Detecting malware infection campaign hidden in fake Windows 11 installer

International security researchers have just issued an urgent notice about a sophisticated malicious attack campaign targeting Windows users worldwide.

In it, malicious actors began mass distributing fake Windows 11 upgrade installations to Windows 10 users, tricking them into downloading and executing RedLine data-stealing software.

Notably, the time of the first attacks coincided with the time Microsoft announced the widespread deployment of Windows 11 globally. Therefore, it can be affirmed that the attackers have been well prepared, and are just waiting for the right time to conduct malicious activities to maximize the success of the campaign.

RedLine is basically one of the tools to steal passwords, browser cookies, credit card information and cryptocurrency wallets widely deployed by malicious actors around the world today. Due to its stable operation and effective stealth, after a successful infection, RedLine can have serious consequences for the victim.

RedLine distribution campaign through fake Windows 11 installer

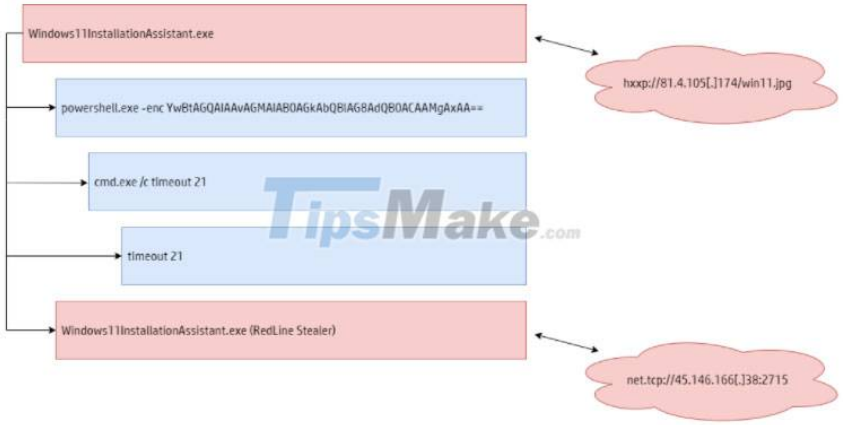
As revealed by researchers at HP, who first discovered the malicious campaign, the actors used the 'windows-upgraded.com' domain at first glance to appear legitimate to distribute malware. in this latest campaign.

Not only has a 'sensitive' domain name, this fake website also owns an interface designed exactly like Microsoft's 'original' website. If a visitor cannot spot the difference and accidentally clicks the 'Download Now' button, they will receive a 1.5 MB ZIP archive named 'Windows11InstallationAssistant.zip', downloaded directly from the Discord CDN.

Decompressing the file creates a folder of 753MB in size, showing an impressive compression ratio of 99.8%. When the victim launches the executable in the directory, the PowerShell process with the encrypted argument starts.

Next, a cmd.exe process will be launched with a timeout of 21 seconds and after it expires a .jpg file will be fetched from the remote web server. This image file contains a DLL file whose contents are arranged in reverse to avoid detection and analysis.

Finally, the original process loads the DLL and replaces the current thread context with it. This DLL is the payload of the RedLine malware, which connects to the hacker's command and control server (C2 server) via TCP. From there, the malicious code will receive specific instructions about the malicious tasks it must run next on the newly compromised system.



Although the site distributed above is now (temporarily) down, there is nothing to prevent the malicious actors from continuing to create a new domain name and restart this campaign. Windows 11 is a major upgrade that many Windows 10 users can't get from official distribution channels because it doesn't meet hardware compatibility requirements. This is a fact that malware operators see as a great opportunity to find new victims.

Earlier in January, there were also numerous reports of threat actors taking advantage of legitimate Windows update clients to execute malicious code on compromised systems. Keep in mind that these dangerous sites are often promoted through forum posts, social media or SMS messages, so don't trust anything other than the

official Windows upgrade system announcement. from Microsoft itself.