US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

September 1, 2007
Volume 2, Issue 3

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 third quarter (FY07 Q3), that is, the period of April 1, 2007 to June 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 third quarter (FY07 Q3).

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.

Category 6 was the second most reported category, with the majority of investigations filed by US-CERT analysts. Together, category 5 and 6 accounted for just over 75% of all incidents reported to US-CERT.

Figure 1: Incidents by Category

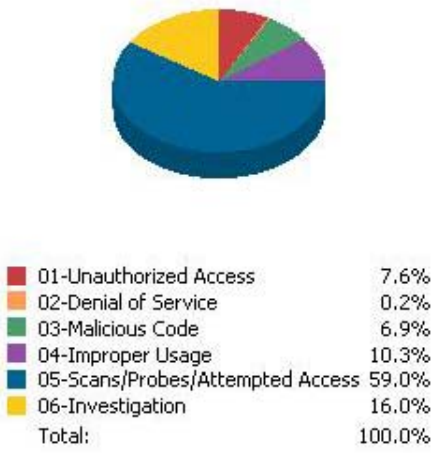
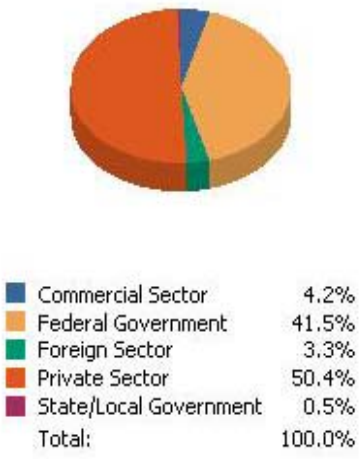


Figure 2 is a breakdown of the incidents reported to US-CERT by sector.

Private sector incidents accounted for 50.4% of all incidents reported in Q3, the majority of which can be attributed to home users who reported phishing incidents. The second highest sector was the federal government, which accounted for 41.5% 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: Incidents and Events by Sector



Social Engineering and the Storm Worm Trojan

Overview

Social Engineering has become a familiar term to most people. It is a strategy used by attackers to obtain sensitive information from unsuspecting victims. The strategy often involves taking advantage of human curiosity and desire for reward to manipulate users into performing actions that they wouldn't normally take. The Storm Worm Trojan exemplifies a social engineering attack that combined tempting email messages with a malware executable.

The Storm Worm Trojan

The Storm Worm Trojan, so named because it first appeared in email messages with subject lines claiming to include breaking news about inclement weather in Europe, is also known as W32/Small.DAM, W32/Zhelatin, or Trojan.Peacomm. The Trojan uses a peer-to-peer (P2P) control channel to download malicious code from infected hosts participating in the P2P network, which makes it more difficult to detect and shut down.

US-CERT has observed an evolving transformation in the tactics used by the Storm Worm to deceive and infect users. Earlier variants arrived as email attachments or links claiming to be electronic cards or patches that, once executed, downloaded the malware to a user's system. Newer propagation techniques include credential confirmation for membership-based sites and links to adult pictures.

Most recently, Storm Worm has taken on a new form in emails claiming that the user has been featured in a new video on YouTube.com. The emails contain a fake link that directs the user to a malicious web site that will attempt to download the Storm Worm Trojan by exploiting a variety of browser and application vulnerabilities.

Attacker Toolkits

The success and infection rate of the Storm Worm Trojan is due in part to the use of attacker toolkits such as MPack. These toolkits provide attackers with the ability to simplify and streamline the process of mass host compromise through the web. The MPack toolkit is a significant threat because it employs a variety of payload delivery options, exploit libraries, and a flexible attack framework that allows it to serve different downloads depending on the victim's browser type and version. Symantec has a write-up on the MPack that provides additional information about the toolkit.

Impact

Storm Worm infection results in the victim's system being added to a robot network (botnet) that can then be remotely controlled by an attacker. Botnets are networks of computer systems that have been compromised by malicious programs so that they can be remotely controlled to send spam, participate in Distributed Denial-of-Service (DDoS) attacks, and perform other malicious actions. The compromised systems are managed remotely through a command and control channel where the botnet's originator, sometimes called the "bot herder," can operate and unite them with other infected systems to increase their effectiveness and redundancy.

How to Avoid Falling Victim

All Storm Worm infections require the users to fall victim to social engineering tactics by opening malicious attachments or following malicious links. As such, US-CERT reminds users of the following preventative measures when working with email:

- Do NOT trust unsolicited email.
- Treat all email attachments with caution.
- Do NOT click links in unsolicited email messages.
- Install anti-virus software, and keep its virus signature files up-to-date.
- Turn off the option to automatically download attachments.
- Block executable and unknown file types at the email gateway.
- Configure your email client for security.
- Employ the use of a spam filter.

For additional information, refer to the following documents located on the US-CERT web site.

- Recognizing and Avoiding Email Scams
- Avoiding Social Engineering and Phishing Attacks
- Technical Trends in Phishing Attacks

Receiving PGP Signed Publications from US-CERT

US-CERT uses PGP (Pretty Good Privacy) signatures to sign all publications that are sent electronically. PGP provides verification that the sender's identity is true and that the message has not been altered. Some of US-CERT's publications that are signed and sent as part of an email distribution list include the following:

- Current Activity
- Cyber Security Alerts
- Technical Cyber Security Alerts
- Cyber Security Bulletins
- Cyber Security Tips

What is PGP?

PGP is an encryption program that uses mathematical algorithms to encrypt files, create digital signatures, and verify identities. Combinations of public keys, private keys, and passwords are used to encrypt and decrypt messages for the intended recipients. PGP was originally created as open source software to enable individuals to secure data and to protect individual privacy. It has since developed into several variations of open source and commercial software implemented across many public, private, and government organizations. The PGP Corporation claims that over 80,000 organizations worldwide have implemented some form of a PGP solution.

Verifying Signatures

Email messages sent from US-CERT are signed with the US-CERT PGP key. Users should validate the key at the end of the message with the key published on the US-CERT web site, http://www.us-cert.gov/pgp/email.html, to ensure the legitimacy of the email message. As a good security practice, users should always validate public keys they receive and should not trust non-validated keys. This is especially important because some public key servers include forged or expired keys.

PGP signatures can provide a strong form of identity verification in situations where fraudulent messages could cause harm. For instance, a malicious user could attempt to impersonate an authority figure or trusted individual to obtain sensitive information or disseminate false information. Simply by verifying the PGP signature of the message, a user could discover that the trusted individual did not send the message. Additional information is available at http://www.cert.org/archive/pdf/PGPsigs_paper2.pdf.

Web 2.0 Vulnerabilities

Today's users have a more robust and visually appealing web browsing experience because of improvements in web development techniques. Referred to as Web 2.0 in industry terms, these newer web sites behave much like interactive applications. Web 2.0 users can post blogs, ratings, comments, and multimedia content across sites. Some of these new generation web sites can run interactive games or maps, function as office applications, or provide real-time content feeds to subscribers. With this increased functionality comes an increased risk: these enhanced functions can introduce malicious code and steal sensitive information from unsuspecting users.

Features and Vulnerabilities

The robust features in Web 2.0 are enabled by web development techniques such as Cross-Site Scripting (XSS) and Asynchronous JavaScript and XML (AJAX). Attacks exploiting JavaScript and XSS have become prevalent. In a May 2007 report, the Common Vulnerabilities and Exposures (CVE) community found that XSS vulnerabilities had become the leading vulnerability type reported in 2005 and 2006. A search of the National Vulnerability Database (NVD) also shows the prevalence of Web 2.0 vulnerabilities. A three-month query (June-August) of the NVD yielded the results displayed in the following table. Please note that as CVE entries are updated, their categorization may change.

Common Vulnerability Exposures (CVE) June – August 2007	
Vulnerability Type	**Number of CVE's***
Cross Site Scripting (XSS)	*267*
ActiveX	*84*
JavaScript	*27*
XML	*17*

**Some CVE's may overlap*

Legitimate web sites using poor security practices can unwittingly host malicious JavaScript code. Earlier this year, Adobe released an update to repair a cross-site scripting vulnerability in the Adobe Acrobat Plug-In. This plug-in allows users to view PDF files inside of a web browser. The vulnerability had been exploited to allow user-supplied JavaScript to execute within the context of the web site hosting the PDF file, causing a cross-site scripting vulnerability. If successfully exploited, this now patched vulnerability could allow an attacker to gain access to sensitive information such as passwords and account numbers.

Web 2.0 Vulnerabilities Con't

Mitigation Steps

Disabling content functions such as ActiveX and JavaScript on web browsers can protect users from these types of vulnerabilities. However, disabling certain content functions also disables some of the functionality and aesthetics of certain Web 2.0 sites.

If users choose to keep those functions active, it is recommended that they use a firewall to monitor data transfers that they did not initiate, use anti-virus software with updated definitions, and avoid interacting with suspicious content or sites.

For more information on securing your web browser, refer to:
http://www.us-cert.gov/reading_room/securing_browser/

Phishing Update

IRS Phishing Updates

Previously reported in May, the Internal Revenue Service (IRS) released a warning to taxpayers about fraudulent emails. The fraudulent emails claimed that recipients were under investigation for submitting false tax returns to the California Franchise Tax Board. In actuality, those emails contained links or attachments to a Trojan horse program that could take control of the recipients' computers.

In June, more fraudulent email emerged under the guise of a "Tax Avoidance Investigation" allegedly conducted by the "IRS Fraud Department." A form included for the recipients to complete activated a Trojan horse program.

Most recently in August, the IRS issued a warning of another new phishing scam involving a customer satisfaction survey. These fraudulent messages claim that recipients could receive $80 by completing an online survey for the IRS. The IRS reiterates that these fraudulent emails should be ignored. The IRS does not initiate contact with taxpayers through email.

For further details, refer to the IRS article:
http://www.irs.gov/newsroom/article/0,,id=170894,00.html

Phishing Update Con't

Hurricane or Disaster-Related Scams

Each year during hurricane season, US-CERT reminds users to remain cautious of email messages containing requests for hurricane or disaster-related relief efforts. This type of scam became prevalent following the Hurricane Katrina disaster-relief efforts. The phishing emails appeared as requests from charitable organizations that asked users to click links that led to fraudulent sites posing as legitimate charities.

If an email request appears to be questionable, attempt to verify it by contacting the requesting organization directly. Do NOT use contact information provided in the request. Verify charitable organizations and their contact information through an independent source, such as http://www.give.org/reports/index.asp.

Users are encouraged to report phishing activities 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.

Stay Informed- New Current Activity Alerts Available!

Email Alerts

In addition to the National Cyber Alert System products (featured on the last page), US-CERT recently launched a new mailing list that allows users to receive Current Activity updates instantly in their inboxes. US-CERT's Current Activity provides up-to-date information about high-impact security events affecting the community at large. Current Activity is updated on an as-needed basis, which could be several times a week or several times a day. Subscribers can expect to receive one update for each entry published to the US-CERT web site.

Alerts via RSS or Atom

Users who wish to stay informed, but who do not want to receive emails, can subscribe to the Current Activity RSS (Really Simple Syndication) or Atom feeds. RSS and RSS-type feeds send information directly to subscribers, allowing them to avoid visiting a multitude

Stay Informed- New Current Activity Alerts Available!

of individual web sites. By subscribing to a feed, users choose topics and information of interest to them and receive notification when new content is available. Using an RSS reader or RSS-enabled web browser, users can quickly scan feeds for the information they want. To learn more, visit http://www.us-cert.gov/cas/signup.html.

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:	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.