US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

December 3, 2007
Volume 2, Issue 4

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 fourth quarter (FY07 Q4), that is, the period of July 1, 2007 to September 30, 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 fourth quarter (FY07 Q4).

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.

Category 6 was the second most reported category, with the majority of incidents opened by US-CERT analysts investigating Einstein Program data. Together, category 5 and 6 accounted for 75% of all incidents reported to US-CERT.

Figure 1: Incidents by Category

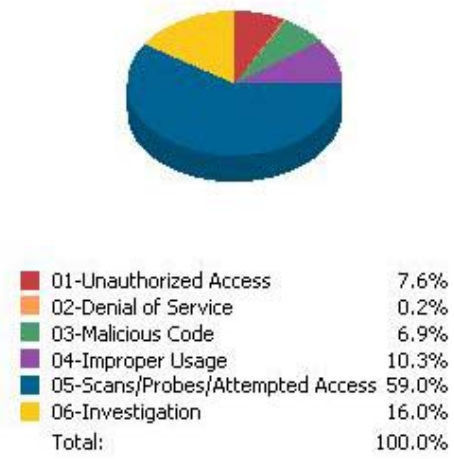
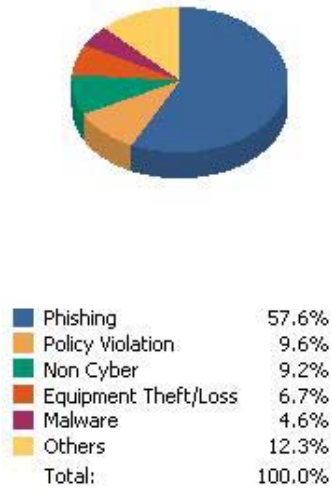


Figure 2 is a breakdown of the top five incidents and events versus all others as reported to US-CERT.

Not surprisingly, phishing incidents accounted to nearly 60% off all incidents reported in Q4.

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



Holiday Guide to Staying Safe Online

Introduction

The ease of online shopping during the holiday season attracts millions of consumers looking for hassle-free shopping away from the holiday crowds. But before you begin your online search, make sure that you are staying safe online.

This guide reviews the basic steps for securing your computer, describes phishing scams, and offers tips for how to shop online safely.

Reviewing the Basics

Whether you're shopping or just surfing the internet, let's review some of the basics for securing your computer:

- Check to make sure that your anti-virus and anti-spyware software is up to date.
- Always ensure that your system is fully patched.
- Install and use a firewall.
- Disable nonessential services, such as file and print sharing.
- Avoid using an open or unencrypted wireless connection to prevent drive-by hackers from intercepting your data.
- Use strong passwords for your computer and online accounts.

For more detailed information on any of these tips, refer to the Securing Your Home Computer document located on the US-CERT web site.

Recognizing Phishing Emails

During the holiday season, the fraudsters come out in full force, trying to capitalize on the high volume of online shopping and charitable donations. Scammers use a variety of phishing techniques to lure users into divulging personal information for exploitation. The following scams are examples of some of the more prevalent phishing tactics seen during the holidays:

- **Online purchase confirmations.** These false confirmations typically trick users into divulging their account information by asking for confirmation of an item they allegedly purchased. These usually include links to fraudulent web sites posing as legitimate ones where users are asked to enter their account information.
- **User account confirmations.** Another scam urges users to confirm their financial account information to avoid having their accounts deleted. Much like the online purchase confirmations, these account confirmation scams attempt to trick users into submitting their information for scammers to exploit.
- **Electronic greeting cards.** Specially crafted e-greeting cards can trick users into unwittingly installing rootkits or other malware on their computers simply by clicking the links. The e-greeting cards will likely be from unknown or anonymous senders.
- **Charity themed scams**. These scams defraud users in a variety of ways. They can pose as requests for recent disaster relief efforts or requests for holiday donations. The scams may be accompanied by a tragic story or plea for help to appeal to the user's sympathy.

US-CERT reminds users NOT to open unsolicited emails. This measure alone will greatly minimize your chances of falling victim to a phishing scam. In addition, users should treat all email attachments with caution and scan documents before opening them.

Shopping Online

So now you are ready to do your shopping, but where do you start? How do you know whom to trust? When shopping online, remember that the cheapest sites are not necessarily the best ones. Examine all factors including reviews, popularity, encryption standards, shipping costs, and return policies. Before you hand over your credit card information, keep these tips in mind:

- When possible, shop from known or trusted web sites.
- Only shop on web sites that use encryption technology such as SSL (Secure Sockets Layer) certificates to prevent hackers from accessing your data. SSL Certificates are issued by a certificate authority who certifies the identities of web site owners. They also encrypt sensitive information during the transaction process. Unfortunately, some hackers have created ways to fake certificates on malicious web sites. To learn more about certificates, including how to verify authenticity, visit http://www.us-cert.gov/cas/tips/ST05-010.html.

Holiday Guide to Staying Safe Online Cont'd

- If you are unsure of where to shop, there are many web sites, including most major search engines, that offer product and web site comparisons. These sites provide user reviews and ratings that are useful in determining where to buy your gifts.
- If you are planning to make a purchase from an online auction web site, examine the seller before you place a bid. Look for sellers who have a higher volume of transactions and are top rated. You should also read their user feedback to find out how others rated their buying experience.

Making the Purchase

Now that you are ready to buy and have researched the web site, make sure you know the following before completing your transaction:

- Review all of the terms and conditions before making a purchase. Verify shipping costs, the shipping date, and the vendor's privacy, order cancellation, and return policies.
- Make sure that you are able to locate a physical address and phone number for the seller in case there is a problem processing your transaction.
- Use your credit card, not your debit card. Most banks offer credit protection policies to limit your financial loss should theft of that card number occur. With your debit card, you are exposing your bank account to greater risk and may not have the same mitigation advantages as a credit card.
- Never enter your information in a pop-up screen. Hackers can use them to intercept your online session while legitimate sites will never use pop-ups to request personal information.
- Before you enter credit card information, look for http**s**:// in the address bar to indicate a secure session has been initiated. Some web sites will also display a closed padlock or unbroken key at the bottom corner of your browser screen.
- Beware of online escrow fraud for larger ticket items. Auction scammers may try to redirect you to a phony escrow site that closely resembles a legitimate site such as PayPal. The phony site will collect payment information but will provide nothing in return. Find more information about phony escrow sites at:

  http://www.bbb.org/Alerts/article.asp?ID=600
  http://www.escrow-fraud.com/
  https://www.escrow.com/fic/ficspot.asp

After the Purchase

- Print out the order confirmation page and keep a record of all purchases so that you can confirm that your items have arrived and have been billed for accurately.
- Log out after your transaction is complete and never share your passwords with others.

Additional Resources

To stay on top of the latest cyber alerts, tips, and news, visit the National Cyber Alert System located at http://www.us-cert.gov/cas/signup.html.

If your merchandise fails to arrive or you have a problem with the vendor you can file a complaint with the Federal Trade Commission at https://rn.ftc.gov/pls/dod/wsolcq$.startup?Z_ORG_CODE=PU01.

Investigate charities before you give to ensure that they are legitimate and will use your donation wisely. The Federal Trade Commission lists some tips on avoiding charity fraud at http://www.ftc.gov/opa/2005/01/charitychecklist.shtm.

The following web sites provide more information about staying safe online during the holiday season.

http://www.staysafeonline.org/news/2006nclncsashoppingtips.html

http://www.bbb.org/ALERTS/article.asp?ID=636

http://onguardonline.gov/index.html

http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt082.shtm

General Trends

Application Attacks become More Prevalent

Today's internet browsing experience is much more engaging with multimedia content, visually appealing design, and interactive features. As a result, malware authors and operators have been utilizing more exploits that target common third-party plug-ins as opposed to attacking vulnerabilities in Internet Explorer or MS Windows operating system. Apple QuickTime, Adobe Flash, and Adobe Acrobat plug-ins were all found to have multiple critical vulnerabilities, which were then

General Trends Con't

exploited by multiple malware packages, including some variants of the Storm Worm, MPack, and others.

Since a great deal of web content now requires plug-ins to operate properly, US-CERT recommends ensuring all software installed on a computer is updated on a regular basis. Users should be made aware that any untrusted content could lead to a system compromise.

Widespread Usage of Professional Malware Toolkits

Several "all-in-one" web attack toolkits such as MPack and IcePack have become more popular in recent months. These toolkits contain a variety of exploits for known and zero-day vulnerabilities, and are sold in underground forums. These tools run a client-aware exploit server, which allows the operator to customize attacks based on victims' system configurations. Victims are usually directed to the toolkit's download server(s) by a redirection script on a compromised web page or by following malicious links in e-mail.

US-CERT recommends timely patching of all systems, maintaining up-to-date AV and Intrusion Detection System (IDS) protection with both signature and behavior-based detection capabilities, and implementing best practices for securing all public web servers against compromise or defacement.

Money Mule Scams

The increase in phishing attacks and identity theft highlights the growing trend that scammers have taken in recruiting "money mules" to launder money for them. These money mules allow scammers to circumvent the restrictions most financial institutions place on international electronic transfers and provide scammers with a means for receiving stolen money or goods to their overseas locations or bank accounts.

Scammers recruit victims, often under the guise of "work from home" job opportunities, to process payments and transfer funds, offering them a small percentage of each transaction. These fraudulent job opportunities are presented in numerous ways. Some scammers have created legitimate looking web sites that include jobs with titles such as "sales representative" or "transfer manager." Most victims are unaware that they are being used to process illegal transactions or that they could face legal consequences if caught and prosecuted.

Victims who fall prey are asked to provide their financial account numbers so that money can be transferred into their accounts. They are then asked to transfer money to the scammers' accounts, often using a wire transfer service. In return, the money mules are given a percentage per transaction or fee for each transfer made. Sometimes, money mules are set up to receive stolen goods and then ship them to new users. This masks the identity of the scammers and allows them to launder the money involved in the transactions.

In late August 2007, Monster.com and USAJOBS.com alerted users to a database compromise that disclosed subscriber names, addresses, phone numbers, and email addresses to attackers. The attackers then used this information to target victims for money mule scams, sending specially crafted email messages appearing to be from Monster.com and USAJOBS.com. The emails guaranteed high monthly incomes and 10% of every money order/check that cleared. Aside from the "too good to be true" language used, the emails also contained many grammatical and spelling errors, which are indicative of many scam and phishing emails.

Job seekers who unknowingly fall victim to the money mule scam should be made aware of the legal ramifications and even the possibility of imprisonment. Law enforcement and investigative agents will likely focus on the money mules, rather than the scammers, because they are easier to trace. The originating scammers tend to close their accounts quickly and leave few traces behind. Money mules who are under investigation can expect to have their assets frozen during the investigation process.

In addition, money mules may become vulnerable to identity theft because they have typically given the scammers bank account and other personal information.

To avoid becoming a victim or participant in this scheme, users should do the following:

- Do not trust unsolicited email.
- Stay informed of phishing scams and tactics.
- Be wary of requests that offer easy ways to earn money, wire transfers, or other activity and sources that are difficult to verify.

For more information, please refer to the following:

Avoiding Social Engineering and Phishing Attacks

http://www.banksafeonline.org.uk/moneymule_explained.html

http://help.monster.com/besafe/email/

Phishing Update

Internal Revenue Service (FTC)

Two more phishing scams involving emails purporting to come from the IRS have been recently reported. According to the IRS, one of the emails solicits charitable donations to the recent Southern California wildfires, while the other email claims that the recipient is eligible for a tax refund. Both contain malicious links that direct the users to a fake IRS web site where they are asked to enter their personal information. The IRS reminds users not to open or click links in unsolicited emails. The IRS does not send emails to solicit charitable contributions. For more information, refer to http://www.irs.gov/newsroom/article/0,,id=170894,00.html

Federal Trade Commission (FTC)
In late October, the FTC warned users not to open emails claiming to be from the "Fraud Department." The emails reference a compliant filed against the recipient and contain malicious links that when clicked, download a virus to the user's computer. The emails appear to come from frauddep@ftc.gov and spoof the return-path and reply-to fields to hide the email's true origin. While the email includes the FTC seal, it has grammatical errors, misspellings, and incorrect syntax. For more information, visit http://www.ftc.gov/opa/2007/10/bogus.shtm.

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 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:	0x7C15DFB9
PGP Key Fingerprint:	673D 044E D62A 630F CDD5 F443 EF31 8090 7C15 DFB9
PGP Key:	https://www.us-cert.gov/pgp/info.asc

Contributors

The following US-CERT personnel contributed to this issue:

Monica Maher
Jonathan Lim
Mary O'Connell
Tim Millar

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.