US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

March 1, 2007
Volume 2, Issue 1

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 first quarter (FY07 Q1), that is, the period of October 1, 2006 to December 31, 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 2007 first quarter (FY07 Q1).

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. Together, category 5 and 6 accounted for just over 80% of all incidents reported to US-CERT.

Figure 1: Incidents by Category

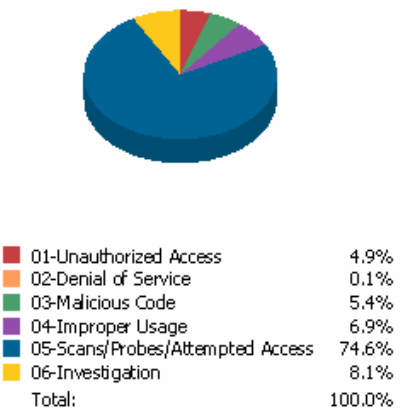
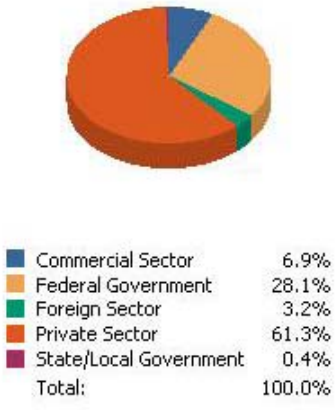


Figure 2 is a breakdown of the incidents reported to US-CERT by sector.

Private sector incidents accounted for 61.3% of all incidents reported in Q1, 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 28.1% 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



Daylight Saving Time Changes for 2007

Overview

The start and end dates for Daylight Saving Time (DST) will change this year in accordance with the Energy Policy Act of 2005, which goes into effect in 2007. With the new schedule, clocks will be set ahead one hour on the second Sunday of March and will be set back one hour on the first Sunday in November. The table below[1] highlights the changes and dates that will take place this year.

Change in Daylight Saving Time:			
Previously, DST started on:	**With the new law, DST will start on:**	**Previous DST ended on:**	**With the new law, DST will end on:**
First Sunday of April	Second Sunday of March	Last Sunday of October	First Sunday of November
Would have been: April 1, 2007	Will now be: March 11, 2007	Would have been: October 28, 2007	Will now be: November 4, 2007

The change will have an effect on and require updates to many computing systems that are time reliant. Below, we highlight the systems at risk and the scope of impact, along with updates required to avoid complications due to DST changes.

Scope of Impact

Many types of systems and devices may be vulnerable to the DST changes occurring this year. Any organization using software to perform scheduling, billing, transaction logging, and other time-related calculations is at risk if upgrades are not performed.

The impact of incorrect system time includes the following types of systems:

Authentication systems that rely on accurate local system time (e.g., Kerberos) can be negatively affected by incorrect time information. While typical deployments of these systems allow for some amount of clock skew, authentication can fail if the clocks are inaccurate. These systems typically “fail close,” denying authentication credentials to an otherwise valid user.

Time-based access control systems or software security systems that rely on accurate local system time may malfunction. This could result in a violation of security policy when access is erroneously granted at a time when it should be denied. Similarly, otherwise valid users may be denied access to systems when it should be granted.

Results from logging systems that provide time-stamped events (e.g., network intrusion detection systems) can be incorrect if the systems use local time. In some cases, this merely results in an inaccurate audit trail. In other cases, failures resulting in a violation of security policy can occur when consequential events are scheduled or programmed based on these results.

Errors can occur when interdependent systems within the same environment have different rules for when the time changes. This can occur in situations when one system has been updated with current time zone information and another has not.

Events scheduled to run automatically, such as those generated by the Unix "cron" system or Windows "Scheduled Tasks," could be run at incorrect times.

Hardware devices may have a preprogrammed schedule for adjusting to DST. This practice is common in many resource-constrained embedded devices. In some cases, this schedule can be changed by applying a firmware update, reconfiguring dual in-line package (DIP) switch settings, making changes through a management terminal port, or applying other physical modifications. Any system that includes an electronic clock with a hard-coded, unmodifiable schedule for adjusting to DST will become obsolete.

Enterprise time management applications for calendar and scheduling (e.g., Microsoft Exchange, Lotus Notes/Domino, and Oracle Collaboration Suite) may experience problems even with patches and the necessary updates. In most cases, manual updating of existing scheduling information will be required for events scheduled for the days within the extended DST period before the patches were made available. While the impact depends on the particular software, most of the major platforms are expected to share this problem.

Custom special-purpose applications that perform date and time calculations may be particularly at risk for suffering problems. Such applications are often expected to operate on both current and historic data and may not have been designed for changes such as

[1]http://support.microsoft.com/gp/dst_topissues

DST Changes for 2007, Cont.

this year's new DST schedule. The problem could be exacerbated if these applications were also designed or configured to store information in local time formats. Such applications may generate erroneous results if they are not reevaluated for the impact of the time change.

Key Recommendations

Vendors, particularly application software and operating system vendors, have been rolling out time-related updates, sometimes bundled with other high-priority updates. Systems maintained using sound patching practices are likely to already have the correct time zone information. Note that many large software systems, including database systems and application runtime environments (e.g., Java), provide their own time and date processing capabilities independent of the underlying operating system. Therefore, users and administrators should be sensitive to updates for all relevant software systems. Additionally, end-user devices that use special-purpose or proprietary operating systems, such as personal digital assistants (PDAs), should be updated with information about the new DST rules. While not updating these devices is unlikely to result in any negative security impact, calendars and other scheduling applications managed on these devices could suffer.

Whenever feasible, configure systems to record time in UTC, not local time. Unlike other time zones, which are subject to changes in local laws and regulations, UTC time is by definition invariant across the globe. Two synchronized clocks reading UTC will be identical regardless of their physical locations.

Ensure that time critical systems are synchronized using a reliable time source. The network time protocol (NTP), when properly configured, can provide a reliable solution. Note, however, that NTP only provides synchronization, ensuring that the relative difference between two clocks is small. The actual recorded time from a system using NTP is still subject to the local time zone setting of that system. Therefore, using NTP alone is inadequate to address the problems associated with the change in DST rules.

Vendor Information and Links

Most of the major IT vendors have web pages devoted to the DST changes occurring this year. They provide information about which products are affected by the DST changes, updates and workarounds, and helpful information to ease the transition. We have assembled a list of links to some of the major vendor's web sites.

US-CERT recommends that you visit the sites frequently as some of them will be updated as more information becomes available.

Apple
http://docs.info.apple.com/article.html?artnum=303411

Cisco
http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a00807ca437.shtml

IBM http://www-1.ibm.com/support/docview.wss?rs=899&uid=swg21245334

Juniper
http://kb.juniper.net/CUSTOMERSERVICE/index?page=kbdetail&record_id=02520301412e75010ed2ca5414006fc5

Microsoft
http://support.microsoft.com/gp/dst_topissues

Sun
http://sunsolve.sun.com/search/document.do?assetkey=1-26-102775-1

Symantec
http://service1.symantec.com/SUPPORT/tsgeninfo.nsf/docid/2007011911191539?Open&src=w&seg=hm&lg=en&ct=us

Summary

All organizations should prepare for the DST changeover by analyzing their systems and applying the appropriate updates. While the level of effort will vary widely across systems, platforms, and industries, every computing environment should be assessed for potential impact, as it is likely that most systems will require some pre-changeover action.

Emerging Threats

Drive-By Pharming

Security researchers at Symantec and Indiana University School of Informatics recently revealed that they have uncovered a serious new security threat for home

Emerging Threats, Cont.

broadband routers. The attack, dubbed drive-by pharming, allows an attacker to change the configuration of a home router when a user unknowingly visits a malicious web site. The web site employs malicious JavaScript code that allows an attacker to log into many types of home routers if the default password has not been changed. Once logged in, the attacker is able to change the configuration of the home router, including the domain name server (DNS) server settings.

This type of attack is of particular concern for several reasons:

- Simply viewing the malicious web page is all that is required for a user to fall victim to this attack.
- Many home users fail to change the default password on their broadband routers. The Symantec report indicates that 50% of all users could fall into this category.
- Changing the DNS server settings allows an attacker to redirect the home user to a DNS server of the attacker's choice. This includes a malicious server set up by the attacker to direct users to other malicious web sites where information such as financial account numbers, passwords, and other sensitive data can be stolen.

Symantec notes that home users can best defend against this type of attack by changing the default password on their broadband routers.

US-CERT also cautions users to avoid clicking on links sent in unsolicited emails. Users should also remain cautious when browsing the web and avoid visiting untrusted sites. More information can be found in the "Securing Your Web Browser" document.

To learn more, check vendor information for changing your password, or to view a flash-animation of the attack, visit http://www.symantec.com/enterprise/security_response/weblog/2007/02/driveby_pharming_how_clicking_1.html.

Botnets

While botnets themselves are not a new threat, the sophistication with which they attack and multiply has caught the attention of security researchers. Microsoft has cited botnets as the top threat to Windows users[1]. McAfee also recently cited botnets as one of the top threats for 2007[2]. Symantec, too, has recognized the threat, stating, "It's difficult to exaggerate how large a role bots play in cybercrime today[3]."

Described as an "army of zombies," botnets are computer systems compromised with malicious software that allows an attacker or central operator to control them for a variety of nefarious actions. Botnets are behind much of the spam that is sent, and are the culprits behind many malicious and illegal scams involving phishing, Trojan horse, and worm activity.

To learn more about botnets and other hidden threats, including what you can do to protect yourself, visit Cyber Security Tip http://www.us-cert.gov/cas/tips/ST06-001pr.html.

Phishing

Phishing continues to rise, with 76,480 phishing incidents reported to the Anti-Phishing Working Group (APWG) between Oct 1st and Dec. 31st (FY07 Q1). This is a 60% increase from the same period of time the year before. Perhaps more surprising is the exponential growth in the number of new phishing sites reported. The number of reports grew by over 500%, with just over 16,000 reports in FY06 Q1, compared to over 103,000 in FY07 Q1.

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. 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.

Groups such as the Anti-Phishing Working Group make information about known phishing attacks available online. To learn more about the Anti-Phishing Working Group, or to view its most recent Phishing Trends Report, visit http://www.antiphishing.org/.

[1]http://news.com.com/Microsoft+Zombies+most+prevalent+Windows+threat/2100-7349_3-6082615.html

[2]http://www.mcafee.com/us/about/press/corporate/2006/20061[3]129_080000_f.html

[3]http://www.symantec.com/avcenter/cybercrime/bots_page2.html

2007 GFIRST Conference–Registration is Open!

The Government Forum of Incident Response and Security Teams (GFIRST) will be hosting its third annual conference June 25-29, 2007 at the Buena Vista Palace Hotel, Orlando, Florida. The theme for this year's conference is **GFIRST: Working to Solve the Cyber Security Puzzle.**

Join top information security professionals and government leaders to hear expert speakers discuss the latest in cyber security.

Conference topics include:

- Emerging cyber threats and attacks
- Information-sharing groups, collaboration methods, and incident response teams
- Increasing situational awareness and improving monitoring, analysis, and intrusion detection practices
- Cyber security trends as seen by senior government leaders, law enforcement, and private industry
- The look ahead – bracing the future

Add to your conference experience by signing up for the Pre-Conference Training. Don't miss key classes taught by top professionals, such as:

- The Security Workshop for Mobile Devices
- Introduction to SCADA and Process Control Systems
- And more!

Seating is limited - Don't miss this important event!

For more information or to register, please visit www.us-cert.gov/gfirst

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 methods below.

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.