Microsoft Help Files Disguise Vidar Malware

By Nate Nelson

Published: 2022-03-24 · Archived: 2026-04-06 00:27:42 UTC

Attackers are hiding interesting malware in a boring place, hoping victims won't bother to look.

Where's the last place you'd expect to find malware? In an email from your mother? Embedded in software you trust and use everyday (actually, that's probably the first place you should look)? How about in a technical documentation file?

In a report published Thursday, Trustwave SpiderLabs revealed a new phishing attack designed to plant the Vidar infostealer on target machines. The trick to this particular campaign is that it conceals its complex malware behind a Microsoft Compiled HTML Help (.CHM) file, Microsoft's proprietary file format for help documentation saved in HTML. In other words, it's the kind of file you almost never look at or even think about.

After all, what better place to hide something interesting than within something boring? That's just what cyberattackers have done in a recent spate of data-stealing attacks: leverage .CHM files in a nested attack that prioritizes obfuscation.

The Latest Phish

Some threat actors will dedicate a tremendous amount of effort to diligently crafting a perfect phishing email. They copy a well-known brand's graphics to a tee, and compose a perfect message conveying legitimacy and professionalism, but also urgency.

Not so here. If the attackers in this case spent any more than three minutes crafting their phishing email, it doesn't show.

The subject line – "**Re: Not read: Coverage Inquiry 3.24.16**" – goes some way to implying that an ongoing discourse is occurring ("Re"), and that the recipient must take action ("Not read") – and is otherwise vague enough to not arouse immediate suspicion. The body of the email does even less:

The important information for you. See the attachment to the email.

Thank You!

Said attachment appears to the recipient as "request.doc," but is, in fact, an .ISO file, Trustwave noted in its analysis. ISOs are used to copy the information on physical optical discs into a single file. However, as the report notes, hackers have learned how to repurpose ISO files as malware containers. According to Trustwave, there was a "notable uptick" in this strategy beginning in 2019. Vidar itself started gaining popularity around the same time.

The Vidar Malware

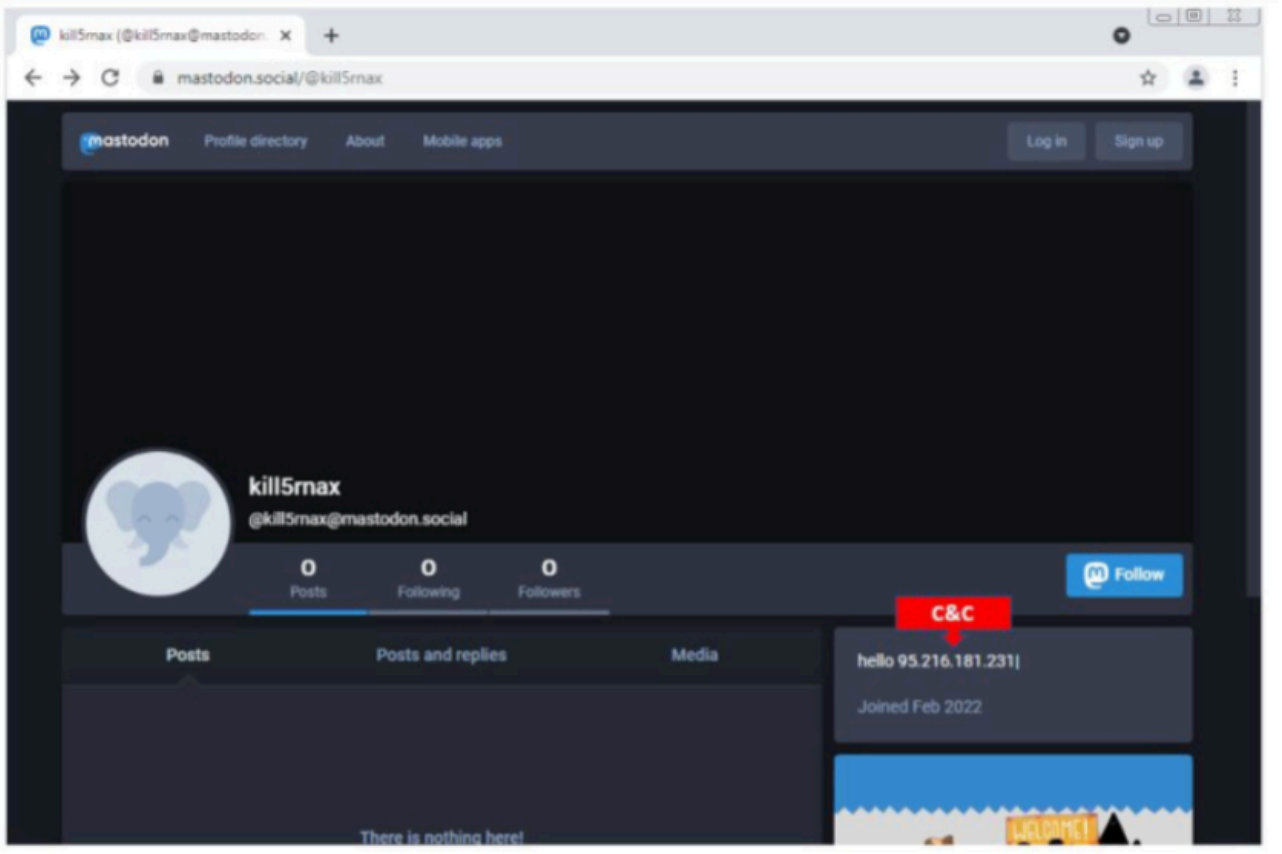
Vidar is a kind of jack-of-all-trades infostealer, forked from the Arkei malware family. As Threatpost has explained in the past, just after it was first discovered:

Vidar steals documents, cookies and browser histories (including from Tor), currency from a wide array of cryptocurrency wallets, data from two-factor authentication software and text messages, plus it can take screenshots. The package also offers malware operators Telegram notifications for important logs. And lastly, threat actors can customize the stealer via profiles, which allows them to specify the kind of data they are interested in.

In this latest campaign, the .ISO file contains a .CHM file named "pss10r.chm." Towards the end of the file's code is a snippet of HTML application (HTA) code containing JavaScript that covertly triggers a second file, "app.exe." This is, in fact, Vidar malware.

"One of the objects unpacked from the .CHM is the HTML file 'PSSXMicrosoftSupportServices_HP05221271.htm' — the primary object that gets loaded once the CHM pss10r.chm is opened," according to the Trustwave writeup. "This HTML has a button object which automatically triggers the silent re-execution of the .CHM "pss10r.chm" with mshta." Mshta is a Windows binary used for executing HTA files.

As soon as app.exe triggers, Vidar downloads its dependencies and configuration settings from a command-and-control (C2) server, which is retrieved from Mastodon, an open-source social networking platform. The malware then searches two hard-coded profiles and nabs the C2 address from the Bio section.



A Mastodon profile containing Vidar's C2 information. Source: Trustwave.

Then, Vidar gets to stealing. Any information it sucks up gets sent back to the C2. Vidar can also download additional malware to the target machine. Once the job is done, the malware covers its tracks by deleting all the files it's created.

This nested approach and the use of unassuming Help files is all in the name of obfuscation, of course.

"We've seen this technique used quite a bit recently," Karl Sigler, senior security research manager at Trustwave SpiderLabs, told Threatpost via email, "and the various attempts at nesting the attack (from .ISO to .CHM to .HTA to JavaScript to execution) shows the lengths that these actors are going to try to obfuscate and hide their attack."

He concluded quite simply. "This TTP is really popular right now."

Moving to the cloud? Discover emerging cloud-security threats along with solid advice for how to defend your assets with our FREE downloadable eBook, "Cloud Security: The Forecast for 2022." We explore organizations' top risks and challenges, best practices for defense, and advice for security success in such a dynamic computing environment, including handy checklists.
