# Become A VIP Victim With New Discord Distributed Malware

blog.minerva-labs.com/become-a-vip-victim-with-new-discord-distributed-malware

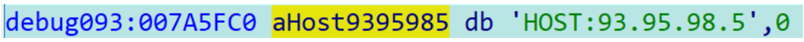
- Tweet
-

Threat actors are always looking for a way to avoid detection, and one of the most popular techniques is to use legitimate services to mask malicious network activity. A recent trend is to abuse Discord (the game-centric text and voice chat platform) as a payload distribution platform.

A new malware (named “VIPSpace.exe” in the wild) will recklessly install up to 25 different malware on a victim PC, effectively destroying infected devices.

As a first stage, the malware is dropped by a self-extracting archive that drops and executes the next module, VIPSpace.exe.  The secondary payload accesses Discord’s servers, downloads a BMP (bitmap) file, and saves it with a DLL extension. As it turns out, the downloaded BMP file is actually an encrypted executable that will be decrypted in the memory and reflectively loaded.

The DLL accesses http://37.0.11[.]8/server.txt to get the IP address of a C&C server.



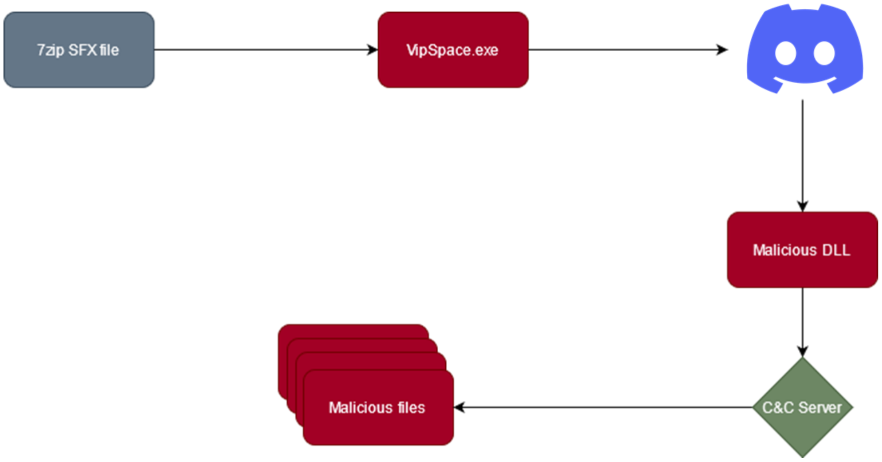
```
debug093:007A5FC0 aHost9395985 db 'HOST:93.95.98.5',0
```

After a successful connection to the C&C server, the in-memory module disables Windows Defender by creating the following registry keys:

- Windows Defender AV - HKLM\SOFTWARE\Policies\Microsoft\WindowsDefender\DisableAntiSpyware
- Automatic Remediation - HKLM\SOFTWARE\Policies\Microsoft\WindowsDefender\DisableRoutinelyTakingAction

- Behavior Monitoring - HKLM\SOFTWARE\Policies\Microsoft\WindowsDefender\Real-TimeProtection\DisableBehaviorMonitoring
- Active Monitoring - HKLM\SOFTWARE\Policies\Microsoft\WindowsDefender\Real-TimeProtection\DisableOnAccessProtection
- Process Scanning - HKLM\SOFTWARE\Policies\Microsoft\WindowsDefender\Real-TimeProtection\DisableScanOnRealtimeEnable
- Real Time Protection - HKLM\SOFTWARE\Policies\Microsoft\WindowsDefender\Real-TimeProtection\DisableRealtimeMonitoring
- Downloaded Files and Attachments Scan- HKLM\SOFTWARE\Policies\Microsoft\WindowsDefender\Real-TimeProtection\DisableIOAVProtection
- Raw Volume Write Notifications - HKLM\SOFTWARE\Policies\Microsoft\WindowsDefender\Real-TimeProtection\DisableRawWriteNotification

The malicious DLL will then access the C&C server to fetch an encrypted list of URLs. After decryption, it becomes clear that each URL stores a different malware that will be downloaded and executed later. The malware's authors have implemented a multithreaded downloading algorithm in order to speed up the infection process.



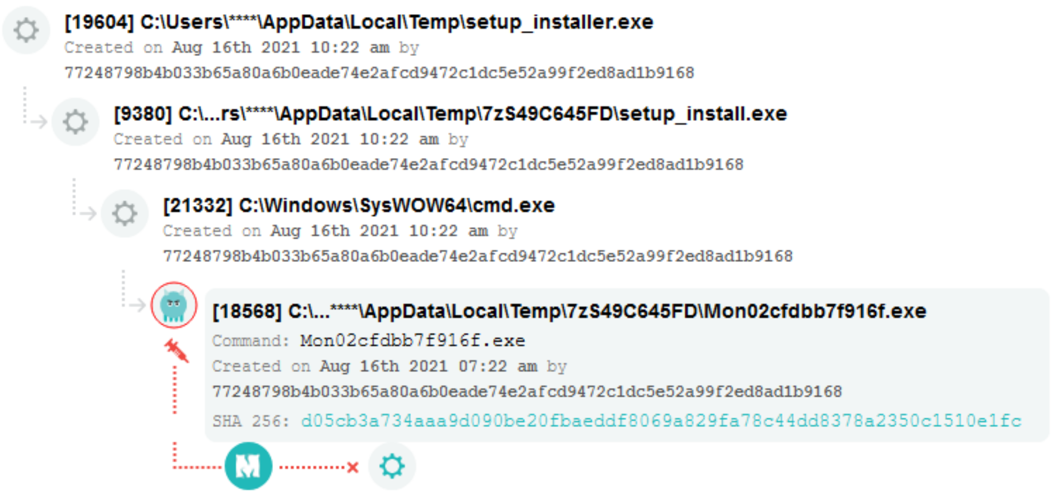
After investigating the multiple files dropped by this malware, most turned out to be benign or open-source malware, such as Redline Stealer. However, each download will still drop a uniquely generated sample. When analyzing this sample, we could not help but notice that this malware is written by an amateur, evident by the following:

- The download of a significant number of malware to PC will most likely lead to a system crash that will not serve the supposed purpose of the threat actor.
- A download of the different variants of the same malware (four variants of RedLine, two variants of BlackNet RAT) seems redundant.
- Dropping an encrypted DLL file with a DLL extension opens up a detection opportunity.
- No significant evasion techniques were implemented in the malware.

Even though this malware lacks sophistication, we cannot honestly know what threat actors will plan in future attacks. Services such as Discord allow hackers to execute an array of malware types during the second stage of the attack (i.e. when a BMP file is downloaded from Discord).  Such malware exploits the vulnerabilities of the world's generally reactive approach to cyber-security.

Request a Meeting

As seen in the image below, Minerva's pre-emptive approach stops the attack before the malicious payload is downloaded from Discord. Our unique patented technology stops the attack at the initial stage, which is critical for preventing any further damage down the line.



```
[19604] C:\Users\****\AppData\Local\Temp\setup_installer.exe
Created on Aug 16th 2021 10:22 am by
77248798b4b033b65a80a6b0eade74e2afcd9472c1dc5e52a99f2ed8ad1b9168

  [9380] C:\...rs\****\AppData\Local\Temp\7zS49C645FD\setup_install.exe
  Created on Aug 16th 2021 10:22 am by
  77248798b4b033b65a80a6b0eade74e2afcd9472c1dc5e52a99f2ed8ad1b9168

    [21332] C:\Windows\SysWOW64\cmd.exe
    Created on Aug 16th 2021 10:22 am by
    77248798b4b033b65a80a6b0eade74e2afcd9472c1dc5e52a99f2ed8ad1b9168

      [18568] C:\...****\AppData\Local\Temp\7zS49C645FD\Mon02cfdbb7f916f.exe
      Command: Mon02cfdbb7f916f.exe
      Created on Aug 16th 2021 07:22 am by
      77248798b4b033b65a80a6b0eade74e2afcd9472c1dc5e52a99f2ed8ad1b9168
      SHA 256: d05cb3a734aaa9d090be20fbaeddf8069a829fa78c44dd8378a2350c1510e1fc
```

## IOCs:

### Domains:

- https://cdn.discordapp[.]com/attachments/873056123240972371/875681686568992788/E_PL_Client.bmp
- http://93.95.98[.]5/base/api/getData.php
- http://37.0.10[.]214/EXT/minepass_settings.png
- http://37.0.10[.]214/WW/file1.exe
- http://37.0.10[.]214/WW/file5.exe
- http://37.0.10[.]214/WW/file4.exe
- http://37.0.10[.]214/WW/file8.exe
- http://37.0.10[.]214/WW/file7.exe
- http://37.0.10[.]214/WW/file2.exe
- http://37.0.10[.]214/WW/file3.exe
- https://fsstoragecloudservice[.]com/campaign1/autosubplayer.exe - check all the https
- https://cdn.discordapp[.]com/attachments/879422002287493133/879653243217670164/app24.bmp
- https://cdn.discordapp[.]com/attachments/879422002287493133/879423887002206228/Passat.bmp
- https://cdn.discordapp[.]com/attachments/879422002287493133/879423620030550088/Real231.bmp
- https://a.goatagame[.]com/userf/2201/snakehi.exe
- http://37.0.10[.]214/WW/fileT.exe
- http://37.0.10[.]214/WW/PB14s.exe
- http://hockeybruinsteamshop[.]com/pub1.exe
- https://cdn.discordapp[.]com/attachments/879433223103459409/879433370159968306/Setup2.exe
- https://cdn.discordapp[.]com/attachments/879422002287493133/879653242093600808/sfx_123_201.bmp
- https://cdn.discordapp[.]com/attachments/879422002287493133/879685414934417479/R24.bmp
- https://cdn.discordapp[.]com/attachments/879422002287493133/879653239560228884/help24.bmp
- https://cdn.discordapp[.]com/attachments/879422002287493133/879653236993318933/Falioca24.bmp
- https://cdn.discordapp[.]com/attachments/870454586861846551/870548989903274054/jooyu.exe
- https://2no[.]co/2GSVH6
- http://privacytoolz123foryou[.]xyz/downloads/toolspab2.exe
- https://cdn.discordapp[.]com/attachments/879422002287493133/879423245999276102/VerminateMechanize_2021-08-18_15-57.bmp
- https://7e10a716-f462-4371-a152-105d67ce51a8.s3.ap-south-1.amazonaws[.]com/offer/GameBox.exe

### Hashes:

- d05cb3a734aaa9d090be20fbaeddf8069a829fa78c44dd8378a2350c1510e1fc (VipSpace.exe)
- DDE32911345A4C9D54355C6D57A72C5177D2A46CB0C507121E3709CADFCC9B44 (minepass_settings.png)
- B483FE7D29CE8EEDCB3E1EC061E0F45BC44D0B48E4F21EAAF67A063388314FF7 (file1.exe)

- 8B57CD06470E93ABF9EA61E86839A3F7EB3B13FBB37C5FEC34888652A65185C3 (file5.exe)
- F4EC629473FBE96FA82FE1C1E30E6784144163D662E1C977ACF5BC1D62B20C0B (file4.exe)
- E1CBEBC0C9A675CA172E7DE1908991F7B0BD0866C1BEA9404AE10BC201DE0FE6 (file7.exe)
- CB54B6471597A9417BCC042D0F0D6404518B647BD3757035A01E9DE6AA109490 (file2.exe)
- 9460FFE580332FE64BB4F35BB63DC6A4302F3613718A04DC0986CEA989160039 (file3.exe)
- EEC05DC9ADE2A7EE74EA5FB115BDD687B457D1F81841238A61E9775D6CC4BFA6 (fileT.exe)
- B9025AEF29F9F9D3126D390E66DF8C55A9C9F7C15520F9A59A963932EE86B815 (PB14s.exe)
- 57381B4DE751F07C4537E2BECBB0F5C93A23897AA1BF1F0274E05F3FF4FD62F5 (toolspab2.exe)
- DBD9CFA3D9B4E482EE79E7726E95168A5E27BB0482A0E4744A1E1C56D75F1C32 (ebook.exe)
- 6D4B28002FC36B27DFDCA0FBD886C73704950EE88B14B805512A938F423D7E1C (autosubplayer.exe)
- 98C781B3FD15D6C7C7624AA1A0C93910DD5D19722A1D9B8CB1C7B9673D311090 (app24.bmp)
- DAB2A18DF66F2E74D0831A8B118DE6B9DF2642AC939CBAD0552E30696D644193 (Passat.bmp)
- 3593247C384586966E5A0E28EB4C4174B31E93C78C7A9E8FEF96EC42A152E509 (Real231.bmp)
- CA46080E121408D9624322E505DC2178BA99E15871C90E101B54E42EA7B54A96 (snakehi.exe)
- 57FB96B12DB08B18906CE22C7E55B81A214EDE326166E772AE87412281044497 (pub1.exe)
- 01550EE84AC5A220197177182FD2F3F9C9E845B416D06A384384E3CD62ECB569 (Setup2.exe)
- 4B95FF6312411ED2EEC0DC2FDB251D985B6E9892E1B2F61AADB94DEA1B3EEB13 (sfx_123_201.bmp)
- 1583FCEEAE47160FD37427A55F1D2122F3654E528E29C55D64DF145122515A55 (R24.bmp)
- 15AD913C094CD58FFFA2067D86B75CF08FBCAC95C16C2D68BAB5B3498F059E31 (help24.bmp)
- 963989F4B4D6E2D7C2281992AE5D62966726E81B5070B792399C7FD2017CA5CA (Falioca24.bmp)
- 8CFA7E9BC6CBD458CEC18A25E6F763A3776802490E6B3D451D864C4DBA50C437 (VerminateMechanize_2021-08-18_15-57.bmp)
- 857DD46102AEA53F0CB7934B96410EBBC3E7988D38DCAFDC8C0988F436533B98 (GameBox.exe)

Resources:

https://news.sophos.com/en-us/2021/07/22/malware-increasingly-targets-discord-for-abuse/

Talk To Minerva Labs