Hackers fake Windows 11 download page to spread malicious code

Hackers are luring naive users into downloading fake Windows 11 containing malicious code that steals browser data and cryptocurrency wallets.

In this still active campaign, the hacker created a website that mimics Microsoft's Windows 11 advertising page. Then, they use dirty SEO tricks to bring this fake website to the top of Google search results.

The fake website has the same logo and icon as the official Microsoft homepage and has an inviting "Download Now" button. When pressing the download button, users will receive an ISO file containing information stealing software inside. The hacker also designed it so that users can only download files directly, not available via TOR or VPN.

This malware has been analyzed in detail by cybersecurity threat researchers at CloudSEK.

Infectious process

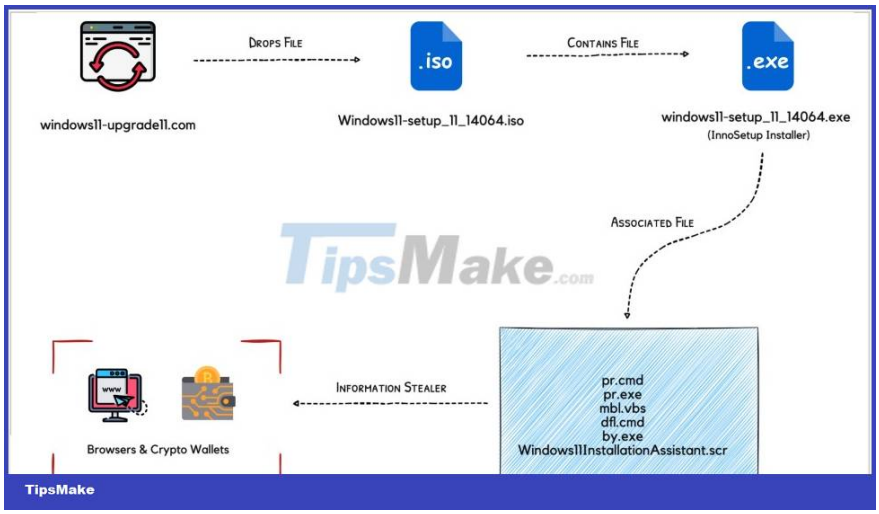
According to CloudSEK, the hacker behind this campaign uses a new piece of malware. The researchers named it "Inno Stealer" because it uses the Inno Setup Windows installer.

The researchers say that Inno Stealer doesn't have any code that resembles the malware currently being used by hacking groups. In addition, there is no evidence of Inno Stealer being uploaded to Virus Total scanning platform.

The loader file (programming in Delphi) is the "Windows 11 setup" executable included in the ISO file. On launch, this file creates a dump of a temporary file named is-PN131.tmp and creates another .TMP file in which the loader writes 3,078KB of data.

CloudSEK explains that the loader creates a new process using the CreateProcess Windows API, which spawns the new process, sets up persistence, and creates four files.

Persistence is created by adding a .LNK file (shortcut) in the Startup folder and using icacls.exe to set its access to stealth.



Two of the four added files are Windows Command Scripts to disable Registry security, add exceptions to Defender, uninstall security products, and remove volume shadows.

According to the researchers, the malware also eliminates security solutions from Emisoft and ESET, possibly because these products detect it as malware.

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

In the second stage of the infection, a file with the extension .SCR is placed in the C:UsersAppDataRoamingWindows11InsstallationAssistant folder of the infected machine.

That file is the agent that unpacks the information-stealing payloads and executes it by creating a new process named "Windows11InstallationAssistant.scr" that is identical to itself.

What can Inno Stealer do?

Inno Stealer has capabilities such as collecting cookies and stored login information of web browsers, data in cryptocurrency wallets and data from the file system. Almost every necessary function of a malware in this regard Inno Stealer has.

The set of browsers and crypto wallets that Inno Stealer targets is wide, 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

TipsMake

Inno Stealer's Target Browsers

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

TipsMake

Another interesting feature of Inno Stealer is that the data stealing and network management functions are multi-threaded. In addition, it can also download other payloads to perform additional operations such as stealing clipboard information and obtaining directory listing data.

What should users do?

This is not the first time hackers have taken advantage of the need to download and install Windows 11 to spread malicious code. You should avoid downloading ISO files from unsecured sources and it is best to upgrade to Windows 11 from the Settings menu of Windows 10.

You finished reading the article "**Hackers fake Windows 11 download page to spread malicious code**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

© 2019 TipsMake.com