Emotet Malware Revives Old Email Conversations Threads to Increase Infection Rates

spamtitan.com/blog/emotet-malware-revives-old-email-conversations-threads-to-increase-infection-rates/

titanadmin

April 12, 2019

Emotet malware was first identified in 2014 and its original purpose was to obtain banking credentials and other sensitive information; however, the malware is regularly updated and new functionality is added. Emotet malware is now one of the most prevalent and dangerous malware threats faced by businesses.

The malware can detect whether it is running in a virtual environment and will generate false indicators in such cases. The malware is polymorphic, which means it changes every time it is downloaded. That makes it difficult to detect using the signature-based detection methods employed by standard anti-virus software.

The malware also has worm-like features which allows it to rapidly spread to other networked computers. Emotet is also capable of spamming and forwarding itself to email contacts. As if infection with Emotet is not bad enough, it can also download other malware variants onto infected devices.

Emotet malware is one of the most destructive malware variants currently in use and cleaning up Emotet attacks can be incredibly costly. The Department of Homeland Security has reported that some attacks on state, local, tribal, and territorial governments have cost more than $1 million to resolve.

Emotet malware is primarily distributed via spam email, either through malicious attachments or hyperlinks to websites where the malware is silently downloaded. The lures used in the messages are highly varied and include most of the commonly used phishing lures such as shipping notifications, fake invoices, payment requests, PayPal receipts.

Now the threat actors behind the malware have adopted a new tactic to increase infection rates. Once installed on a device, the malware accesses email conversation threads and forwards the message to individuals named in the thread.

The original email conversation is unaltered, but a hyperlink is added to the top of the message. The link directs the recipient to a webpage where a file download is triggered. Opening the document and enabling macros will see Emotet downloaded. Email attachments may also be added to previous conversation threads in place of hyperlinks.

Since the messages come from a known individual with whom an email conversation has taken place in the past, the probability of the document being opened is greater than if messages come out of the blue or are sent from an unknown individual.

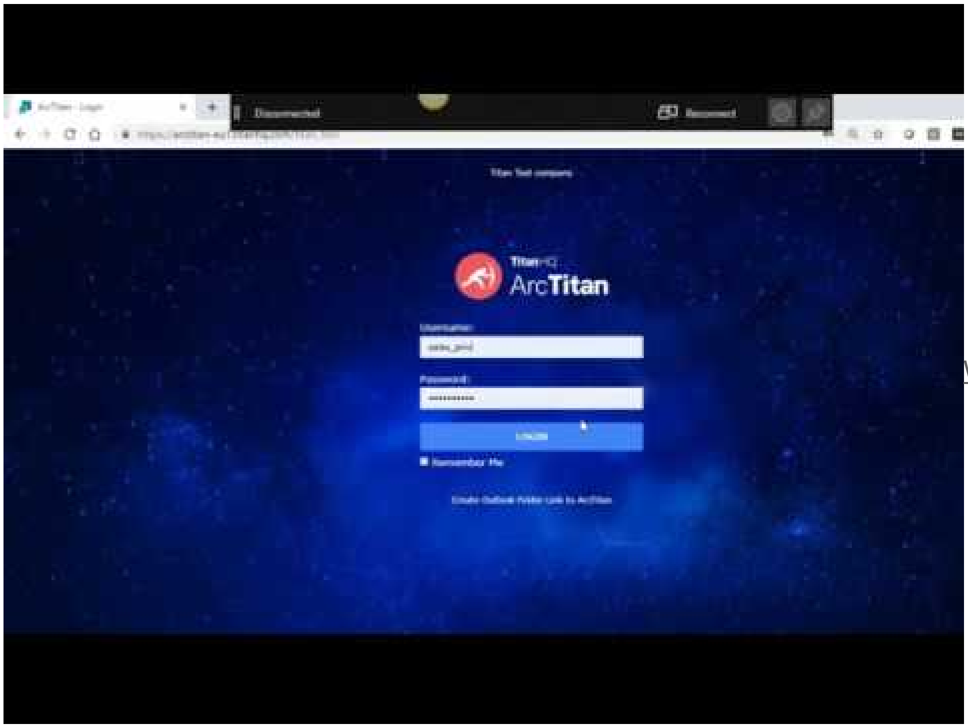
Several cybersecurity firms have identified a campaign using this tactic, including phishing intelligence provider Cofense and security researcher Marcus Hutchins (MalwareTech).

The current campaign uses revived conversations from before November 2018, although more recent conversations may be revived in further campaigns. Any revived old email conversation that contains a link or an attachment could indicate a user has been targeted and that at least one member of the email exchange has been infected with Emotet.

The current campaign is not only extensive, it is also proving to be extremely successful. Spamhaus reports that there have been 47,000 new infections in the past two months alone, while Cofense reports that it has identified more than 700,000 infections in the past 12 months.

Protecting against this dangerous malware requires a powerful anti-spam solution and good security awareness training for staff. SpamTitan's new features can help to detect malicious emails spreading Emotet malware to better protect businesses from attack.

To find out more about SpamTitan and how the solution can protect your business, give TitanHQ a call today.



Watch Video At:

https://youtu.be/S0OSwl1NQ1s