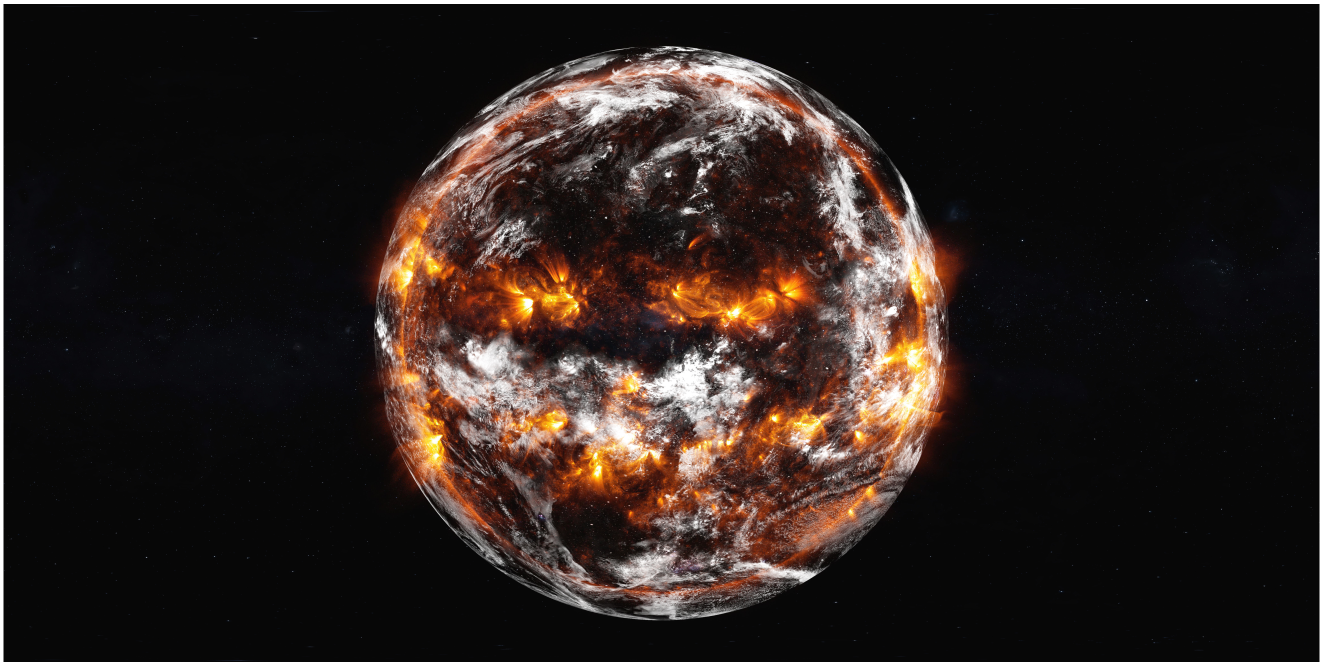
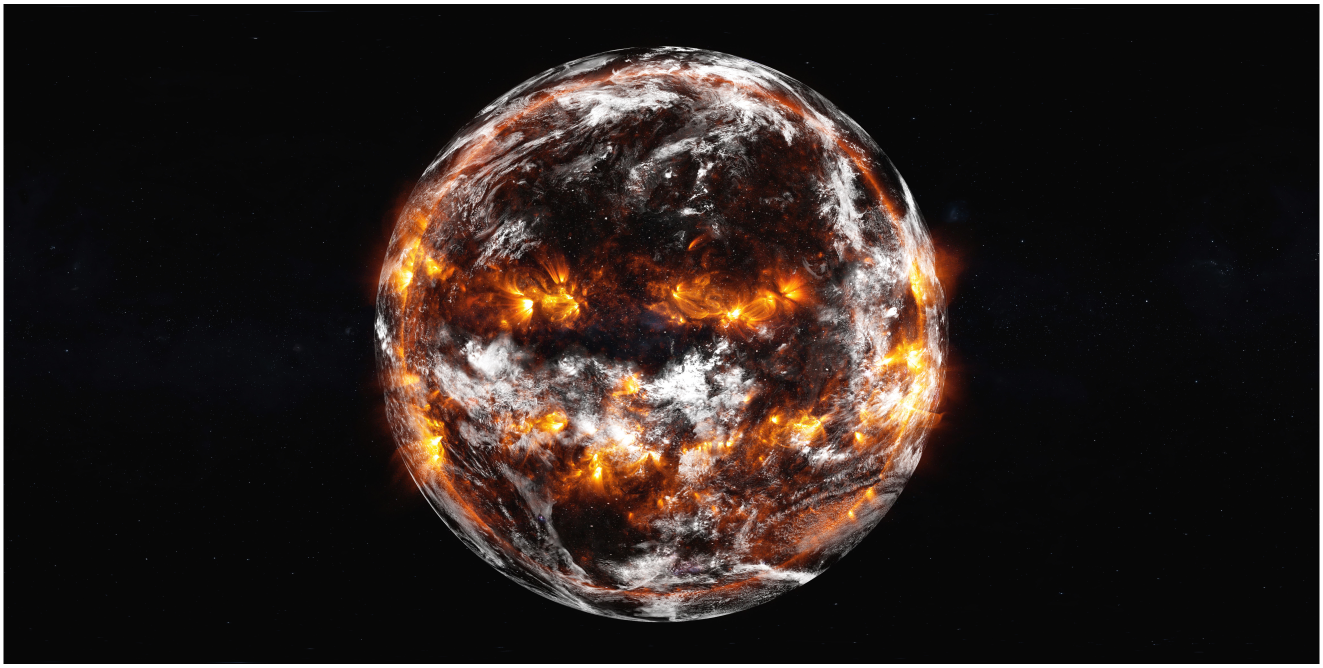
Thwarting Jupyter Stealer

blog.minerva-labs.com/new-iocs-of-jupyter-stealer





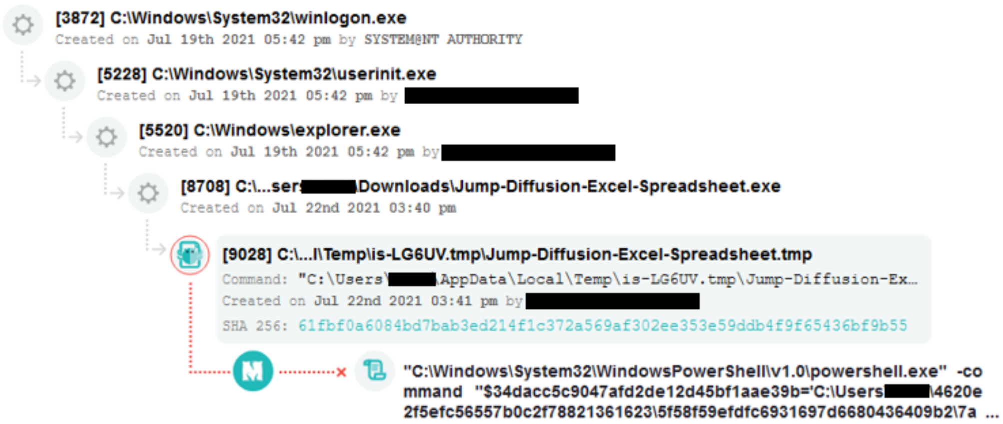
- Tweet
-

Jupyter Stealer is an evolving info stealer that is commonly spread using backdoored installations. We have recently encountered a new and improved version of this malware, which allows its operator to upload and execute new payloads to infected devices.

The sample we analyzed came bundled with YTD Video Downloader & Video Converter, which is a popular software for downloading music and videos from the web. This installation orchestrates the whole infection process by dropping an encrypted PowerShell script that will be decrypted and executed by a hidden PowerShell process. Once decrypted, the script is responsible for setting up persistence, using the algorithm described here.

Our variant connects to its C&C server and sends back the computer information (in an encrypted form). It does not include the credentials stealing functionality hardcoded anymore, instead, it gets **all** functional modules from the C&C server. One of the malware's capabilities, is to upload and execute .exe and .ps1 files to the victim’s machine. This leaves an attacker with the ability not only to execute different types of attacks, but also to steal any information from the victim’s computer.

Minerva Labs prevents Jupyter malware with our Living-off-the-Land Prevention technology, which interferes with attempts to misuse tools built into the system with the intention of causing damage. This module prevents threats from “trampolining” off such tools to infect the endpoint or cause damage.



```
[3872] C:\Windows\System32\winlogon.exe
Created on Jul 19th 2021 05:42 pm by SYSTEM@NT AUTHORITY
  [5228] C:\Windows\System32\userinit.exe
  Created on Jul 19th 2021 05:42 pm by [redacted]
    [5520] C:\Windows\explorer.exe
    Created on Jul 19th 2021 05:42 pm by [redacted]
      [8708] C:\...ser[redacted]Downloads\Jump-Diffusion-Excel-Spreadsheet.exe
      Created on Jul 22nd 2021 03:40 pm
        [9028] C:\...l\Temp\is-LG6UV.tmp\Jump-Diffusion-Excel-Spreadsheet.tmp
        Command: "C:\Users\[redacted]AppData\Local\Temp\is-LG6UV.tmp\Jump-Diffusion-Ex…
        Created on Jul 22nd 2021 03:41 pm by [redacted]
        SHA 256: 61fbf0a6084bd7bab3ed214f1c372a569af302ee353e59ddb4f9f65436bf9b55
          "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -co
          mmand "$34dacc5c9047afd2de12d45bf1aae39b='C:\Users[redacted]\4620e
          2f5efc56557b0c2f78821361623\5f58f59efdfc6931697d6680436409b2\7a ...
```

IOC’s:

Hash:

C5C5B2D3F6E37851DEE79B1B2B19AA7D

DNS:

http://185.244.213[.]64

http://37.120.247[.]125

« Previous Post
Next Post »

Interested in Minerva? Request a Demo Below