Spammers Revive Hancitor Downloader Campaigns

By Tom Spring

Published: 2017-01-11 · Archived: 2026-04-05 18:26:45 UTC

A recent lull in the distribution of spam linking to the malicious downloader Hancitor has been snapped as researchers warn of new campaigns.

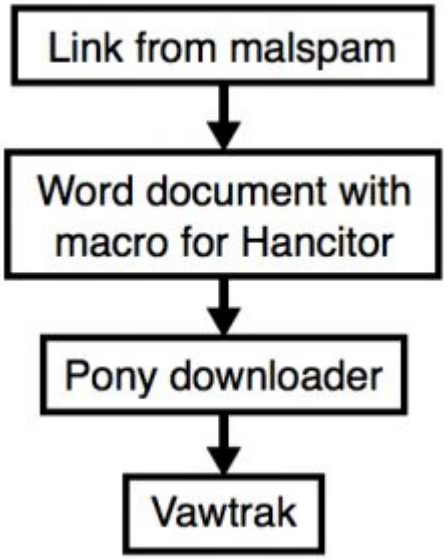
A recent lull in the distribution of spam spreading information-stealing malware via the Hancitor downloader has been snapped.

Researchers at the SANS Internet Storm Center are currently tracking an increase in spam purporting to be a forwarded parking ticket notification. The message prompts the recipient to click a link to pay a parking ticket; the hyperlink is to a Microsoft Word document.

“The document contains a malicious VB macro described has Hancitor, Chanitor or Tordal,” wrote Brad Duncan, handler at the SANS Internet Storm Center in blog post warning of the spam campaign. “If you enable macros, the document retrieves a Pony downloader DLL. The Pony downloader then retrieves and installs Vawtrak malware.”

There doesn’t appear to be anything unique when it comes to the Word Document and its standard ploy of pushing recipients to “enable content” and run a malicious macro. An analysis of the link from the phishing e-mail contains a base64-encoded string representing the recipient’s address. Using that string, attackers insert the recipient’s name into the filename of the World document.

“I used a base64 string for *bert@shotts123.com* (a made-up name/address) and received a file named *parking_bert.doc*,” Duncan said.



Other aspects of the spam campaign are similar to previous waves of Hancitor-related spam reported in 2016 by Palo Alto Networks and FireEye. “Pattern-wise, URLs from this infection are similar to previous cases of Hancitor/Pony/Vawtrak malspam reported during the past two or three months,” Duncan wrote.

In August, a variant of the Hancitor downloader was identified by Palo Alto Networks that shifted away from leveraging the latest incarnation of H1N1 and distributed the Pony and Vawtrak executables. In September, FireEye reported the way that Hancitor’s payload was delivered differed from previous iterations. Researchers said the downloader had shifted to depend on native Windows API callback functions to execute shellcode.

While malicious Hancitor campaigns fluctuate in volume, researchers say overall spam-based macro attacks are on the rise. In a study released in October, Microsoft said incidents of macro-based malware hiding in Office documents has steadily been on the rise. In the enterprise, Microsoft reports, 98 percent of Office-targeted threats still use old-school macro-based attacks.

“We often become jaded as yet another wave of malspam does the same thing it’s done before. Patterns behind such activity are often well-documented. So why bother with discussion, if there’s nothing new?” Duncan wrote. “That attitude only encourages the criminal groups behind malspam.”

Duncan reminds that there are a number of technical means to prevent these types of infections such as new protections from Microsoft for its Office suite introduced in October.
