Microsoft help files repurposed to contain Vidar malware in new campaign

csoonline.com/article/3654849/microsoft-help-files-repurposed-to-contain-vidar-malware-in-new-campaign.html

Jon Gold

A new email campaign designed to spread the Vidar spyware package uses a novel technique involving Microsoft Compiled HTML help files, according to a blog post released today by Trustwave.

The help files, which use the suffix “CHM,” are packaged in an ISO along with the Vidar payload in what appears to be a Word document. If the attacker successfully hoodwinks the target into extracting the phony document, executing either file triggers the malicious package and compromises the system, Trustwave researcher Diana Lopera wrote in the post.

The CHM file used in the attack is mostly a copy of a legitimate CHM, but has appended HTML application code – that extra code silently runs the malicious executable in the background when the CHM file is run.

The particular flavor of Vidar used in the attack, Lopera noted, is version 50.3, and receives its command-and-control (C&C) instructions from accounts on open-source social networking platform Mastodon. Once up and running, the malware downloads configuration information from C&C servers identified by the Mastodon page and starts its work – first collecting system information and password data from browsers and other applications, sending that information as a ZIP file back to the C&C server, and then deleting itself, potentially after pulling additional malware onto the infected machine.

“Appending a malicious file to an unsuspecting file format is one of the tricks our adversaries use to evade detection,” wrote Lopera.

What is Vidar?

Vidar was first observed in the wild in late 2018, according to a report from cloud security vendor Infoblox, which noted that it’s a variant of the earlier Arkei infostealer. It’s sold commercially in online forums, and has the ability to steal a wide variety of user information and valuable data from infected computers, including credit card numbers, usernames and passwords, desktop screenshots, and cryptocurrency wallets. It can even bypass some types of two-factor authentication, particularly targeting the Authy 2FA stack.

As ever, strong email security practices can mitigate or eliminate the risks posed by Vidar – extreme caution should be used when opening email attachments from unfamiliar senders with generic subject lines, and verification either over the phone or in person should be the first move if there is any doubt about such a message’s legitimacy.