

**PANEL DISCUSSION POINTS - SMART INTERNET CRC SEMINAR
SYDNEY, 21-22 SEPTEMBER, 2006.**

Professor William J (Bill) Caelli, AO
Asst Dean – Faculty of Information Technology
Senior Researcher – Information Security Institute
Queensland University of Technology
Brisbane. Qld. 4000
AUSTRALIA

Phone: 07-3864 2752
Mobile: 0414 987 952
Email: w.caelli@qut.edu.au

TECHNOLOGY

1. **PC UNSUITABLE - UNMODIFIED**
The hardware and software bases of the personal computer developed over the last 30 years was never designed or developed for the performance of secure transactions of personal, business and governmental significance.
2. **INTERNET – NOT END-TO-END**
The design of the packet-switch oriented Internet intended it to be “bit agnostic”, i.e. ignorant of the data content being transported, and to only warrant safe delivery of those “bits” on a node-to-node basis, not end-to-end.
3. **I&A – NEEDS TRUSTED CHANNEL**
Any technique used for user/system identification and authentication depends fully upon a trusted channel or pathway between the identity “claimant” and the associated identity “verifier”; a situation that does not exist over the Internet with untrusted PC nodes.
4. **WEB SERVICES / SERVICE ORIENTED ARCHITECTURE – SECURITY DISASTER**
The rapid move to script-oriented, fast-developed information systems and applications based around service oriented architectures (SOA), including web services, AJAX, etc. poses a real and present security problem to users of such systems because of a lack of robust security architecture and security enforcing sub-systems.

POLICY

5. **SUPPLIER KNOWS BETTER**
The manufacturers and suppliers of PC based systems knows much more about their products than the user of the product, public policy developers, corporate executives and others and the opinions of that supplier must be acknowledged and cannot reasonably be ignored or contradicted.
6. **STOP BLAMING THE END-USER**
The end-user of PC/Internet/WWW based information services is not, and cannot be reasonably assumed to be, an ICT expert with the result that any system must be totally tolerant of that situation.
7. **RESPONSIBILITY IS WITH THE ENTERPRISE**
Any enterprise wishing to use a “customer-owned” PC coupled via the Internet to its information systems and services must ensure that appropriate sub-systems are supplied at its cost to meet the security requirements of the associated transactions and the skill levels of the end-user.

SUPPORTING DOCUMENTS

A) ROOTKITS AND BOTNETS HAVE CHANGED THE RISK ASSESSMENT RADICALLY.

<http://www.eweek.com>

Money Bots: Hackers Cash In on Hijacked PCs : September 8, 2006

By Ryan Naraine

Botnet hunters tracking the latest MS06-040 worm attack estimate that one malicious hacker earned about \$430 in a single day by installing spyware programs on thousands of commandeered Windows machines. Security researchers at the German HoneyNet Project discovered a direct link between the botnet-building attack and DollarRevenue, a company that pays between a penny and 30 cents per installation of its heavily criticized ad-serving software.

Within 24 hours, the IRC-controlled botnet hijacked more than 7,700 machines via the Windows Server Service vulnerability and hosed the infected computers with the noxious DollarRevenue files. During a four-day stretch, researchers at the Manheim, Germany, honeyNet project counted about 9,700 infections from a single command-and-control center and calculated that the attacker was making hundreds of dollars a day in commissions from DollarRevenue alone.

"This is a lucrative business," said Thorsten Holz, a project founder who spends much of his life monitoring botnets. "He's earning more than \$430 in a single day with DollarRevenue, and that's not the only piece of adware he's installing. He's installing others and also renting his botnet out to spammers," Holz said in an interview with eWEEK.

DollarRevenue describes itself as "one of the best pay-per-install affiliate programs on the Internet," offering Web site owners "an alternative to traditional advertising methods." The company offers a per-installation commission every time one of its programs is downloaded onto a computer, going as far as encouraging installs via ActiveX pop-up windows or bundled executables within third-party software.

The payouts vary according to the location of the infected computer. For example, an adware installation in China only pays a penny, while an executable loaded on a PC in the United States or Canada pays between 20 cents and 30 cents, according to information posted on the DollarRevenue Web site. In this case, Holz counted 998 installations in the United States, 20 installations in Canada, 103 in the United Kingdom, 756 in China and about 5,800 in other countries.

Anti-virus vendor Sunbelt Software, in Clearwater, Fla., describes DollarRevenue's software as "high-risk threats" that are typically installed without user interaction via security exploits. Using a network of machines set up with intentional vulnerabilities to lure and trap Internet attackers, Holz's honeyNet project was able to monitor the instructions being sent by the botnet controller to thousands of compromised computers.

Holz explained that a main IRC channel is being used to dispatch all incoming bots to join four different channels. The first sends instructions to propagate further by scanning for other vulnerable Windows machines. The second channel installs adware on all the machines, and a third was set up especially for the DollarRevenue installations.

A fourth channel was used to install an additional binary on all bots. This is believed to be a spam proxy that can be rented out to spammers. "This is a lucrative business. He's using this botnet to make big money," Holz said.

Infiltrating a botnet command-and-control center.

In early August, researchers at LURHQ's Threat Intelligence Group were able to infiltrate a botnet command-and-control center linked to the latest wave of attacks and found a sophisticated spam operation that included the use of a proxy Trojan, forged e-mail addresses and botnet drones. Holz said some botnets have also been used to install keyloggers and other malware files to steal personal data from an infected user's browser. "Adware installs are the most lucrative but once a herder has a few thousand machines under control, he can sit back and make a lot of money," he said.

Holz's team has seen botnets that control between 10,000 and 25,000 compromised computers, and he says high-profile flaws in widely used applications are "quickly turned into exploits."

"It's pretty standard to see about 7,000 infections per day whenever there's a new exploit. They [bot herders] keep the size of the botnets low on purpose to avoid too much noise," he said.

"In this case with the DollarRevenue installations, the owner compromised about 33,000 machines in five days. On the fifth day, he changed the command-and-control server and moved right along," Holz said. The command-and-control infrastructure is most often an IRC server installed illegally on a high-bandwidth educational or corporate network. A botnet (short for "robot network") is a collection of broadband-enabled computers infected with worms and Trojans that leave back doors open for communication with the malicious attacker.

Michael Sutton, a security evangelist at Atlanta-based SPI Dynamics, said Holz's findings are an accurate reflection of the severity of the botnet problem. "These botnets give attackers tools to do a lot of different things. The goal is to control bandwidth and CPU cycles to make money," Sutton said in an interview with eWEEK. Sutton, a well-known security researcher who previously worked as director of Verisign-owned iDefense Labs, said botnet-related crime is a "billion-dollar business."

"On one side, you have these big advertisers pumping money into the adware business," he said.

"On the other side, you have these shady companies with shady affiliate deals, cashing in. I've seen reliable estimates that the business of serving ads via adware is worth \$1.6 billion a year. That's a phenomenal industry."

Copyright (c) 2006 Ziff Davis Media Inc. All Rights Reserved.

B) UK – BARCLAYS'S BANK SMART CARD SCHEME – BEST PRACTICE?

British Computer Society

Barclays device to tighten online security : Aug 4 2006

High street bank Barclays plans to issue card readers to its 1.6 million online banking customers in an effort to help improve internet security and combat ID theft. The calculator-sized two-factor authentication devices, which are based on card readers developed by banking body Apacs, will read chips on debit cards and then provide a one-time password for customers to use with online banking.

Card-not-present fraud increased by 21 per cent last year and costs banks and other financial institutions some £183.2 million. Barclays, which will issue the devices throughout 2007, wants all its customers to benefit from increased security.

'We plan to issue the card readers to all online banking customers and not just business customers,' Barnaby David, director of online banking at Barclays, told Computing.

'We've gone for this model of two-factor because it resists all known methods of fraud,' he said. Lloyds TSB is also trialling a key ring-based one-time password generating device with 23,500 of its customers.

C) WEB SERVICES – SECURITY DISASTER?

URL – <http://www.eweek.com>

AJAX Vulnerabilities Could Pose Serious Risks : August 3, 2006

By Matt Hines

News Analysis: Sloppy programming and the rush to add Web 2.0 technology to Web sites could create a significant attack vector that threatens businesses and private users alike.

LAS VEGAS—AJAX technology is rapidly being adopted by online businesses to help boost the interactivity of their Web sites, but a long list of potential vulnerabilities introduced by inexperienced programmers could create a troubling security landscape for Web 2.0 technologies.

Speaking at the ongoing Black Hat security conference being held here July 31 - Aug. 3, Billy Hoffman, lead research engineer in the labs division of Atlanta-based security software maker SPI Dynamics, outlined a range of shortcomings he sees in the current development process for most common AJAX (Asynchronous JavaScript and XML) applications. AJAX is an extension to the JavaScript programming language that is used to improve the responsiveness of Web sites by automating the exchange of information between browsing software and sites' back-end Web servers.

For instance, the technology can allow a Webmail site to automatically download messages into a user's inbox without requiring the individual to refresh their browser screen. Well-known sites such as Google Maps, Yahoo and MySpace already employ AJAX tools in a number of ways. Hoffman maintains that the current push by businesses to add AJAX tools to improve their sites and Web applications could create a slew of serious vulnerabilities, as inexperienced developers fail to properly protect their work and attackers learn to use the benefits of AJAX to their advantage.

"AJAX applications have a huge attack surface, much larger than traditional applications," Hoffman said. "And the buzz around AJAX is creating immense security implications, as the available knowledge bases and types of resources available for developers are poor." PointerFor advice on how to secure your network and applications, as well as the latest security news, visit Ziff Davis Internet's Security IT Hub.

As more programmers begin to work with AJAX, there will be an opportunity for hackers to launch a range of serious threats against sites with insufficient defenses in place, according to Hoffman. The Yamanner virus that struck Yahoo's Webmail system and the Samy worm attack that targeted users of the popular MySpace social networking site reflect the types of attacks that Hoffman said he believes will be more prevalent in the years to come as AJAX becomes more pervasive.

Whereas the data used in more traditional Web applications exists largely on back-end servers, AJAX extends programs across both the client device and the server, creating far more opportunities for hackers to deliver malware onto sites. While a traditional online form requires users to hit submit to transmit all of their information to a Web site, creating a single communication that could be targeted by malware programs, an AJAX-enabled form that automatically relays the data from each field as data is entered will launch multiple transmissions that virus writers can latch into, Hoffman said.

By exploiting shortcomings in AJAX programmers' work, hackers may also be able to gain access to Web applications themselves and wreak havoc with online businesses. "Now [an attacker] is inside your application and can create a pipeline that allows them to see all the function names,

variables and parameters of your site," Hoffman said.

AJAX could also serve to amplify the potential of so-called cross-site scripting attacks, which seek to inject code onto legitimate Web sites in order to mislead users and steal their information. So-called screen-scraping attacks and Web session hijacking attempts, both of which also seek to steal users' data, could also be performed more easily by taking advantage of AJAX. By allowing attackers to utilize the behind-the-scenes nature of the technology to escalate their threats by requesting multiple streams of data from sites, outsiders could garner even greater levels of information, Hoffman said.

"AJAX is already present in every modern browser, and it has nothing to do with the Web server, that's part of the reason it's so bad," he said. "Even though AJAX says you're only allowed to talk back to a host, that's still a problem, as it can be used to amplify scripting on a site; short of two-factor authentication, it can get through any log-in sequence."

Hoffman directly criticized publishers of AJAX development manuals, who he said are adding to the problem by failing to warn programmers how to protect their work adequately. Inexperienced AJAX programmers' use of widely available AJAX code in their own programs, a common practice, will create even more problems, he said. Black Hat attendees appeared impressed by the presentation, which included an example of an AJAX attack Hoffman discovered in the wild that targets Microsoft's Atlas development tool kit.

Andrew van der Stock, a security architect at National Australia Bank, based in Melbourne, Australia, said the threats posed by improper use of AJAX likely won't discourage companies from aggressively adopting the technology until major attacks take down popular Web sites and businesses come to understand the potential impact on their bottom lines.

"It will take a number of serious worm attacks on big sites for people to get the message. Customers love AJAX so there's a lot of demand right now," van der Stock said. "Adoption won't slow down and most AJAX developers don't know anything about security."

Other attendees observed that it will take time for awareness of AJAX security issues to become more widely recognized, but said most of the issues touched upon in the session could be easily eliminated once discovered.

"Programming over the Web will require due diligence, but the fixes are fairly simple and easily analyzed," said Chris Hoffman, director of special projects for browser maker Mozilla, in Mountain View, Calif. "The delivery mechanism for fixing the problems is also much faster than client software, and there are other security advantages to AJAX as well."