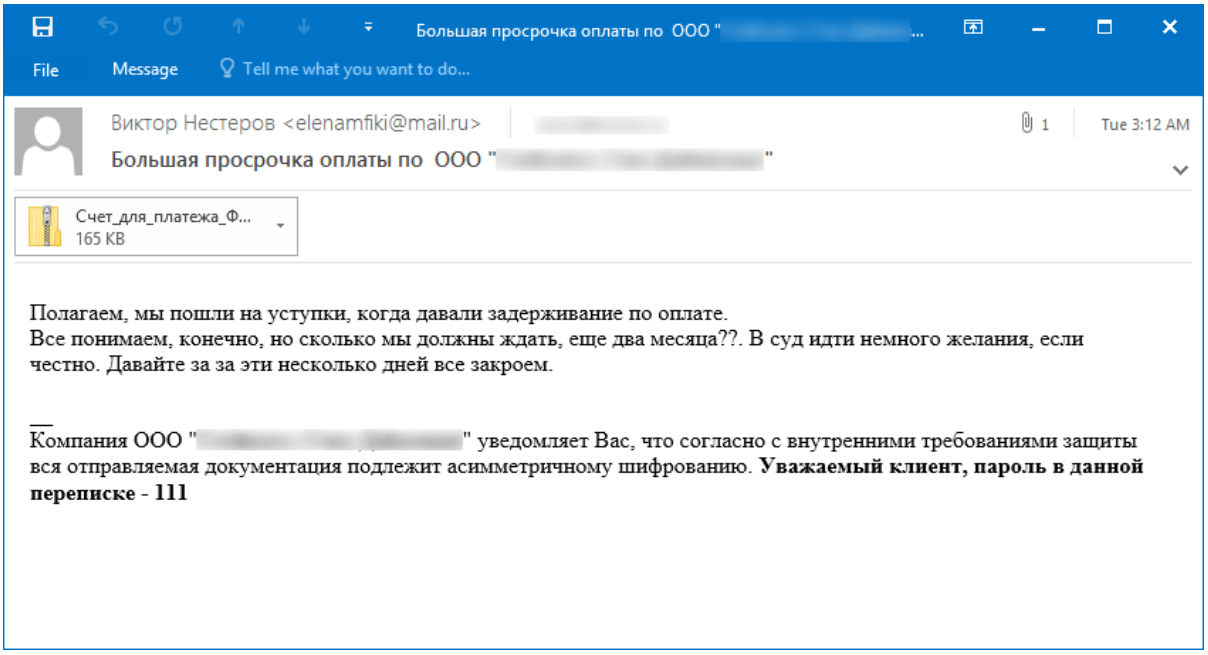
Pony Stealer Malware

knowbe4.com/pony-stealer

Pony Stealer is a password stealer that can decrypt or unlock passwords for over 110 different applications including VPN, FTP, email, instant messaging, web browsers and much more. Pony Stealer is very dangerous and once it infects a PC it will turn the device into a botnet, allowing it to use the PCs it infects to infect other PCs.



Pony Stealer, which is tied closely to Reveton worm, is also well-known for spreading malware, thanks to an e-mail campaign that was started in late 2014. The e-mail is supposedly sent from the shipping company Maersk Line. The writer of this e-mail informs potential victims that they have an overdue invoice from an account with the company. The victims are then provided with a link to a PDF download so they can download the overdue invoice and then pay for what they owe. Toward the end of the e-mail, victims are provided with phone numbers for a “sales representative” and the Maersk customer service line—and both of these phone numbers have a Vietnamese area code. In an effort to make the e-mail seem more legitimate, the writer provides the URL of Maersk’s official website.

A quick inspection would reveal that, while Maersk does have a way to contact their Vietnamese branch, the phone number on their official website is completely different from the ones provided in the e-mail. Furthermore, in January 2014, Maersk warned their customers about the fraud, instructing them not to click the suspicious links in the e-mails and not to provide anyone with security information like account passwords.

Is Your Network Vulnerable To Ransomware Attacks?

Find out now with KnowBe4's Ransomware Simulator "RanSim", get your results in minutes.

Get RanSim!

« Back To Ransomware Knowledgebase

Get the latest about social engineering

Subscribe to CyberheistNews