

Self-extracting files and simple, straightforward files could pose a problem for static machine learning file detection. All self-extracting files may look similar by structure, regardless of the content. Unpacked binaries with limited features may not look malicious either. In other words, the way Cerber is packaged could be said to be *designed* to evade machine learning file detection. For every new malware detection technique, an equivalent evasion technique is created out of necessity.

This new evasion technique does not defeat an anti-malware approach that uses multiple layers of protection. Cerber has its weaknesses against other techniques. For instance, having an unpacked .DLL file will make it easy to create a one-to-many pattern; alternately having a set structure within an archive will make it easier to identify if a package is suspicious. Solutions that rely on a variety of techniques, and are not overly reliant on machine learning, can still protect customers against these threats.

Trend Micro Solutions

Threats will always try to get around the latest solutions, and users should avoid relying on any single approach to security. A proactive, multilayered approach to security is more effective— from the gateway, endpoints, networks, and servers..

Endpoint solutions such as Trend Micro™ Smart Protection Suites, and Worry-Free™ Business Security can protect users and businesses from these threats by detecting malicious files, and spammed messages as well as blocking all related malicious URLs. Trend Micro Deep Discovery™ has an email inspection layer that can protect enterprises by detecting malicious attachment and URLs.

Trend Micro OfficeScan™ with XGen™ endpoint security infuses high-fidelity machine learning with other detection technologies and global threat intelligence for comprehensive protection against ransomware and advanced malware. Our machine learning capabilities have been tuned to account for attacks using these types of evasion techniques.

Indicators of Compromise

Files with the following SHA256 hashes are associated with this threat:

- 09ef4c6b8a297bf4cf161d4c12260ca58cc7b05eb4de6e728d55a4acd94606d4 (Detected as VBS_CERBER.DLCYG)
- a61eb7c8d7a6bc9e3eb2b42e7038a0850c56e68f3fec0378b2738fe3632a7e4c (Detected as Ransom_CERBER.ENC)
- e3e5d9f1bacc4f43af3fab28a905fa4559f98e4dadede376e199360d14b39153 (Detected as Ransom_CERBER.VSAGD)
- f4dbbb2c4d83c2bbdf4faa4cf6b78780b01c2a2c59bc399e5b746567ce6367dd (Detected as TROJ_CERBER.AL)

Additional Analysis By Brian Cayanan and Jon Oliver.

Tags

Endpoints | Research | Ransomware