

WEEKLY THREAT REPORT

Vol. III, No. 31

iDEFENSE Threat Intelligence Team
VeriSign Inc.

INSIDE THIS REPORT 1 August 2005

- 2 *Executive Summary/Recent Developments*
- 4 *Trends in the Risk/Threat Environment*
- 5 *Critical Infrastructure Protection*
US GAO Claims DHS Still Failing in its Cybersecurity Responsibilities
GAO testimony says still little progress in 13 key areas of cybersecurity
- 8 *Global Threat and Regional Focus*
Reports of new China-Japan “cyber war” believed highly exaggerated
Once again, there are threats of an upcoming attack but little to back them up
- 10 *Cyber Crime*
Russian Criminal Hacking Marketplace
Recent prices for “services” outside of the standard carding scene
- 14 *State of the Hack*
Top 10 Spyware Threats
A review of some the main spyware threats and mitigation issues
- 18 *Terrorism and Homeland Security*
New Forums Replacing Closed Ones
Reasons behind why some discussion forums are down is still not clear

01. Executive Summary/Recent Developments

The Cisco IOS Incident at Black Hat

The Cisco Internetwork Operating System (IOS) issue presented at Black Hat by security researcher Michael Lynn in Las Vegas on July 27 dominated the news this past week. According to Computerworld.com, Lynn "detailed a way to shut down a Cisco router by taking advantage of a known and already patched flaw in the vendor's Internetworking Operating System software." Details on this specific vulnerability (ID# 417835) are covered in the Trends section of this report.

The public relations aspect of the incident – which saw Cisco filing a federal injunction against Lynn and having more than thirty pages of Black Hat handouts ripped out of the conference proceedings – completely overshadowed the actual vulnerability itself. A Cisco spokesman said "we believe that Lynn's presentation contained proprietary information that he illegally obtained." In a settlement Lynn reportedly later agreed not to further disseminate the information related to the vulnerability. He said, "There was a potential for a serious problem coming in the future. I didn't think that the nation's interests were served by waiting a year, when there would be a possibility of a router worm." Lynn is represented by the well-known attorney Jennifer Granick.

(Machlis, Sharon, "Cisco's blunder," July 28, 2005, <http://www.computerworld.com/blogs/node/672> and Vijayan, Jaikumar, "Dispute over Cisco flaw sparks criticism, debate," Computerworld.com, July 29, 2005, <http://www.computerworld.com/securitytopics/security/hacking/story/0,10801,103577,00.html?source=x583>, Lemos, Robert, "Settlement reached in Cisco flaw dispute," Security Focus, July 29, 2005, http://www.theregister.co.uk/2005/07/29/cisco_settles_rogue_researcher_dispute/ and Naraine, Ryan, "Cisco Comes Clean on Extent of IOS Flaw," July 29, 2005).

While most news accounts have centered on Cisco's actions and the public relations aspect of this particular vulnerability, this incident highlights the fact that the transition from IPv4 to IPv6 will be fraught with numerous obstacles and dangers.

The Scots Hacker

The case of the so-called "Scots Hacker" has been adjourned until October 18, 2005. Gary McKinnon (aka "Solo"), who was on trial in London for allegedly hacking into numerous US government networks in 2001 – two weeks after the Sept. 11 terrorist attacks – is now free on bail. For now, McKinnon is barred from accessing the Internet.

McKinnon reportedly deleted various system files on nine computers at two military bases in February 2002. According to a spokesman, "Deletion of these files shut down the entire U.S. Army's Military District of Washington network of over 2,000 computers for 24 hours." McKinnon also reportedly deleted nearly 2,500 user accounts belonging to the computer network of the Fort Myer Army base. Arrested in June, if convicted, McKinnon now faces a prison sentence of up to 70 years. He is also sought in the US where he has been indicted on eight counts of cyber-related crimes (RedNova.com, "The Scots Hacker 'Who Crippled the U.S. Battle Fleet From His Bedroom' ; Computer Infiltrator Struck in Wake of Sept 11, Court is Told," July 30, http://www.rednova.com/news/technology/192253/the_scots_hacker_who_crippled_the_us_battle_fleet_from/index.html).

The UK and the Shutting Down of Pro-Terrorist Websites

There are various news reports that numerous pro-terrorist websites have been taken down in the wake of recent terrorist incidents in the U.K. According to comments by an author in this area named Neil Doyle cited in a British tabloid, "Britain is al-Qaeda's central communications hub and much of its online activities are coordinated from here. There are signs that the British security services are now pushing hard to close off their communications channels. Most of the best-known UK jihad sites went off the air on July 7 and that has now spread to the Middle East." (Bell, Peter, "Hackers fight terrorists," Sun Online (UK), Aug. 1, 2005, <http://www.thesun.co.uk/article/0,,2004600000-2005330747,00.html>)

iDEFENSE analysts have not seen any evidence to support the view that al Qaeda has any fixed "hub" from which it oversees its online activities. Although pro-terrorist hackers may exist who are operating underground from the UK, when looking at the servers that were and are hosting the best-known propaganda and recruiting sites of organized terrorist organizations, they are hosted in many different countries, including the United States, the Netherlands, France and Canada, to name a few.

At the same time, it is true that many pro-terrorist discussion forums have recently been shut down or are otherwise unavailable (this is covered in part in today's Terrorism section). The reasons are unknown. However, it is also true that new forums are popping up to take their place.

UK officials are also reportedly seeking new formal powers to take the offensive against pro-terrorist websites. These come in the form of recommendations to Parliament from the Association of Chief Police Officers (ACPO). Failure by suspects to disclose encryption keys to computers would be one of the areas covered in the new legislation and "would provide some sanction against suspects failing to cooperate with investigations," according to an ACPO statement.

Ilett, Dan, "Police ask for power to hit terrorist websites + SyS64738's comment," Zone-H.org, July 25, 2005 <http://www.zone-h.org/en/news/read/id=205957/> and Bell, Pete, "Hackers vs terrorists: online anti-jihad," July 31, 2005, <http://www.crime-research.org/news/07.31.2005/1396/> and <http://www.thesun.co.uk/article/0,,2004600000-2005330747,00.html>).

Upcoming Anniversaries of Note:

- August 2** **Kuwait:** Iraq invades Kuwait (1990)
- August 15** **China/Japan/S. Korea:** Date of alleged planned anti-Japanese cyber attacks (2005)

02. Trends Affecting the Risk/Threat Environment

More on the Cisco IOS Issue

Remote exploitation of a design vulnerability in Cisco System Inc. Internetwork Operating System (IOS) 12.x and IOX XR 3.x allows attackers to either crash susceptible IOS-running devices behind a router or execute arbitrary code on a targeted Cisco Systems router itself (ID# 417835, Aug. 1, 2005).

iDEFENSE is unaware of publicly available exploits; however, one private exploit reportedly exists. Both patches and workarounds are available.

IPv6 is designed to replace the widely used IPv4 Internet protocol. It quadruples the number of network address bits from 32 bits (in IPv4) to 128 bits, or approximately 3.4×10^{38} addressable nodes. This provides a sufficient amount of globally unique IP addresses for the growing number of network devices connecting to the Internet.

A censored presentation was presented during the 2005 Black Hat USA Security Conference on July 27, 2005. However, an uncensored presentation was released on the Internet, and has been mirrored in various locations, such as <http://www.securitylab.ru/Exploits/2005/07/lynn-cisco.pdf>

iDEFENSE analysis indicates that a review of the uncensored presentation does not contain enough detail to allow for easy exploit development; rather, the materials highlight a series of techniques that could be useful during exploit development.

This vulnerability appears to be a collection of several known issues, such as heap memory allocation exploitation on IOS that, when combined, allow an attacker to send specially crafted IPv6 packets that will cause errors in heap allocation, resulting in a denial of service or potentially in arbitrary code execution.

Cisco Systems is reporting that this issue can only be exploited from local network segments and cannot be triggered if the attacker is one or more hops away from the network device. Cisco Systems has also indicated that only IPv6-enabled systems are vulnerable. However, even if IPv6 unicast routing is enabled on any interface, the system will be vulnerable.

Exploitation against IOS-running devices behind a router could allow for arbitrary code execution, or could crash the device and prevent further processing of legitimate packets. Packets destined for the router could in fact corrupt the router's IOS and grant an attacker complete control over the router itself. An attacker could then divert traffic entirely to network segments. Potentially sensitive information, such as financial documents, user credentials, etc., could later be gleaned from a review of the diverted packet traffic.

Internet Security Systems Inc. (ISS) has released updates for several of its products that detect exploitation attempts against this vulnerability. The update names - "ICMPv6_Malformed_Option_Segment" and "IPv6_Bad_Fragment_Chain" - appear to indicate the affected areas of IOS code for this particular vulnerability. While this information does not appear to be enough for an attacker to construct an exploit, it would narrow down the areas of research for an interested exploit developer.

As such, iDEFENSE rates this issue of HIGH severity because of the extremely widespread nature of vulnerable systems.

03. Critical Infrastructure Protection

Highlights of GAO-05-827T Testimony: GAO Claims that DHS Still Failing to Fulfill Its 13 Cybersecurity Responsibilities

On July 19, 2005, David A. Powner, Director of Information Technology Management Issues for the US General Accounting Office, testified before a subcommittee of the Senate Homeland Security and Governmental Affairs Committee. Powner's testimony was quite critical of the Department of Homeland Security's cybersecurity efforts. The statement was largely a repetition of the recent GAO report issued in May 2005, GAO-05-234 (available at <http://www.gao.gov/new.items/d05434.pdf>) and covered in our recent reporting (see *WTR*, Vol. III, No. 22 (Part I) and 23 (Part II), May 30 and June 6, 2005, on US GAO report GAO-05-434, May 2005 "Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities").

Transcripts of Powner's statement and report GAO-05-827T are available for download at <http://www.gao.gov/new.items/d05827t.pdf>.

Failure to Meet 13 Cybersecurity-Related Responsibilities

In his testimony, Powner claims that DHS has still failed to fulfill 13 key cybersecurity responsibilities as defined "in law and policy." Those responsibilities, as DHS's progress (or lack thereof) in meeting them, are described at length in a chart on pages 9-10 of the testimony, (for more on the testimony and the Senate's reaction, see Goss, Grant, "Senators Call on DHS to Improve Cybersecurity," *Computerworld*, July 25, 2005, <http://www.computerworld.com/industrytopics/energy/story/0,10801,103395,00.html>).

DHS's Challenges

Powner says that the DHS and its National Cyber Security Division (NCS) in particular are failing to fully meet their responsibilities because of a number of factors, including:

Organizational Stability: Turnover within the NCS has been high, particularly at the upper levels. Examples of top officials that have all resigned include the NCS director, the deputy director for outreach and awareness, the director of the US-CERT control systems security center and the under secretary for the information analysis and infrastructure protection directorate. The report claims that this rapid turnover "has hindered [NCS's] ability to adequately plan and execute activities" (p. 11).

Organizational Authority: Powner claims that "NCS does not have the organizational authority it needs to effectively serve as a national focal point for cybersecurity" (ibid.), stating that the NCS's lack of authority within DHS has led to "some missteps," such as DHS's cancellation without explanation of a major cyber-related event. In addition, DHS took "almost one year to issue formal responses to private sector recommendations ... even though responses were drafted in months." One piece of good news on this front is that, as Powner acknowledges, DHS has recently announced that it is creating an assistant secretary-level position for cybersecurity (pp. 11-12).

Hiring and Contracting: "Ineffective DHS management processes have impeded the department's ability to hire employees and maintain contracts," Powner said (p. 12). He also said that NCS has experienced difficulty hiring personnel to fill positions, and cites one case in which a candidate accepted a position only to turn it down because he felt that the hiring process was taking too long.

Lack of Awareness of DHS's Roles and Capabilities: Powner claims that many "infrastructure stakeholders" lack a clear understanding of DHS's responsibilities in the cyber realm, and that NCSA needs to better educate the private sector about the organization's mission and purpose (p. 12).

Lack of Effective Partnerships with Stakeholders: DHS has reportedly failed to pursue partnerships with "mutually developed goals; shared benefits and responsibilities; and tangible, measurable results" (p. 13). "For example, it has often informed the infrastructure sectors about government initiatives or sought input after most key decisions have been made," Powner says. Additionally, the rapid turnover in NCSA's leadership, as cited above, has significantly hindered attempts at partnering.

Insufficient Information Sharing: An "effective, two-way exchange of information" is not yet in place with entities outside DHS (p. 14). DHS "has not matched private sector efforts to share valuable information with a corresponding level of trusted information sharing (p. 14). In one example cited by Powner, "an official with the water sector noted that when representatives called DHS to inquire about a potential terrorist threat, they were told that DHS could not share any information and that they should 'watch the news'" (p. 15).

Failure to Provide Sufficient Value: Sector representatives often reportedly claim that they are receiving no real information of value from DHS and that "without a clear benefit, they are unlikely to pursue further information sharing" with the agency (p. 15). Other government officials have complained that US-CERT's alerts "lack essential details or are based on already available information" (p. 15).

Implementation of Previous GAO Recommendations for Improvement

Powner testified that the GAO previously recommended that the following steps be taken to help meet these responsibilities and gives the current status of DHS's responses to those recommendations:

Develop a Capability for Strategic Analysis and Warnings: Powner notes that this recommendation has not yet been pursued by DHS and urges that DHS establish a methodology for analyzing strategic cyber-based attacks (i.e., terminology, standard set of factors to consider, established thresholds of sophistication, etc.). He also says that DHS must obtain industry-specific data on critical systems components (i.e., known vulnerabilities and interdependencies) (p. 16).

Defend Against Threats to Control Systems: Powner recommends that DHS develop a plan for coordinating with the private sector and other government agencies to defend against cyber-related threats to control systems. He notes that DHS has formulated such a strategy, but does not yet have "underlying details and milestones for completing activities" (p. 17).

Information Sharing: In 2004, the GAO recommended that DHS develop a plan and milestones for sharing information with ISAC sector coordinators and agencies. Powner notes that DHS has not yet formulated such a plan (p. 17).

Threat and Vulnerability Assessment: Powner reports that "much needs to be done" to fulfill DHS's "basic responsibilities," which Powner describes as assessing threats and vulnerabilities and developing appropriate recovery plans (p. 17).

Analysis

As already mentioned, these criticisms are by no means new and are primarily a repetition of comments that first appeared in May 2005 in the GAO-05-434 report. What is significant is the fact that the GAO usually goes out of its way to find constructive statements to help offset its criticisms — especially if

there are indications that progress is underway. Powner's lack of additional qualifying statements in this regard is telling.

Therefore, the most notable part of this testimony is that it shows how little progress has been made on these issues since the GAO first raised them. What is most disappointing is that many of DHS's efforts to address its responsibilities are still at the *initial planning* stage nearly three years after these responsibilities were assigned.

For its part, DHS says that in the next few months it will release a draft of a national infrastructure vulnerability assessment plan that will include a cyber component (Goss, Grant, "Senators Call on DHS to Improve Cybersecurity"). In addition, DHS is reportedly working on "a plan for Internet recovery after a major attack" and is "supporting efforts to push IPv6, a more secure version of the current Internet Protocol."

As discussed, one potential bright spot is the announcement of a plan to create an assistant secretary-level position for cybersecurity within DHS. In theory, this should help overcome some of the obstacles that cybersecurity has faced in the past within the organization, most notably a lack of organizational authority. However, it remains to be seen how this will play out in practice.

04. Global Threat and Regional Focus

Reports of Upcoming China-Japan “Cyber War” Highly Exaggerated

Last week various media sources reported on an alleged recent threat by the Association of China’s Red Hackers or The RedHackers’ Alliance (www.redhacker.cn and www.CNRedHacker.org) to attack multiple Japanese websites beginning on Aug. 15, 2005. Aug. 15, 1945, also known as “VJ Day,” was the date when Japan’s Emperor Hirohito announced in a broadcast to the Japanese people that Japan’s involvement in World War II was over. iDEFENSE believes that these reports are overblown; while Chinese hacking and possible Japanese hacking counter-attacks are certainly an issue of sensitivity and concern, it is unlikely that a “cyber war” of any substance will break out on that date.

Information from Media Sources

According to some reports, the Chinese hacking group is made up of current and former members of Beijing University, and is divided into three groups, each focusing on a different task — information collection, attacking the websites and preparing for Japanese counterattacks. As of July 13, the hacking group reportedly claimed it had some 45,000 people who have volunteered to join in the attacks and that targets include several Japanese websites that are anti-China. (See, for example, Millman, Rene, “Asian Cyber War to Start Mid-August,” *SC Magazine*, July 15, 2005, <http://www.scmagazine.com/news/index.cfm?fuseaction=newsDetails&newsUID=d0689c6e-28e1-4a99-a6af-67d51dc70cae&newsType=Latest%20News>).

Some South Korean sources are reportedly concerned that the hackers will launch their attacks through Korean servers (reportedly including servers of a gaming company and a university) to disguise their origin. According to a story in Donga.com, a Chinese hacker reportedly told a Korean acquaintance that the Chinese hacking group has “chosen three candidate servers of a Korean gaming company and universities as their hacking routes. The security level of those servers is lower than expected. So they are thought to be proper for avoiding IP tracking.” None of this has been independently confirmed. (Park, Sun-Hong, “Chinese Hackers Might Hit Japanese Websites via Korean Servers,” Donga.com, July 14, 2005, <http://english.donga.com/srv/service.php3?bicode=040000&biid=2005071460188>).

A Japanese Hacker Counter-Attack?

At the same time, some “Chinese Internet activists” reportedly expect a Japanese hacking attack on Aug. 15. Kyodo News says that contributors to the Chinese website “2222222.cn” anticipate that pro-Japanese hackers will attack on that date (“Chinese Internet activists brace for Japan hacker attack Aug. 15,” July 30, 2005, <http://www.japantoday.com/e/?content=news&cat=1&id=344983>).

More on The RedHackers’ Alliance

iDEFENSE has previously written about The RedHackers’ Alliance or T.R.A. (see *WTR*, Vol. III, No. 2, Jan. 10, 2005, and Vol. III, No. 18, May 2, 2005). The group has posted anti-Japanese material in the past and is strongly opposed to Japanese membership on the U.N. Security Council.



July 2005 screenshot of homepage of Association of China's Red Hackers (aka The RedHackers' Alliance or TRA). (<http://www.redhacker.cn/index.html> and www.CNRedHacker.org)

Analysis

Although these reports initially seem troubling, iDEFENSE Intelligence Operations believes them to be largely misleading. Although some attacks may occur on Aug. 15, they are not expected to be of major significance at this time.

This situation appears similar to the announced plans for a cyber attack on July 7, 2005, which turned out to be a non-event (that alleged attack was to be in commemoration of the so-called Marco Polo Bridge incident on July 7, 1937, see *WTR*, Vol. III, No. 27, July 4, 2005, "China/Japan: Possible minor attack planned for July 7"). In the same way, there was also a call for an alleged attack to be launched today, Aug. 1, 2005, but, as yet, there is no indication that anything occurred ([kker.cn](http://www.kker.cn), July 19, 2005, <http://www.kker.cn/art/list.asp?id=1040>).

Nevertheless, iDEFENSE will continue to monitor activity surrounding this topic and will report on any additional developments as appropriate. The comments about the potential use of South Korean servers as intermediate points in an attack on Japan to try to mask Chinese IP addresses do constitute an area of concern.

05. Cyber Crime

Russian Criminal Hacking Marketplace: Current Prices and Services on Web-Hack.ru

The Criminal Carding Marketplace and the Arrest of “Script”

In much previous reporting we have discussed the criminal carding marketplace, which is dominated by Russian carders and hackers. In a recent development, one of the individuals perhaps most responsible for facilitating the early development of that underground marketplace, Dmitro Ivanovich Golubov (aka “Script”), the founder of the original main site of carding, Carderplanet.com, was recently arrested by Ukrainian authorities. Larry Johnson, a Secret Service special agent cited by The Wall Street Journal, said that Golubov’s arrest “represents one of the most significant apprehensions of a high level Eastern European responsible for criminal activity on the Internet.” (Bryan-Low, Cassell, The Wall Street Journal, July 19, 2005, p. B9).

Over a year ago we published an account of an interview with Golubov where he discussed his involvement in the early days of the carding scene and his reported “retirement” (*WTR*, Vol. II, No. 21, May 24, 2004, Cyber Crime: “Analysis of Interview with Russian Carder”).

Impact of the Arrest of Golubov, aka “Script”

The arrest of Golubov could provide major insights into the origin and early years of the illegal carding marketplace in the former Soviet Union. However, it will probably do little to stem the flow of illegal online activity that his founding efforts at Carderplanet.com helped spawn.

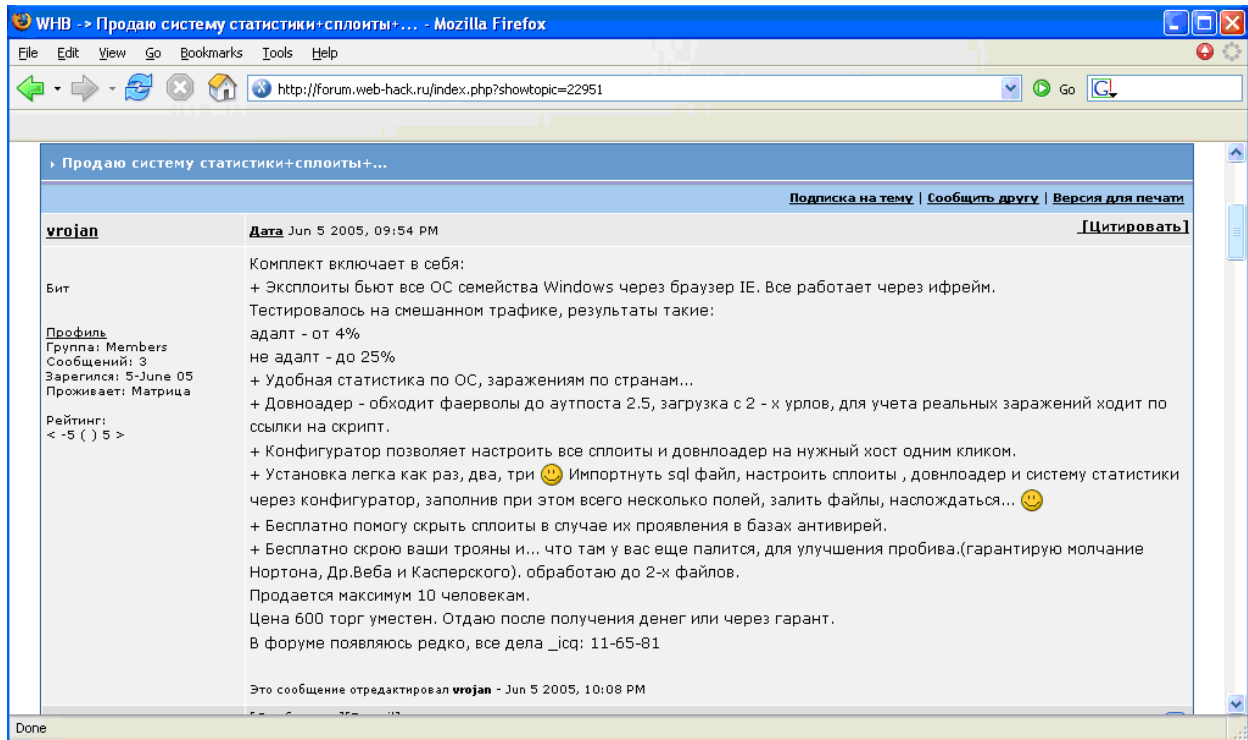
Non-Carding Products and Services

Many of our previous reports in this area have centered on carding itself and related services. However, a broader underground market has emerged in many other areas of criminal hacking. In today’s report, we will look at some of those areas as represented on a currently very active underground Russian forum, Web-hack.ru.

Specific DDoS Trojan Sought — Made to Order

A July 7, 2005 posting on Web-hack.ru, is amazing for both its brazenness and specificity. It seeks a specific kind of Trojan for a DDoS attack. The size should be up to 50 kilobytes, administered through http:// (and not IRC), offer to the buyer three choices for ports for the attack and four types of attack and to include SYN and ICMP flood attacks. The price is variable based on negotiation. Interested parties are told to contact: sfsdsd@tut.by. The posting is found at: <http://forum.web-hack.ru/index.php?showtopic=23961>.

IFRAME Vulnerability Exploits for Sale along with a “Statistical System” for Measuring Their Effectiveness

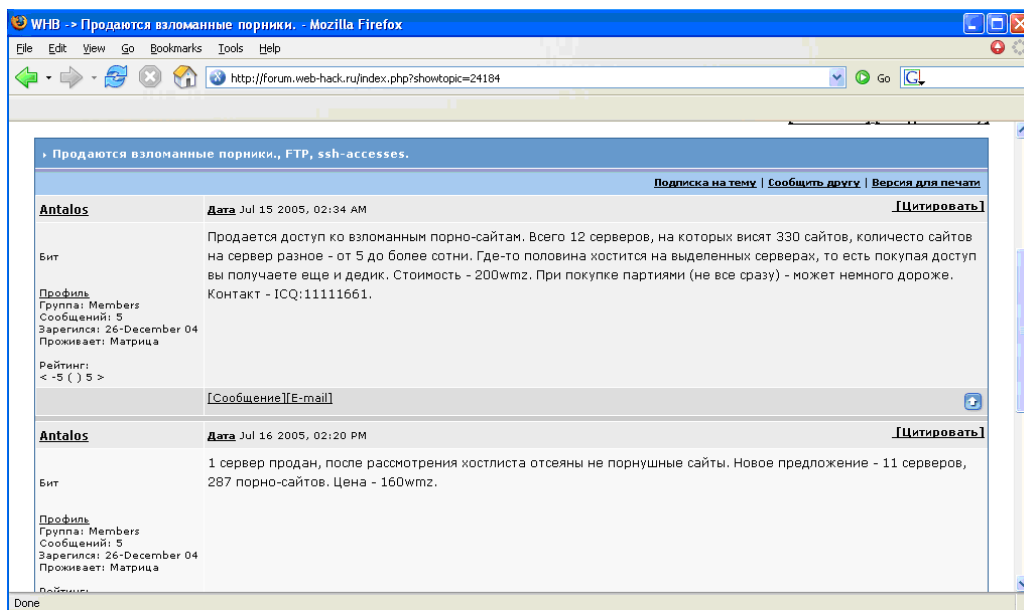


A June 5, 2005 posting on Web-hack.ru concerning IFRAME vulnerability exploits for sale, including a statistics service (<http://forum.web-hack.ru/index.php?showtopic=22951>).

In a June 5, 2005 posting on Web-hack.ru, the poster, named “vrojan,” is offering exploits that use the IFRAME vulnerability and a statistical service that measures their effectiveness (*Note: We first became aware of the existence of this service as a result of research into Russian carder reaction to the CardSystems incident and promised to look into it in more detail. See WTR, Vol. III, No. 25, June 20, 2005, p. 12*).

These IFRAME-related exploits operate against the Windows family of operating systems using the Internet Explorer browser. Vrojan says he has tested them out on both “adult” and “non-adult” sites, getting different levels of responses for each. He says installation is as easy as “one, two, three” through importing an SQL file that has the exploits and a statistical system for measuring their effectiveness. He says that he will offer to help hide exploits “for free” from anti-virus databases in the event that these exploits should appear in them. He also says that he will hide “your Trojans” for free and that he “guarantees” that Norton, Dr. Web and Kaspersky will not pick them up. He says he will sell this service to a maximum of ten persons.

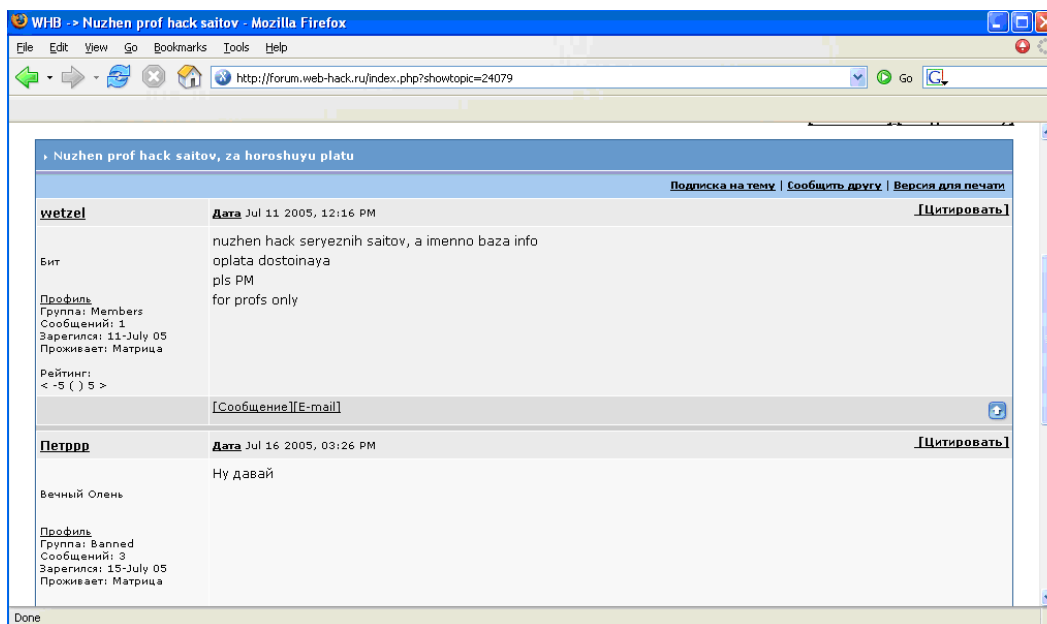
Access to Hacked Pornography Sites for Sale



July 15-16, 2005 postings on Web-Hack.ru, <http://forum.web-hack.ru/index.php?showtopic=24184>.

In another example, in a July 15, 2005 posting a seller named Antalos offers “access to hacked porno sites.” He says there are “twelve servers” in all carrying some 330 sites. The number of sites “per server varies — from 5 sites to more than a hundred.” The cost for access to these 12 servers is 200 WMZ (\$200 US). By the next day, July 16, Antalos put up another posting saying that “one server had been sold” and that the new price for the 11 remaining servers, with access now to 287 hacked porno sites (instead of the original 330 sites) would be 160 WMZ (\$160 US).

Posting Seeking Hacker Services



Posting seeking for hacker services and response (July 2005) <http://forum.web-hack.ru/index.php?showtopic=24079>.

In a July 11, 2005 posting (and a July 16 response), a poster named “wetzels” says he “needs a hack of [some] serious sites, namely, for database information.” He says that payment for this service, which is open to “professionals only,” will be “adequate.” Some five days later, a response inquired more information on the offer.

Analysis

These are just a sampling of the wide variety of illegal cyber-related services now offered on Web-hack.ru and similar sites. They demonstrate that the underground marketplace for hacking has developed far beyond the stolen credit card market that Golubov and Carderplanet.com helped create. In the future we will look at additional types of services and attempt to assess their overall impact.

06. State of the Hack

a. Top 10 Spyware Threats and Mitigation Issues

Fortinet Inc., makers of an anti-virus firewall product, recently published a Top 10 list of spyware in their July 14, 2005 FortiGuard bulletin. This article reviews each top spyware component and associated risks. A list of potentially hostile URLs is also provided at the end of this article.

Fortinet's list of top spyware threats is based on actual interceptions made by the appliance network supported by the company. The Top 10 spyware list is as follows, with percentage of interceptions:

Spyware	Percentage of Interceptions
1. Adware/BetterInternet	41.41
2. Adware/180Solutions	38.51
3. Download/Px	8.80
4. Joke/Renos.A	2.30
5. Adware/Websearch	1.88
6. Adware/ExitFuel	1.55
7. Adware/ShopAtHomeSelect	1.00
8. BHO/Clientman	0.53
9. Adware/RBlast.A	0.52
10. Adware/180SA	0.30

Top 10 Spyware List

The malicious code classification schemes supported by Fortinet are configured by Joe Wells and Shane Coursen, some of the best recognized and most respected names in the business for malicious code sample handling and naming. Their classifications for adware and spyware hit the mark and do a good job from an appliance perspective on how to properly identify and mitigate such threats. Naming conventions in this article are from the Fortinet database.

BetterInternet and 180Solutions dominate the spyware charts, comprising almost 80 percent of all interceptions noted by Fortinet. These same programs have been seen in many other spyware incidents this year, some of which involved these legal codes being installed using illegal methods. An overview of each top spyware threat is discussed below.

Adware/BetterInternet

BetterInternet is a downloader that "upgrades" software. Downloads are typically performed from <http://www.abetterinternet.com> and <http://download.abetterinternet.com>. Executables may initially connect to <http://thinstall.abetterinternet.com> to download additional files: Ceres.cab (Adware/Betterinternet), Csnopol.cab (Adware/Betterinternet), Polau2c.exe (Download/Agent.AY), and Farmmext.exe (Download/Stubby.C). Once installed the software hooks into the windows registry to run upon Windows startup.

Adware/180Solutions

180Solutions is used to display pop-up ads on a computer. When executed, this software displays a privacy policy that indicates that it will collect information on the user's IP address, web browser version, and other data. Once installed, it displays targeted pop-up ads on the computer. It may run in memory via

a dozen or more processes and hook into the Windows registry in multiple locations. It is very aggressive and very invasive, and is very difficult to remove from most computers.

Download/Px

This spyware threat name is based upon a Computer Antivirus Research Organization (CARO)-type standard. The first component clearly identifies it as a downloader. It may be used to download as many as 90 different programs. It may attempt to connect to 2nd-thought.com, and many other sites via installations and downloads performed as directed by the actor prior to distribution of the code into the wild.

Joke/Renos.A

Interestingly enough, Renos.A is a joke file that is designed to scare a user into thinking they have spyware. Normally a file called wininstall.exe is installed into a Program Files directory called SpywareNo. A system Tray icon is then launched and an image is displayed to scare the user into thinking their computer is infected with various malicious codes and spyware. It may also display a fake error message and runs at Windows startup. It is not viral nor spyware, just a hoax.

Adware/Websearch

This is a toolbar for Internet Explorer that may be downloaded from www.websearch.com. User interaction is typically required to accept an installation of the toolbar. Once installed, it can be found under the Start Menu in the Programs Group, runs in memory, and is visible from the taskbar. It modifies the Windows registry to run at Windows startup.

Adware/ExitFuel

This adware is based in JavaScript and opens random websites. When executed by a browser it minimizes the current window and opens a new browser window to display the website promoted by the code. The following URLs are associated with this code:

- ads.primeinteractive.net
- anserver.internetfuel.com
- auctioncities.com
- banners.valuead.com
- bsads.valuead.com
- cdn.fastclick.net
- crystalpalacecasino.com
- dldw.fordaleltd.com
- download.fordaleltd.com
- download.targetnetworks.net
- dserv.internetfuel.com
- friendfinder.m7z.net
- ifcol.exitfuel.com
- nitrous.internetfuel.com
- PartyBingo.com
- passion.com
- update.contentdeliverymodule.com
- www.accessmedia.tv
- www.auctioncities.com
- www.crystalpalacecasino.com

- www.date.com
- www.netbroadcaster.com
- www.netbroadcaster.com/new/movies/groovy.html
- www.onlinemediasales.com
- www.partybingo.com, tracker.partybingo.com
- www.promotionstat.com
- www.streamwaves.com
- www2.fordaleltd.com
- www-web.real.com
- z1.adserver.com

Adware/ShopAtHomeSelect

ShopAtHomeSelect is like a rebate reminder utility that may be downloaded from www.ShopAtHomeSelect.com. It installs multiple files and hooks into the Windows registry to run at Windows startup. It also modifies Internet Explorer security settings to allow for downloads of unsigned Active-X controls.

BHO/Clientman

Clientman is a browser help object (BHO) that updates browser settings and modifies Windows registries. It may send and receive information to and from a specific HTTP site. It may attempt to connect to odysseusmarketing.com and omi-update.net. It modifies the Windows registry to ensure it is run at Windows startup.

Adware/RBlast.A

RBlast.A is a CAB file that is digitally signed by "Integrated Search Technologies." The CAB files contain the file `ysbactivex.dll` (57,344 bytes).

Adware/180SA

180SA may display pop-up ads and redirect browsers to websites of choice. The End User License Agreement (EULA) also allows for additional software and updates to be installed on the computer. If removed manually, it may attempt to display a pop-up window offering to reinstall itself. It typically results in 180Solutions being installed and hooks into the Windows registry to run at Windows startup.

b. URLs

The following URLs are the primary addresses related to top spyware as identified by Fortinet. Companies that wish to avoid the installation of questionable or potentially unwanted software such as adware and spyware may want to block these URLs.

- www.abetterinternet.com
- download.abetterinternet.com
- thinstall.abetterinternet.com
- www.180solutions.com
- 2nd-thought.com
- www.websearch.com
- ads.primeinteractive.net
- anserver.internetfuel.com

- auctioncities.com
- banners.valuead.com
- bsads.valuead.com
- cdn.fastclick.net
- crystalpalacecasino.com
- dldw.fordaleltd.com
- download.fordaleltd.com
- download.targetnetworks.net
- dserv.internetfuel.com
- friendfinder.m7z.net
- ifcol.exitfuel.com
- nitrous.internetfuel.com
- PartyBingo.com
- passion.com
- update.contentdeliverymodule.com
- www.accessmedia.tv
- www.auctioncities.com
- www.crystalpalacecasino.com
- www.date.com
- www.netbroadcaster.com
- www.netbroadcaster.com/new/movies/groovy.html
- www.onlinemediasales.com
- www.partybingo.com, tracker.partybingo.com
- www.promotionstat.com
- www.streamwaves.com
- www2.fordaleltd.com
- www-web.real.com
- z1.adserver.com
- www.ShopAtHomeSelect.com
- odysseusmarketing.com
- omi-update

Analysis

Adware and spyware are fueled by big marketing dollars, also supplemented by illicit installation by hackers seeking monetary gain, making these types of threats increasingly likely and problematic for organizations that want to stop all such installations. While adware and spyware are rapidly growing in prevalence, they often utilize the same downloader URLs and affiliate domains. This is because they are legal software, and affiliate programs rely upon such sites to perform the downloads to get paid. As a result, unlike traditional malicious code attacks, blocking known domains for common spyware may prove to be highly effective in mitigating many of these potentially unwanted installations. Additionally, identifying known adware and spyware filenames, sizes and checksum values may also prove helpful in mitigating threats on the client level if implemented through aggressive policy management of hosts on a network.

07. Terrorism and Homeland Security

New Forums Replacing Closed Discussion Forums

On July 7, 2005, claims of responsibility for the terrorist attacks in London were posted on the pro-terrorist forum Qal3ah.org by a previously unknown group calling itself "The Secret Organization Group of the al Qaeda for the Jihad in Europe." Shortly thereafter, the discussion forum was shut down, possibly by website administrators (see *WTR*, Vol. III, No. 28, July 11, 2005).

Since that time, many other discussion forums have been shut down. iDEFENSE analysts know of at least five popular pro-terrorist discussion forums that are now unavailable. The reason for this drop in active pro-terrorist websites is unknown at this time. However, it is interesting that the time frame for these websites being shut down coincides with the London terrorist attacks and claims of responsibility posted online.

As some pro-terrorist websites begin to be shut down, others are beginning to spring up in their place. For example, membership at Moqawmh.com (meaning "The Resistance") has increased, and the website now contains an active forum discussing cyber attacks, also known as electronic jihad or e-jihad.

Within the e-jihad forum, a member calling himself "Ahmed44" posted an invitation to others for an orientation on hacker attacks. In the message, posted July 28, 2005, Ahmed44 provides his e-mail address for future contact with any potential participants.

Ahmed44's motivations, which could be political, are unclear. Also, a specific time or target was not listed within his message, which, if it goes forward, will probably be organized later via private e-mails between participants.



Logo of the Moqawamah Forums located at <http://www.moqawmh.com/vb/index.php> translates as "the Resistance Forums."

Analysis

Although this e-jihad is considered a LOW-level threat since it is in its infancy, it illustrates that discussions are undoubtedly continuing as members of the previous forums move around the Internet and begin to congregate on new extremist pro-Islamic forums.

iDEFENSE analysts have located more than 20 popular new forums in which members are discussing cyber attacks or e-jihads. These websites will be reviewed and any significant findings reported in future *Weekly Threat Reports*.

Additionally, we will be reporting on reactions in the extremist forums to the death of Saudi Arabian King Fahd. Extremists believe the royal family of Saudi Arabia is a false government because they say there are no "kings" in Islam and that everyone should follow the clerics and the Sharia (Islamic Law).

NOTE TO USERS: The **WEEKLY THREAT REPORT** is an overview of key trends and developments in the area of worldwide cyber threats and terrorism/homeland security issues. It is intended to assist key decision makers in pursuing policies that will help in mitigating threats. We view our clients as a very important part of that process and invite your feedback and observations as to how we can make this product serve you better. Please send your comments to: di@idefense.com.

For users of this product who desire a more focused approach to specific problems affecting their own organization or a particular topic, iDEFENSE offers **FOCUSED INTELLIGENCE REPORTS (FIRs)** to enhance clients' intelligence production needs. All trademarks and registered trademarks are the property of their respective owners.