

IBM Internet Security Systems X-Force® Threat Insight Monthly

March 2007

**IBM Internet Security Systems
Ahead of the threat.™**

Contents

● About this report	1
● Internet Protocol Television (IPTV)	2
● Modern Profile of the Malicious Web site	3
● Prolific and Impacting Issues of February 2007	5
● References	9

*IBM Internet Security Systems
X-Force® Threat Insight Monthly*

March 2007

About this report

The IBM Internet Security Systems X-Force® Threat Insight Monthly is designed to highlight some of the most significant threats and challenges facing security professionals today. This report is a product of IBM Managed Security Services and is compiled by IBM Internet Security Systems (ISS) X-Force research and development team. Each issue focuses on a specific challenge and provides a recap of the most significant recent online threats.

The X-Force is a primary security research organization that discovers vulnerabilities and security flaws in computer networks and tracks emerging Internet threats. The X-Force serves as trusted security advisor to the U.S. Department of Homeland Security as well as many other federal, state and local government organizations, helping create governmental security standards and initiatives.

X-Force research helps form the basis for the IBM protection platform. By researching vulnerabilities, IBM ISS is able to update its products and services to prevent attacks before they negatively impact an organization. IBM ISS products and services rely on X-Force research to preempt threats. Questions or comments regarding the content of this report should be addressed to X-ForceThreatIQ@iss.net.

Internet Protocol Television (IPTV)

What is IPTV, and is it a security risk?

As marketing buzz begins swirl around television services such as Video-on-Demand and Pay-Per-View being offered over IP networks, IBM Internet Security Systems (ISS) customers have asked if such offerings pose a security risk. This idea concerns some enterprise network operators. They imagine a future in which many office workers view streaming media from a window on their desktops – causing a deluge of traffic which could bring critical applications to a crawl. The following overview will hopefully put some of these fears to rest.

Internet Protocol Television (IPTV) servers typically use the exact same media server software that is used for Internet streaming media; Windows® Media Server, Darwin/QuickTime Media Server, or Helix/RealVideo Server depending on the format of the video stream. However, there are a few specialty products that focus on the IPTV market. Clients typically connect to these servers over HTTP or an IETF standard known as Real Time Streaming Protocol (RTSP). In addition, Microsoft® also employs a proprietary protocol called Microsoft Media Service (MMS).

In the case of HTTP and MMS connections, the video content is transmitted back to the client over the same connection that was used to make the request. In the case of RTSP, the request is used to control a separate Realtime Protocol (RTP) stream back to the client containing the MPEG encoded video.

Realtime Streaming Protocol (RTSP)

A protocol which allows a client to remotely control a streaming media server and time-based access to files on a server. (IETF: RFC 2326) ¹

Realtime Transport Protocol (RTP)

A standardized packet format for delivering audio and video over the Internet developed by the Audio-Video Transport Working Group. (IETF: RFC 3550) ²

Microsoft Media Service (MMS)

A protocol used to transfer unicast data (communication between a single sender and a single receiver over a network).

Typically video served via the Internet is low-resolution and has a low impact on bandwidth. This is a product of both the cost associated with serving high resolution video, and users' expectation that the video they access be displayed immediately on their computers over typical home broadband connections. Certainly these costs continue to fall every year, but at a gradual pace. It is unlikely that typical online video streams are going to move to HDTV format overnight.

The reason for the recent buzz around IPTV is that telecommunications and cable carriers are starting to deploy the exact same IP-based streaming video technologies to supply services to cable TV customers. Carriers are installing set top boxes in their customers' homes which support the standard streaming formats, as well as architecting IP Multicast networks with gigabit Ethernet to connect media servers with broadband connections.

We do not consider what the cable carriers are offering to be an Internet service since the customers receive video from servers that are located close to the end points for their physical network connections. We believe the bandwidth and latency requirements for high resolution video and audio are still too great for scalable realtime transport over the Internet backbone. Furthermore, technologies such as IP Multicast work best on smaller networks rather than with Internet-wide Multicast groups. However, it is exciting to see standard Internet and Ethernet protocols being used to supply video services.

Do IPTV services present security risks?

Yes, of course. Client software that displays videos is just as susceptible to remote code execution vulnerabilities as any other complex piece of software. The vendors who maintain client software programs provide regular security updates. Another major concern with IPTV is the possibility for denial-of-service attacks. Certainly, IPTV networks are not intended to transmit HDTV video over the Internet backbone. However, if one could be coaxed into doing so by a malicious party, the volume of traffic generated could have a significant impact on the receiving party. That risk is heightened by the fact that RTSP control channels are totally separate from RTP video streams, and RTSP can be used to direct video streams to a different destination IP address than the one originally requested.

For this reason, we believe it is important that carriers deploying IPTV systems have proper security measures in place to prevent streams from being requested from or directed to IPs outside of their networks. To prepare for this sort of situation, enterprise network operators should be aware that RTP floods are possible. Fortunately, it is relatively easy to filter this traffic via router access lists.

Consumer use of Internet-based video has risen rapidly in recent months. Google Video and YouTube have made serving video clips essentially free in many cases, and the use of these services is impacting bandwidth utilization. Furthermore, services like Amazon.com UnBox, video offerings on the Apple iTunes Store, and a streaming video feature recently offered by Netflix do allow consumers to download fairly high-resolution content.

In the case of the Netflix service, Realtime 1mbps streams of movies can be accessed from the Netflix Web site. A few users watching these videos on a corporate LAN can quickly add up to performance problems and productivity concerns.

We do not expect the widespread consumer use of high bandwidth streams to emerge for several years. According to Reed Hastings, CEO of Netflix, International Herald Tribune "The market is microscopic; DVD is going to be a very big market for a very long time."³

Modern Profile of the Malicious Web site

How long has it been since you last visited a simple HTML Web site? Chances are that it has been a while. Today dynamic content and customization through scripting makes Web sites far more interesting and productive. However, features like scripting make it difficult to identify malicious content when obfuscated and/or self-decrypting.

Our latest findings only reinforce the challenges of Web application complexity. During a recent research project, we investigated features of encrypted and malicious Web pages, and examined the plausibility of detection heuristics. While it might seem complicated to design a heuristics system to detect encrypted Web pages, it is fairly straightforward.

The encryption we see is not "strong" in the way ciphers protect SSL connections. Rather, the encryption involves convoluted, simple ciphers with the decoding algorithm present in either Java® Script or VBScript. With scripting languages, there are infinite ways to write an encryption algorithm.

The basic premise is to identify both attributes present and missing in the encrypted content. For example, one heuristic might identify scripting that performs a decoding-like action, while another might notice that the page is void of Web links. Although it is simple to identify when the links are missing, there are various ways to detect a decoding-like action is present.

The most logical approach is to notice when a function inside of a script performs arithmetic manipulations and executes a buffer as script coded. The combination of the two heuristics may appear sufficient; however, good detection logic requires more elements to withstand potential false-positive scenarios.

False-positives:

An incident in which software incorrectly identifies legitimate traffic as malicious in nature.

After writing our detection logic, we began refining the heuristics against some of the most popular Web sites such as Yahoo! ⁴. This refinement process produced very encouraging results as we identified a far higher concentration of detection elements in the encrypted, malicious Web page samples. The initiation of a broader test was merited.

The research project led us to a startling conclusion: The shocking truth about today's Web sites is that legitimate pages utilize a myriad of encryption. Content theft is the most likely reason behind its presence.

```
<script language=JavaScript>function decrypt_p(x){
Array(63,23,60,12,56,28,59,7,41,55,0,0,0,0,0,0,62,
,57,29,38,26,30,15,20,21,19,43,0,0,0,36,0,11,49,
,50,5,47,8,44,52,42);for(j=Math.ceil(1/b);j>0;j--){
(t[x.charCodeAt(p++)-48])<<s;if(s){r+=String.fromCharCode
document.write(r)}}
decrypt_p("uSp6bFuludBtkvxcOtP4JN1ZpdP4_7@So@TSbKU
bK01E1ry51BGrCryg9RyCTxcLa4So@TDuLrDuLrDuLrDuLw6EA
ysT5t3M2teJ3bXJBFRFlZuLrDuLrDuLrDpzcobX01Fkz3eNh
xQkK3Ga7hQH1hc7LoNJLwzvS8csOBKX7RDeKp4FCDeM5eZ4K
@TDYY2cufIbeKxta7V9XM3SXlpDo@TDYY2cuTI4x7OC08bwFQ
a9o08JV6DKwzvLrDulBzvLrDuLrDuLrDuLrDut2GudotSakKw
```

```
1024,i,j,r,p=0,s=0,w=0,t=
Array(63,55,52,6,17,56,23,3,14,60,0,0,0,0,0,0,2,47,2
,45,40,33,31,30,54,28,34,51,0,0,0,0,10,0,46,15,59,57
,41,39,36,11,5,38,0);for(j=Math.ceil(1/b);j>0;j--){r
(t[x.charCodeAt(p++)-48])<<s;if(s){r+=String.fromCharCode
document.write(r)}}
decodeRContent("rBRh6ZXI4Arg_Cs2179o4AS6ZK2nu95o6ny
ckH8yHfAEWH0TC_ijVytYfC9Is6q2CByfC9Is6q23Fo7D0zX
8dS78yH89Tx8bdt7b5nVihHatKsEry_BRh6ZXI4ArgC9Is6q203
HXgzA9Txa8dS78yHo0Tx8bdt7b5nVihHatKsEry_BRh6ZXI4adGr
b7HbV4dT07921782UfEF208UfE215UfE8...08V4dT77TC_33
```

BAD
GOOD

This prompted us to take a look at emulating the page rendering process on-the-wire, and alternatively, directly protecting the desktop/browser.

Duplicating the page rendering process on the wire would require JavaScript and VBScript engines. This approach presents multiple issues. First, writing the engines from scratch requires significant development overhead, making it impractical. While the engines might be available via an open-source license, they may not feasibly integrate into a commercial offering. Second, conducting a denial-of-service (DoS) attack against the engines – or even obfuscating content prior to “seeing” malicious activity – would be trivial. Finally, the JavaScript and VBScript engines could prove vulnerable to additional attacks – other than DoS.

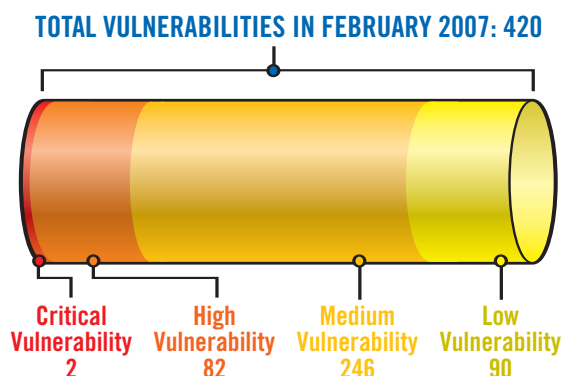
Providing protection at the browser level provides another approach. Some commercial offerings “sandbox” the browser by blocking system calls based on whether or not certain rules are followed. However, the reliability of such offerings may depend on whether the exploit is in a native or third party component, a buffer overflow, or abusing a feature or logic bug. With so much variety in terms of technique and quality, only some of these factors will apply to any given product. In today’s market, a product that specifically protects the browser before incoming content is processed does not exist. Though no small feat, protecting at the browser level has a bright future.

Prolific and Impacting Issues of February 2007

Significant Disclosures

This section of the report features the noteworthy cyber security-related issues that arose during the month of February 2007.

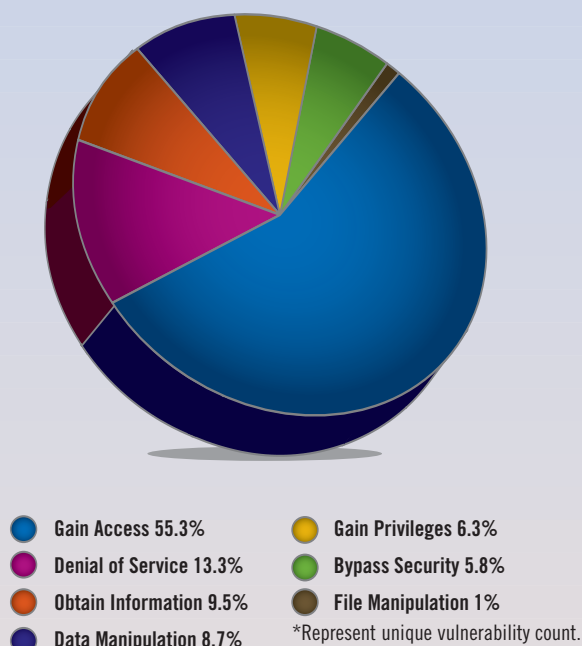
X-Force has noted a decrease in the number of vulnerabilities identified and cataloged comparatively between February 2006 and February 2007. For the first time in many years, the number of vulnerabilities disclosed over a month's time did not exceed the total of a comparative timeframe a year prior. In February 2006, we reported 554 vulnerabilities, representing 25 percent more disclosures over February 2007.*



Despite the decline in totals, issues allowing an attacker to gain access to its target rose within February. During the same timeframe last year, 40 percent of the vulnerabilities identified allowed an attacker to gain access; whereas the ability to gain access affected 55 percent of vulnerabilities found in February 2007.

Vulnerabilities researched by X-Force analysts in February 2007

The chart below categorizes the vulnerabilities researched by X-Force analysts according to what we believe would be the greatest category of security consequence that could result from exploitation of the vulnerability. The categories are: Bypass Security, Data Manipulation, Denial of Service, File Manipulation, Gain Access, Gain Privileges and Obtain Information.*



Bypass Security

An attacker can bypass security restrictions such as a firewall or proxy, an IDS system or a virus scanner.

Data Manipulation

An attacker is able to manipulate data stored or used by the host associated with the service or application.

Denial of Service

An attacker can crash or hang a service or system, or take down a network.

File Manipulation

An attacker can create, delete, read, modify or overwrite files.

Gain Access

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

An attacker can gain privileges on the local system only.

Obtain Information

An attacker can obtain information such as file and path names, source code, passwords or server configuration details.

* Numbers in this report are subject to change. The numbers being reported are based on the date the vulnerability is publicly disclosed, but does not include publicly reported vulnerabilities that are still being investigated. Also, vulnerabilities can be subtracted due to the discovery of duplicate or false vulnerabilities.

In February, X-Force analysts researched and assessed 420 security-related threats. A significant percentage of the vulnerabilities featured within the X-Force research database became the focal point of malicious code writers whose productions include malware and targeted exploits.

On February 11th, a critical “zero-day” issue affecting the Sun Solaris telnet daemon surfaced. The flaw could allow a remote attacker to bypass authentications and gain elevated privileges on a targeted system via telnet by connecting as any user on that system — ultimately allowing the attacker to execute arbitrary commands with the privileges of that user. However, remote root login must be enabled to gain root privileges. Sun released a security alert for the Solaris telnet daemon vulnerability, noting that the Solaris 10 SPARC Platform and x86 Platform releases are affected; whereas Solaris 8 and 9 are not. Recommendations are to disable telnet, alternatively using SSH, (svcadm disable telnet), or to restrict access by blocking port 23 traffic at the perimeter where plausible. A reference to the IBM ISS Protection Alert on this issue appears below.

- IBM Internet Security Systems Protection Alert: Solaris Telnet Login Authentication Bypass⁵

- Sun Alert ID: 102802: Security Vulnerability in the in.telnetd (1M) Daemon May Allow Unauthorized Remote Users to Gain Access to a Solaris Host⁶

- CVE-2007-0882⁷

As February came to a close, a worm was discovered in the wild that utilized the Sun Solaris telnet daemon for its propagation. Sun released a Korn shell script, *inoculate.local*, in response to the malware, which can remove the worm infection, if run locally on a system as root.⁸ The script also prevents systems from re-infection by disabling the telnet service.

On February 11th, Microsoft Security Bulletins MS07-005 through MS07-016 were released—a mixture of previously released and newly disclosed issues. The 12 updates, of which six received a maximum security rating of "Important" and the remaining six received a "Critical" rating, addressed a total of 20 issues.

The X-Force discovered the integer overflow issue that affects the Microsoft Malware Protection Engine in MS07-010. Due to the manner in which it parses Portable Document Format (PDF) files, an attacker could send a maliciously crafted PDF, resulting in the execution of arbitrary code once the engine scans the file. Products affected by the issue include Microsoft OneCare, Antigen, Windows Defender and Forefront Security — including Microsoft Windows Defender for Windows Vista. Reference to the IBM ISS Protection Advisory for this issue appears next.

- IBM Internet Security Systems Protection Advisory: Microsoft Windows Protection Engine Remote Heap Overflow⁹

- Microsoft Security Bulletin MS07-010: Vulnerability in Microsoft Malware Protection Engine Could Allow Remote Code Execution (932135)¹⁰

- CVE-2006-5270¹¹

Of the drop, the most critical was one of three issues addressed in the Microsoft Security Bulletin MS07-016. A remote code execution vulnerability exists due to the way Internet Explorer (IE) interprets FTP server responses. The issue should be taken seriously as directing a Web browser to an FTP URL is trivial. If a remote attacker could persuade a victim to visit a malicious FTP server using Internet Explorer, the attacker could exploit this vulnerability to execute arbitrary code on the system with the privileges of the victim. Reference to the IBM ISS Protection Alert for this issue appears below.

- IBM Internet Security Systems Protection Alert: Microsoft Internet Explorer FTP Response Remote Code Execution¹²

- Microsoft Security Bulletin MS07-016: Cumulative Security Update for Internet Explorer (928090)¹³

- CVE-2007-0217¹⁴

The X-Force discovered that versions of the Snort IDS and Sourcefire Intrusion Sensor IDS/IPS are vulnerable to a stack-based buffer overflow due to a flaw in the DCE/RPC reassembly process. This vulnerability is in a dynamic-preprocessor enabled in the default configuration, and the configuration for this preprocessor allows for auto-recognition of SMB traffic to perform reassembly on. No checks are performed to see if the traffic is part of a valid TCP session, and multiple Write AndX requests can be chained in the same TCP segment.

As a result, an attacker can exploit this overflow with a single TCP Protocol Data Unit (PDU) sent across a network monitored by the affected versions. Exploitation of this vulnerability, which does not require user interaction, could allow a remote attacker to execute arbitrary code with root or SYSTEM level privileges. The IBM ISS Protection Advisory for this issue appears below.

- IBM Internet Security Systems Protection Advisory: Sourcefire Snort Remote Buffer Overflow¹⁵

- 2007-02-19 Sourcefire Advisory: Vulnerability in Snort DCE/RPC Preprocessor¹⁶

- CVE-2006-5276¹⁷

Additional February Highlights

This section of the report briefly covers some of the additional threats that security professionals faced in the month of February.

Root Server Attack

On February 6th, the Internet's root DNS servers were attacked.¹⁸ Although, the event was touted as the largest since an incident which occurred in 2002, the overall stability of the Internet remained unaffected – leaving the average user unaware. According to US-CERT at 00:01 GMT on February 6th, a significant uptick in malformed DNS queries was noted on a number of the servers. This was apparently a “warm-up” attack to a subsequent incident, which began at 10:00 GMT. The G (U.S. DOD Network Information Center), L (Internet Corporation for Assigned Names and Numbers), and M (WIDE Project) DNS servers were the most impacted by the incident.¹⁹⁻²¹

Investigation into the true origin of the attack has revealed that a significant percentage of the data collected by the North American Network Operators' Group (NANOG) originated from South Korea.²² To be more exact, the Korean government confirmed that 61 percent of the malicious activity NANOG collected originated from within Korea. However, Lee Doo-won, a director at the Ministry of Information and Communication stated that, “a host server in Coburg, Germany ordered a flurry of Korean computers to stage DOS assaults on the root servers,” and that the South Korean systems “acted like zombies.”²³

2007 Daylight Saving Time (DST) Changes

This year, a Congressional mandate will take effect in the U.S. which initiated a significant alteration to the 2007 Daylight Savings Time (DST) schedule. The Energy Policy Act of 2005 dictates that DST will start three weeks earlier this year than in previous years (March 11th) and will end one week later (November 4th).²⁴ The statute was passed by the United States Congress on July 29, 2005, and signed into law by President George W. Bush on August 8, 2005, as a means of combating the growing energy problems facing the United States.

This alteration could constitute a myriad of issues for many consumers. Mail servers and handheld devices (i.e. BlackBerry, cellular phones, etc.) are examples of products possibly affected by this event.

IBM ISS takes the support of its clients very seriously. IBM ISS products are designed to accurately receive, process and/or provide date and time data, including data affected by the Daylight Savings Change and correctly store, create, and process information related to date and time data, including data affected by the Daylight Savings Changes. Our customers are encouraged to contact IBM ISS Support regarding questions pertaining to our products (issupport@iss.net), and to review the *IBM ISS Daylight Saving Time Change Alert* available here: http://www.iss.net/support/announcements/daylight_savings.html.²⁵⁻²⁷

The impact of DST changes to an organization should be communicated to both the internal and external customers. We strongly recommend paying extra attention to meetings and appointments scheduled during the initially-extended DST period (March 11, 2007 through April 1, 2007). It is equally important to note that similar implications may occur when DST ends in November. Steps should be taken to evaluate the procedures performed during the initial time change, so improvements may be made in advance of the second time change.

The Month of PHP Bugs

Stefan Esser, the Hardened-PHP Project and PHP Security Response Team Founder, made an interesting announcement during a recent interview with Federico Biancuzzi, a freelance writer. Esser announced his plans to initiate another disclosure initiative called, the *Month of PHP Bugs* (MoPB), to commence on March 1st.²⁸⁻³⁰

Similar to earlier disclosure initiatives, Esser intends to shed light on a new issue on each day of the targeted month. In the last X-Force Threat Insight Monthly (IM), the *Month of Apple Bugs* (MoAB) disclosure initiative was discussed. The MoAB focused on issues affecting Apple products, whereas the MoPB will focus on bugs in PHP.

Malcode

Socially Engineered

Last month, X-Force observed the circulation of a widespread spam campaign due to the propagation of the W32.Worm.Nuwar.Gen.³¹ The worm assisted in the distribution of the W32.Trojan.Peacomm (CME-711).³² The e-mails used a variety of subject headings. One of the initial headers, “Storm in Europe,” was considered a clever means to invoke user curiosity, as Europe was experiencing devastating storms at the time.

Many of the recent variants are designed to evade anti-virus detection. This malware is also capable of downloading additional files onto the system. Once this blended threat is received and executed, it builds a peer-to-peer spam botnet.

Prior to the end of January, X-Force began to observe the propagation of variants with romance-themed subject headings. We suspected that the alteration was an early attempt to take advantage of Valentine's Day.

On February 13th, over a 19-hour span starting at 3:00 PM EST, 55 new samples of the W32.Worm.Nuwar.Gen were captured. As we thought, the malware attempts to utilize holiday/romantic-themed verbiage to entice users to infect themselves by clicking the malcode attachment. The e-mail messages circulating contain subject lines such as, “Send Love On Valentines,” “Valentine Love Song,” “My Valentine” and “A Valentine Love Song” among others.

As tax season in the U.S. approaches, we predict that the appearance of “tax-themed” threats will surface. In response to such threats last year, the Internal Revenue Service (IRS) instituted a means for U.S. citizens to report suspected incidents involving the IRS name or logo.³³

Consistently and historically, attackers attempt to utilize holidays and significant events, such as Valentine’s Day and the U.S. tax season, as a means to capitalize on unsuspecting individuals via security threats such as phishing scams and malware. By such basic means, end users are enticed into continually breathing life into the socially-engineered security threats.

The Casus Backdoor

When initially detected on January 9, only three of the 30 anti-virus vendors we tested actually detected the malware W32.Backdoor.Casus.AA. This backdoor could allow a remote attacker to execute commands on the system once infected. The commands include, but are not limited to, the downloading and execution of files, causing a system restart and formatting the hard drive. In addition, the malware transmits system information to the attacker via e-mail.

On February 22, the IBM ISS patented Virus Prevention System (VPS) discovered another variant of W32.Backdoor.Casus.AA. More than a month later, the number of security vendors providing protection remained stagnant.

Sample Harvesting

It is worth noting that as part of the X-Force’s continued strengthening of IBM ISS anti-virus, anti-spyware and anti-malware protection, we investigated and added another 27,413 new samples to our malware zoo this month.

List of Contributors for this paper include:

Vernon Jackson - Engineering Manager, IBM ISS X-Force VPS Team
Tom Cross - Researcher, IBM ISS X-Force Advanced Research
Robert Freeman - Researcher, IBM ISS X-Force Advanced Research
Michelle Alvarez - Analyst, IBM ISS X-Force Threat Analysis Service
Maria A. Ciavarró - Manager, IBM ISS X-Force Threat Analysis Service
Luann Johnson - Manager, IBM ISS X-Force Database

References

Internet Protocol Television (IPTV)

IPTV World Forum 2007
<http://www.iptv-forum.com/>

¹ IETF: RFC 2326
<http://www.ietf.org/rfc/rfc2326.txt>

² IETF: RFC 3550
<http://www.ietf.org/rfc/rfc3550.txt>

³ Last motion picture show not imminent for Netflix
<http://www.iht.com/articles/2007/01/16/business/download.php>

Profile of the Malicious Web site

⁴ Yahoo! Web site
<http://www.yahoo.com>

Prolific and Impacting Issues of February 2007

⁵ IBM Internet Security Systems Protection Alert: Solaris Telnet Login Authentication Bypass
<http://www.iss.net/threats/2541.html>

⁶ Sun Alert ID: 102802: Security Vulnerability in the in.telnetd (1M) Daemon May Allow Unauthorized Remote Users to Gain Access to a Solaris Host
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-102802-1>

⁷ CVE-2007-0882
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0882>

⁸ Solaris in.telnetd worm seen in the wild + inoculation script
http://blogs.sun.com/security/entry/solaris_in_telnetd_worm_seen

⁹ IBM Internet Security Systems Protection Advisory: Microsoft Windows Protection Engine Remote Heap Overflow
<http://www.iss.net/threats/255.html>

¹⁰ Microsoft Security Bulletin MS07-010: Vulnerability in Microsoft Malware Protection Engine Could Allow Remote Code Execution (932135)
<http://www.microsoft.com/technet/security/Bulletin/ms07-010.msp>

¹¹ CVE-2006-5270
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5270>

¹² IBM Internet Security Systems Protection Alert: Microsoft Internet Explorer FTP Response Remote Code Execution
<http://www.iss.net/threats/256.html>

¹³ Microsoft Security Bulletin MS07-016: Cumulative Security Update for Internet Explorer (928090)
<http://www.microsoft.com/technet/security/Bulletin/ms07-016.msp>

¹⁴ CVE-2007-0217
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0217>

Microsoft Security Bulletins
<http://xforce.iss.net/xforce/bulletins/microsoft>

¹⁵ IBM Internet Security Systems Protection Advisory: Sourcefire Snort Remote Buffer Overflow
<http://www.iss.net/threats/257.html>

¹⁶ 2007-02-19 Sourcefire Advisory: Vulnerability in Snort DCE/RPC Preprocessor
<http://www.snort.org/docs/advisory-2007-02-19.html>

¹⁷ CVE-2006-5276
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5276>

¹⁸ Anomalous DNS Activity
<http://www.us-cert.gov/current/#dnsanom>

¹⁹ U.S. DOD Network Information Center
<http://www.nic.mil/>

²⁰ Internet Corporation for Assigned Names and Numbers (ICANN)
<http://www.icann.org/>

²¹ WIDE Project
<http://www.wide.ad.jp/index.html>

²² North American Network Operators' Group (NANOG)
<http://www.nanog.org/>

²³ Korea Becomes Haven for Hackers
<http://times.hankooki.com/lpage/tech/200702/kt2007021916025512350.htm>

²⁴ Energy Policy Act of 2005 (see page 52) (PDF)
http://energy.senate.gov/public/_files/ConferenceReport0.pdf

²⁵ IBM - Daylight Saving Time alert
<http://www.ibm.com/support/alerts/us/en/daylightsavingstimealert.html>

²⁶ Changes to Daylight Saving Time (DST) in the USA, Canada and Bermuda- 2007
<http://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/FLASH10483>

²⁷ IBM ISS - Daylight Saving Time alert
http://www.iss.net/support/announcements/daylight_savings.html

²⁸ The Month of Apple Bugs
<http://projects.info-pull.com/moab/>

²⁹ PHP Security From The Inside
<http://www.securityfocus.com/columnists/432>

³⁰ PHP Security Blog
<http://blog.php-security.org/>

³¹ W32.Worm.Nuwar.Gen
<http://www.iss.net/threats/W32.Worm.Nuwar.Gen.html>

³² CME-711
<http://cme.mitre.org/data/list.html>

³³ IRS Establishes e-Mail Box for Taxpayers to Report Phony e-Mails
<http://www.irs.gov/newsroom/article/0,,id=155663,00.html>

GLOBAL HEADQUARTERS

6303 Barfield Road
Atlanta, GA 30328
United States
Phone: (404) 236-2600
e-mail: sales@iss.net

REGIONAL HEADQUARTERS

Australia and New Zealand

Internet Security Systems Pty Ltd.
Level 6, 15 Astor Terrace
Spring Hill Queensland 4000
Australia
Phone: +61 (0)7 3838-1555
Fax: +61 (0)7 3832-4756
e-mail: aus-info@iss.net

Asia Pacific

Internet Security Systems K. K.
JR Tokyu Meguro Bldg. 3-1-1
Kami-Osaki, Shinagawa-ku
Tokyo 141-0021
Japan
Phone: +81 (3) 5740-4050
Fax: +81 (3) 5487-0711
e-mail: jp-sales@iss.net

Europe, Middle East and Africa

Ringlaan 39 bus 5
1853 Strombeek-Bever
Belgium
Phone: +32 (2) 479 67 97
Fax: +32 (2) 479 75 18
e-mail: issueur@iss.net

Latin America

6303 Barfield Road
Atlanta, GA 30328
United States
Phone: (404) 236-2709
Fax: (509) 756-5406
e-mail: isslatam@iss.net

*Information in this document concerning non-IBM products was obtained from the suppliers of these products, published announcement material or other publicly available sources. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All performance data contained in this publication was obtained in the specific operating environment and under the conditions described above and is presented as an illustration. Performance obtained in other operating environments may vary and customers should conduct their own testing.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.
Apple, iTunes and Mac OS are registered trademarks of Apple Computer, Inc., registered in the U.S. and other countries.
RealAudio, RealVideo, and RealPlayer are registered trademarks of RealNetworks, Inc.
Microsoft, Windows are either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries.
Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
GOOGLE is a trademark of Google Inc.
Amazon.com is a registered trademark of Amazon.com, Inc.
Netflix is a trademark of Netflix, Inc.
The International Herald Tribune is a trademark of I.H.T. Corporation.
YouTube is a registered trademark of YouTube, Inc.
The BlackBerry and RIM families of related marks, images, and symbols are the exclusive properties of Research In Motion Limited.
The CA brand, Brightstor, ARCserve and product names referenced herein are either registered trademarks or trademarks of Computer Associates International, Inc.
Cisco is a registered trademark Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.
Hewlett-Packard is a registered trademark of Hewlett-Packard Development Company, L.P., a Texas Limited Partnership.
Oracle, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates.
Symantec and Symantec AntiVirus are trademarks of Symantec Corporation or its affiliates in the U.S. and other countries.
Adobe, Acrobat and Reader are registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.
NetWare is a registered trademark of Novell, Inc., in the United States and other countries.
Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Other company, product and service names may be trademarks or service marks of others.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.

U.S. Patent No. 7,093,239

© Copyright IBM Corporation 2007

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the
United States of America
03-07

All Rights Reserved

IBM and the IBM logo are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

ADDME, Ahead of the threat, BlackICE, Internet Scanner, Proventia, RealSecure, SecurePartner, SecurityFusion, SiteProtector, System Scanner, Virtual Patch, X-Force and X-Press Update are trademarks or registered trademarks of Internet Security Systems, Inc. in the United States, other countries, or both. Internet Security Systems, Inc. is a wholly-owned subsidiary of International Business Machines Corporation.

IBM Internet Security Systems Ahead of the threat.™