# Unofficial Windows 11 upgrade installs info-stealing malware

bleepingcomputer.com/news/security/unofficial-windows-11-upgrade-installs-info-stealing-malware/

Bill Toulas


By
Bill Toulas

- April 18, 2022
- 01:18 PM
- 0

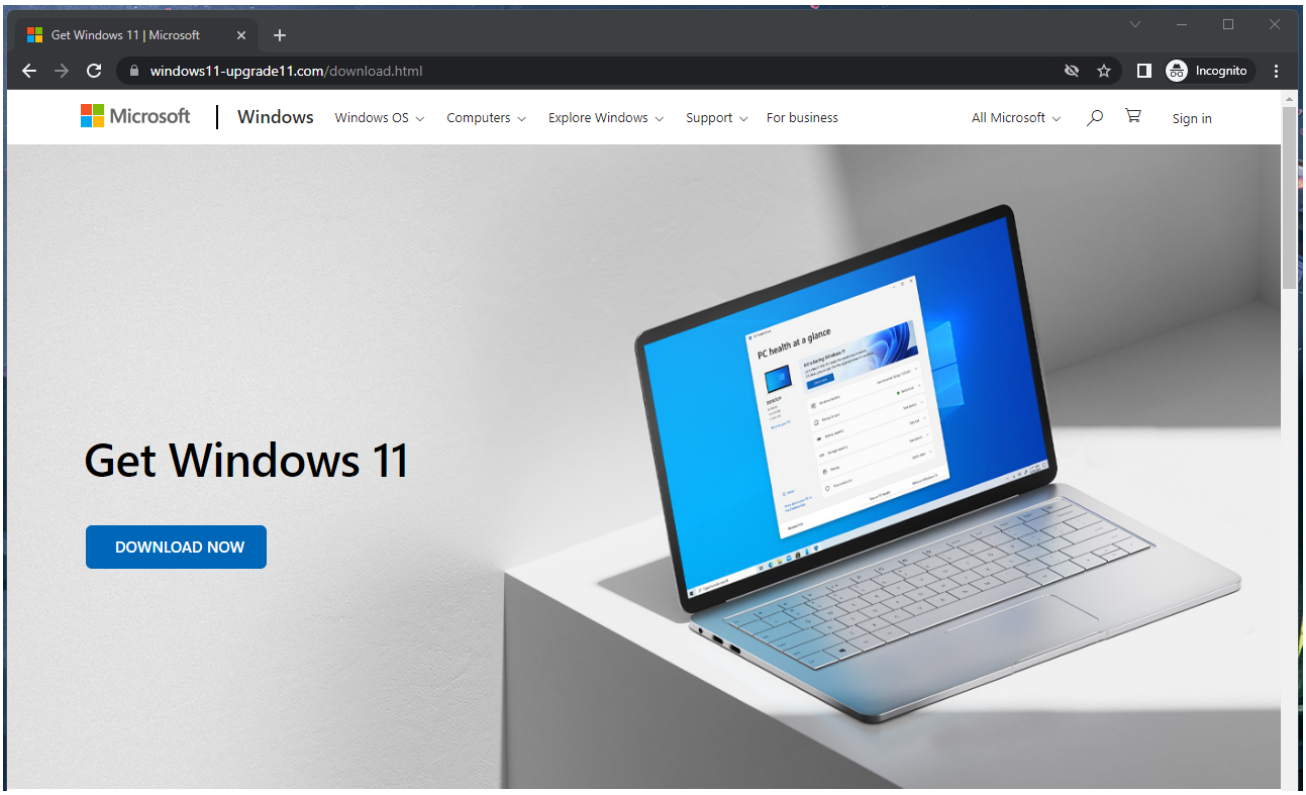

Hackers are luring unsuspecting users with a fake Windows 11 upgrade that comes with malware that steals browser data and cryptocurrency wallets.

The campaign is currently active and relies on poisoning search results to push a website mimicking Microsoft's promotional page for Windows 11, to offer the information stealer.

Microsoft offers an upgrade tool for users to check if their machine supports the latest operating system (OS) from the company. One requirement is support for Trusted Platform Module (TPM) version 2.0, which is present on machines that not older than four years.

The hackers are preying on users that jump at installing Windows 11 without spending the time to learn that the OS needs to meet certain specifications.

The malicious website offering the fake Windows 11 is still up at the time of writing. It features the official Microsoft logos, favicons, and an inviting “Download Now” button.




**Malicious website used in the campaign (windows11-upgrade11[.]com)**

If the visitor loads the malicious website via direct connection - download is unavailable over TOR or VPN, they will get an ISO file that shelters the executable for a novel info-stealing malware.

Threat researchers at CloudSEK have analyzed the malware and shared a technical report exclusively with BleepingComputer.

## Infection process

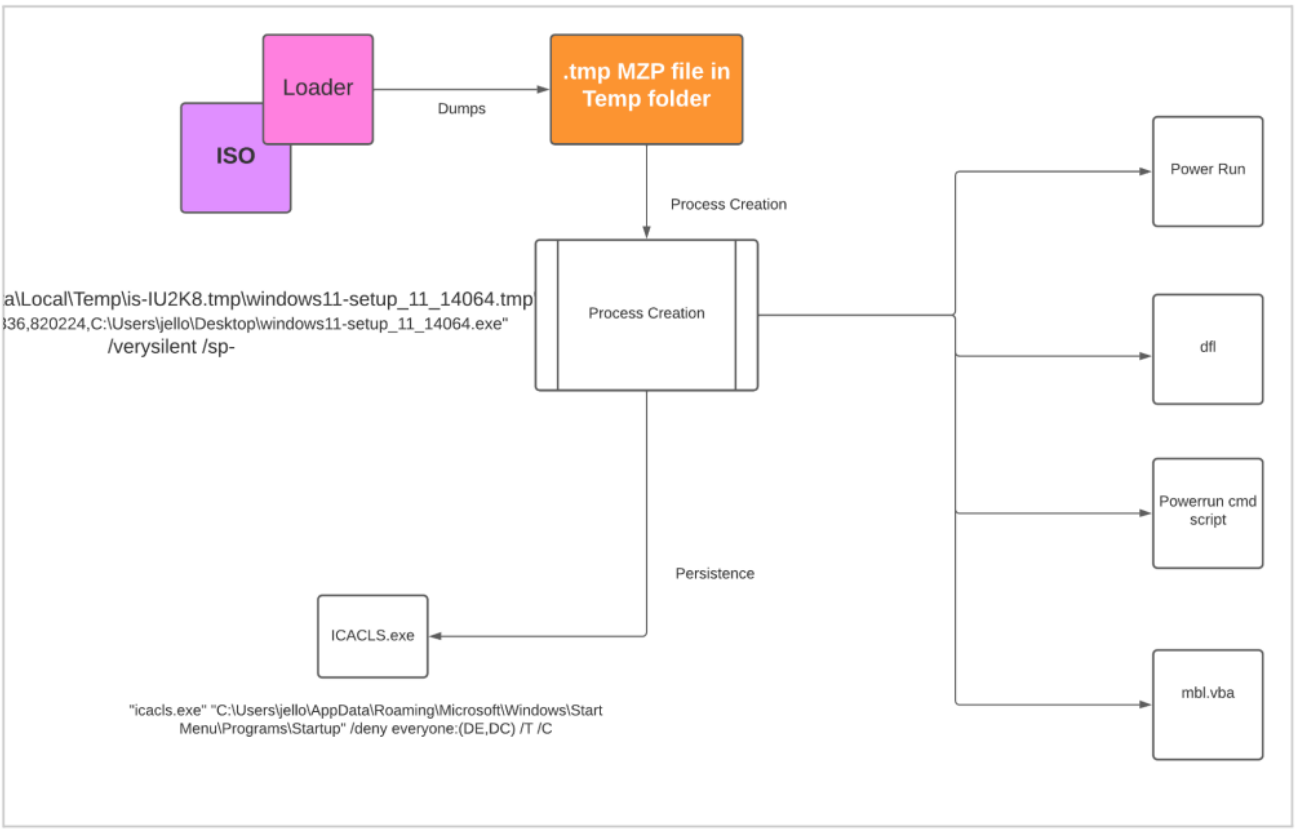
According to CloudSEK, the threat actors behind this campaign are using a new malware that researchers named “Inno Stealer” due to its use of the Inno Setup Windows installer.

The researchers say that Inno Stealer doesn’t have any code similarities to commodity other info-stealers currently in circulation and they have not found evidence of the malware being uploaded to the Virus Total scanning platform.

The loader file (Delphi-based) is the “Windows 11 setup” executable contained in the ISO, which, when launched, dumps a temporary file named *is-PN131.tmp* and creates another .TMP file where the loader writes 3,078KB of data.

CloudSEK explains that the loader spawns a new process using the *CreateProcess* Windows API the helps spawn new processes, establish persistence, and plant four files.

Persistence is achieved by adding an .LNK (shortcut) file in the Startup directory and using *icacls.exe* to set its access permissions for stealthiness.




**Creating a process to establish persistence** *(CloudSEK)*

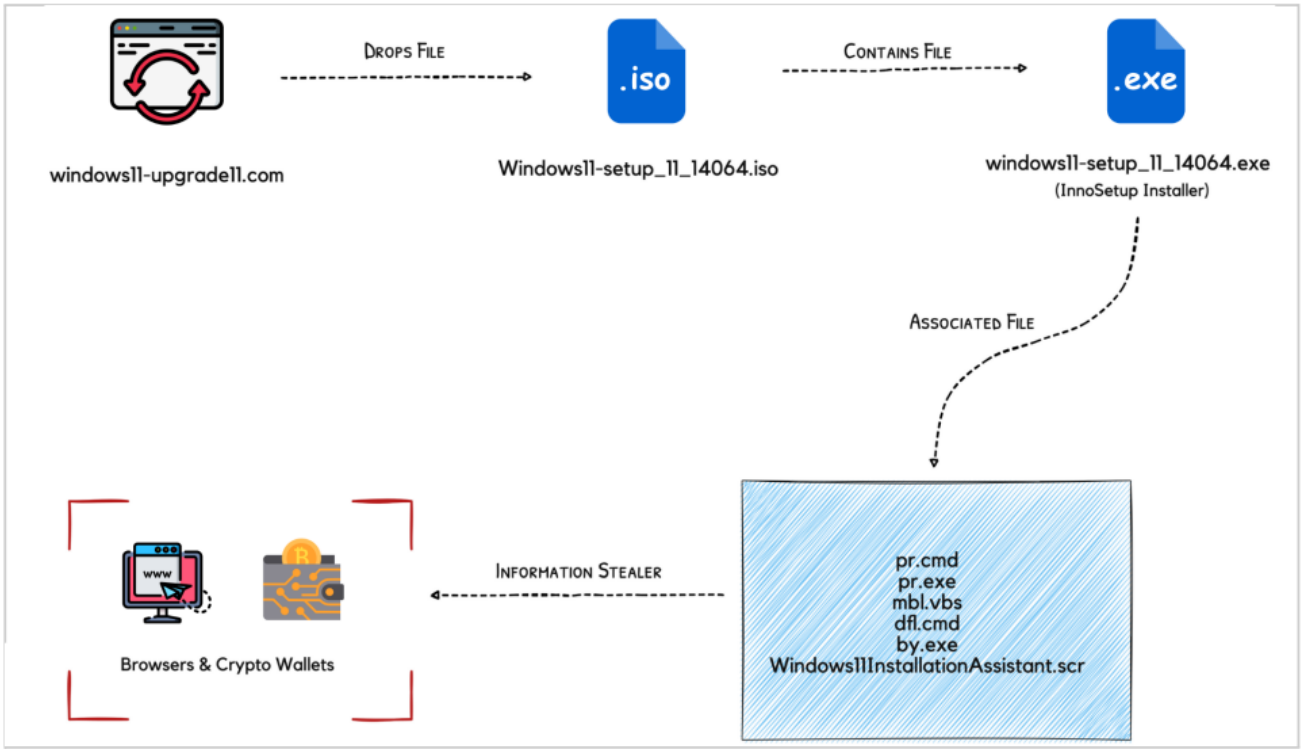
Two of the four dropped files are Windows Command Scripts to disable Registry security, add Defender exceptions, uninstall security products, and delete the shadow volume.

According to the researchers, the malware also removes security solutions from Emsisoft and ESET, likely because these products detect it as malicious.

The third file is a command execution utility that runs with the highest system privileges; and the fourth is a VBA script required to run *dfl.cmd*.

At the second stage of the infection, a file with the .SCR extension is dropped into the C:\Users\\AppData\Roaming\Windows11InstallationAssistant directory of the compromised system.

That file is the agent that unpacks the info-stealer payload and executes it by spawning a new process called “Windows11InstallationAssistant.scr”, the same as itself.




**The Inno Stealer's infection chain** *(CloudSEK)*

## Inno Stealer capabilities

The capabilities of Inno Stealer are typical for this kind of malware, including collecting web browser cookies and stored credentials, data in cryptocurrency wallets, and data from the filesystem.

The set of targeted browsers and crypto wallets is extensive, including Chrome, Edge, Brave, Opera, Vivaldi, 360 Browser, and Comodo.

| | | | | |
|---|---|---|---|---|
| Chrome | opera | Chromex86 | Chromium | BraveBrowser |
| amigo | Vivaldi | orbitum | MailRuatom | Kometa |
| Torch | Comodo | Slimjet | 360Browser | Maxthon3 |
| Sputnik | Nichrome | CocCocBrowser | uCozMediauran | Chromodo |
| edgeChromium | ChromePlus | iridium | 7Star | CentBrowser |
| elementsBrowser | Sleipnir6 | Citrio | liebaoBrowser | Coowon |
| epicPrivacyBrowser | ComodoDragon | K-Meleon | Chedot | QiPSurf |

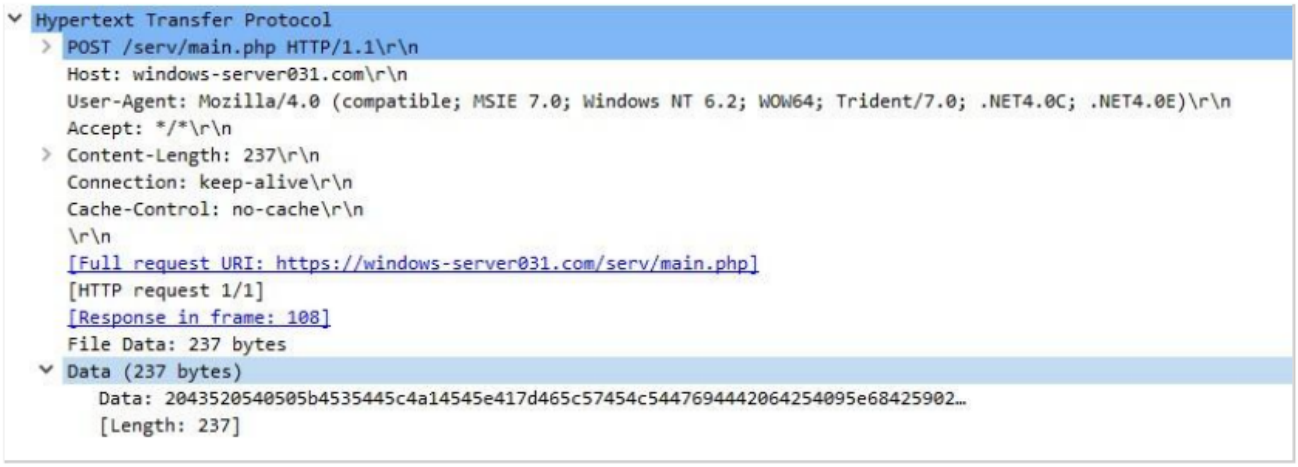
**Web browsers targeted by Inno Stealer** *(CloudSEK)*

| | | |
|---|---|---|
| wallet-backup\\ | wallet-unenc-backup\\ | mbhd.wallet |
| \wa\corewallet | WalletWasabi | \wa\WalletWasabi |
| owallet | \wa\owallet | \wa\exodus.wallet |
| \wa\YoroiWallet | \wa\RoninWallet | \wa\CloverWallet |
| \wa\MathWallet | \wa\iWallet | \wa\NiftyWallet |
| \wa\GeroWallet | \wa\GuardaWallet | \wa\GuildWallet |
| \wa\LeafWallet | \wa\SaturnWallet | \wa\EqualWallet |
| \wa\BraveWallet | wallet.dat | electrum_data\\wallets\\ |
| Electrum-DASH\\wallets\\ | \.wallet.aes | \\Coinomi\\wallets\\ |
| \\wallet-backup\\ | \\wallet-unenc-backup\\ | \\mbhd\.wallet |
| WalletWasabi\\Client\\Wallets\\ | \\WalletBackup\\ | \\BackupWallet\\ |
| Bisq\\btc_mainnet\\wallet\\ | \\wallet\.dat | \\atomex\.wallet |
| \.tezwallet | \\default_wallet | \\backups\\wallet\\ |

**Crypto wallets targeted by Inno Stealer** *(CloudSEK)*

An interesting characteristic of Inno Stealer is that the network management and the data-stealing functions are multi-threaded.

All stolen data is copied via a PowerShell command to the user's temporay directory, encrypted, and later sent to the operator's command and control server ("windows-server031.com")




**Malware communication with the C2** *(CloudSEK)*

The stealer can also fetch additional payloads, an action only performed at night time, possibly to take advantage of a period when the victim is not at the computer.

These additional Delphi payloads, which take the form of TXT files, employ the same Inno-based loader that fiddles with the host's security tools and use the same persistence-establishment mechanism.

Their extra capabilities include stealing clipboard information and exfiltrating directory enumeration data.

## Security advice

The whole Windows 11 upgrade situation has created a fertile ground for the proliferation of these campaigns, and this is not the first time that something like that has been reported.

It is recommended to avoid downloading ISO files from obscure sources and only perform major OS upgrades from within your Windows 10 control panel or get the installation files straight from the source.

If an upgrade to Windows 11 is unavailable to you, there's no point attempting to bypass the restrictions manually, as this will come with a set of downsides and severe security risks.

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.

- Previous Article
- Next Article



## You may also like: