US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

May 29, 2008
Volume 3, Issue 2

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 second quarter (FY08 Q2), that is, the period of January 1, 2008 to March 31, 2008.

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 second quarter (FY08 Q2).

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.

Category 5 reports increased 21% from the previous quarter. This increase is due to a higher number of phishing incidents reported that involved scams related to the U.S. Internal Revenue Service, including those related to the tax filing deadline and the economic stimulus rebate checks.

Figure 1: Incidents and Events by Category

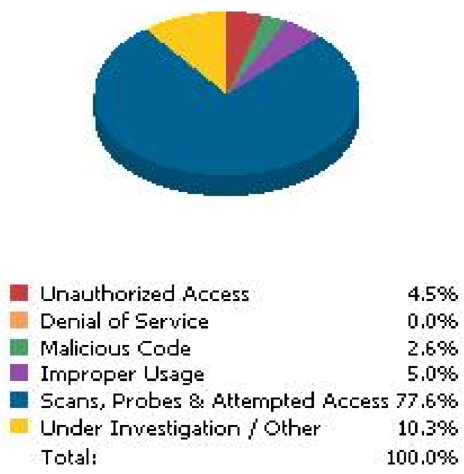
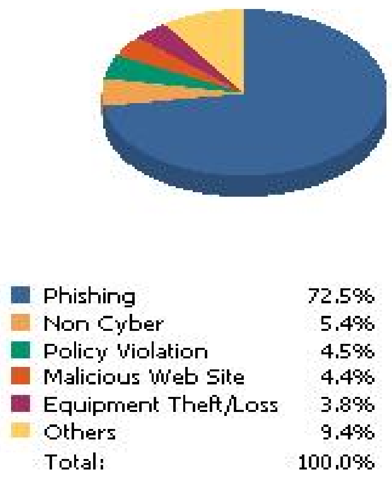


Figure 2 is a breakdown of the top five incidents and events versus all others. The top incident type reported to US-CERT was phishing, accounting for just over 72% of all incidents reported.

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



Massive Website Infections

US-CERT has been following reports of widespread attacks that have compromised thousands of web pages since the beginning of the year. The attacks use a variety of techniques including SQL injection attacks that enable attackers to insert malicious JavaScript files into legitimate web pages, and search engine IFRAME attacks.

SQL Injection Attacks

In early March 2008, US-CERT reported on a large-scale attack affecting more than 10,000 web pages. The attack involved injecting script into valid web pages to include a reference to a malicious JavaScript (.js) file. Users who visited any of these infected websites may have unknowingly executed malicious code.

Unfortunately, these attacks continue to infect vulnerable web pages in an attempt to infect users with malware or steal passwords from unsuspecting users.

Search Engine IFRAME Attacks

US-CERT has also received reports of attackers using specially crafted URLs that inject IFRAMEs as terms into search engines on legitimate websites. The affected URLs included popular search terms that were being elevated by attackers manipulating page rank algorithms within search engines (called Search Engine Optimization (SEO) poisoning). If the site hosting the search engine was vulnerable to cross-site scripting, users who followed the affected URLs may have unknowingly been redirected to malicious websites. These sites would then attempt to exploit web browser vulnerabilities, entice users to download and install malicious code, or display unsolicited advertisements.

It's important to note that with both of these attacks, many of the affected web pages have since been sanitized. However, it's likely that some are still affected and hosting malicious code. US-CERT recommends maintaining up-to-date patches and disabling JavaScript and ActiveX as described in the Securing Your Web Browser document.

For more information on these attacks, refer to the Current Activity page on the US-CERT website (www.us-cert.gov).

Cyber Storm II

From March 10-14, 2008, the Department of Homeland Security (DHS) sponsored Cyber Storm II, the largest cyber security exercise ever organized. Thousands of players took part in the multimillion-dollar exercise, which included representatives from four foreign governments, nine states, 18 federal agencies, and 40 private companies. In addition, Information Sharing and Analysis Centers (ISACs) from multiple critical infrastructure sectors participated.

The purpose of Cyber Storm II was to examine the processes, procedures, tools, and organizational responses to a multi-sector coordinated attack through, and on, the global cyber infrastructure. Hundreds of planners spent 18 months designing exercise scenarios modeled after real world challenges and developing nearly 1,800 "injects." These injects were specific pieces of information regarding an event that might require players to respond or share information through the proper channels. Injects were delivered via email, fax, telephone, exercise websites, and occasionally, in person. These injects simulated adverse effects through which the participants were able to exercise their cyber crisis response systems, policies, and procedures.

Now that Cyber Storm II is over, DHS is hosting several post-exercise conferences to discuss the findings and finalize an After Action Report. In addition, each participating organization will assess its own performance and develop a plan of action for strengthening its cyber security.

The final report on Cyber Storm II should be released at the end of the summer and will be published on this website when available.

Symantec and Microsoft Publish Security Trends Reports

In April 2008, Symantec and Microsoft published their security threat and trends reports for the second half of 2007. The reports include security highlights and attack trends related to software vulnerabilities and exploits, malicious code, phishing, and general security breaches. The reports also provide recommendations and best practices strategies.

The reports are compiled from data that is collected and analyzed throughout the six month time period. Symantec gathers data from more than 40,000 sensors monitoring networks in over 180 countries through their products and services as well as third-party sources. Microsoft gathers data from multiple vulnerability databases, third party sources, and reports provided by various Microsoft security tools.

More information can be found in the Microsoft Security Intelligence Report and Symantec Internet Security Threat Report.

Phishing Update

The Anti-Phishing Working Group (APWG) recently released its Phishing Trends Activity report for January 2008. One of the report's key findings indicates that 364 unique keylogger crimeware variants were detected in January – a record high. Consistent with previous months, financial services continue to be the most targeted sector accounting for 92.4% of all phishing attacks in January 2008. Additionally, the number of phishing reports submitted to APWG increased by more than 3,600 reports from the previous month, for a total of 29,284 in January 2008.

Q2 Summary of Activity

US-CERT published current activity updates on a variety of phishing scams affecting the general public this past quarter:

- Email attacks related to the U.S. presidential election - these email messages instructed users to follow a link to download a video of a candidate interview. If a user clicked this link, an executable file would be downloaded that contained the malware "Trojan.Srizbi."

- Storm Worm emails - some new variants contained romantic or Valentine's Day greetings. If users clicked the link provided, they were directed to a malicious website that attempted to exploit a variety of vulnerabilities and install malware onto the users' systems.

- A series of email scams related to the United States Internal Revenue Service (IRS) - the first set of phishing emails were related to the tax filing deadline and attempted to convince users to open bogus tax documents that may have contained malicious code, follow a link to an unofficial tax website that contained malicious code or requested personal information, or call an unofficial phone number that requested personal information. Another scam involved the IRS economic stimulus rebate and attempted to convince users to follow a link to a website before a deadline to expedite the rebate process.

Phishing Forecast - Beware of Charity Scams

Recent natural disasters happening domestically and internationally have led to an increased need for charitable donations. Unfortunately, scammers often create bogus charities to take advantage of people's desire to help those in need. US-CERT warns users to be cautious of emails claiming to be from charitable organizations. These emails may contain malware or links to fraudulent sites that request personal or financial information from unsuspecting users.

US-CERT recommends reviewing the Federal Trade Commission's Charity Checklist before you react to any request for charity. Further sources of information include the Better Business Bureau's (BBB) National Charity Report Index . This index provides extensive information about registered charities. You can request information from the BBB about charities that do not appear in the index by completing a form on the website.

US-CERT further recommends that users never open attachments or click 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.

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 learn more.

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.