Threat Advisory: DoubleZero

blog.talosintelligence.com/2022/03/threat-advisory-doublezero.html

This post is also available in:

Українська (Ukrainian)

Overview

The Computer Emergency Response Team of Ukraine released an advisory on March 22, 2022 disclosing another wiper dubbed "DoubleZero" targeting Ukrainian enterprises during Russia's invasion of the country. This wiper was detected as early as March 17, 2022. DoubleZero is yet another wiper discovered in addition to previously disclosed attacks we've seen in Ukraine over the past two months, such as "CaddyWiper" "HermeticWiper" and "WhisperGate."

DoubleZero is a .NET-based implant that destroys files, registry keys and trees on the infected endpoint.

Cisco Talos is actively conducting analysis to confirm the details included in these reports.

Wiper analysis

The malware first checks if the current endpoint is one of the domain's controllers. If the endpoint's name is found, the wiper simply stops executing.

The wiper begins by obtaining the following privileges on the endpoint:

- SeTakeOwnershipPrivilege
- SeRestorePrivilege
- SeBackupPrivilege
- SeShutdownPrivilege

It aims to overwrite all files in all drives by destroying all files in all drives except for a specific list of the locations hardcoded in the wiper. The malware intends to destroy non-system files first, then system-related files. Destroying system related files while the overwriting of other files is pending can create instability and may lead to bricking the system before the complete destruction of the user's files is completed. In such cases, it may be possible to recover the files from the disk that haven't been overwritten yet.

The system folders reserved for destruction *after* all other files have been destroyed:

- <Root_drive>\Windows\Microsoft.NET
- <Root_drive>\Windows
- <Root_drive>\\Users\\\\.*?\\\\Local Settings.*
- <Root_drive>\\Users\\\\.*?\\\\AppData\\\\Local\\\\Application Data.*
- <Root_drive>\\Users\\\\.*?\\\\Start Menu.*
- <Root_drive>\\Users\\\\.*?\\\\Application Data.*
- <Root_drive>\\ProgramData\\\\Microsoft.*
- <Root_drive>\\Users\\\\.*?\\\\AppData\\\\Local\\\\Microsoft.*
- <Root_drive>\\Users\\\\.*?\\\\AppData\\\\Roaming\\\\Microsoft.*
- <Root_drive>\Documents and Settings
- <Root_drive>\ProgramData\Application Data
- <Root_drive>\Users\All Users
- <Root_drive>\Users\Default User
- <Root_drive>\system\drivers
- <Root_drive>\Windows\NTDS

The wiper will enumerate all file paths and decide if the file is "safe" to destroy immediately i.e., not a system file.

For each file that is deemed "safe" to destroy (i.e., not in the exclusions listed above), the wiper will:

- Change the access control of files by giving the Local System Account (WellKnownSidType.LocalSystemSid) full control of the file.
- Use one of the two wiper functions to destroy the files.

Wiper function No. 1

This routine will use APIs such as NtfsControlFile with a control code of FSCTL_SET_ZERO_DATA (0x980C8) to fill up the file with all zero bytes.

```
num2 = GClass6.NtFsControlFile(safeFileHandle, IntPtr.Zero, IntPtr.Zero, IntPtr.Zero, ref gstruct2, 622792UL, intPtr2, (ulong)((long)Marshal.SizeOf<GClass6.GStruct3>
  (gstruct4)), IntPtr.Zero, (ulong)((long)aG1ItHZ3wd0hGc.JwbyZ0j7ANqJRl(new int[]
```

NtfsControlFile used against a file to zero it out.

Wiper function No. 2

The second routine used to overwrite the files is relatively simpler. It opens the target file as a FileStream and simply overwrites it with an array containing all zeros.

```
fileStream.Write(array2, xH2BZMNfuO.ivFpj3d4f16Ef(new int[]
```

File being overwritten by an array containing all zeros.

Then the wiper moves on to the destruction of system files which is also carried out by the two wiper functions illustrated above. The order of destruction of the system files is:

First:

<Root_drive>\system\drivers

Second:

- <Root_drive>\\Users\\\\.*?\\\\Local Settings.*
- <Root_drive>\\Users\\\\.*?\\\\AppData\\\\Local\\\\Application Data.*
- <Root_drive>\Windows\NTDS
- <Root_drive>\\Users\\\\.*?\\\\AppData\\\\Local\\\\Microsoft.*
- <Root_drive>\\Users\\\\.*?\\\\AppData\\\\Roaming\\\\Microsoft.*

Third:

<Root_drive>\Windows

The wiper then proceeds to destroy entries in the registry hives:

- HKLM
- HKCU
- HKU

It will first kill all processes on the system named "lsass". Then, it will set the current user as the owner of the registry keys under these hives, change the access rights to get full control of the reg keys and then overwrite the values. The wiper will also delete subkey trees recursively.

```
RegistryAccessRule rule = new RegistryAccessRule(securityIdentifier, RegistryRights.FullControl, InheritanceFlags.ContainerInherit | InheritanceFlags.ObjectInherit, PropagationFlags.None, AccessControlType.Allow);
```

Wiper creating a rule to obtain full access to registry keys

```
registryKey.DeleteSubKeyTree(OqA84Tq0.Cx0rwbl25lW(new byte[]
```

Wiper deleting subkey trees in registry.

Once all the destructive activity has been completed, the wiper will then shutdown the system using the ExitWindowsEx API call.

Coverage

Ways our customers can detect and block this threat are listed below.

Product	Protection
Cisco Secure Endpoint (AMP for Endpoints)	✓
Cloudlock	N/A
Cisco Secure Email	✓
Cisco Secure Firewall/Secure IPS (Network Security)	✓
Cisco Secure Malware Analytics (Threat Grid)	✓
Umbrella	✓
Cisco Secure Web Appliance (Web Security Appliance)	N/A

Cisco Secure Endpoint (formerly AMP for Endpoints) is ideally suited to prevent the execution of the malware detailed in this post. Try Secure Endpoint for free here.

Cisco Secure Web Appliance web scanning prevents access to malicious websites and detects malware used in these attacks.

Cisco Secure Email (formerly Cisco Email Security) can block malicious emails sent by threat actors as part of their campaign. You can try Secure Email for free here.

Cisco Secure Firewall (formerly Next-Generation Firewall and Firepower NGFW) appliances such as Firepower Threat Defense (FTD), Firepower Device Manager (FDM), Threat Defense Virtual, Adaptive Security Appliance can detect malicious activity associated with this threat.

Cisco Secure Malware Analytics (formerly Threat Grid) identifies malicious binaries and builds protection into all Cisco Secure products.

Cisco Secure Network/Cloud Analytics (Stealthwatch/Stealthwatch Cloud) analyzes network traffic automatically and alerts users of potentially unwanted activity on every connected device.

For guidance on using Cisco Secure Analytics to respond to this threat, please click here.

Meraki MX appliances can detect malicious activity associated with this threat.

Umbrella, Secure Internet Gateway (SIG), blocks users from connecting to malicious domains, IPs and URLs, whether users are on or off the corporate network. Sign up for a free trial of Umbrella here.

Additional protections with context to your specific environment and threat data are available from the Firewall Management Center.

Cisco Duo provides multi-factor authentication for users to ensure only those authorized are accessing your network.

Open-source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

The following ClamAV signatures available for protection against this threat:

Win.Malware.DoubleZeroWiper-9942171-0

IOCs

d897f07ae6f42de8f35e2b05f5ef5733d7ec599d5e786d3225e66ca605a48f53
8dd8b9bd94de1e72f0c400c5f32dcefc114cc0a5bf14b74ba6edc19fd4aeb2a5
3b2e708eaa4744c76a633391cf2c983f4a098b46436525619e5ea44e105355fe
30b3cbe8817ed75d8221059e4be35d5624bd6b5dc921d4991a7adc4c3eb5de4a