US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

June 1, 2007
Volume 2, 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 2007 second quarter (FY07 Q2), that is, the period of January 1, 2007 to March 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 2007 second quarter (FY07 Q2).

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

Table 1: Federal Agency Incident & Event Categories

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.

The percentage distribution remains similar to last quarter's statistics with category 4 and 6 incidents rounding out the top three and accounting for 90% of all incidents reported.

Figure 1: Incidents by Category

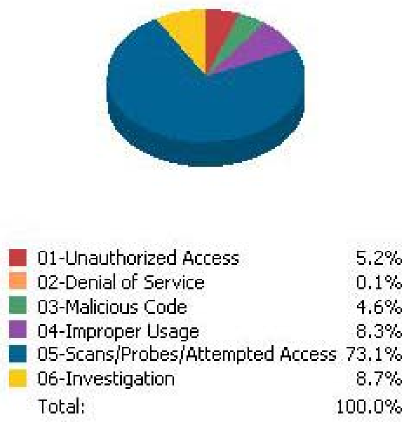
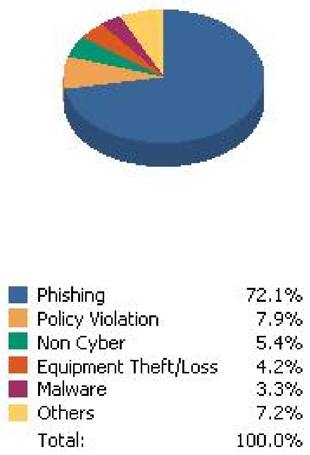


Figure 2 is a breakdown of the top five incidents and events versus all others. The top incident type reported to US-CERT was phishing, making up 72% of all incidents reported. The number of phishing reports continues to remain steady, while the number of unique phishing sites detected by the Anti-Phishing Working Group experienced staggering growth in April. Please see page 4 in this report for more details and a phishing update.

Policy violation was the second most reported incident, and includes the usage of unauthorized applications such as filesharing software and anonymizing software. More information about the risk of filesharing technologies can be found in US-CERT security tip http://www.us-cert.gov/cas/tips/ST05-007.html .

Figure 2: Top Five Incidents vs. All Others



Protecting your Mobile Computing Device

Overview

They allow you to stay connected, on top of things, and in the know. Most people have at least one. Many have more than one. Mobile computing devices such as laptops, cell phones, PDAs, smartphones, and other wireless-enabled devices are now considered commonplace business tools, allowing users to stay connected from almost anywhere, anytime. However, while these devices provide convenience and functionality, they also introduce new risks and considerations.

Why is it important to secure these devices?

Devices that were once considered "safe" are now a target for thieves and cyber criminals. According to the 11th annual CSI/FBI Computer Crime and Security Survey, the top four threats responsible for 74% of all financial losses are

1. virus attacks
2. unauthorized access to networks
3. lost or stolen laptops or mobile hardware
4. theft of proprietary information or intellectual property

In addition, an unsecured device could allow an attacker to harvest your personal information such as financial account information, passwords, and other sensitive information.

How do I secure my mobile computing device?

Physical Security

Make sure to secure your portable devices to protect both the machine and the information it contains. Ways in which you can do so include the following:

- Keep an inventory of your mobile devices.
- Use physical security devices (branding, alarm, laptop lock, privacy filter, etc.).
- Store you devices in a locking car trunk, securing the mobile device to the trunk lid when possible.
- Conceal your laptop or PDA: There is no need to advertise to thieves that you have a laptop or PDA.
- Avoid using your portable device in public areas, and consider a non-traditional bag such as a backpack for carrying your laptop.
- Destroy the mobile device at the end of its lifecycle if the information cannot be completely removed from the device.
- Understand and have available the procedure for reporting a lost/stolen device.

Protecting your data

In addition to taking precautions to protect your portable devices, it is important to add another layer of security by protecting the data itself. Ways to do so include the following:

- Create a mobile device security policy (acceptable usage, hardening guidelines, and termination policies).
- Use additional security features where possible, such as a firewall and anti-virus.
- Consider a vulnerability assessment (including a wireless assessment) of your mobile devices and architecture.
- Change the default password and enable password protection using a strong password (mix of upper/lowercase characters, 8 or more characters, symbols, etc.).
- Backup your information to a fixed source (i.e., network file server), not another mobile device (e.g., thumb drive and/or external hard drive).
- Consider using file or whole disk encryption where possible if you plan on storing any sensitive information on your mobile device.

Protecting your communications

Other techniques for securing your device include the following:

- Disable functions you don't use (IRDA, Bluetooth, etc.).
- Secure the functions you do use (VPN, WPA, etc.).
- Enable encryption within your mail client.
- Avoid synchronizing across multiple sources (thumb drive, camera memory card, laptop, desktop, home PC) to avoid cross-contamination.
- Use encryption when transmitting sensitive information.

What are some things I should avoid doing?

Don't …

- leave your mobile device unattended at a conference, in the office, etc.

Protecting Mobile Devices, Cont.

- install third party applications that are not approved by your IT department.
- sell/donate your used mobile device without first wiping it electronically and/or removing memory cards or electronic media.
- store sensitive, personal information on or with your mobile device (ATM PIN, social security numbers, passwords, etc.) in a briefcase or purse since access to one will give you access to the other.
- load production data (credit card numbers or social security numbers) onto your mobile device for a client presentation.

When you think about cybersecurity, remember that mobile computing devices are also vulnerable to theft or cyber attack. Take the appropriate precautions to limit your risk.

Additional Information can be found in the following US-CERT cyber security tips

Cyber Security Tip ST04-017 “Protecting Portable Devices: Physical Security”http://www.us-cert.gov/cas/tips/ST04-017.html

Cyber Security Tip ST04-020 “Protecting Portable Devices: Data Security”http://www.us-cert.gov/cas/tips/ST04-020.html

Cyber Security Tip ST05-011 “Effectively Erasing Files” http://www.us-cert.gov/cas/tips/ST05-011.html

Phishing Update

In a report published by the Anti-Phishing Working Group (APWG),[1] the number of unique phishing web sites in April was the highest on record, with 55,643 detected by the APWG. The massive 166% increase from the previous month was attributed to phishers using the tactic of putting a large number of phishing URLs on the same domain. This has led to a staggering 400% increase in unique phishing sites from the same time period during the previous year.

The financial services sector continues to be the most targeted, with more convincing web sites luring users in an attempt to steal passwords and infect PCs.

Recent Phishing Schemes

The Better Business Bureau (BBB)

In March, the Better Business Bureau (BBB) issued an alert[2] to warn businesses and consumers of a new phishing scheme that spoofs a BBB email address to lure users into following malicious links. Spoofing, a common practice for phishers and spammers, makes their emails appear as though they originated from a legitimate source.

The email contains a malicious attachment that, when opened, downloads a keylogging Trojan horse program. What makes this particular phishing scheme so effective is that it targets specific individuals and includes the company name, and, in some cases, an executive’s name and email address in the body of the email. Various reports, not confirmed by US-CERT, indicate that as many as 1,400 executives PCs have been infected via this phishing email.

The Internal Revenue Service (IRS)

On May 30, the Internal Revenue Service (IRS) released an alert[3] warning taxpayers about the latest versions of an email scam intended to fool people into believing they are under investigation by the agency’s Criminal Investigation division.

According to the alert, the email (falsely) states that the recipient is under a criminal probe for submitting a false tax return to the California Franchise Tax Board. The email seeks to entice recipients to click on a link or open an attachment to learn more information about the complaint against them. The IRS warned people that the email link and attachment is a Trojan horse that can take over the recipient’s computer hard drive and provide the attackers remote access to the computer.

The IRS has urged people not to click the link in the email or open the attachment. Similar email variations suggest a customer has filed a complaint against a company and the IRS can act as an arbitrator. The latest versions appear aimed at business taxpayers as well as individual taxpayers.

It’s important to note that the IRS does not send unsolicited emails or ask for detailed personal and financial information. Additionally, the IRS never asks people for their PIN numbers, passwords, or similar

[1] http://www.antiphishing.org/reports/apwg_report_april_2007.pdf

[2] http://www.bbb.org/alerts/article.asp?ID=754

[3] http://www.irs.gov/newsroom/article/0,,id=170894,00.html

Phishing Update, Cont.

secret access information for their credit card, bank, or other financial accounts.

US-CERT, along with the IRS and the Treasury Inspector General for Tax Administration, have worked with various Internet service providers and international CERT teams to have the phishing sites taken offline as soon as they are reported.

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

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

To learn more about avoiding social engineering and phishing attacks, see US-CERT Cyber Security Tip http://www.us-cert.gov/cas/tips/ST04-014.html.

All about Web Feeds

You've seen the icons before: they're everywhere on the web, allowing you to receive up-to-date information from various media sources or websites. Web feeds such as RSS and Atom are becoming popular with web enthusiasts. Most major media websites offer them, and newcomers in academia and the medical fields have also begun to embrace their usage. US-CERT also offers RSS and Atom feeds as an alternate way to receive a variety of notifications including:

- Current Activity updates
- Vulnerability Notes
- Technical Alerts
- Security Tips
- Non-Technical Alerts
- Security Bulletins

Why would I want to subscribe to RSS feeds?

RSS and RSS-type feeds save you the trouble of going to various web sites to look for new articles and information. Instead, RSS (Really Simple Syndication) feeds send this information to you. By subscribing to a feed, you choose which topic or information you're interested in and receive notification when new content about this topic is available. Using your RSS reader or RSS-enabled web browser, you can quickly scan your feeds for the information you want.

For instance, let's say you have lived in Los Angeles, New York, and Chicago and you want to keep up with local news in each of these cities. To get this news, you could go to the *Los Angeles Times*, *Chicago Tribune Review*, and *New York Times* web sites individually and browse each paper's local news section. This could take a lot of time. By subscribing to the RSS feeds for each paper's local news, you could receive local headline feeds from all three papers and quickly scan them for articles that interest you.

What exactly is a "feed?"

A feed is a summary of new web site articles. It's published to people who choose to receive it by subscribing to the feed. This summary is usually a list of titles that link to full articles, and may sometimes include the first line or two of each article. The RSS and Atom buttons on the US-CERT web site show what content is available through US-CERT feeds.

What are RSS and Atom?

RSS and Atom are the feed formats used by US-CERT. They were chosen because most RSS readers understand these formats.

What is an RSS reader?

RSS readers (also called RSS aggregators) allow you to subscribe to feeds. The RSS reader will download and display the feeds you select. A number of free and commercial readers are available on the web for download. You can also subscribe to feeds using a web browser that has the reader software built in, or using a web-based RSS reader.

How do I subscribe to a US-CERT feed?

There are a number of ways to subscribe to US-CERT feeds. The following are the most common:

- **Subscribe using an RSS-enabled browser -** Some web browsers, such as Mozilla Firefox, include the ability to subscribe to RSS feeds. Using Firefox, look for the orange icon in the bottom right corner of the Firefox browser window, and then click it to subscribe to either the RSS or Atom feed. Microsoft's Internet Explorer 7 automatically detects RSS feeds on

All about Web Feeds, Cont.

sites and illuminates an icon on the toolbar. A single click on the icon allows you to preview and subscribe to the RSS feed.

- **Subscribe using a "stand-alone" RSS reader** - A growing number of RSS reader programs are available on the web for download. A web search on the terms "RSS download. A web search on the terms "RSS reader" will provide you a number of choices. Download and install the reader of your choice, browse to US-CERT pages containing the feeds you're interested in, and subscribe by following the instructions in your RSS reader's help file.
- **Subscribe through a web-based reader** - Some major web sites provide registered users the ability to subscribe to RSS feeds. For instance, Yahoo! does so through its My Yahoo! service and Google is testing its Google Reader. These readers are comparatively simple to use. Registered users of these sites should see the sites' help pages to learn about using these web-based RSS readers.

To subscribe to a US-CERT RSS or Atom feed, visit http://www.us-cert.gov/cas/signup.html.

Stay Informed

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

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.

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.

Produced 2007 by US-CERT, a government organization.