US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

September 1, 2006
Volume 1, Issue 1

QUARTERLY TRENDS AND ANALYSIS REPORT

www.us-cert.gov

Introduction

Welcome to the first edition of the United States Computer Emergency Readiness Team (US-CERT) Quarterly Trends and Analysis Report. This report summarizes and provides analysis of incident reports submitted to US-CERT during the U.S. Government fiscal year 2006 third quarter (FY06 Q3), that is, the period of April 1, 2006 to June 30th, 2006.

The 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. The report also provides information on notable security topics and trends, including emerging threats and updates to previous topics discussed in the issues.

Cyber Security Trends, Metrics, and Security Indicators

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.

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

Table 1: Federal Agency Incident & Event Categories

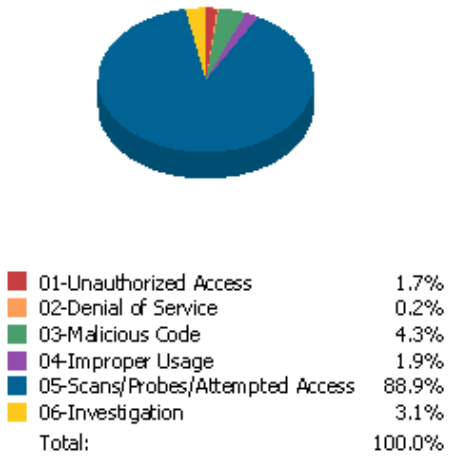
Category	Name	Description
CAT 1	Unauthorized Access	In this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource.
CAT 2	Denial of Service (DoS)	An attack that *successfully* prevents or impairs the normal 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, bots, 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.

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 third quarter (FY06 Q3).

US-CERT has seen a number of threats mature during the third quarter of FY06. Attackers have moved away from forceful, noisy attacks and more toward less detectable, "under the radar" methods.

Figure 1 displays the overall distribution of cyber security incidents and events across the six major categories described in Table 1.

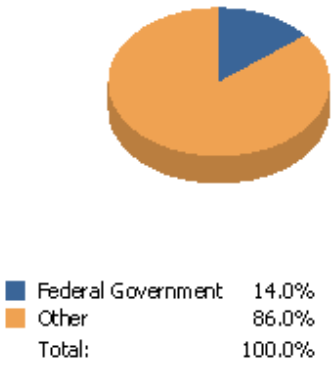
Figure 1: Incidents by Category



The large number of category 5 reports can be attributed to the high number of phishing incidents that are reported by non-government organizations, including foreign CERTs, private sector businesses, and home users.

Figure 2 displays the affected sector for all incidents reported.

Figure 2: Affected Sector for Total Incidents



DNS Recursion Update

US-CERT continues to investigate and warn of an increase in distributed denial-of-service (DDoS) attacks using spoofed recursive DNS requests. These attacks are troublesome because all systems communicating over the internet need to allow DNS traffic.

The attacks occur when a malicious attacker sends several thousand spoofed requests to a DNS server that allows recursion. The DNS server processes these requests as valid and then returns the DNS replies to the spoofed recipient (i.e., the victim). When the number of requests is in the thousands, the attacker could potentially generate a multi-gigabit flood of DNS replies. This is known as an *amplifier attack* because this method takes advantage of misconfigured DNS servers to reflect the attack onto a target while amplifying the volume of packets.

Potential Targets
Any system configured to provide DNS recursion is susceptible to this attack, including

- Windows systems running Domain Name Services
- Unix systems running Domain Name Services (BIND)
- DNS appliances (Infoblox, MiningWorks, BlueCat)
- Any device capable of proxying DNS lookups recursively, such as customer premises equipment (CPE)

In addition, the inbound network transport infrastructure is put at risk during such an attack because of the volume of traffic generated.

What can I do to protect my DNS servers from abuse?
Typically, DNS servers only provide DNS services to machines within a trusted domain. Restricting recursion and disabling the ability to send additional delegation information can help prevent DNS-based DDoS attacks and cache poisoning. It can also improve performance on your network by reducing the vulnerability of your DNS servers to use as a reflector in such an attack. Additionally, US-CERT recommends implementing filtering, described in Best Current Practice 38 (BCP-38,) to prohibit attackers from using forged source addresses that do not reside within a range of legitimately advertised prefixes.

Therefore, if an ISP is aggregating routing announcements for multiple downstream networks, strict traffic filtering should be used to prohibit traffic that claims to have originated from outside of these aggregated announcements. Implementing this type of filtering also enables the originator to be easily traced to its true source, since the attacker would have to use a valid, and legitimately reachable, source address.

For more information or for specific safety measures, please visit http://www.us-cert.gov/reading_room/DNS-recursion033006.pdf.

Emerging Threats

Microsoft Critical Security Update

On August 8th, Microsoft issued critical security update patches for multiple vulnerabilities in their Windows operating system that could have a significant impact on any users utilizing Windows platform. An attacker who successfully exploits these vulnerabilities could take control of an affected system(s) remotely and install programs, view, change, or delete data, or create new accounts with full user rights. Several of the vulnerabilities have a maximum severity rating of critical because they can be accessed remotely without user interaction, spread quickly to unpatched systems, and impact all critical infrastructure sectors.

US-CERT has been working closely with Microsoft to minimize the impact. US-CERT has also issued alerts via the National Cyber Alert System (see links below) and has conducted a series of briefings with Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs), as well as the critical infrastructure sectors through Information Sharing and Analysis Centers (ISACs). Additionally, all federal agencies are required to provide US-CERT with regular updates on their patching status.

US-CERT has recommended that all public and private organizations install the critical security patches developed by Microsoft not only to protect themselves, but also to prevent these vulnerabilities from being exploited. US-CERT is aware of active exploitation for one of the vulnerabilities and has further recommended that patches be installed as

Emerging Threats Con't

soon as possible. Information and links to the patches can be found at http://www.microsoft.com/technet/security/bulletin/ms06-040.mspx.

More information about these vulnerabilities can be found in Vulnerability Note http://www.kb.cert.org/vuls/id/650769

and Technical Cyber Security Alert http://www.us-cert.gov/cas/techalerts/TA06-220A.html

Reverse Proxy Attacks

Phishing email campaigns and web sites are expanding their reach and are now targeting a variety of institutions. One technique that is rising in popularity is known as a *reverse proxy attack.* In this type of attack, the HOSTS file on a user's system is modified to make certain web sites point to malicious copycat web sites. For example, assume the web site www.bankwebsite.com is supposed to point to 10.10.10.10. A reverse proxy attack would modify users systems to make www.bankwebsite.com point to 192.168.10.10. Then, when the users attempt to check their bank accounts at www.bankwebsite.com, they would be re-directed to a phishing site. This phishing site would likely mirror (proxy) the content from the real www.bankwebsite.com to appear as legitimate as possible. Report or learn more about phishing by visiting

http://www.us-cert.gov/nav/report_phishing.html.

Threats to Electronic Mobile Devices

Malicious code authors are increasing their attacks against various mobile electronic devices, such as cell phones and PDA's. In time, there may be a significant malicious code threat to mobile electronic devices, but as of the publication date of this report, the threat is still in its early stages.

Data Security and Privacy

US-CERT has been monitoring recent trends involving the acquisition of personally identifiable information (PII) by unauthorized, malicious users. PII is a term that is frequently associated with information security and privacy to indicate pieces of information that can be used as a point of reference for locating, identifying, or contacting an individual. It is information that helps to uniquely describe an individual. The following are examples of PII:

- Full name
- Email address
- Postal address
- Telephone number
- Driver's license number
- Unique physical characteristics such as face and fingerprints
- National Identification Number or Social Security Number

US-CERT recently received information regarding keystroke logger attacks on personal home computers, allowing PII information to be exposed. US-CERT emphasizes the importance of computer security for home users to avoid this type of attack. Individuals can help protect themselves by following these safeguards:

- Maintain updated antivirus signatures, and keep systems up to date with the latest patches
- Home users should utilize a personal firewall on home computers.
- All laptops, desktops and removable media containing PII should be identified and encrypted.
- Only discuss personal information with those individuals/companies who have a need to know.
- Dispose of personal mail or information appropriately (shred, burn, etc.).
- Any PII that is electronically transmitted should be encrypted to ensure increased protection against loss of data.
- Periodically check your credit report 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.

In situations where access to PII records is necessary, US-CERT recommends that proper safeguards and access controls be established. PII records should always be stored in a secure environment, and strictly adhered-to ground rules must be established for access to, checking-out, and checking-in such information.

Visit http://www.us-cert.gov/cas/tips/ST05-019.html for more information.

Stay Informed

Stay informed and involved by subscribing to the products included in the US-CERT National Cyber Alert System. There are four 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 sign or learn more.

Contacting US-CERT

US-CERT has made an effort to make communicating with our staff as easy and flexible as possible. Please use any of the below methods to submit an incident, ask a question, or provide a tip of suspicious activity to US-CERT.

Web Site Address:	http://www.us-cert.gov
Email Address:	info@us-cert.gov
Phone Number:	+1 (888) 282-0870
PGP Key ID:	0xF714B00
PGP Key Fingerprint:	DE1B B89B 0E79 1F79 9F29 92D6 5860 D02C F71F 4B00
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.