Fake Windows 11 upgrade installers infect you with RedLine malware

bleepingcomputer.com/news/security/fake-windows-11-upgrade-installers-infect-you-with-redline-malware/

Bill Toulas

By
Bill Toulas

- February 9, 2022
- 07:58 AM
- 3

Threat actors have started distributing fake Windows 11 upgrade installers to users of Windows 10, tricking them into downloading and executing RedLine stealer malware.

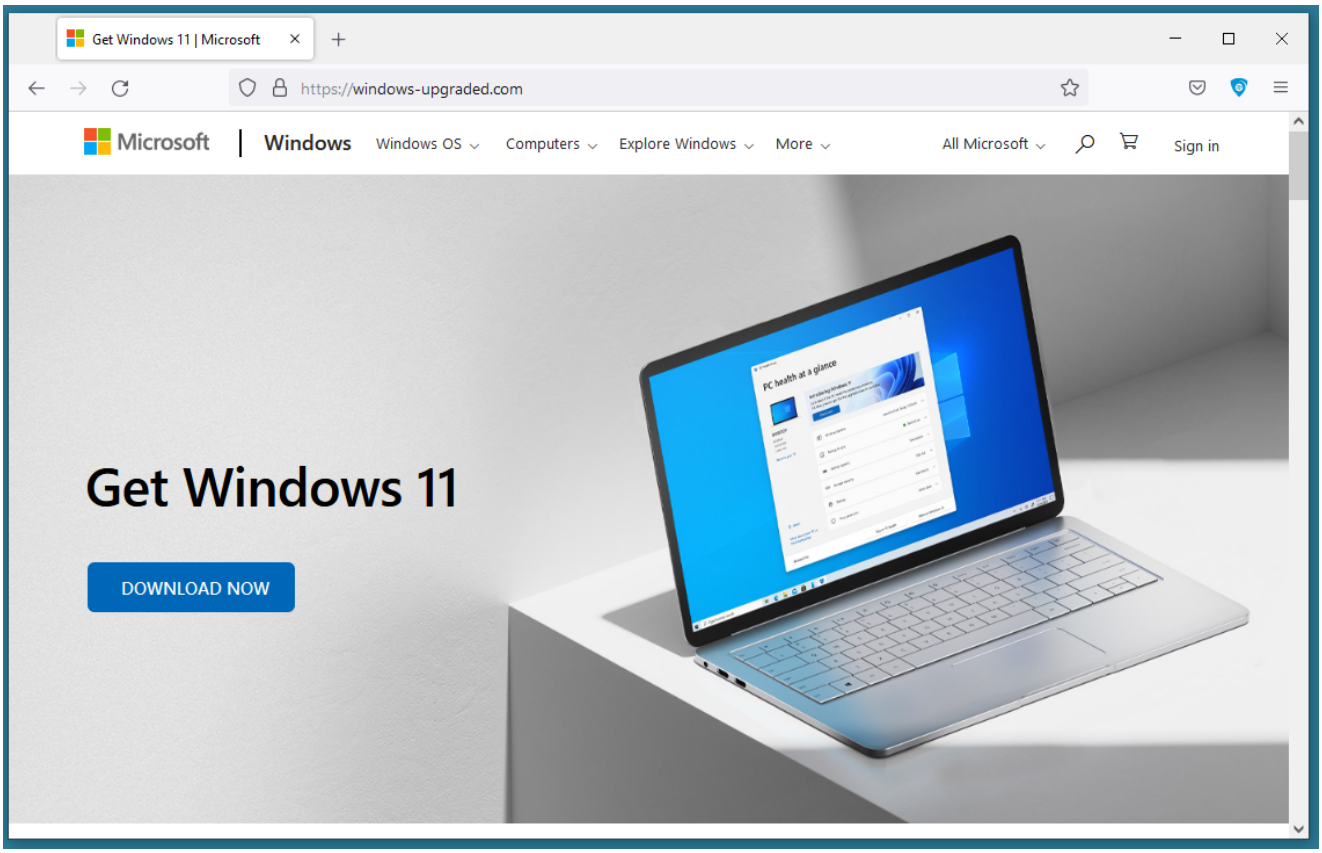
The timing of the attacks coincides with the moment that Microsoft announced Windows 11's broad deployment phase, so the attackers were well-prepared for this move and waited for the right moment to maximize their operation's success.

RedLine stealer is currently the most widely deployed password, browser cookies, credit card, and cryptocurrency wallet info grabber, so its infections can have dire consequences for the victims.

The campaign

According to researchers at HP, who have spotted this campaign, the actors used the seemingly legitimate “windows-upgraded.com” domain for the malware distribution part of their campaign.

The site appears like a genuine Microsoft site and, if the visitor clicked on the ‘Download Now’ button, they received a 1.5 MB ZIP archive named “Windows11InstallationAssistant.zip,” fetched directly from a Discord CDN.



Fake website used for malware distribution (HP)

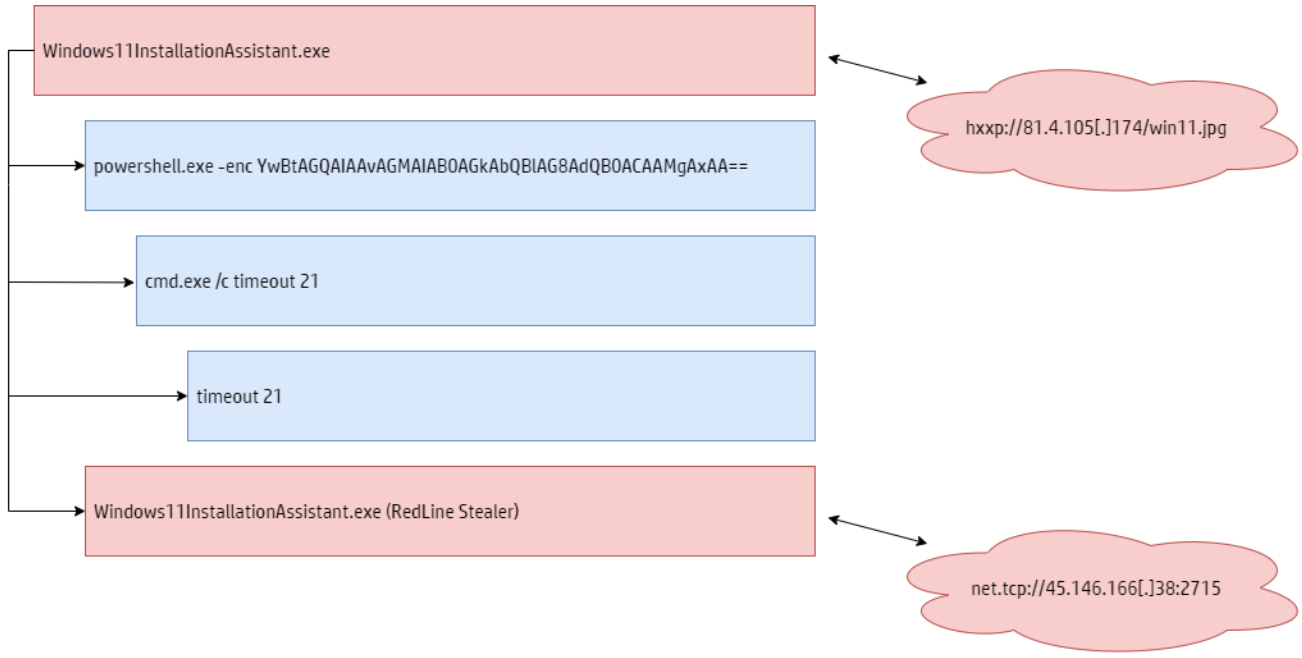
Decompressing the file results in a folder of 753MB of size, showcasing an impressive compression ratio of 99.8%, achieved thanks to the presence of padding in the executable.

When the victim launches the executable in the folder, a PowerShell process with an encoded argument starts.

Next, a cmd.exe process is launched with a timeout of 21 seconds, and after that expires, a .jpg file is fetched from a remote web server.

This file contains a DLL with contents arranged in reverse form, possibly to evade detection and analysis.

Finally, the initial process loads the DLL and replaces the current thread context with it. That DLL is a RedLine stealer payload that connects to the command-and-control server via TCP to get instructions on what malicious tasks it has to run next on the newly compromised system.



RedLine execution and loading chain (HP)

Outlook

Although the distribution site is down now, nothing stops the actors from setting up a new domain and restarting their campaign. In fact, this is very likely already happening in the wild.

Windows 11 is a major upgrade that many Windows 10 users cannot get from the official distribution channels due to hardware incompatibilities, something that malware operators see as an excellent opportunity for finding new victims.

As BleepingComputer reported in January, threat actors are also leveraging Windows' legitimate update clients to execute malicious code on compromised Windows systems, so the tactics reported by HP are hardly surprising at this point.

Remember, these dangerous sites are promoted via forum and social media posts or instant messages, so don't trust anything but the official Windows upgrade system alerts.

Related Articles:

Microsoft adds Office subscriptions to Windows 11 account settings

Sophos antivirus driver caused BSODs after Windows KB5013943 update

Windows admins frustrated by Quick Assist moving to Microsoft Store

Microsoft: Sysrv botnet targets Windows, Linux servers with new exploits

New cryptomining malware builds an army of Windows, Linux bots

Bill Toulas

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.