Crackonosh - The Hidden Crypto Mining Malware

blog.minerva-labs.com/crackonosh-the-hidden-crypto-mining-malware

Minerva Labs Blog

News & Reports

- Tweet
-

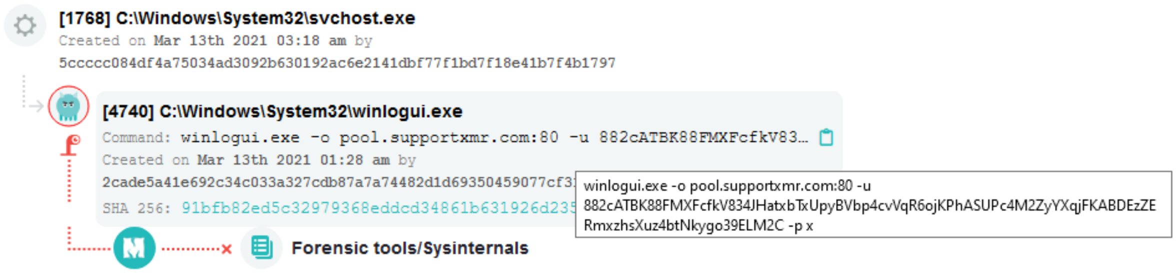
An article by Avast has introduced a novel malware by the name Crackonosh. This computer virus spreads through cracked software, specifically through illicit video game copies. The malware's main purpose is Monero crypto mining, which is quite a conspicuous activity that should be detected by security products. With that in mind, the malware's authors have incorporated multiple evasion techniques into the malware. Despite its blatant behavior, Crackonosh has not received much cover from security vendors, and its developers have managed to mine approximately 2 million dollars' worth of cryptocurrency.

As described by Avast, upon installation the malware disables security products such as Windows Defender. It will even replace Defender's executable with a custom binary that will place the Windows security icon inside the system tray. Another method the malware uses to evade detection is a registry key check for VMware and VirtualBox keys. This is done in multiple stages of the attack, to avoid execution of each of the malicious payloads inside a sandbox. Finally, the actual crypto-jacking binary will verify that no analysis process resides in memory and will not execute if one is found.

When searching for IOCs of this threat in our telemetry, we found an infection that was thwarted by our product in March of this year. After examining the files involved in this breach, we can confirm they are indeed a part of this highly profitable operation. We even found a version of the file winscomrssrv.dll that was not present in the IOC section of the original Avast article, but contained the exact same functionality as the binary described there.

Crackonosh's main agenda is evasiveness and that is why it has successfully stayed hidden since 2018. For the cyber security industry to tackle these events in real time, a change in paradigm is needed. Moving the pressure into the malware developer's territory is exactly what Minerva Labs Hostile Environment Simulation does. By simulating a sandbox environment for each process on the system we prevent live infections from detonating in corporate endpoints.

Crackonosh's miner prevented:

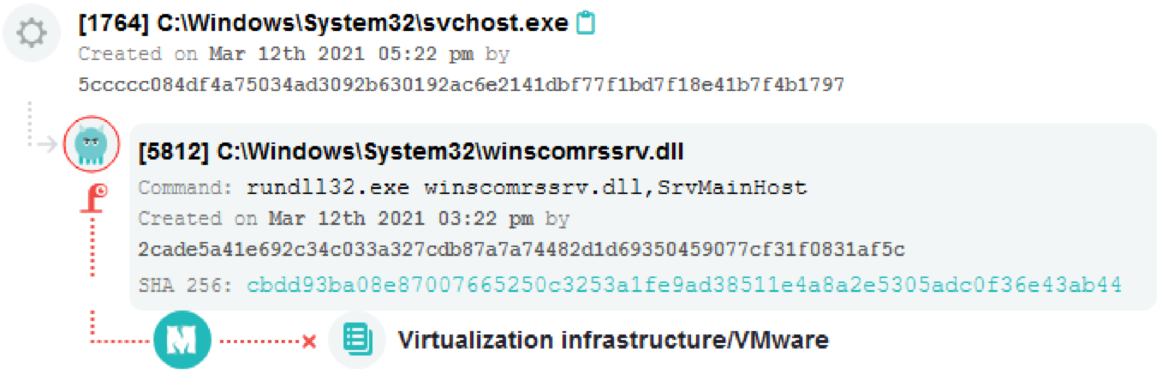


```
[1768] C:\Windows\System32\svchost.exe
Created on Mar 13th 2021 03:18 am by
5ccccc084df4a75034ad3092b630192ac6e2141dbf77f1bd7f18e41b7f4b1797

[4740] C:\Windows\System32\winlogui.exe
Command: winlogui.exe -o pool.supportxmr.com:80 -u 882cATBK88FMXFcfkV83…
Created on Mar 13th 2021 01:28 am by
2cade5a41e692c34c033a327cdb87a7a74482d1d69350459077cf3
SHA 256: 91bfb82ed5c32979368eddcd34861b631926d235

winlogui.exe -o pool.supportxmr.com:80 -u
882cATBK88FMXFcfkV834JHatxbTxUpyBVbp4cvVqR6ojKPhASUPc4M2ZyYXqjFKABDEzZE
RmxzhsXuz4btNkygo39ELM2C -p x
```

winscomrssrv.dll querying for VMware registry keys, which are simulated by Minerva:



```
[1764] C:\Windows\System32\svchost.exe
Created on Mar 12th 2021 05:22 pm by
5ccccc084df4a75034ad3092b630192ac6e2141dbf77f1bd7f18e41b7f4b1797

[5812] C:\Windows\System32\winscomrssrv.dll
Command: rundll32.exe winscomrssrv.dll,SrvMainHost
Created on Mar 12th 2021 03:22 pm by
2cade5a41e692c34c033a327cdb87a7a74482d1d69350459077cf31f0831af5c
SHA 256: cbdd93ba08e87007665250c3253a1fe9ad38511e4a8a2e5305adc0f36e43ab44
```

IOCs:

cbdd93ba08e87007665250c3253a1fe9ad38511e4a8a2e5305adc0f36e43ab44 (winscomrssrv.dll)

8f8c635949fd4a315dc7c2d30fc9a6a18149621e72b9598abf50d54a4bf116ac

(StartupCheckLibrary.dll)

91bfb82ed5c32979368eddcd34861b631926d2352d16adf189944c4ba8ccf4e1

(winlogui.exe)

5b85ceb558baaded794e4db8b8279e2ac42405896b143a63f8a334e6c6bba3fb
(winrmsrv.exe)

« Previous Post
Next Post »

Interested in Minerva? Request a Demo Below