US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

November 28, 2006
Volume 1, 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 2006 fourth quarter (FY06 Q4), that is, the period of July 1, 2006 to September 30th, 2006.

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 2006 fourth quarter (FY06 Q4).

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.

In the fourth quarter, 45.5% of all incidents reported were from federal agencies, and the remaining 54.5% were from non-federal reporting entities or individuals.

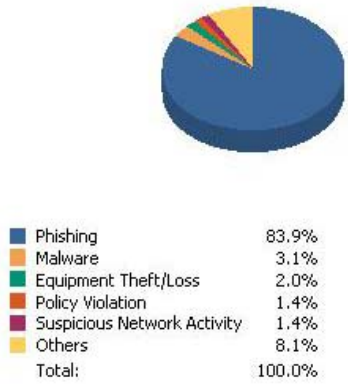
Figure 1 displays the overall distribution of cyber security incidents and events across the six major categories described in Table 1. The large number of category 5 reports can be attributed to the high number of phishing incidents that US-CERT received from its constituents and the general public.

Category 6 was the second most reported category, with the majority of investigations filed by US-CERT analysts reviewing collected data. Together, category 5 and 6 accounted for just over 90% of all incidents reported to US-CERT.

Figure 1: Incidents by Category

Figure 2 is a representative breakdown of the activity type as reported to US-CERT. As with Figure 1, phishing incidents made up the bulk of all incidents reported to US-CERT, accounting for 84% of all incidents handled. The second highest category was "others", the bulk of which generally fell into two main areas: investigations, which were incidents found by US-CERT analysts combing through data, and incidents involving personally identifiable information (PII) information, both cyber and non-cyber in nature. The remaining 8% of incidents were spread across malware, equipment theft/loss, policy violations, and suspicious network activity.

Figure 2: Top Five Incidents & Events vs. All Others



Zero-Day Exploits

What is a Zero-Day Exploit?

While the term "zero-day exploit" has been around for several years, the recent surge of zero-day activity has raised many questions for those tasked with safeguarding networks. A zero-day exploit is one that takes advantage of a security vulnerability previously unknown to the general public. In many cases, the exploit code is written by the same person who discovered the vulnerability. By writing an exploit for the previously unknown vulnerability, the attacker creates a potent threat since the compressed timeframe between public discoveries of both makes it extremely difficult to defend against. The critical nature of this exploit also puts the vendor in the spotlight with the pressure to create a fix as soon as possible.

This past September, a zero-day exploit affecting Microsoft's Vector Markup Language (VML) in Internet Explorer was reported. It enabled an attacker to run arbitrary code on an affected system. Fully patched Internet Explorer browsers (v. 5.0 and later) became vulnerable, and reports of infected websites began to grow. Shortly after discovery, the code was made public on the Internet, further providing any would-be attackers with the means to create their own variants and execute new attacks. During this time a third-party patch was released, generating controversy over whether or not organizations should use it. To protect its customer base and address public concern, Microsoft released an out-of-cycle patch to address the exploit.

The Value Proposition

The market for exploit information is a controversial topic that concerns all vendors. It's no secret that vendors encourage researchers to report security flaws directly to them as a matter of responsible disclosure. This gives the vendor an opportunity to publish a patch before news of the vulnerability has a chance to reach the public. Not surprisingly however, many researchers prefer other means of disclosure that offer industry recognition and/or compensation. A handful of companies have built programs around zero-day threats, offering compensation for exploit and vulnerability information. Their interest lies in using the information to protect their customer base, while alerting the affected vendor so that a patch can be created. Still, there are others who choose to trade or sell their information in the Internet black market, where hackers discuss techniques and toolkits for exploitation.

With the various channels of disclosure available, it's easy to understand why these exploits are growing in number. News of a new zero-day is a headline grabber in the cyber security world, translating into big business for those who author them.

Third-Party Patches and Risk Mitigation

The third-party patch that was recently released for the Microsoft VML exploit resurrected the debate over whether or not they should be applied. Some feel that the patches give the public an option for a temporary fix, while placing additional pressure on the vendor to patch the flaw. Others feel that the risks are unknown, making it too dangerous to introduce into their computing environment. Even some of the third-party patch creators agree that, when possible, it's always a good idea to wait for a vendor-supplied patch. US-CERT does not endorse the use of third-party patches for they are considered "buyer-beware" and could introduce new problems or configuration issues. Instead, US-CERT recommends that all organizations consider their options carefully and work with the vendor when faced with a zero-day threat.

Defending against zero-days is a difficult task for even the most vigilant administrator, or experienced computer user. Establishing and following best-practices is still the best defense in network security. These practices will help your organization decrease risks and determine incident response procedures should a compromise occur.

Emerging Threats

Blended Threats

US-CERT has seen an increase in the level of sophistication and complexity of attacks against the users. Blended threats combine several attack methods (viruses, worms, Trojans, etc.) to increase the level of destruction and reach. These threats often result in the loss of sensitive data and propagate quickly via multiple attack vectors.

Some examples of blended threats include

- Unsolicited email (spam) that has a malicious attachment or URL that either contains a Trojan or redirects to a malicious website where a Trojan is downloaded onto the user's computer

Emerging Threats, Con't

- Compromised wireless router firmware that has been reconfigured by an attacker to redirect unsuspecting users to a malicious website where personal or financial information can be captured

Threats to Electronic Devices

As previously reported, malicious code authors are increasing their attacks against various mobile electronic devices, such as MP3 players, PDAs, and other types of electronic devices.

In October, Apple posted a notification on their support site that a small number of video iPods were shipped with the Windows RavMonE.exe virus. Along with the notification, Apple quickly published links to allow potentially affected users to download trial versions of antivirus software packages to detect and destroy the worm.

In another example, McDonald's reported that 10,000 MP3 players were infected with a variant of the QQPass Trojan, which is configured to steal user passwords. The MP3 players were distributed as prizes for a contest that ran in various McDonald's locations throughout Japan. McDonald's has since recalled the 10,000 MP3 players and released software to remove the malicious code.

Phishing

The sophistication of phishing attacks continues to increase, with the bulk of phishing still directed toward the home user. Phishing gangs have emerged, using phishing toolkits such as "WebAttacker" or "Nuclear Grabber" (aka "Haxdoor") to compromise or create malicious websites that fool unsuspecting visitors. Users who are lured to a rigged website could have their system infected with a Trojan, allowing attackers to execute code and extract logins and passwords, steal bank account and other sensitive information, or take complete control of a system.

The Anti-Phishing Working Group (APWG) recently reported that the total number of unique phishing reports had increased nearly two fold since the same time last year. The same increase applied to the number of phishing sites detected with over 10,000 unique sites identified in August alone.

To learn more about the Anti-Phishing Working Group, or to view their Phishing Trends Report published in October, visit http://www.antiphishing.org/ .

Data Security and Privacy

In our previous report, we discussed protecting personally identifiable information (PII). For this edition, we will elaborate on one method cyber criminals use to steal PII: the keystroke logger, or keylogger attack.

A keylogger is surveillance hardware or software that records keystrokes in order to capture information typed on a keyboard. Keyloggers are run locally on a victim machine and are usually configured to capture specific keyword data or network sessions of interest (e.g., login screens), and pass the captured information to a file or drop-site accessible to the keylogger owner.

Keylogger software can be legally purchased and is often used by employers or parents to monitor the activities and surfing habits of their employees or children. However, keyloggers can also be embedded in spyware and used by attackers to perform a variety of nefarious actions, including stealing PII related information.

So how does keylogger software typically end up on a victim's machine? In the case of a malicious keylogger, installation usually occurs when a user opens an executable believed to be trustworthy, such as an email attachment. An attacker can also install software by exploiting an existing security vulnerability on a victim system.

If you know or think you have been infected with a keylogger, US-CERT recommends that you report your findings or suspicion to your IT department immediately. Your system administrators will be able to examine your PC and take measures to sanitize your system if a compromise has occurred.

If you are a home user, you can use keylogger detectors or anti-spyware programs to determine if your computer has been infected. If you are unsure or need additional assistance, US-CERT recommends that you seek a professional to assist with diagnostics and repair.

As always, US-CERT emphasizes the importance of preventative computer security measures to help avoid this and other types of attacks. Individuals can help protect themselves by following these safeguards:

- Think before you click: don't open emails, websites, or applications that you do not trust.
- Maintain updated antivirus signatures, and keep systems up to date with the latest patches.

Data Security and Privacy, Con't

- Utilize a personal firewall on home computers.
- Identify and encrypt all laptops, desktops, and removable media containing PII.
- Encrypt any PII that is electronically transmitted to ensure increased protection against loss of data.
- Check your credit report periodically to monitor for fraud; under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus.

For more information, visit

Recognizing and Avoiding Spyware
http://www.us-cert.gov/cas/tips/ST04-016.html

Coordinating Virus and Spyware Defense
http://www.us-cert.gov/cas/tips/ST06-009.html

New Incident Reporting Form

US-CERT has launched a new and improved Incident Reporting Form on the US-CERT web site. A critical function of US-CERT is to coordinate defense against, and response to, cyber attacks across the nation. Consequently, US-CERT relies on individuals not only within the federal government, but from all other organizations including home users to report suspicious cyber activities that qualify as an incident.

A good working definition of an incident is *the act of violating an explicit or implied security policy.* Unfortunately, this definition relies on the existence of a security policy that, while generally understood, varies among organizations. In general, types of activity commonly recognized as being in violation of a typical security policy include but are not limited to

- Attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information (PII)
- Unwanted disruption or denial of service
- The unauthorized use of a system for processing or storing data
- Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent

For the federal government, an incident, defined by NIST Special Publication 800-61, is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In addition, an executive order was released on July 12th requiring all federal agencies to report any incident involving the compromise of PII to US-CERT within one hour of discovery.

For more information about federal incident reporting guidelines, including definitions, incident categories, and reporting timeframes, visit http://www.us-cert.gov/federal/reportingRequirements.html.

The form uses Secure Sockets Layer (SSL) to provide secure communications for your information. As always, we will protect your information and keep anything specific to your site confidential.

To report an incident, visit https://forms.us-cert.gov/report/.

You can also report phishing-related scams or vulnerabilities by visiting www.us-cert.gov and clicking on the corresponding reporting button on the left.

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 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 2006 by US-CERT, a government organization.