Resources for DFIR Professionals Responding to WhisperGate Malware

cadosecurity.com/resources-for-dfir-professionals-responding-to-whispergate-malware/

January 17, 2022

Blog

January 17, 2022

Overview

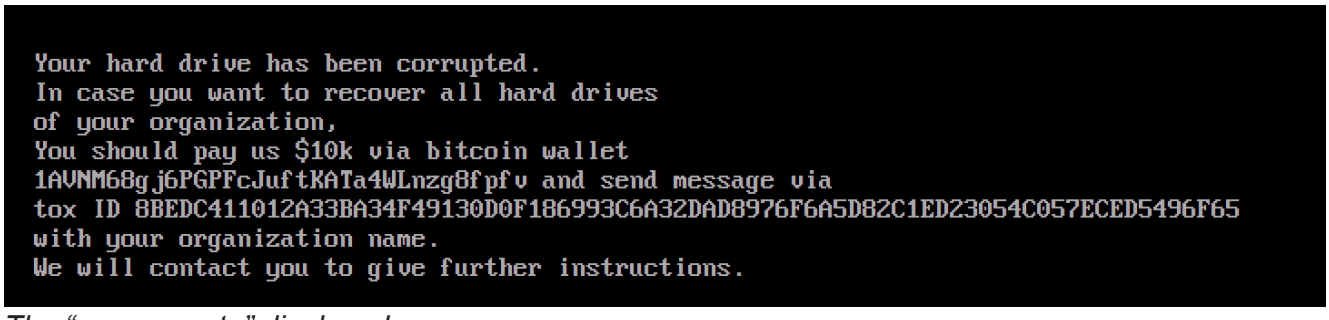
On Saturday January 15th, Microsoft released a blog titled "Destructive malware targeting Ukrainian organizations". Microsoft's blog outlines an ongoing attack against organisations in Ukraine by a currently-unknown threat actor and provides a detailed analysis of the malware samples involved. We have provided additional resources below that may be of use to those responding or investigating the attacks.

We have shared copies of the malware samples, decompiled code and YARA rules on our Github:

https://github.com/cado-security/DFIR_Resources_Whispergate

Malware Analysis References

In summary, the malware deployed in this campaign blocks access to computing systems by corrupting the Master Boot Record (MBR) section of the hard drive. The MBR is overwritten with a ransom note, such as those commonly seen in ransomware attacks, preventing the machine from booting and resulting in the corruption of files stored on the filesystem. However, as Microsoft notes, there is no recovery mechanism for the corrupted MBR, suggesting the ransom note is fake. This means the malware is likely masquerading as ransomware to hide its true capabilities or foil attribution attempts.



The "ransom note" displayed

Given the geopolitical climate in Ukraine, this attack has attracted interest from the cybersecurity research community. We've referenced additional analyses below:

We have published a playbook on how to respond to ransomware investigations that you can download here.

Indicators of Compromise

We have provided links to download the samples and the decompiled source code.

Indicator
stage1.exe A196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92 – [VirusTotal] [Decompiled Source]
stage2.exe Dcbbae5a1c61dbbbb7dcd6dc5dd1eb1169f5329958d38b58c3fd9384081c9b78 – [VirusTotal] [Decompiled Source]
Tbopbh.jpgDownloaded by stage2.exe from https://cdn.discordapp[.]com/attachments/928503440139771947/930108637681184768/Tbopbh.jpg and decodes to Frkmlkdkdubkznbkmcf.dll below 923eb77b3c9e11d6c56052318c119c1a22d11ab71675e6b95d05eeb73d1accd6 – [VirusTotal]
Frkmlkdkdubkznbkmcf.dll 9ef7dbd3da51332a78eff19146d21c82957821e464e8133e9594a07d716d892d – [VirusTotal] [Decompiled Source]

YARA Rules

```
rule Whispergate_Stage_1 {
    meta:
      description = "Detects first stage payload from WhisperGate"
      author = "[email protected]"
      date = "2022-01-17"
      license = "Apache License 2.0"
      hash = "a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92"
    strings:
      $a = { 31 41 56 4E 4D 36 38 67 6A 36 50 47 50 46 63 4A 75 66 74 4B 41 54 61 34 57 4C
6E 7A 67 38 66 70 66 76 }
      $b = { 38 42 45 44 43 34 31 31 30 31 32 41 33 33 42 41 33 34 46 34 39 31 33 30 44 30
46 31 38 36 39 39 33 43 36 41 33 32 44 41 44 38 39 37 36 46 36 41 35 44 38 32 43 31 45 44
32 33 30 35 34 43 30 35 37 45 43 45 44 35 34 39 36 46 36 35 }
      $c = { 24 31 30 6B 20 76 69 61 20 62 69 74 63 6F 69 6E 20 77 61 6C 6C 65 74 }
      $d = { 74 6F 78 20 49 44 }
    condition:
      uint16(0) == 0x5A4D and all of them
}

rule Whispergate_Stage_2 {
    meta:
      description = "Detects second stage payload from WhisperGate"
      author = "[email protected]"
      date = "2022-01-17"
      license = "Apache License 2.0"
      hash = "dcbbae5a1c61dbbbb7dcd6dc5dd1eb1169f5329958d38b58c3fd9384081c9b78"
    strings:
      $a = { 6D 5F 49 6E 74 65 72 63 65 70 74 6F 72 }
      $b = { 6D 5F 62 31 36 65 37 33 65 30 64 61 61 63 34 62 34 33 62 36 35 36 36 39 30 31
62 35 34 32 34 63 35 33 }
      $c = { 6D 5F 34 33 37 37 33 32 63 65 65 35 66 35 34 64 37 64 38 34 61 64 64 37 62 64
33 30 39 37 64 33 63 61 }
      $d = { 6D 5F 30 64 62 39 37 30 38 63 66 36 34 39 34 30 38 32 39 66 39 61 66 38 37 65
64 65 65 64 66 36 30 65 }
      $e = { 6D 5F 65 31 34 33 33 31 36 38 32 30 62 31 34 64 30 33 38 38 61 37 32 37 34 34
33 38 65 63 30 37 38 64 }
      $f = { 6D 5F 66 33 31 30 39 30 63 37 31 35 64 65 34 62 30 62 61 62 64 33 31 61 36 33
34 31 31 30 34 36 63 38 }
      $g = { 6D 5F 36 31 31 64 31 61 62 63 33 32 66 63 34 66 64 38 61 33 34 65 30 34 34 66
39 37 33 34 34 31 64 61 }
      $h = { 6D 5F 37 37 34 62 39 32 31 30 64 39 38 31 34 32 65 62 62 34 34 31 33 35 35 39
64 61 61 65 35 61 34 34 }
    condition:
      uint16(0) == 0x5A4D and all of them
}
```

About Cado Security

Cado Security provides *the* cloud investigation platform that empowers security teams to respond to threats at cloud speed. By automating data capture and processing across cloud and container environments, Cado Response effortlessly delivers forensic-level detail and unprecedented context to simplify cloud investigation and response. Backed by Blossom Capital and Ten Eleven Ventures, Cado Security has offices in the United States and United Kingdom. For more information, please visit https://www.cadosecurity.com/ or follow us on Twitter @cadosecurity.

Prev Post Next Post