



X-Force Research & Development Newsletter

June 2006

Trends in Disclosure

Since the early days of ISS, our hardcore security researchers and analysts have been analyzing and cataloguing every vulnerability as it became known to the world. We continue this process today: providing daily analysis of the latest threats and adding this new vulnerability information to the X-Force Database (XFDB) — the largest and most authoritative vulnerability database in the world.

Since we began the XFDB, we have observed a number of significant trends in the public disclosure of vulnerabilities. For example, the number of vulnerabilities disclosed each year since 1997 has increased at an average of slightly more than 50 percent. Even last year, though relatively slow, saw a 32 percent increase over the previous year.

The ability to access such an extensive library of vulnerability information that goes back so many years makes it simpler to understand and identify new trends in vulnerabilities — particularly those related to public disclosure and exploitation. It is a unique advantage X-Force security analysts and researchers have at their beck and call.

In this month's X-Force Newsletter, we would like to share with you our analysis of security vulnerabilities since 1997 and why the day of the week in which they are publicly disclosed has recently changed.

Most Popular Day to Disclose

Most people assume that Friday is the most common day for vulnerability disclosure, but in reality, Friday is the quietest day of the work-week for new vulnerability disclosures.

Over the last nine years, the early part of the work-week has been more popular, with Wednesday as the most popular day for releasing vulnerability information (Figure 1).

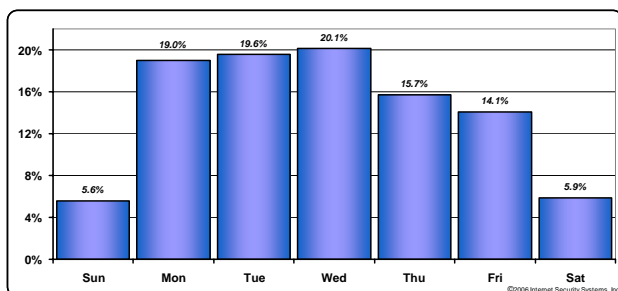


Figure 1. Day-of-week public disclosure, 1997-2005.

If we focus on just the Critical and High Risk vulnerabilities (Figure 2), we observe almost the same distribution except that the popularity of a Wednesday disclosure day is even more pronounced.

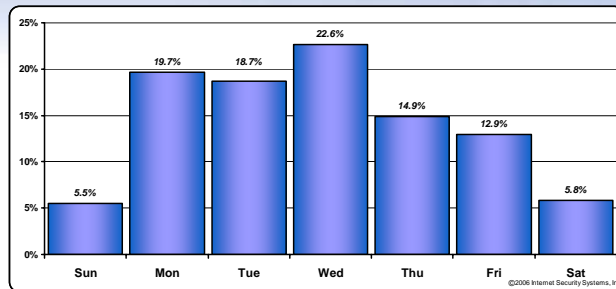


Figure 2. Day-of-week public disclosure, 1997-2005, Critical and High Risk Vulnerabilities

However, since the tail end of 2004, there has in fact been a steady migration away from the Wednesday disclosure day to one day earlier — Tuesday.

Ever since 2002, there has been a noticeable trend in which vulnerability discoverers and the vulnerable vendors have increasingly coordinated their disclosures with patch releases.

When Microsoft moved to a “Super-Tuesday” patch release cycle and worked hard to coordinate public vulnerability disclosures with the discoverers, it started the migration to Tuesday disclosures (see Figure 3).

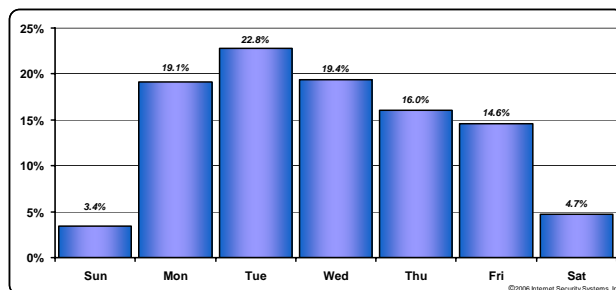


Figure 3. Day-of-week public disclosure, 2005

While some may contend that the overall move to Tuesday disclosures is purely due to the volume of Microsoft vulnerabilities, after removing all Microsoft vulnerabilities from our analysis the migration to Tuesday disclosures persists. X-Force expects Tuesday to continue to be the most popular disclosure day for 2006.

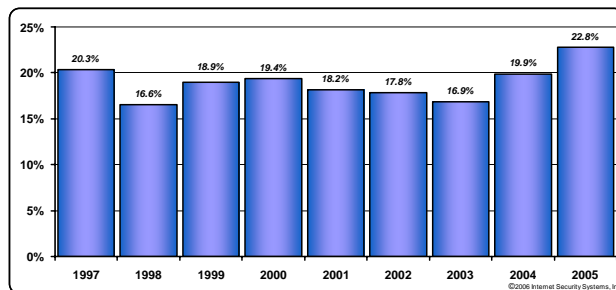


Figure 4. Tuesday disclosures since 1997

The move to disclosures earlier in the week is advantageous to most organizations as it gives them more time to fix the problem or roll out patches. But the cynical reader may associate Tuesdays with the day most frequently cited for press deadlines.

Consequently, a Tuesday disclosure helps ensure maximum media exposure for the vulnerability discoverers.

Bedroom Warriors and Weekend Disclosures

Just as Friday is mistakenly perceived to be a busy day for vulnerability disclosures, many security professionals are equally surprised to learn that weekends are not as popular as first thought.

While the overall number of High, Medium and Low Risk vulnerabilities has been increasing per annum, the number of weekend disclosures has remained relatively static (see Figures 5 and 6).

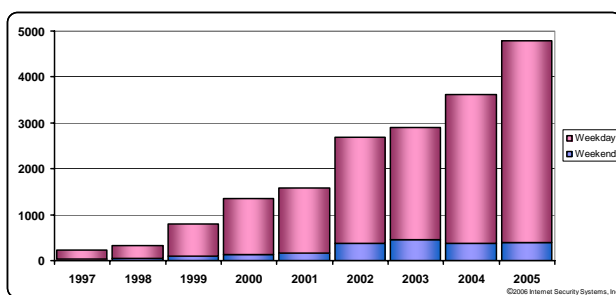


Figure 5. High, Medium and Low Risk vulnerabilities per annum by weekday and weekend

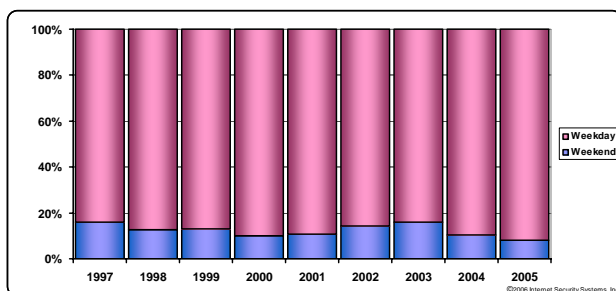


Figure 6. Percentage of weekend disclosures per annum

While the percentage of weekend vulnerability disclosures per annum is in decline (and expected to continue in 2006), it is important to acknowledge that the number of newly created exploits or malware tends to be much higher over weekends.

So, what does this mean for ISS customers and other enterprise organizations around the world? Ideally, they should ensure that their top security resources are available earlier in the week rather than at the end of the week. Finally, the best time to patch systems is at the end of the week (if using a weekly patching strategy) — ideally before the weekend.

– Gunter Ollmann, Director of X-Force

– Luann Johnson, Manager X-Force Research

Threat Research

How Does X-Force Test a Scanner Check?

In order to ensure that a scanner check is working correctly for either Internet Scanner or Enterprise Scanner, someone needs to test it for false positives and false negatives. The only way to do this is to execute the check against a large set of both Vulnerable and non-Vulnerable hosts, and verify the results. This, as I am sure you can imagine, requires a huge number of hosts and devices to scan against, as well as a comprehensive list of what is actually installed and running on each one. Fortunately for our customers, the X-Force has the largest vulnerability lab in the world.

X-Force maintains over 600 different systems in our test lab environment. The systems are all kept in pairs (often likened to Noah's Ark) — with one in a vulnerable state and the other not. Some of these host environments are on hardware that you cannot buy anymore, with versions of software that have been out of support for years — but that our customers still use! HP-UX on 64 bit processors? Got it! Windows 98? Got it!

The lab is the result of years and years of hoarding systems, building our ability to test the scanner checks and ensure that they are comprehensive and contain as few errors as possible. With a number of the older systems, X-Force is looking to back them up onto virtual hosts using VMWare, thus reducing our risk should one of them give up the ghost and leave us without the physical system to test. This project is proceeding apace, with several hundred VMWare images added to the labs on a monthly basis.

Each scanner check is tested by running it across the X-Force lab, with the results then correlated against the lab database. The lab database contains a list of every application and service pack installed on each of the hosts in the lab. False positives and negatives often have to be checked by hand, though, which involves logging onto the host in question and checking for the files or the vulnerable condition. For Enterprise Scanner, the X-Force goal is to have near-100 percent accuracy on the checks.

Our competition, which does not have labs like the X-Force lab, cannot compete with this accuracy, nor are they able to verify vulnerability checks if they do major upgrades to their core scanner engines.

If you would ever like to see the lab, come by and we will be glad to give you a tour.

– Steve Jenks, Manager X-Force QA

Malcode Corner

A Hidden Threat: Steganography

Consider the threat of intellectual property loss and its devastating effect in the corporate environment. Corporate e-mail in many organizations is monitored for keywords that may relate to various degrees of policy violations. E-mail messages that contain Microsoft Office or PDF documents draw scrutiny when sent outside the particular organization. Certainly, this potential for inspection is extremely undesirable for intellectual property theft. Using encryption utilities such as PGP may make it very difficult to determine the content being stolen; however, it is still an undesirable approach due to the additional attention it provokes. Optimally, for stealthy theft, stolen intellectual property would be undetectable during transmission.



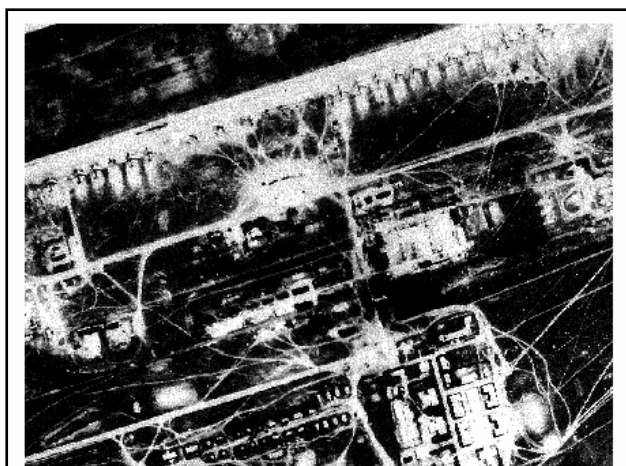
Steganography is both an art and a science by which information is encoded within other data with the hope of not drawing attention to it. While steganography may be used to hide information within any of a number of common computer file formats, the most common security concern is that criminals and terrorists may use it to conceal information within innocuous images that may be posted online, e-mailed or distributed through other means. Hence, it is the study of image steganography detection that has merited the most attention from X-Force.

Detection of steganographic content in images is difficult due to superior techniques for encoding hidden information in the JPEG image format. The JPEG format is special for a couple of reasons. First, it is clearly the most popular image format including among digital camera users. Second, by its nature it is a lossy compression format that can heavily compress the original image and still produce a relatively nice image upon decompression. This second reason enables the development of more

advanced algorithms to hide content than with lossless image formats.

Freeware utilities such as F5, JPHS, JSteg, Outguess and StegHide do a good job of hiding data in JPEG images. Today, commercial utilities for hiding content in JPEG images do not exist. However, there is a strong likelihood that better utilities are privately funded. There are a couple of reputable tools that can detect JPEGs with hidden content. These are WetStone Technologies' Stego Suite and Niels Provos' StegDetect. Stego Suite is an expensive commercial utility and there is not much online information on how well it works. StegDetect, on the other hand, is free and its source code is readily available. StegDetect's largest problem is that it produces a significant amount of false positives for JPHS and is somewhat weak in terms of detecting recent iterations of steganographic encoders. Both of these utilities work as digital forensics tools for local review only.

X-Force R&D has investigated JPEG steganography and discovered that commonly employed statistical analysis techniques for image detection can be improved. For example, StegDetect's main technique is highly redundant, with various filters to narrow down diagnoses to a particular encoder. This



approach has its downside — mediocre detection rates and high false positives on some steganographic encoders. By enhancing statistical analysis towards more encoder-neutral filtering, it is possible to obtain higher detection rates and lower false positives. Next, it is possible to detect the latest iterations of steganographic encoders at impressive rates by reinvigorating existing technology. The ability to detect this at the perimeter would enhance an organization's security toward reducing the threat of intellectual property loss by either blocking outgoing content or by flagging communications for further investigation.

— Robert Freeman, X-Force R&D Researcher

A Month in Review

In this section of the newsletter, X-Force briefly covers some of the security content developed or processed in the month of May.

Vulnerabilities:

Last month saw 618 new vulnerabilities being disclosed, processed and analyzed by X-Force. This represents a 30 percent increase compared with May last year.

Overall, thus far in 2006, X-Force has covered 36 percent more vulnerabilities than for the same period in 2005.

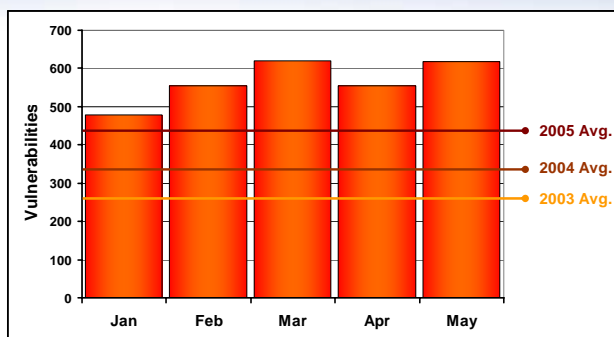
	Reported					YTD
	Crit.	High	Med.	Low	Total	
May	2	114	376	126	618	2825

Of these vulnerabilities, 564 were remotely exploitable, 69 could only be exploited locally and 15 could potentially be exploited both remotely or locally.

Vulnerability Breakdown	
Bypass Security	32
An attacker can bypass security restrictions such as a firewall or proxy, an IDS system or a virus scanner.	
Data Manipulation	74
An attacker is able to manipulate data stored or used by the host associated with the service or application.	
Denial of Service	43
An attacker can crash or hang a service or system, or take down a network.	
File Manipulation	6
An attacker can create, delete, read, modify or overwrite files.	
Gain Access	334
An attacker can obtain local and remote access. This also includes vulnerabilities in which an attacker can execute code or execute commands, because this usually allows the attacker to gain access to the system.	
Gain Privilege	30
An attacker can gain privileges on the local system only.	
Obtain Information	82
An attacker can obtain information such as file and path names, source code, passwords or server configuration details.	

* Right-hand column represents unique vulnerability count

Vulnerabilities per Month vs. Annual Average



Top 5 Vulnerable Vendors	
Apple	32
Microsoft	13
BEA	11
Linux Kernel	10
IBM	9

* Right-hand column represents unique vulnerability count

Whiro:

The Whiro 0-day Web crawler project was kept busy last month identifying and classifying hundreds of new Web sites that utilize exploits to compromise vulnerable Web browsers and install malware or other malicious material.

For the month of May, Whiro repeatedly identified exploits embedded within Web sites that targeted 11 vulnerabilities affecting Microsoft Internet Explorer. The following table lists these exploit attempts by prevalence:

Most Prevalent Web Exploits	
MS-ITS CHM file code execution (<i>MS04-013</i>)	*****
IE createTextRange() (<i>MS06-013</i>)	*****
RDS.Dataspace ActiveX (<i>MS06-014</i>)	****
IE javaprxy.dll COM object (<i>MS05-037</i>)	***
IE createControlRange() (<i>MS05-014</i>)	***
IE window() (<i>MS05-054</i>)	***
DHTML Objects (<i>MS05-020</i>)	**
IE COM Objects (<i>MS05-038</i>)	*
IE COM Objects (<i>MS05-052</i>)	*
Media Player BMP Handling (<i>MS06-005</i>)	*
IE Media Player Plugin (<i>MS06-006</i>)	*

Malcode:

In May, the X-Force alpha-testing platform for VPS (codename Catfish) identified 7 unique 0-day malcode attacks — i.e., before any other antivirus vendor. These 0-day threats comprised variants of four malcode families:

- 3 new variants of W32.Worm.Kidala – a derivative of the Mytob family of mass mailing worms
- 2 new variants of a W32.Downloader.Delf – each W32.Downloader.Delf variant attempts to download and execute two additional pieces of malware
- 2 downloader Trojans:
 - W32.Downloader.Agent.AMQ – downloads and executes a variant of W32.PWS.Goldun
 - W32.Downloader.Small.CIG

Sample Harvesting:

It is worth noting that as part of the X-Force continued strengthening of ISS antivirus, anti-spyware and anti-malware protection, we investigated and added another 35,222 new samples to our malware zoo this month.

X-Force Security Content:

Level-0 XPU's:

In May, the X-Force team responded to one level-0 vulnerability and its public exploits, and we remained *Ahead of the threat*.

Extended Protocol Support:

During May, X-Force engineers extended 5 existing PAM protocol parsers. This included the following protocols:

- MS RPC
- VoIP
- HTTP
- LDAP
- SSL

New and Extended Content Support:

X-Force engineers extended 5 PAM content parsers, including the following content formats:

- JavaScript
- HTML
- LDAP
- ZIP
- ARJ

New Vulnerability Discovery Algorithms:

X-Force added the following security coverage to our products, with 21 new events to address new vulnerabilities in VoIP, LDAP, Javascript and a critical vulnerability in Microsoft Exchange Server, along with 7 new vulnerability scanner checks:

- HTML_JS_showHelp_Code_Exec
 - HTTP_MailEnable_Auth_Overflow
 - LDAP_Sun_Search_Dos
 - Zip_Directory_Traversal
 - ARJ_Header_Block_BO
 - Script_IE_IsComponentInstalled_BO
 - JavaScript_WScript_Shell_Object
 - Email_Exchange_Calendar_Malformed
 - JavaScript_Flash_AddressBar_Spoofing
 - MSRPC_MSRTC_VA_DoS
 - VOIP_DRDoS
 - VOIP_New_Call_Dos
 - HTML_Object_Styles_Overflow
 - SSL_Google_Desktop_Indexing
 - HTTP_Google_Desktop_Installed
 - Proxy_Bounce_Deep
 - HTTP_GET_SQL_Select_Count
 - HTTP_POST_SQL_Select_Count
 - VOIP_Account_Without_Passwd
 - VOIP_Brute_Force
 - VNC_RealVNC_Auth_BypassOracleFtpPas
sBo
 - DamewareUsernameBo
 - MysqlRunning
 - RealvncAuthBypass
 - WinMs06kb913433Update
 - WinMs06kb917627Update
 - WinMs06kb913580Update
 - WinMs06kb916803Update
-

Copyright© 2006 Internet Security Systems, Inc. All rights reserved worldwide.

Internet Security Systems, the Internet Security Systems logo, Proventia, the Proventia logo, SiteProtector and Ahead of the Threat are trademarks or registered trademarks of Internet Security Systems, Inc. Other marks and trade names mentioned are the property of their owners, as indicated. All marks are the property of their respective owner and used in an editorial context without intent of infringement. Specifications and content are subject to change without notice.