



QUARTERLY TRENDS AND ANALYSIS REPORT

www.us-cert.gov

Introduction

This report summarizes and provides analysis of incident reports submitted to US-CERT during the U.S. Government fiscal year 2009 first quarter (FY09 Q1), which is the period of October 1, 2008 to December 31, 2008.

US-CERT is charged with providing response support and defense against cyber attacks for the Federal Civil Executive Branch (.gov) and information sharing and collaboration with state and local government, industry and international partners.

US-CERT interacts with federal agencies, industry, the research community, state and local governments, and others to disseminate reasoned and actionable cyber security information to the public.

US-CERT provides the following support:

- 24 x 7 x 365 triage support to federal, public, and private sectors, and the international community
- cyber security event monitoring and predictive analysis
- advanced warning on emerging threats
- incident response capabilities for federal and state agencies
- malware analysis and recovery support
- trends and analysis reporting tools
- development and participation in national and international level exercises

The purpose of this report is to provide awareness of the cyber security trends as observed by US-CERT. The analysis in this report is based on incident information that has been reported to US-CERT, incidents identified by US-CERT, and public/private sector information identified when correlating and analyzing the data. A computer incident within US-CERT is, as defined by NIST Special Publication 800-61, a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices.

This report also provides information on notable security topics and trends, including emerging threats and updates to topics discussed in previous issues.

INSIDE THIS ISSUE

<i>Introduction</i>	<i>1</i>
<i>Cyber Security Trends, Metrics, and Security Indicators</i>	<i>2</i>
<i>Torpig Trojan</i>	<i>3</i>
<i>Proliferation of Malware via USB Media</i>	<i>3</i>
<i>Phishing and Spamming Trends</i>	<i>3</i>
<i>National Cyber Alert System</i>	<i>4</i>
<i>Contacting US-CERT</i>	<i>4</i>
<i>Disclaimer</i>	<i>4</i>

Cyber Security Trends, Metrics, and Security Indicators

US-CERT interacts with federal agencies, industry, the research community, state and local governments, and others to collect reasoned and actionable cyber security information and to identify emerging cyber security threats. Based on the information reported, US-CERT was able to identify the following cyber security trends for fiscal year 2009 first quarter (FY09 Q1).

The definition of each reporting category is delineated in Table 1 shown below.

Category	Description
CAT 1 Unauthorized Access	In this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource.
CAT 2 Denial of Service (DoS)	An attack that <i>successfully</i> prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.
CAT 3 Malicious Code	<i>Successful</i> installation of malicious software (e.g., virus, worm, spyware, bot, Trojan horse, or other code-based malicious entity that infects or affects an operating system or application). Agencies are <i>not</i> required to report malicious logic that has been <i>successfully quarantined</i> by antivirus (AV) software.
CAT 4 Improper Usage	A person violates acceptable computing use policies.
CAT 5 Scans, Probes, or Attempted Access	Any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.
CAT 6 Investigation	<i>Unconfirmed</i> incidents of potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.

Figure 1 displays the overall distribution of cyber security incidents and events across the six major categories described in Table 1.

The percentage of Category 5 reports decreased for the second consecutive quarter. This was a 2.9% decrease in CAT 5 incidents compared to the previous quarter. The percentage of Malicious Code incidents increased by 3.3%.

Figure 1: Incidents and Events by Category

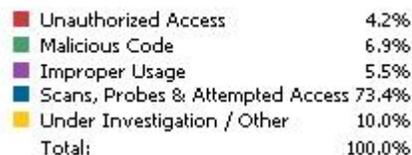
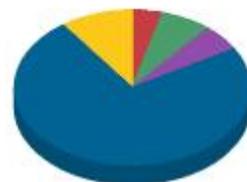
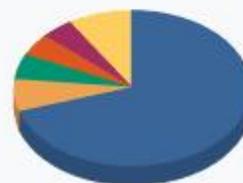


Figure 2 is a breakdown of the top five incidents and events versus all others. Phishing remained the most prevalent incident type, accounting for 70% of all incidents reported. This was a slight percentage decrease of 1.8% from the previous quarter.

US-CERT encourages all users and organizations to report any activities that you feel meet the criteria for an incident. To learn more about incidents, visit <https://forms.us-cert.gov/report/>. To report phishing, visit http://www.us-cert.gov/nav/report_phishing.html.

Figure 2: Top Five Incidents vs. All Others



Torpig Trojan

In November 2008, public reports were circulating regarding the compromise of a high volume of financial accounts by new variants of the Torpig (aka Sinowal or Anserin) Trojan. The Torpig Trojan was first identified in 2006, but new variants have appeared since then.

This Trojan uses HTML injection to add fields to web pages to convince users to provide additional credentials or financial account information. Compromised systems were used by attackers to obtain banking information, FTP credentials, email addresses, and digital certificates of the current user.

The new Torpig variant is delivered via the Neosploit attack framework, with operating system, web-browser, and third-party application vulnerabilities as potential entry points. Upon successful installation, the Torpig Trojan attempts to modify the master boot record (MBR) to make it more difficult to detect. The MBR code, commonly referred to as Mebroot, can read memory and execute tasks before the operating system is fully loaded. This rootkit contains configuration information for the Trojan as well as techniques used to keep it undetectable. Torpig injects new web pages or information fields into the affected victim's web browser, which appear legitimate to the user, that then prompts the user to enter additional personal information. This is done when a victim visits a website that has been specified in the Trojan's configuration file.

Proliferation of Malware via Removable Media

US-CERT released a Current Activity update on its public website (www.us-cert.gov) on November 20, 2008, to notify users that it was aware of public reports¹ of an increase in malicious code propagating via USB flash drive devices. The Current Activity entry encouraged users to review Cyber Security Tip ST08-001, [Using Caution with USB Drives](#), and CERT's Vulnerability Analysis Blog entry, [The Dangers of Windows AutoRun](#), for recommendations to help mitigate the risks.

Because of their small size, portability, and reasonable price, USB drives have become a popular method of storing and transporting data from one computer system to another. An attacker can introduce malware onto a computer that detects when a USB device is plugged in; the malware then automatically downloads itself to the USB drive.

¹ https://forums.symantec.com/t5/blogs/blogarticlepage/blog-id/malicious_code/article-id/220

There are two commonly used methods used to propagate malware to USB flash drives. The first of these methods is referred to as simple file copy. This means that the malicious code initially resides on an infected computer and copies itself to all the storage devices connected to the affected computer. This method requires the user to access the USB drive and execute the malicious code.

The second method modifies the Windows AutoRun.inf feature that allows USB devices to automatically load content when inserted into a system. In this case the malicious code alters or creates an autorun.inf file on targeted storage devices connected to the affected computer. When an infected USB device is connected to another computer, the malicious code can be automatically executed with no additional user interaction. The infected device may also reintroduce the infection onto a previously cleaned system.

Microsoft has since released recommendations for disabling AutoRun.inf in an article entitled *How to correct "disable Autorun registry key" enforcement in Windows*.²

Phishing and Spamming Trends

Shutdown of Malicious Web-Hosting Firm

In November 2008, the shutdown of the web-hosting firm, McColo Corp., caused a dramatic yet temporary decrease in spam distribution. McColo had been identified as a leading producer of online scams and spam. Internet providers terminated their connections to McColo after becoming aware of the firm's malicious activities.³ This led to a sharp decrease in the percentage of spam compared to total email volume from approximately 75% to 55%, according to data compiled by Symantec.⁴ This reduction was short-lived; however, as spam volume gradually increased through December 2008 as spammers transitioned their operations to other web-hosting firms willing to offer services. According to McAfee, spam levels were still lower than the period prior to the shutdown of McColo during December.⁵ Spam levels began to regain their previous levels in January 2009.⁶

² <http://support.microsoft.com/kb/967715>

³ http://voices.washingtonpost.com/securityfix/2008/11/major_source_of_online_scams_a.html

⁴ http://eval.symantec.com/mktginfo/enterprise/other_resource/s/b-state_of_spam_report_01-2009.en-us.pdf

⁵ http://www.mcafee.com/us/local_content/reports/mfe_spam_report_jan09.pdf

⁶ http://www.pcworld.com/article/158326/after_mccolo_taked_own_spam_surges_again.html?tk=rss_news

Current Events and Holidays

Spam and phishing campaigns continued to coincide with major news headlines and the holiday season. Examples include activity related to bank acquisitions, the presidential election, malicious electronic greeting cards, and airline tickets. Many campaigns also coincide with vulnerabilities that have been recently patched, such as Adobe Flash Player and Reader.⁷

Other phishing campaigns

Other phishing campaigns involved propagation via social networking sites. One campaign used an email that contained a message that instructed users to follow a link to view a YouTube video. If users clicked on the link, they would be prompted to download malicious code disguised as an update to Adobe Flash Player.⁸

Additionally, public reports of a fraudulent email scam circulated during November 2008 that falsely appeared to originate from the U.S. Federal Reserve. These email messages contained information about a phishing scam and links for users to follow to obtain additional information about the scam. If users follow the links, they will be redirected to a malicious website where a PDF exploit is used to install malicious code on the affected system.

National Cyber Alert System

Stay informed and involved by subscribing to the products included in the US-CERT National Cyber Alert System (NCAS). There are five products available for various technical levels and needs. They are as follows:

Current Activity – Notifies users of the most frequent, high-impact types of security incidents currently reported to US-CERT.

Technical Cyber Security Alerts – Provides timely information about current security issues, vulnerabilities, and exploits.

Cyber Security Bulletins – Summarizes information that has been published about new vulnerabilities.

Cyber Security Alerts – Alerts non-technical readers to security issues that affect the general public.

Cyber Security Tips – Provides information and advice for non-technical readers about a variety of common security topics.

Visit <http://www.us-cert.gov/cas/signup.html> to learn more

⁷<http://www.kb.cert.org/vuls/id/593409>

⁸http://www.us-cert.gov/current/archive/2008/12/16/archive.html#malware_spreading_via_social_networking

Contacting US-CERT

If you would like to contact US-CERT to ask a question, submit an incident, provide a tip of suspicious activity, or just learn more about cyber security, please use one of the below methods.

If you would like to provide feedback on this report, or if you have comments or suggestions for future reports, please email info@us-cert.gov.

Web Site Address:	http://www.us-cert.gov
Email Address:	info@us-cert.gov
Phone Number:	+1 (888) 282-0870
PGP Key ID:	CF5B48C2
PGP Key Fingerprint:	01F1 9C58 0817 D612 45ED 3FCF 3004 FE8C CF5B 48C2
PGP Key:	https://www.us-cert.gov/pgp/info.asc

Disclaimer

The purpose of the analysis within this report is to provide awareness and information on cyber threats as seen and reported to US-CERT. The content of this report was developed with the best information available at the time of analysis; if further information becomes available, US-CERT may publish it in a future report.