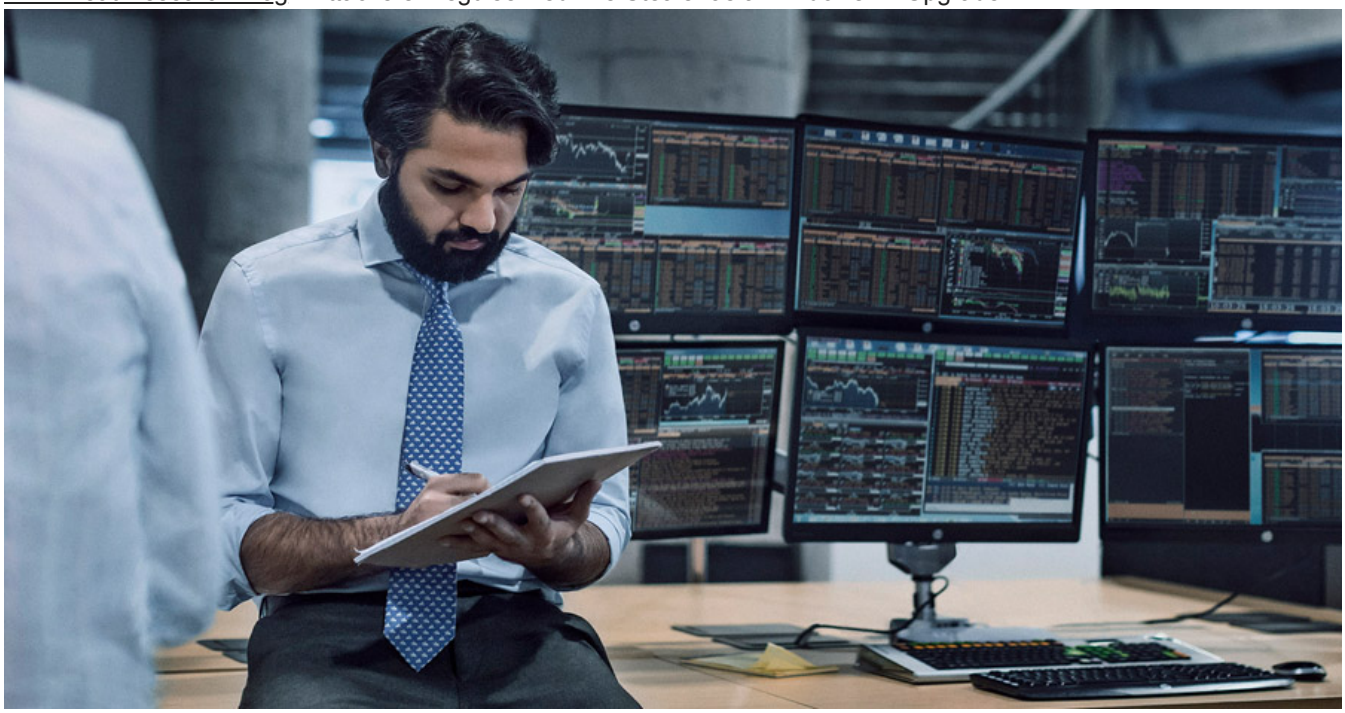
Recent Posts

threatresearch.ext.hp.com/redline-stealer-disguised-as-a-windows-11-upgrade/

February 8, 2022

HP Threat Research Blog • Attackers Disguise RedLine Stealer as a Windows 11 Upgrade



Attackers Disguise RedLine Stealer as a Windows 11 Upgrade

Threat actors are always looking for topical lures to socially engineer victims into infecting systems. We recently analyzed one such lure, namely a fake Windows 11 installer. On 27 January 2022, the day after the final phase of the Windows 11 upgrade was announced, we noticed a malicious actor registered the domain *windows-upgraded[.]com*, which they used to spread malware by tricking users into downloading and running a fake installer. The domain caught our attention because it was newly registered, imitated a legitimate brand and took advantage of a recent announcment. The threat actor used this domain to distribute RedLine Stealer, an information stealing malware family that is widely advertised for sale within underground forums.

```
Domain Name: windows-upgraded.com
Creation Date: 2022-01-27T10:06:46Z
Registrar: NICENIC INTERNATIONAL GROUP CO., LIMITED
Registrant Organization: Ozil Verfig
Registrant State/Province: Moscow
Registrant Country: RU
```

The attackers copied the design of the legitimate Windows 11 website, except clicking on the “Download Now” button downloads a suspicious zip archive called *Windows11InstallationAssistant.zip*. The file was hosted on Discord’s content delivery network.

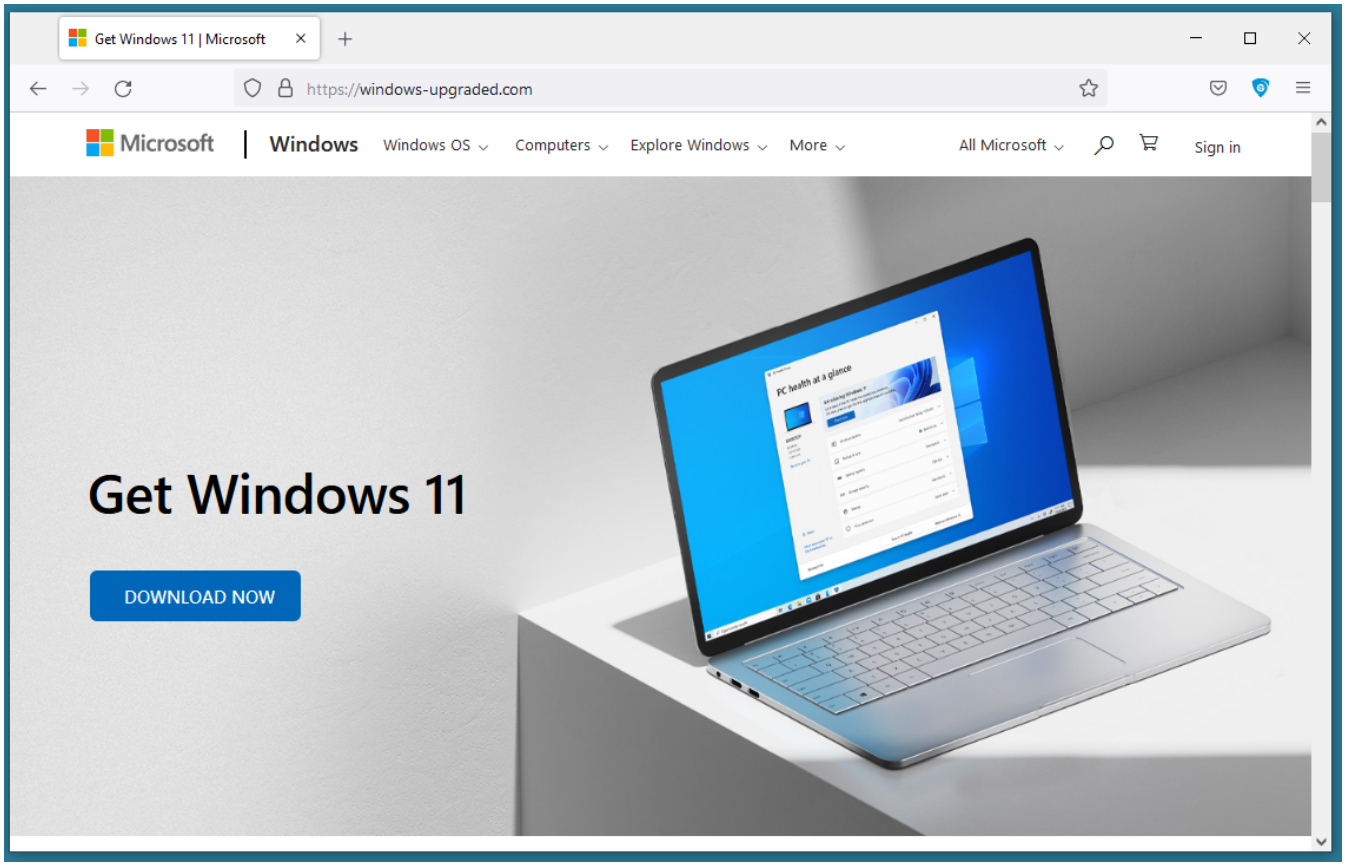


Figure 1 – Fake Windows 11 website hosted on windows-upgraded[.]com.

File Analysis

Windows11InstallationAssistant.zip is only 1.5 MB and contains six Windows DLLs, an XML file and a portable executable.

```
Windows11InstallationAssistant/
Windows11InstallationAssistant/AdditionalFile/
Windows11InstallationAssistant/AdditionalFile/ReAgent.xml
Windows11InstallationAssistant/DLL/
Windows11InstallationAssistant/DLL/AppxProvider.dll
Windows11InstallationAssistant/DLL/AssocProvider.dll
Windows11InstallationAssistant/DLL/CbsProvider.dll
Windows11InstallationAssistant/DLL/CompatProvider.dll
Windows11InstallationAssistant/DLL/DismCore.dll
Windows11InstallationAssistant/DLL/DismCorePS.dll
Windows11InstallationAssistant/Windows11InstallationAssistant.exe
```

Figure 2 – Zip archive contents.

After decompressing the archive, we get a folder with a total size of 753 MB. The executable *Windows11InstallationAssistant.exe* was the largest file at 751 MB.

```
4.0K    ./AdditionalFile
2.0M    ./DLL
751M    ./Windows11InstallationAssistant.exe
```

Figure 3 – File sizes after decompression.

Since the compressed size of the zip file was only 1.5 MB, this means it has an impressive compression ratio of 99.8%. This is far larger than the average zip compression ratio for executables of 47%. To achieve such a high compression ratio, the executable likely contains padding that is extremely compressible. Viewed in a hex editor, this padding is easily spotted (Figure 4).

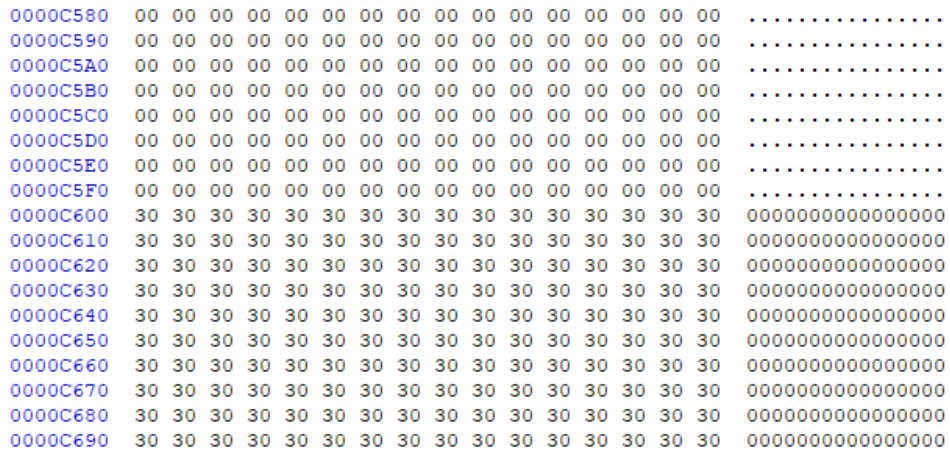


Figure 4 – 0x30 filler area inside *Windows11InstallationAssistant.exe*.

A large part of the file is padded with 0x30 bytes and is irrelevant to run the file. Since many sandboxes and other malware analysis tools are unable to process very large files, we must either analyze the file manually or shrink it to a reasonable size. The large filler area is located at the end of the file just before the file signature. Due to a digest mismatch, the signature verification results in an error, which is why we did not include it further in the analysis. By truncating the filler area as well as the signature, we obtain a valid portable executable. One reason why the attackers might have inserted such a filler area, making the file very large, is that files of this size might not be scanned by an anti-virus and other scanning controls, thereby increasing the chances the file can execute unhindered and install the malware. Figure 5 shows the sections of the executable after removing the padding.

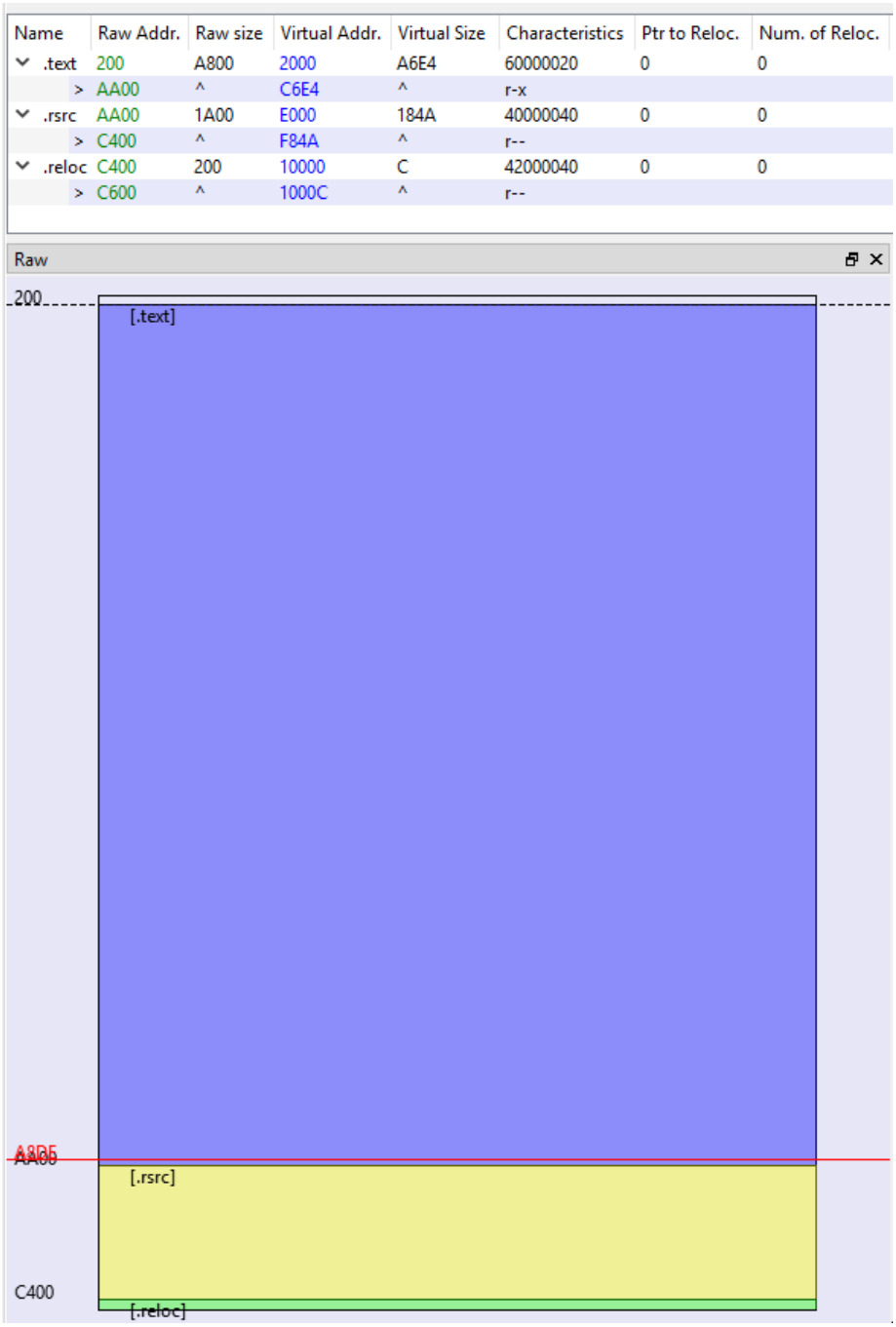


Figure 5 – File sections of *Windows11InstallationAssistant.exe* (padding removed) viewed in PE-bear.

Dynamic Analysis

We can now analyze this file dynamically in a sandbox or with static malware analysis tools. Immediately after execution, the malware starts a PowerShell process with an encoded argument. This causes a cmd.exe process to be launched with a timeout of 21 seconds. Once this timeout expires, the initial process downloads a file named *win11.jpg* from a remote web server (Figure 6).

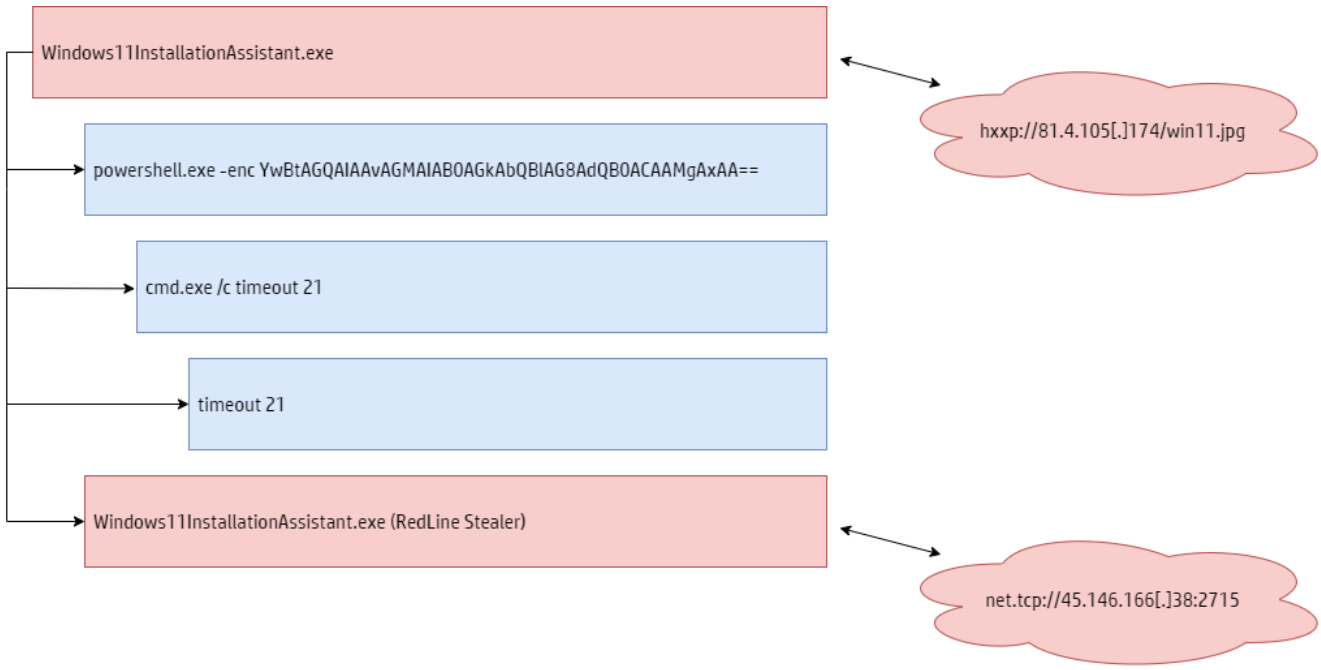


Figure 6 – Process execution leading to RedLine Stealer.

Running the *file* utility against *win11.jpg* fails to identify its file type, suggesting that it is encoded or encrypted. However, opening the file in a text editor revealed that the contents are simply stored in reverse order.

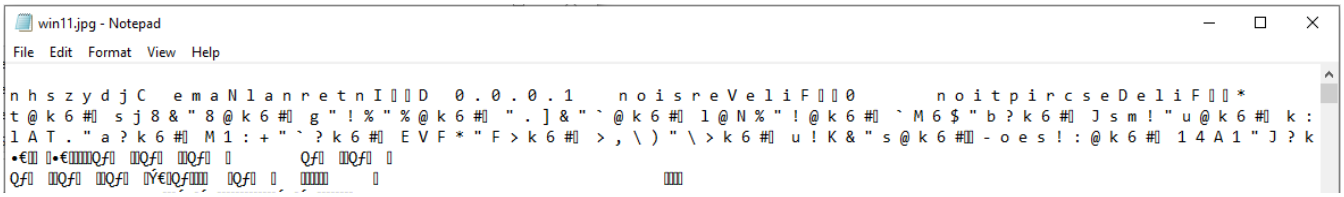


Figure 7 – Reversed DLL file viewed in a text editor.

Once the contents of the file are reversed, we get a dynamic link library (DLL). This DLL is loaded by the initial process, which executes itself again then replaces the current thread context with the downloaded DLL. This is the RedLine Stealer payload, a classic information stealer. It collects various information about the current execution environment, such as the username, computer name, installed software and hardware information. The malware also steals stored passwords from web browsers, auto-complete data such as credit card information, as well as cryptocurrency files and wallets. To exfiltrate information or receive further instructions, RedLine Stealer opens a TCP connection to a configured command and control (C2) server, in this case 45.146.166[.]38:2715.

Links to December 2021 RedLine Stealer Campaign

The tactics, techniques and procedures (TTPs) in this RedLine Stealer campaign are similar to a campaign we analyzed in December 2021. In that campaign, the malicious actor registered discrodappp[.]com, which they used to serve RedLine Stealer disguised as an installer for the popular messaging app. In both campaigns, the threat actor used fake websites mimicking popular software to trick users into installing their malware, registered the domains using the same domain registrar, used the same DNS servers, and delivered the same family of malware.

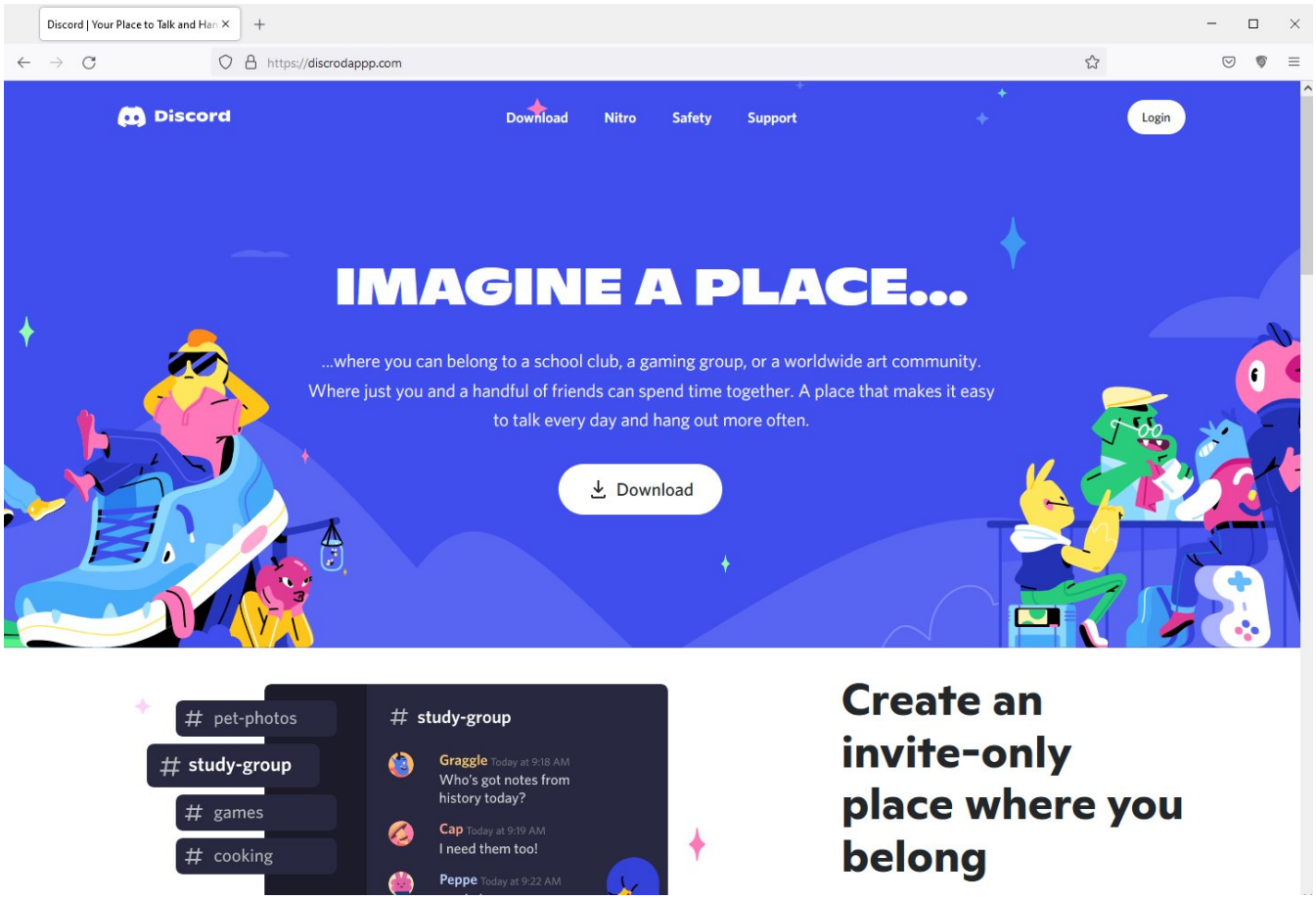


Figure 8 – Fake Discord website distributing RedLine Stealer, December 2021.

Conclusion

This campaign highlights once again how attackers are quick to take advantage of important, relevant and interesting current events to create effective lures. Prominent announcements and events are always interesting topics for threat actors, which can be exploited to spread malware. Since such campaigns often rely on users downloading software from the web as the initial infection vector, organizations can prevent such infections by only downloading software from trustworthy sources.

Indicators of Compromise

Files

Windows11InstallationAssistant.zip
4293d3f57543a41005be740db7c957d03af1a35c51515585773cedee03708e54

Windows11InstallationAssistant.exe
b50b392ccb07ed7a5da6d2f29a870f8e947ee36c43334c46c1a8bb21dac5992c

Windows11InstallationAssistant.exe – no filler area
7d5ed583d7efe318fdb397efc51fd0ca7c05fc2e297977efc190a5820b3ee316

win11.jpg
c7bcdc6aecd2f7922140af840ac9695b1d1a04124f1b3ab1450062169edd8e48

win11_reversed.dll
6b089a4f4fde031164f3467541e0183be91eee21478d1dfe4e95c4a0bb6a6578

Network connections

windows-upgraded[.]com

hxxps://cdn.discordapp[.]com/attachments/928009932928856097/936319550855716884/Windows11InstallationAssistant.zip

hxxp://81.4.105[.]174/win11.jpg

45.146.166[.]38:2715

Tags

redline stealer windows 11