# DocuSign Phishing Campaign Includes Hancitor Downloader

By Tom Spring

Published: 2017-05-16 · Archived: 2026-04-05 22:33:35 UTC

DocuSign warns of a breach and subsequent theft of email addresses that are part of a phishing campaign that employs malicious macro-laced Word documents.

Electronic document exchange vendor DocuSign warned on Monday of a wave of phishing emails targeting its customers with links to malicious Word documents. The campaign, it said, was tied to an earlier breach of its computer networks where hackers were able to gain “temporary access” and exfiltrate an undisclosed number of customer email addresses.

DocuSign, with 100 million users and 250,000 business accounts, said “no names, physical addresses, passwords, social security numbers, credit card data or other information” were stolen by the hackers.

Phishing emails spoofed the DocuSign brand and included a hyperlink to a Word document that contained a malicious macro. If the document is downloaded and the macro is enabled, it delivers the Hancitor downloader. Next, Hancitor downloads either the credential stealing Pony, EvilPony or ZLoader malware, said Gregor Perotto, senior director, global corporate marketing and communications for DocuSign.

Earlier this year, researchers had reported a lull in the distribution of spam spreading information-stealing malware via Hancitor. That dry spell ended in January when SANS Internet Storm Center noted a sharp increase in spam containing links to download Word documents with macros that, if enabled, downloaded Hancitor.

The DocuSign malicious email campaign began last week, according to the company. That’s when DocuSign said it began tracking emails that featured the subject line “Completed: docusign.com – Wire Transfer Instructions for recipient-name Document Ready for Signature”.

On Monday, DocuSign again reached out to customers informing them that it was continuing to track the malicious email campaign and that the subject line changed. It now read, “Completed *company name* – Accounting Invoice *number* Document Ready for Signature”, according to the company. Emails also had links to downloadable Word documents that contained Hancitor. Spoofed sender email address included @docusign.com or @docusign.net domains, DocuSign said.

“As part of our ongoing investigation, today we confirmed that a malicious third party had gained temporary access to a separate, non-core system that allows us to communicate service-related announcements to users via email. A complete forensic analysis has confirmed that only email addresses were accessed; no names, physical addresses, passwords, social security numbers, credit card data or other information was accessed,” the company said.

It reiterated that the breach did not impact the privacy of customer documents sent through DocuSign's eSignature platform. It is encouraging customers who receive malicious emails to forward them to spam@docusign.com.

Still unknown is how many DocuSign email addresses were stolen.

Security experts report incidents of macro-based malware have steadily been on the rise in 2016. In the enterprise, Microsoft reports, 98 percent of Office-targeted threats still use old-school macro-based attacks.

The increase in macro-based attacks began earlier last summer, and criminals have been increasingly turning to Office macros to deliver malware versus using more traditional means such as exploit kits.

---