Technical Analysis of the WhisperGate Malicious Bootloader

crowdstrike.com/blog/technical-analysis-of-whispergate-malware/

CrowdStrike Intelligence Team

January 19, 2022

On Jan. 15, 2022, a set of malware dubbed *WhisperGate* was reported to have been deployed against Ukrainian targets. The incident is widely reported to contain three individual components deployed by the same adversary, including a malicious bootloader that corrupts detected local disks, a Discord-based downloader and a file wiper. The activity occurred at approximately the same time multiple websites belonging to the Ukrainian government were defaced.

This blog covers the malicious bootloader in more detail.

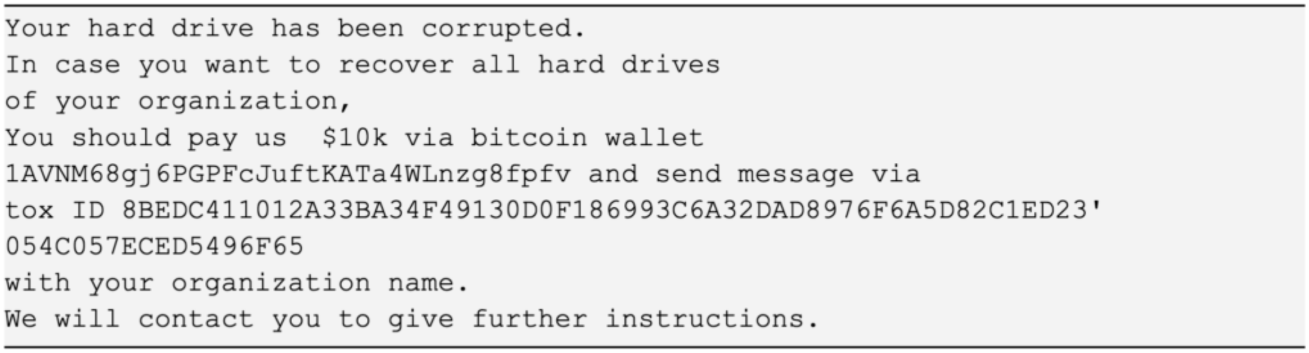
Details

The installer component for the bootloader has an SHA256 hash of

`a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92` and contains a build timestamp of 2022-01-10 10:37:18 UTC. It was built using MinGW, similar to the file-wiper component. This component overwrites the master boot record (MBR) of an infected host with a malicious 16-bit bootloader with a SHA256 hash of

`44ffe353e01d6b894dc7ebe686791aa87fc9c7fd88535acc274f61c2cf74f5b8`

that displays a ransom note when the host boots (Figure 1) and, at the same time, performs destructive operations on the infected host's hard drives.



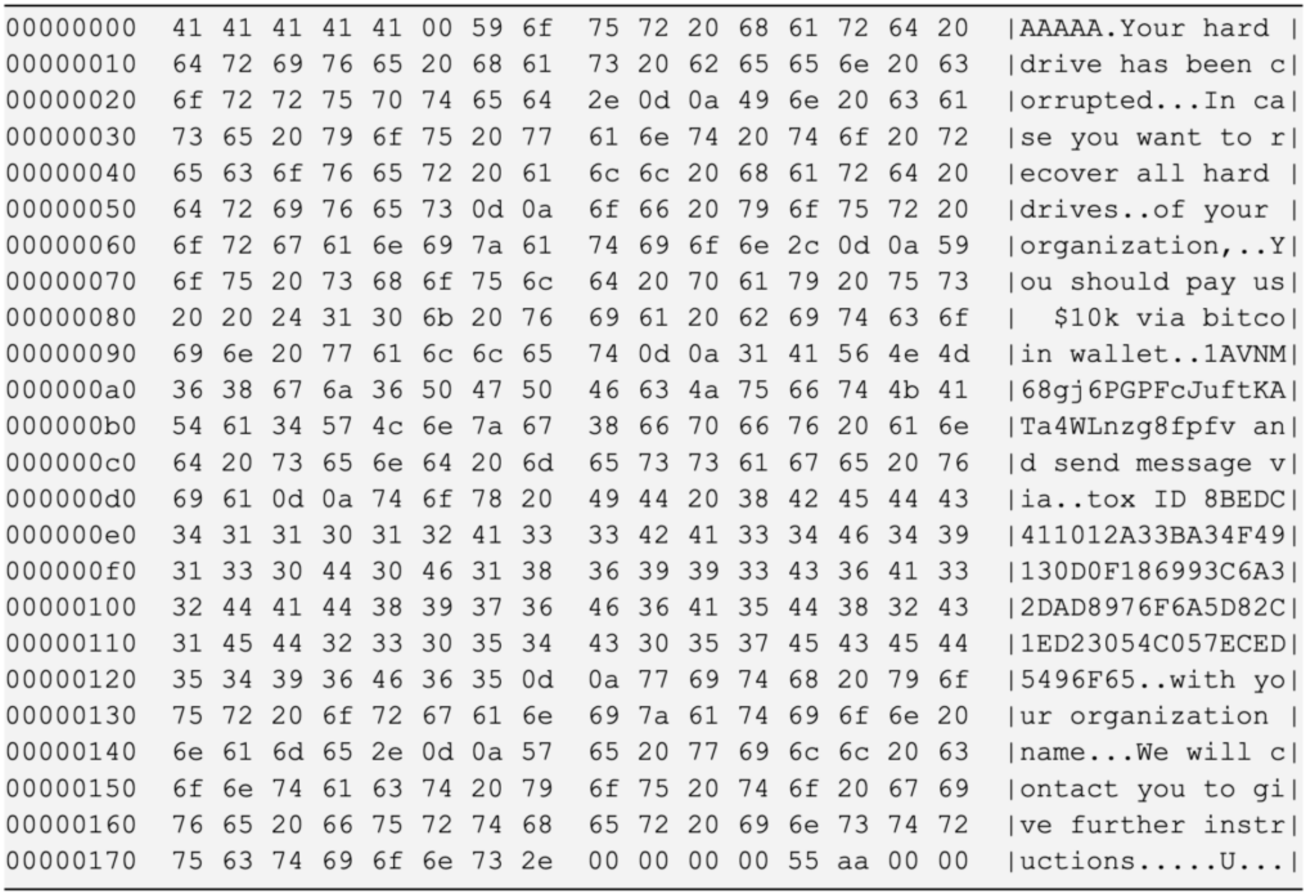
```
Your hard drive has been corrupted.
In case you want to recover all hard drives
of your organization,
You should pay us  $10k via bitcoin wallet
1AVNM68gj6PGPFcJuftKATa4WLnzg8fpfv and send message via
tox ID 8BEDC411012A33BA34F49130D0F186993C6A32DAD8976F6A5D82C1ED23'
054C057ECED5496F65
with your organization name.
We will contact you to give further instructions.
```

Figure 1. Fake ransom note

The destructive wiping operation has the following pseudocode:

```
for i_disk between 0 and total_detected_disk_count do
   for i_sector between 1 and total_disk_sector_count, i_sector += 199, do
      overwrite disk i_disk at sector i_sector with hardcoded data
   done
done
```

At periodic offsets, the bootloader overwrites sectors of an infected host's entire hard drive, with a message similar to the ransom note, padded with additional bytes (Figure 2).



```
00000000  41 41 41 41 41 00 59 6f  75 72 20 68 61 72 64 20  |AAAAA.Your hard |
00000010  64 72 69 76 65 20 68 61  73 20 62 65 65 6e 20 63  |drive has been c|
00000020  6f 72 72 75 70 74 65 64  2e 0d 0a 49 6e 20 63 61  |orrupted...In ca|
00000030  73 65 20 79 6f 75 20 77  61 6e 74 20 74 6f 20 72  |se you want to r|
00000040  65 63 6f 76 65 72 20 61  6c 6c 20 68 61 72 64 20  |ecover all hard |
00000050  64 72 69 76 65 73 0d 0a  6f 66 20 79 6f 75 72 20  |drives..of your |
00000060  6f 72 67 61 6e 69 7a 61  74 69 6f 6e 2c 0d 0a 59  |organization,..Y|
00000070  6f 75 20 73 68 6f 75 6c  64 20 70 61 79 20 75 73  |ou should pay us|
00000080  20 20 24 31 30 6b 20 76  69 61 20 62 69 74 63 6f  |  $10k via bitco|
00000090  69 6e 20 77 61 6c 6c 65  74 0d 0a 31 41 56 4e 4d  |in wallet..1AVNM|
000000a0  36 38 67 6a 36 50 47 50  46 63 4a 75 66 74 4b 41  |68gj6PGPFcJuftKA|
000000b0  54 61 34 57 4c 6e 7a 67  38 66 70 66 76 20 61 6e  |Ta4WLnzg8fpfv an|
000000c0  64 20 73 65 6e 64 20 6d  65 73 73 61 67 65 20 76  |d send message v|
000000d0  69 61 0d 0a 74 6f 78 20  49 44 20 38 42 45 44 43  |ia..tox ID 8BEDC|
000000e0  34 31 31 30 31 32 41 33  33 42 41 33 34 46 34 39  |411012A33BA34F49|
000000f0  31 33 30 44 30 46 31 38  36 39 39 33 43 36 41 33  |130D0F186993C6A3|
00000100  32 44 41 44 38 39 37 36  46 36 41 35 44 38 32 43  |2DAD8976F6A5D82C|
00000110  31 45 44 32 33 30 35 34  43 30 35 37 45 43 45 44  |1ED23054C057ECED|
00000120  35 34 39 36 46 36 35 0d  0a 77 69 74 68 20 79 6f  |5496F65..with yo|
00000130  75 72 20 6f 72 67 61 6e  69 7a 61 74 69 6f 6e 20  |ur organization |
00000140  6e 61 6d 65 2e 0d 0a 57  65 20 77 69 6c 6c 20 63  |name...We will c|
00000150  6f 6e 74 61 63 74 20 79  6f 75 20 74 6f 20 67 69  |ontact you to gi|
00000160  76 65 20 66 75 72 74 68  65 72 20 69 6e 73 74 72  |ve further instr|
00000170  75 63 74 69 6f 6e 73 2e  00 00 00 00 55 aa 00 00  |uctions.....U...|
```

Figure 2. Hexadecimal dump of the pattern written to the disks of an infected host

The data consists of the string `AAAAA`, the index of the infected drive, the ransom note and the MBR footer magic value `55 AA`, followed by two null bytes.

The bootloader accesses the disk via BIOS interrupt `13h` in logical block addressing (LBA) mode and overwrites every 199th sector until the end of the disk is reached. After a disk is corrupted, the malware overwrites the next in the detected disk list.

This process is unsophisticated but reminiscent of the more evolved implementation of *NotPetya*'s malicious MBR that masqueraded as the legitimate `chkdsk` disk-repair utility while actually corrupting the infected host's file system.

The bootloader installer does not initiate a reboot of the infected system, as has been observed in past intrusions such as *BadRabbit* and *NotPetya*. The lack of forced reboot suggests the threat actor took other steps to initiate it (e.g., via a different implant) or decided to let users perform the reboot themselves. A delayed reboot may allow other components of the *WhisperGate* intrusion to run (e.g., the file wiper).

Assessment

The *WhisperGate* bootloader malware complements its file-wiper counterpart. Both aim to irrevocably corrupt the infected hosts' data and attempt to masquerade as genuine modern ransomware operations. However, the *WhisperGate* bootloader has no decryption or data-recovery mechanism, and has inconsistencies with malware commonly deployed in ransomware operations.

The displayed message suggests victims can expect recovery of their data, but this is technically unachievable. These inconsistencies very likely indicate that *WhisperGate* activity aims to destroy data on the impacted assets. This assessment is made with moderate confidence as technical analysis of the *WhisperGate* activity continues.

The activity is reminiscent of VOODOO BEAR's destructive *NotPetya* malware, which included a component impersonating the legitimate `chkdsk` utility after a reboot and corrupted the infected host's Master File Table (MFT) — a critical component of Microsoft's NTFS file system. However, the *WhisperGate* bootloader is less sophisticated, and no technical overlap could currently be identified with VOODOO BEAR operations.

CrowdStrike Intelligence Confidence Assessment

High Confidence: Judgments are based on high-quality information from multiple sources. High confidence in the quality and quantity of source information supporting a judgment does not imply that that assessment is an absolute certainty or fact. The judgment still has a marginal probability of being inaccurate.

Moderate Confidence: Judgments are based on information that is credibly sourced and plausible, but not of sufficient quantity or corroborated sufficiently to warrant a higher level of confidence. This level of confidence is used to express that judgments carry an increased probability of being incorrect until more information is available or corroborated.

Low Confidence: Judgments are made where the credibility of the source is uncertain, the information is too fragmented or poorly corroborated enough to make solid analytic inferences, or the reliability of the source is untested. Further information is needed for corroboration of the information or to fill known intelligence gaps.

Additional Resources

- *Find out how to stop adversaries targeting your industry — schedule a free 1:1 intel briefing with a CrowdStrike threat intelligence expert today.*
- *Learn about the powerful, cloud-native CrowdStrike Falcon® platform by visiting the product webpage.*
- *Get a full-featured free trial of CrowdStrike Falcon Prevent™ to see for yourself how true next-gen AV performs against today's most sophisticated threats.*