US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

February 20, 2008
Volume 3, Issue 1

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 2008 first quarter (FY08 Q1), that is, the period of October 1, 2007 to December 31, 2007.

US-CERT is a partnership between the Department of Homeland Security (DHS) and the public and private sectors. Established in 2003 to protect the nation's internet infrastructure, US-CERT coordinates defense against and responses to cyber attacks across the nation. The organization interacts with federal agencies, state and local governments, industry professionals, and others to improve information sharing and incident response coordination and to reduce cyber threats and vulnerabilities.

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

INSIDE THIS ISSUE

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.

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 2008 first quarter (FY08 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 *successfully* 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	*Successful* 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 *not* required to report malicious logic that has been *successfully quarantined* 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	*Unconfirmed* 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 large number of category 5 reports can be attributed to the high number of phishing incidents that US-CERT received from its constituents and the general public.

Consistent with the previous quarter's reporting, category 5 and 6 incidents accounted for just over 75% of all incidents reported to US-CERT.

Figure 1: Incidents by Category

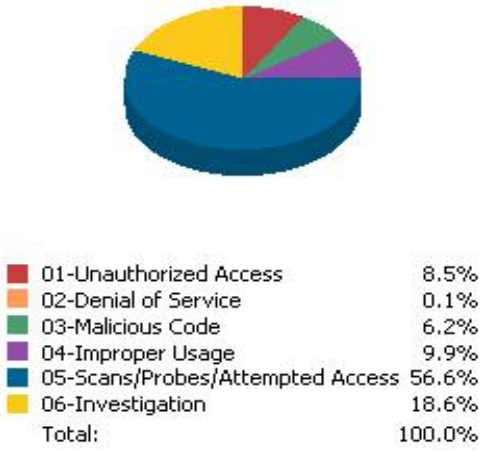
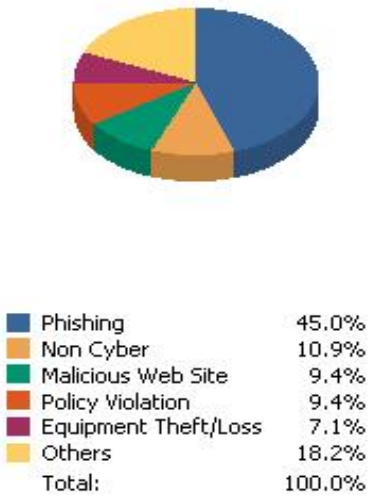


Figure 2 is a breakdown of the top five incidents and events versus all others. The top incident type reported to US-CERT was phishing, accounting for 45% of all incidents reported.

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



Malware Authors Target Mobile Phones

The growing popularity of mobile phones as computing tools has prompted malware authors to create exploits that target these phones. Recently, there were two high profile incidents involving malware that targeted well-known mobile phone carriers.

In early January, the first Trojan targeting Apple iPhone users was identified. Viewed as more of a prank than an actual threat, the Trojan reportedly targeted iPhones that had been modified to allow for the installation of third-party applications. The website hosting the malware was quickly removed, but the incident highlights the importance of securing mobile devices.

In a separate incident, a worm surfaced that was targeting mobile devices running SymbianOS. The worm, dubbed SymbOS/Beselo.A!, disguised itself under media file extensions with names such as Beauty.jpg, Sex.mp3 and Love.rm. Affecting multiple mobile carriers, this worm propagated by sending malicious files to the contacts listed in an infected phone. Several vendors have offered anti-virus updates and disinfection tools for users who think they may have been compromised.

Cyber security is no longer limited to protecting your computer or devices within your organization. These two incidents highlight the need to protect your mobile devices and remain vigilant against unknown messages, prompts, or files. Attacks such as these can damage your mobile device (i.e., making it inoperable) and/or be used by an attacker to gain remote access to the device to steal sensitive or personally identifiable information (PII).

US-CERT reminds users to review the following recommendations for protecting your mobile device:

- Disable functions you don't use (IrDA, Bluetooth, etc.).
- Secure the functions you do use (VPN, WPA, etc.).
- Create a mobile device security policy (acceptable usage, hardening guidelines, and termination policies).
- Use additional security features where possible (password protection, firewalls, and anti-virus software).
- Use encryption if you plan on storing any sensitive information on your mobile device.
- Avoid storing or transmitting sensitive or PII related information if additional security measures or encryption cannot be enabled.

Additional information can also be found in US-CERT Cyber Security Tip ST04-020, "Protecting Portable Devices: Data Security."

FBI Announces Results of Bot Roast II

In late November, the FBI announced the results of the second phase of its continuing investigation into a growing and serious problem involving the criminal use of botnets. Botnets are armies of computers that have been remotely taken over by attackers after they have installed malicious software on compromised systems without the owner's knowledge. Attackers leverage botnets to help them conduct malicious activity, such as denial-of-service attacks, mass spam campaigns, and identity theft scams.

Since Operation Bot Roast was announced last June, eight individuals have been indicted, pled guilty, or been sentenced for crimes related to botnet activity. Additionally, thirteen search warrants were served in the U.S. and overseas in connection with this operation. Though damage is still being assessed, it is anticipated that there will be more than $20 million in economic loss and more than one million victim computers discovered during Bot Roast II.

US-CERT works closely with the FBI to investigate and identify cyber criminals and threats. This collaboration is integral in defending America's internet infrastructure.

Users are encouraged to practice safe computing by ensuring updated anti-virus software, strong passwords, firewalls, and caution in opening email attachments, especially from unknown individuals.

US-CERT and the FBI will continue to monitor this activity and provide updates as needed. For more information on the scope and progress of Operation Bot Roast II, please visit: http://www.fbi.gov/page2/nov07/botnet112907.html.

Storm Worm and Botnet Activity Update

During the winter holidays, US-CERT noted an increase in Storm Worm related activity centering on Christmas and New Year's themed messages and attachments. Not surprisingly, the latest activity involved messages that contained romantic or Valentine's Day greetings. As with previous Storm Worm emails, the links direct users to malicious websites that attempt to exploit a variety of vulnerabilities and install malware onto users' systems.

Users are urged to be cautious of emails that focus on holidays, sporting events, elections, natural disasters, and other noteworthy current events.

Another botnet, known as Nugache[1] for the worm that is used to infect systems, has grown quickly over the past several months. Some researchers feel that it may even rival the Storm Worm botnet in the coming year.[2] Nugache features many of the same sophisticated levels of development, customization, and adaptability of Storm Worm. Like Storm Worm, Nugache operates over peer-to-peer (P2P) networks with highly decentralized command and control functions. According to a PC World article, the hackers behind this worm recently gave Nugache a facelift, copying many of the successful characteristics of Storm Worm, such as encryption, rootkit functionality, and the ability to spread as web-borne malware.[3]

Botnets, such as Storm Worm and Nugache, have spawned a new trend of botnet services for hire. Spamming services through Nugache botnets have been advertised for as little as $100 per 1 million messages.[4]

US-CERT reminds users of the following preventative measures to help mitigate the security risks when working with email:

- Do not trust unsolicited email.
- Do not click links in unsolicited email messages.
- Install anti-virus software, and keep its virus signature files up-to-date.
- Block executable and unknown file types at the email gateway.
- Employ the use of a spam filter.

For more information, refer to the following US-CERT documents:

- FY2007- Q3- Public Trends and Analysis Report (Storm Worm write up)
- Recognizing and Avoiding Email Scams
- Avoiding Social Engineering and Phishing Attacks
- Technical Trends in Phishing Attacks

Phishing Update

The Anti-Phishing Working Group (APWG) recently reported that the number of unique phishing-based Trojans (keyloggers) in October 2007 was the highest on record for the past year with 359, almost twice that detected by APWG in September. Phishing-based Trojans are used to collect information about the user in order to steal that user's credentials for access to financial based websites, ecommerce sites, and web-based mail sites.[5]

The APWG also reported that 34,266 unique phishing websites were identified in October 2007, an increase of over 6,200 from September. APWG attributes this increase to one financial institution that was targeted more than usual. Not surprisingly, financial institutions continue to be the most targeted sector, making up 92.5% of all phishing attacks in October 2007.

Spear Phishing

Spear phishing exploits use highly targeted, socially engineered email messages to trick recipients into providing usernames and passwords, or opening attachments that contain malicious code. Unlike regular spam or phishing attacks, which are sent out to the masses, these emails are sent to individuals or smaller groups of employees at specific organizations. The sender's email address is often spoofed to appear to come from a trusted source, such as government agency, company employee or department, or another familiar source. Because they spoof the identity of a trusted source, these messages appear to be legitimate. The information required to spoof identities can come from various open sources such as public forums, online publications, or social networking sites. It can also come from lost or stolen electronic devices. For more information on limiting the amount of personal information that gets posted online, refer to US-CERT Cyber Security Tip ST05-013 "Guidelines for Publishing Information Online."

1 http://www.symantec.com/security_response/writeup.jsp?docid=2006-043016-0900-99

2 http://www.pcworld.com/article/id,141134-c,worms/article.html

3 http://www.pcworld.com/article/id,141134-c,worms/article.html

4 http://www.darkreading.com/document.asp?doc_id=142690&WT.svl=news2_1

5http://www.antiphishing.org/reports/apwg_report_oct_2007.pdf

Examples of spear phishing from this quarter include:

- Malicious hackers used spear phishing tactics to gain access to data at a national laboratory. Employees at the lab received a variety of emails that appeared to be genuine, directing them to open attachments purporting to contain information about an upcoming scientific conference or a complaint filed with the Federal Trade Commission (FTC).
- Individuals with commercial bank accounts in the United States., the United Kingdom, and other countries were the targets of spear phishing attacks attempting to gain access to their accounts in order to wire large sums of money to criminal groups.[6]
- Employees at a medical center in Georgia received email notification of their job termination. The emails provided a link to a website that allegedly offered career counseling. Instead, users who clicked on the link unwittingly downloaded and installed a keylogger program onto the medical center's computers.[7]

Despite security awareness training and organizational guidelines or policies in place, some users still open email and attachments from malicious sources. Users cite carelessness, not paying attention to warnings, and curiosity as reasons for opening malicious email.[8]

US-CERT reminds users that if you are not certain if an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website referred to in the request; rather, check previous statements or credit cards for contact information.

Department of Justice Phishing Attacks

US-CERT recently reported on a phishing campaign that involved targeted email messages claiming to be from the Department of Justice (DOJ). A DOJ template was used in these attacks. The messages were designed to convince recipients that they were the subject of a business complaint filed through the DOJ. Initial reports indicated that as many as 20,000 users had been targeted, representing a wide range of companies in the US, Canada, and Australia.

The Department of Justice released a statement on its website indicating that it does not, and would not send that type of information to the public via email. The statement includes an example of the template being used.

To help protect against this type of attack, US-CERT recommends that users never open attachments or click on links contained in unsolicited email messages. More information on how to avoid becoming a victim of such an attack can be found in the US-CERT Cyber Security Tips Using Caution with Email Attachments and Avoiding Social Engineering and Phishing Attacks.

You can report phishing to US-CERT by sending an email to phishing-report@us-cert.gov.

To learn more about avoiding social engineering and phishing attacks, refer to US-CERT Cyber Security Tip ST04-014.

The National Cyber Alert System

Stay informed and involved by subscribing to the products included in the US-CERT National Cyber Alert System. 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 – Provide timely information about current security issues, vulnerabilities, and exploits.

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

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

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

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

6 http://www.theregister.co.uk/2007/12/17/prg_bank_trojan/

7 http://www.networkworld.com/news/2006/110106-spam-spear-phishing.html

8 http://cio-asia.com/ShowPage.aspx?pagetype=2&articleid=6907&pubid=5&issueid=126 or http://www.technewsworld.com/story/60520.html

Monthly Activity Summary

US-CERT has a created a new product to summarize general activity as well as updates made to the National Cyber Alert System on a monthly basis. The information provided in this report includes current activity updates, technical and non-technical cyber security alerts, cyber security bulletins, and cyber security tips, in addition to recapping newsworthy events or highlights. It can be found on the US-CERT website in Security Publications under Monthly and Quarterly Reports.

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:	0x17B1C7F7
PGP Key Fingerprint:	3219 08A0 716E 50DA 3ECF 501D 6780 28A0 17B1 C7F7
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.