



Information on ZeuS Trojan & Best Practices

Recently the Office of Domestic Security of the Florida department of law enforcement issued the following cyber alert.

+++ Cyber Alert +++

The groups behind the ZeuS Trojan appear to be getting ready to use Department of Homeland Security, DHS, themed domains for ZeuS seeding. The following domains were recently created and will probably be used for the next Phishing campaign:

DHSinfo[dot]info, which was created on 09-Mar-2010

DHSorg[dot]org, which was created on 11-Mar-2010

GreyLogic[dot]org, which was created on 11-Mar-2010

GreyLogic[dot]info, which was created on 09-Mar-2010

IntelFusion[dot]org, which was created on 12-Mar-2010

IntelFusion[dot]info, which was created on 08-Mar-2010

It is recommended that these domains be added to your spam filter block lists.

Also, in the coming days be on the look-out for emails originating from these domains. Do not click on any links that originate or appear to originate from these domains.

+++++

In addition the following best practices are recommended:

1. Implement all security controls available within Internet banking applications, including dual approvals, transfer dollar limits, IP address lockdown etc.;
2. Implement a multi-factor (at least two-factor) authentication methodology for user access to all Internet banking applications;
3. Ensure anti-virus software is properly installed and configured with automatic updates enabled and a full system scan is completed weekly on each

workstation/desktop/notebook with access to Internet banking applications;

4. Ensure operating system software is enabled to automatically download and install security updates on each workstation/desktop/laptop with access to Internet banking applications;

5. If a network firewall is not in place, ensure a personal firewall is properly installed, configured and regularly updated on each workstation/desktop/notebook with access to Internet banking applications;

6. Ensure general user accounts have no administrative rights and the right/permission to install any software is restricted to administrators only;

7. Conduct a full review of your wire transfer process being sure that all appropriate verification steps are in place and being followed;

8. Simply do not trust unsolicited email and never click-on links and attachments in unsolicited email messages;

9. Implement a spam filter;

10. Require employees to review US-CERT Cyber Security Tip ST04-014, "Avoiding Social Engineering and Phishing Attacks." <http://www.us-cert.gov/cas/tips/ST04-014.html>

11. Consider dedicating a single workstation/desktop/notebook that is never used for email or Web browsing to be used exclusively for Internet banking.

March 23, 2010