



X-Force Research & Development Newsletter

January 2006

Looking Back to the Future

Welcome to the inaugural monthly newsletter from X-Force R&D. As we begin our launch into the year, X-Force are expecting 2006 to be more demanding than any period before. The security challenges facing ISS and our customers this year will be great, and many of the worrying trends observed in past years will continue to plague their organizations.

We expect the number of vulnerability disclosures in 2006 to increase. Last year X-Force investigated and processed 5195 vulnerabilities and we expect that figure to jump to over 6000 this year. Of these vulnerabilities, we expect the proportion of disclosures related to Low or Medium risk vulnerabilities to decrease as many research teams and “bedroom security warriors” choose not to bother passing details of these low value discoveries on to the vendors – deeming it below their technical level and lacking kudos.

Unfortunately, we expect number of irresponsible disclosures and 0-day exploits to increase as researchers find more financially profitable routes for their discoveries. In 2005 projects such as Microsoft’s “Honey-Monkey” crawled large swathes of the web and uncovered numerous instances of 0-day exploits being used to propagate spyware and other money generating ventures. Similarly, the financial motivations to rapidly develop exploit material for High or Critical risk vulnerabilities for inclusion into malware (before vendor protection is generally available) will necessitate an even more vigilant X-Force rapid reaction team – and result in more level-0 XPU content releases for our customers.

Depending upon which news channels you follow, you’ll have seen estimates of around 55 million electronic identities were stolen in 2005. As laws around the world become more stringent, requiring organizations to publicly disclose successful hacks and the data that may have been exposed, we can expect to see this number to increase in 2006 – despite increased vigilance. But is it really as bad as it appears? – did 55 million people lose funds from their bank accounts or incur unexpected expenditure on their credit cards? - apparently not. It seems that the hackers have bitten off more than they can chew – with only a few percent of these stolen credentials being actually used – so the chances of personally being a victim are less than they may first appear.

An unexpected sector that did get caught-out dealing with stolen identities included those organizations running donation websites. During high-volume submission periods, such as during telethons and post-catastrophic events, the hackers used the donation process to rapidly validate stolen credit card information and ensure that the cards had yet to be cancelled. This meant that the charitable organizations spent several months following their event refunding monies to the hackers victims – as well as incurring expensive processing charges.

-- *Gunter Ollmann, Director of X-Force*

Threat Research

Upcoming Rootkits

Public awareness of rootkits was raised to new levels recently due to Sony’s decision to include rootkit functionality that hid DRM protection from would-be thieves. While the rootkit was quickly discovered by security researchers, there was a protracted period in which customers were vulnerable to attacks that either made use of the hiding functionality or exploited flaws in the rootkit and its uninstallers. The rootkit deployed by Sony was of a very basic design – some of the latest rootkit research and developments are likely to cause major headaches for their targeted victims this year.

The problem with rootkits is that, by their very design, they’re supposed to be very difficult to detect and remove. Capable of modifying the systems operating system in such a way that detection is impossible without using an external (trusted) host to conduct the investigation, most security consultants would recommend that a compromised (or suspected) host be rebuilt from original installation media. Current developments look likely to change this recommendation.

Numerous research groups have been focusing their attention on rootkits capable of infecting hosts and storing their malicious code on devices other than the hard-drive or removable media.

For example, all modern operating systems rely on a basic input/output system (BIOS) interface to communicate with the computer's hardware and is typically located within a special chip soldered to the motherboard, which can be updated through various means. Developments in more advanced BIOS interfaces, such as ACPI and PnP, have meant that it is now possible to install other meaningful code within the BIOS chip and modify core input/output functionality. This is now being leveraged by rootkit developers to install their own malicious code to compromise host integrity. Similarly, hardware devices such as video cards have updatable instruction sets and huge amounts of memory – easily capable of hosting a hidden “full” operating system such as Linux.

The next wave of advanced rootkits will utilize these input/output devices to store and execute their malicious payloads. Whether they install themselves within the BIOS, video card, or even the microcode of the latest CPU's, the classic “rebuild from safe media” response will not be enough. These rootkits are specifically designed to be resilient to this kind of “fix”.

To help accelerate rootkit development, technical conferences such as BlackHat have already announced speakers for 2006 which are going to cover their latest advances in rootkits and release proof-of-concept samples. In the meantime, talk of rootkits capable of providing network scanning functionality whilst the host is in a powered-down or “standby” mode are already doing the rounds.

By the end of 2006, detection of rootkit installation will be a moot point – all efforts will be focused on pre-installation detection – since reinstalling windows from the shrink-wrapped CD isn't going to clear up the infection.

-- X-Force Advanced Research

Malcode Corner

Analysis of GDI32.DLL vulnerability and its adaptability into the latest malcode

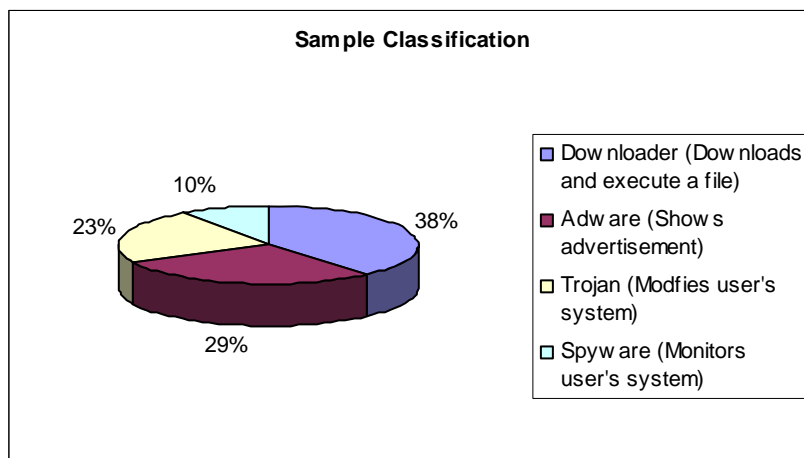
Late December saw the discovery of a malware propagation mechanism that uses exploits of a previously unknown Windows GDI32.DLL vulnerability as an aggressive new attack vector. This GDI32.DLL vulnerability was responsible for a spate of infections that immediately followed the discovery. The infections were caused by an error in the processing of WMF (Windows Metafile) files which allows arbitrary code to be executed when applications directly or indirectly make use of the SETABORTPROC GDI Escape function. This function is obsolete but has been provided within the GDI32.DLL for compatibility with 16-bit versions of Windows. The exploits occurred when images within infected WMF files that contain the arbitrary code are rendered by applications including Windows Picture and Fax Viewer, which can be launched by double clicking on the image file (e. from an email) or automatically by Internet Explorer by simply visiting a malicious site that hosts an infected image. To increase the probability of users visiting the malicious sites, links to these sites are also sent out in emails.

Since the initial report of the vulnerability on December 27, infection rates were reported to have risen to as much as 10% of all users as at 3 January. This is attributed to the fact that fully patched Windows machines are vulnerable and that infection occurs by simply browsing to malicious sites or viewing infected image files sent by email or Instant Messaging. Users have typically become weary about executing unknown email attachments, but this threat vector bypasses these common mitigating practices and infects machines with little or no user intervention.

Whilst nothing in particular is unique about the malware families themselves which use the exploits to propagate, the propagation mechanism is both new and formidable. The arbitrary code that is executed as a result of the exploit files causes a wide variety of malcode to be downloaded from various locations that are hard-coded within the exploit files, and subsequently executed on the infected users' machine. The number of exploit files has been growing at an increasing rate, helped by the generation of easy-to-use WMF construction kits and similar tools. Most malicious WMF files that have been crafted as exploits contain embedded URL locations that have been purposefully established to provide the malcode that is downloaded and executed.

X-Force has been able to gather many of the infected WMF files, extract the embedded URL locations, and obtain the malicious payloads associated with them. These have been carefully

analyzed by X-Force's virus researchers. Below is a categorization breakdown of the malware based on behavior that was derived from this investigation:



This series of events serves as an example of how new malware propagation mechanisms can suddenly appear which in turn have a significant effect upon the prevalence of various types of malware that is "In The Wild" at any given point in time. This in turn reinforces the need for pre-emptive protection against not only the exploits, but also the malicious payloads that are delivered by them at an ever increasing rate.

-- Vernon Jackson, X-Force VPS Manager

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.

Vulnerabilities:

Month	Reported					Total	Year to date
	Critical	High	Medium	Low	Other		
December	3	77	397	88	0	565	5195

Malcode:

In December the X-Force alpha-testing platform for VPS (codename Catfish) identified 19 unique 0-day malware attacks – i.e. before any other anti-virus vendor. 13 of these were new serial-variant permutations of Bagle worm attacks, the remaining 6 were new Trojans. Of particular note, one of the 0-day Trojans detected targeted Yahoo! Messenger users and was able to read Messenger window contents.

X-Force Security Content:

Level-0 XPU's:

In December the X-Force team responded 3 times to level-0 vulnerabilities and their public exploits. These special XPU releases covered the following vulnerabilities:

- Microsoft Picture and Fax Viewer WMF Buffer Overflow
- Symantec RAR File Parser Remote Heap Overflow
- Internet Explorer JavaScript Window Remote Code Execution

Extended Protocol Support:

During this month, X-Force engineers extended 14 existing PAM protocol parsers. This included the following protocols:

- TNS
- HTTP
- SQL
- MS-RPC
- WINS
- TCP
- Telnet
- TIP
- SSH
- UDP
- ISAKMP
- Yahoo Messenger
- Microsoft Messenger
- AOL Instant Messenger

New and Extended Content Support:

During this month, X-Force engineers created 3 and extended 7 existing PAM content parsers. This included the following content formats:

- ARJ
- Microsoft PE Executables
- HTML
- SDP
- Symbian
- Javascript
- Flash
- RAR
- TNEF
- WMF

New Vulnerability Discovery Algorithms:

X-Force added the following security coverage to our products:

- Image_WMF_Generic_RecordSize_Overflow
- Image_WMF_RecordSize_Overflow
- RAR_SubBlock_IO
- MSRPC_EventLog_Null_Session
- ARJ_AV_Evasion
- PE_AV_Evasion
- Image_WMF_MaxRecordSize_Overflow
- Image_WMF_HeaderFileSize_Overflow
- Image_WMF_NumObjects_Corrupt
- SQL_Empty_Password
- SQL_Empty_Password_Failed
- ISAKMP_ProtosTool
- ISAKMP_Hdr_BadVersion
- HTML_JS_Dialog_Delay
- WinMs05kb905915Update

Upcoming Technical Security Conferences:

Members of X-Force will be attending the following upcoming technical conferences:

- BlackHat Federal 2006, January 25-26, Washington DC
“SCADA Security and Terrorism: We’re Not Crying Wolf!”, David Maynor & Robert Graham
- BlackHat Europe 2006, March 2-3, Amsterdam
“The Science of Code Auditing”, Neel Mehta & Mark Dowd
- BlackHat Europe 2006, March 2-3, Amsterdam
“Stopping Automated Application Attack Tools”, Gunter Ollmann