National Computer Board
Computer Emergency Response Team of Mauritius
(CERT-MU)

Threat Alert

New variant of Zeus banking Trojan concealed in JPG images

Issued on: February 2014

Severity Rating: High

Description:

The Zeus/Zbot Trojan is one the most notorious banking Trojans ever created. The Trojan attempts to steal information from the compromised computer and download configuration files and updates from the Internet. A new variant of the nefarious Zeus banking Trojan dubbed "ZeusVM" has recently been uncovered concealed in JPG image files. The malware uses the steganography technique, which is the act of concealing messages or images in other messages or images. This piece of malware can be distributed in many different ways, but most typically through phishing emails or a web-based attack. It can also spread via malvertising, which involves websites hosting ads that spread malware.

The malware code of ZeusVM is hidden in unassuming JPG images and these pictures serve as misdirection for the malware to retrieve its configuration file. The JPG contains the malware configuration file, which is essentially a list of scripts and financial institutions - but does not need to be opened by the victim themselves. In fact, the JPG itself has very little visibility to the user and is largely a cloaking technique to ensure it is undetected from a security software standpoint. The infection by the ZeusVM Trojan allows man-in-the-middle and man-in-the-browser attacks. Moreover, visiting certain URLs such as banking websites will cause the Trojan to respond and begin interacting in real-time. Attackers can obtain certain information by altering a login page using webinjects, or they could perform wire transfers while altering the victim's account balance to make it seem like funds were never moved.

Methodology

1. When an infected user loads their banking website, the Trojan is activated and starts acting as man-in-the-middle.
2. The user is properly authenticated into the banking system.
3. While the user is conducting banking transactions, the Trojan ZeusVM can steal banking information and empty out the user's bank account in total discretion, without the user's knowledge.

Recommendations

- Ensure that your anti-virus software is up-to-date
- Do not click on links in e-mails, unless you know the source
- Use a firewall to block all incoming connections from the Internet to services that should not be publicly available. By default, you should deny all incoming connections and only allow services you explicitly want to offer to the outside world
- Enforce a password policy. Complex passwords make it difficult to crack password files on compromised computers. This helps to prevent or limit damage when a computer is compromised
- Turn off file sharing if not needed. If file sharing is required, use ACLs and password protection to limit access. Disable anonymous access to shared folders. Grant access only to user accounts with strong passwords to folders that must be shared
- Turn off and remove unnecessary services. By default, many operating systems install auxiliary services that are not critical. These services are avenues of attack. If they are removed, threats have less avenues of attack
- Ensure that programs and users of the computer use the lowest level of privileges necessary to complete a task. When prompted for a root or UAC password, ensure that the program asking for administration-level access is a legitimate application
- Disable AutoPlay to prevent the automatic launching of executable files on network and removable drives, and disconnect the drives when not required. If write access is not required, enable read-only mode if the option is available
- If a threat exploits one or more network services, disable, or block access to, those services until a patch is applied
- Always keep your patch levels up-to-date, especially on computers that host public services and are accessible through the firewall, such as HTTP, FTP, mail, and DNS services
- Configure your email server to block or remove email that contains file attachments that are commonly used to spread threats, such as .vbs, .bat, .exe, .pif and .scr files
- Isolate compromised computers quickly to prevent threats from spreading further. Perform a forensic analysis and restore the computers using trusted media
- Train employees not to open attachments unless they are expecting them. Also, do not execute software that is downloaded from the Internet unless it has been scanned for viruses. Simply visiting a compromised Web site can cause infection if certain browser vulnerabilities are not patched

For more information please contact CERT-MU team on:

Hotline No: (+230) 800 2378

Fax No: (+230) 208 0119

Gen. Info. : info@cert-mu.gov.mu

Incident: incident@cert-mu.gov.mu

Website: http://www.cert-mu.org.mu