



## X-Force<sup>®</sup> Research and Development Newsletter

February 2006



For Internal Use Only - CONFIDENTIAL

## Anatomy of a PAM Decode

As most Internet Security System (ISS) employees know, the brains behind Proventia® Network Intrusion Detection System (Network IDS) and Proventia Network Intrusion Prevention System (Network IPS) protection is the Protocol Analysis Module (PAM). It is the responsibility of ISS' X-Force to ensure that this protection engine is continuously updated and capable of thwarting the latest threats.

For many, the process by which X-Force updates PAM, via decodes and X-Press Updates™ (XPUs) is a dark art. I hope to shed some light on this important operational process—one which lies at the heart of X-Force research and development (R&D).

Each PAM Decode (or protection element) is derived from many different sources:

- X-Force Research (also known as the XFDB team) is the most common input; it performs Internet reconnaissance looking for information on vulnerabilities. It scours Web sites, IRC channels, blogs and newsgroups for information on new vulnerabilities and updates on existing vulnerabilities or exploits.
- The Advanced R&D team performs security audits on many products throughout the year. When it finds vulnerabilities in these products, the X-Force team follows a responsible disclosure process for the vulnerabilities and helps develop “ahead of the threat” protection.
- Customers can request security content to evaluate using the enhancement request form on the ISS Web site.
- The final input stream is the X-Force Development team, which uses its experience and knowledge to write audits, generic attack decodes and anomaly detection decodes.

Representatives from all teams within X-Force meet weekly to review all the collected data and determine what vulnerability detection/protection can be added to ISS products. With hundreds of vulnerabilities discovered each week, X-Force analyzes and prioritizes each vulnerability based on the popularity of the software or hardware, cost and customer impact as well as the likelihood of future exploitation.

The XPU development team reviews the list of security coverage destined for inclusion in PAM and begins work on the highest priority issues—balancing the new security content with customer requests and developer input to decide what makes it into that month's XPU. X-Force engineers research

the vulnerability information to determine the best detection algorithms.

As part of ISS' quality processes, every code change is reviewed by at least one other developer and includes the development of regression test cases. PAM is built hourly and all of the code changes are tested with an automated regression system. Any defects are likely to show up quickly—allowing X-Force to fix them promptly. Each day the new PAM engine is shipped out to the PAM Alpha systems at specific customer sites for field testing. This testing is critical for X-Force and enables it to respond to security issues quickly.

New PAM decodes are typically not blocked by default when an XPU is released. To ensure maximum reliability, each decode must be in the field for one XPU cycle before it is considered for default blocking. Both ISS' Managed Security Services and PAM Alpha systems are used to uncover any potential false positives. If a decode has been set to block by default and a false positive is reported, blocking is turned off for that decode in the next regularly scheduled XPU. If appropriate, X-Force makes a fix and the decode repeats the false positive evaluation process.

When X-Force determines that a security threat is important enough to warrant an out-of-band XPU (Level-0), the vulnerability is generally deemed serious enough to warrant blocking. However, if there is any chance of a false positive triggering the decode, then it will not be set to block until it has been proven in the field.

Every PAM decode goes through the process described above. The process itself is not static; as new threats emerge, X-Force continues to evolve and improve the delivery of this vital protection.

You can find more information regarding PAM at the links below:

- PAM Information: <http://pam.iss.net>
- PAM Decodes: <https://issintranet.iss.net/xforce/PamDecodeList.htm>
- PAM Block List: <https://issintranet.iss.net/xforce/PAMblocklist.htm>

-- Lamar Bailey, X-Force Senior Manager

---

## Threat Research

### Hidden Malware Payloads

As broadband availability has increased over the past few years, the computer virus community has evolved to make the best use of higher bandwidths and always-on systems. While computer virus groups still exist – seeking to distribute knowledge

and proof-of-concept viruses – almost every new “virus” in the wild recently has been motivated by profit. Infections have led to distributed denial of service (DDoS) attacks, spam forwarding, extortion, spyware installation and bot-network agents that could do all of these.

As a result, security professionals are prioritizing efforts to unlock the secrecy of information such as URL links hidden within the malware (which are used to command and control the installation).

Recent Win32.Sober variants have been identified featuring encrypted URL control links that are only decrypted when they are meant to be used. Because it is not exactly a new technique, it indicates to X-Force that advances in obscuring malware payloads have been largely stagnant. In the case of Sober.X, there was sufficient time for security experts to decrypt the URL links, spread the information and respond accordingly. Security vendors were able to block the URLs, shut down the content hosts and block the related accounts. Had the intended URLs been better obfuscated, Sober would have successfully downloaded a supplementary Trojan that could have caused a higher degree of damage and financial loss.

In the future we may not be so lucky, and will have to deal with malware that features hidden payloads.

The recent Oracle Voyager worm beta that was posted to the Web security-related message board “Full Disclosure,” while lacking a propagation mechanism, features a slick way to add additional functionality. Voyager makes a Google query to search for code updates that are posted to the Full Disclosure list. Since neither Google nor Full Disclosure is likely to take itself offline, this is a fairly robust method – capable of thwarting non-proactive protection technologies.

A future Windows worm may use a similar mechanism to obtain a 0-day posting of new download URLs or payload scripts. Unlike the encrypted URLs in the binaries like Sober.X or easily identifiable bot-network IRC channels, worms using postings to online message boards will be more problematic because there is not a filter on Usenet news and there probably is no filter on many security-related Web forums. In fact, even if one had a filter available, it may not be possible to reliably create a signature for the communication without the potential for high false positives. This problem only increases with malware innovation. Consider the threat of a worm with a decentralized peer-to-peer (P2P) communication channel. One has at best a moving target, and at worst, a situation in which bot-network control becomes sufficiently anonymous.

The best defense against hidden malware payloads is proactive security solutions that remain “ahead of the threat.”

-- Robert Freeman, X-Force Advanced R&D

---

## Malcode Corner

### Beyond the Brain: 20 Years Later

Last month saw the 20th anniversary of the first generally accepted MS-DOS virus known as the Brain, which was first discovered in the wild on January 19, 1986. This was just two years after the term “virus” was first introduced as the definition for a self-replicating program, in a research paper by Fred Cohen titled “Experiments with Computer Viruses.” When executed, the Brain virus changed the name of infected diskettes to contain “© Brain” and it spread by attaching itself to the boot sector of floppy disks. This was similar in design to the 1982 Elk Cloner viral program of the Apple II that predated the name “virus,” but served as a demonstration of the technique of boot sector infection.

With the advent of much more efficient delivery mechanisms, computer viruses evolved from relatively innocuous applications like the Brain and Elk Cloner, which relied on individuals exchanging infected diskettes in order to propagate, to mass-mailing worms such as the BlackWorm, which was discovered around the same time as the 20th anniversary of the Brain. In contrast to Brain, BlackWorm (aka Blackmal, Nyxem and MyWife) is both destructive and virulent, with a damaging payload capable of corrupting files and spreading via e-mail and network shares. It is programmed to unleash its payload on the third day of every month, destroying a wide range of files including Word, PowerPoint, Excel and Acrobat on infected machines. It also attempts to disable antivirus software.

By the end of January 2006, hundreds of thousands of computer were reported as infected. As part of their ongoing operations, advanced malware researchers within X-Force confirmed that users of Proventia Desktop were proactively protected against last month's outbreak of BlackWorm.

The last 20 years has seen the era of the Brain virus transform into an era plagued with a voracious smorgasbord of malicious programs. During this transformation period, various infection techniques have arisen and subsequently declined in prevalence, the most notable being the creation and spread of macro viruses which exploited security vulnerabilities in Microsoft Office applications.

The malicious payloads delivered by today's malware ranges in severity from the spread of propaganda to the gross financial loss of individuals

and corporations. Just as in the past two decades since the Brain virus was first released, the future is likely to see continued rapid changes in malcode infection techniques and delivery mechanisms as existing security holes are eliminated and new ones are discovered.

-- Vernon Jackson, X-Force VPS Manager

## A Month in Review

Below is a brief summary of security content developed or processed in the month of January 2006.

### Malcode:

In January the X-Force alpha-testing platform for the Virus Prevention System (VPS) (codename Catfish) identified nine unique 0-day malcode attacks—before any other antivirus vendor. Six of these were new IRC bot variants capable of allowing a remote attacker to delete files and executable programs on a compromised machine. The remaining three malcodes were “downloaders” whose main function is to connect to a remote PHP Web page where they retrieve information regarding the files to be downloaded to the affected machine.

### Vulnerabilities:

Last month saw 479 new vulnerabilities disclosed and processed by X-Force. This represents a 13 percent increase over last year.

	Reported					YTD
	Crit.	High	Med.	Low	Total	
Jan	1	88	271	119	479	479

Of these vulnerabilities, 423 were remotely exploitable, 67 could only be exploited locally and 11 could potentially be exploited both remotely and locally.

### Vulnerability Breakdown

<b>Bypass Security</b>	<b>20</b>
An attacker can bypass security restrictions such as a firewall or proxy, an IDS system or a virus scanner.	
<b>Data Manipulation</b>	<b>72</b>
An attacker is able to manipulate data stored or used by the host associated with the service or application.	
<b>Denial of Service</b>	<b>78</b>
An attacker can crash or hang a service or system or take down a network.	
<b>File Manipulation</b>	<b>9</b>
An attacker can create, delete, read, modify or overwrite files.	
<b>Gain Access</b>	<b>202</b>
An attacker can obtain local and remote access. This also includes vulnerabilities by which an attacker can execute code or commands, because this usually allows the attacker to gain access to the system.	
<b>Gain Privileges</b>	<b>31</b>
Privileges can be gained on the local system only.	
<b>Obtain Information</b>	<b>57</b>
An attacker can obtain information such as file and path names, source code, passwords or server configuration details.	
<b>YTD Total</b>	<b>479</b>

\* Right-hand column represents unique vulnerability count

### Top 5 Vulnerable Vendors

Oracle	<b>89</b>
BEA	<b>12</b>
IBM Lotus	<b>12</b>
Microsoft	<b>12</b>
Apple	<b>10</b>

\* Right-hand column represents unique vulnerability count

**X-Force Security Content:**

	Level-0	PAM Sig.	PAM Blocks	IS	ES
Jan	2	5	1	0	969

\* IS = Internet Scanner, ES = Proventia Enterprise Scanner

**Level-0 XPUs:**

In January the X-Force team responded to two Level-0 vulnerabilities and their public exploits. These special XPU releases covered the following vulnerabilities:

- Microsoft Picture and Fax Viewer WMF Buffer Overflow
- Microsoft Exchange Server Transport Neutral Encapsulation Format (TNEF) MIME attachments

**Extended Protocol Support:**

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

- SMB
- TIP
- DNS
- HTTP
- Veritas
- TNS
- XMPP

**New Vulnerability Discovery Algorithms:**

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

- Image\_WMF\_Code\_Exec\_Function
- HTTP\_iGateway\_Overflow
- Content\_TNEF\_Attribute\_Overflow
- Flash\_ActionDefineFunction\_Name\_BO
- HTTPS\_Proxy\_Info\_Disclosure

**New and Extended Content Support:**

X-Force engineers created three and extended eight existing PAM content parsers, including the following content formats:

- JavaScript
- HTML
- WMF
- Flash
- gzip
- zlib
- pkzip
- cab
- TNEF
- MOV
- TIFF

**New Default Blocking Decodes:**

- Image\_WMF\_Code\_Exec\_Function
- Content\_TNEF\_Attribute\_Overflow

**Upcoming Technical Security Conferences:**

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

- BlackHat Europe 2006, March 2-3, Amsterdam  
"Stopping Automated Application Attack Tools," Gunter Ollmann

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.  
Distribution: **CONFIDENTIAL**