



Stealth New Zeus Infection Campaign Targets Enterprises

Trusteer
October 15, 2009

Executive Summary

Zeus (AKA Zbot) is a highly effective Trojan that steals personal information and website login credentials. Once downloaded, the Trojan injects itself into the browser and monitors all traffic. It then steals login credentials to sensitive websites. Zeus also changes web pages that users view, asking for additional sensitive information and sending it to the attackers.

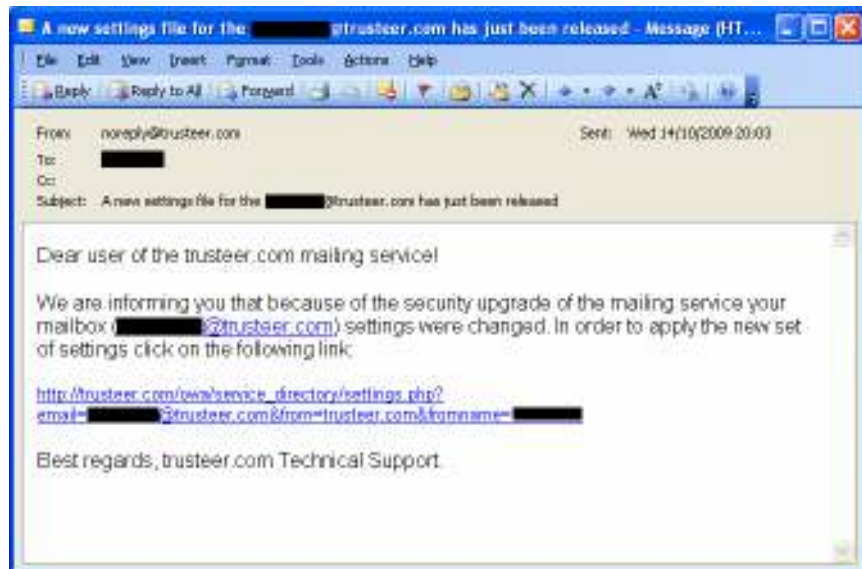
Zeus now actively targets corporate users through an effective email campaign that asks Outlook Webmail users to update their settings. The goal of this attack is to harvest credentials used to access enterprise web accounts such as banking, webmail, and CRM, financial, etc., SaaS applications.

Since Zeus is poorly detected by most antivirus programs, enterprises are advised to take special precautions to protect their assets including: educating employees about fraudulent emails regarding Outlook Web Access upgrades, blocking downloads of executable files and zip files through the web, and locking down browser settings to prevent the injection of unauthorized code into web sessions.

Attack Details

Yesterday (October 14th) afternoon GMT, Trusteer discovered that a highly effective spam campaign was launched to target corporate email accounts. The campaign ultimately attempts to install the Zeus/Zbot Trojan on users' machines.

The campaign is well executed, and as such is highly effective. It begins with an email like this (the recipient name is blacked-out):

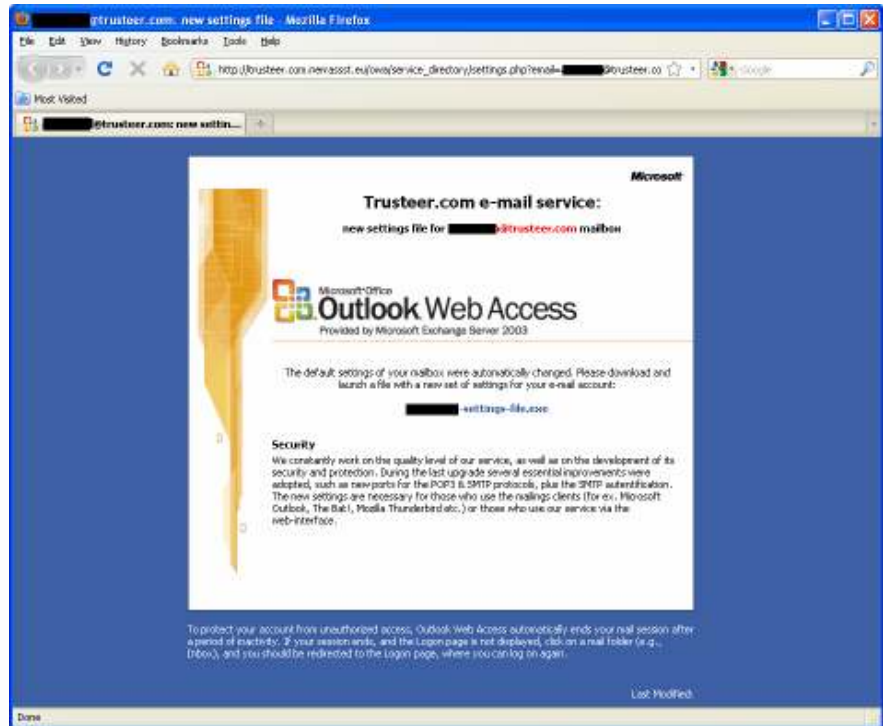


Note how well the message is customized – the “From” address appears to be from within the enterprise (there are several “from” mailboxes observed, e.g. noreply@corporate, info@corporate and notifications@corporate), and how the corporation’s name and recipient name are embedded in the email body. The text itself makes a lot of sense in the enterprise world – requesting that the user modify their email settings as a result of an upgrade. Finally, the link itself appears to be to the enterprise’s site. However, looking at the HTML source of this email, the real link is actually to a site in nerrassst.eu:

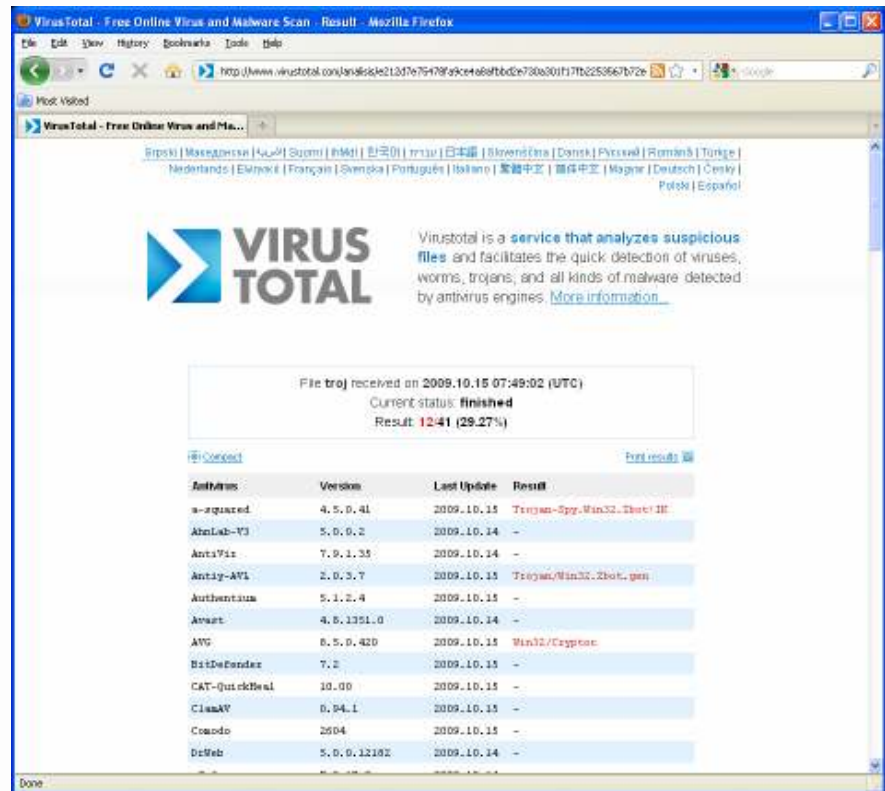
[http://trusteer.com.nerrassst.eu/owa/service_directory/settings.php?email=\[REMOVED\]@trusteer.com&from=trusteer.com&fromname=\[REMOVED\]](http://trusteer.com.nerrassst.eu/owa/service_directory/settings.php?email=[REMOVED]@trusteer.com&from=trusteer.com&fromname=[REMOVED])

When the victim clicks on the link they arrive at a legitimate looking website which uses the Outlook Web Access design and themes. This is clever since many corporate employees use Outlook Web Access to manage email remotely.

Just like the email, the landing page is customized to look like the enterprise’s real website and personalized with the recipient’s name (the latter is blacked out):



The user is asked to “download and launch a file with a new set of settings for their e-mail account”. This file is actually a flavor of the ZeuS/Zbot Trojan (MD5 signature 642ff076c8bc5b3be5b9e853337d1820), which had a relatively low rate of detection at the time of writing – only recognized by 12 out of 41 anti-virus vendors:



Once the user runs the executable file, their system is infected with ZeuS/Zbot. This is a very flexible and powerful financial Trojan that can capture credentials, impersonate online banking websites to steal additional information from the user, and in general perpetrate identity theft and financial fraud. This new Phishing attack is designed to compromise enterprise bank accounts, which typically control considerably larger amounts of money than consumer bank accounts.

Recommendations

1. Educate employees regarding this specific attack. Most enterprises educate employees regarding phishing. However, since this attack looks as an internal email, it is deceiving
2. Block the download of exe files and zip files from the web. This is not a fool proof solution, since the fraudulent website many use adobe and other types of browser add-on vulnerabilities to download itself into the browser. However, it is a good security practice.

3. Use browser lockdown tools to prevent unauthorized code from executing inside the browser. These tools, including our Rapport product, can block Zeus and other Trojans from executing and stealing information from employees.

-End-