Femtosecond®
www.femto-second.com

In the News

Volume 1 Issue 7

May 11, 2008

Software Exploits

For some, discovering 0day exploits has become a game. For example, a researcher from Israel has hidden a zero day Internet Explorer exploit on his web page in the form of a treasure hunt [1]. In other news, a hacker server was discovered with 1.4 billion bytes of sensitive data tied to 5,878 Internet locations [2]. It is thought that the hacker was not very sophisticated as no encryption was used to protect the cached information. The continued criminal attacks against web servers have become so prevalent, it is difficult to know which sites can be trusted [3].

Hackers continue targeting the newest operating systems. In the case of Microsoft, one report indicates the PC operating system Vista allowed more hackers though than did the older version, Windows 2000 [4]. One way vendors try to maintain software integrity is to issue patches. Microsoft, for example, will be patching 4 security problems during May [5]. When properly configured, the central patch distribution can be a good approach. However, if a customer of any software product can be tricked into installing a patch generated by a bad actor, rogue software can be installed. Moreover, there are warnings of patch update exploits [6]. Case in point, there is a report that the HP Software Update Tool has flaws that could allow remote code execution [7]. Patch problems are not limited to personal computers but include mobile devices. In one instance, an Apple iPhone Trojan horse exploit was purported to be an important firmware update [8]. In the old *Orange Book* [9] days, secure distribution of software was only required at the highest level (A1 level of assurance). Today a product without trusted distribution would not last long. Fortunately, digitally signed software and patches can provide the assurance that the product is legitimate and from the correct source. Unfortunately, cryptographically strong patch protection is not universally used.

At the Microsoft BlueHat hacker sessions, holes in anti-virus software were easily discovered [10]. Given these products are a key safeguard in protecting systems we could be in for more unpleasant surprises in the near future. Once vulnerabilities are discovered and patches are distributed; however un-patched products are still at risk. Some vendors believe that providing few vulnerability details restricts malware writers from exploiting their product. Perhaps this is why the Adobe security patch issued in February contained little information on the actual vulnerabilities [11]. As long as software is exposed to the Internet, patching security vulnerabilities will remain a critical IT security task. Vendors are improving the time it takes to issue patches with the time between vulnerability discoveries and patch distribution decreasing [12].

There are programs called rootkits designed to take full control of the

(Continued on page 2)

Malicious Attacks

Some hackers are trying to inflict physical pain on their victims. Recently, hackers compromised an epilepsy forum and posted flashing images designed to trigger near-seizure reactions [1]. Hackers willing to cause physical pain might be tempted to attack critical infrastructure controlled computers with more dire consequences.

However, the main motivation for malicious attacks continues to be profit. Consider as the US annual tax deadline approached, tax related phishing attacks emerged [2]. Some malware is used to support unwanted advertisements. For example, over 500,000 instances of a Trojan horse *Downloader-UA.h* have been detected in multi-media files (MP3 and MPEG) [3].

In other news, the Srizbi botnet is estimated to be

(Continued on page 2)

Inside this issue:

Special points of interest:

- Counterfeit Cisco routers were installed in Government networks
- Police nab suspects after remotely controlled picture taken by the stolen computer
- US regulators close $2.1 billion FDIC insured bank

Software Exploits

(Continued from page 1)

computer. Root has its origins in the UNIX world and represented the highest privileged user. Recently, a proof-of-concept rootkit was designed to run in the protected portion of a processor's memory space, outside of the operating system, completely undetectable by security software [13]. This is a compelling reason for considering hardware based solutions that operate independent of the operating system memory space. A properly configured BitLocker or smart card implementation may eventually be a necessity for Internet applications.

1. McMillan, Robert, IDG News Service, *0day Treasure Hunt: Researcher Hides IE Attack on Web*, May 7, 2008.
2. Miller, Chuck, SC Magazine, *Massive hacker server discovered*, May 6, 2008.
3. Gage, Deborah, *San Francisco Chronicle, Internet criminals gaining ground, experts say*, May 6, 2008.
4. Claburn, Thomas, Information Week, *Windows Vista More Vulnerable To Malware Than Windows 2000*, May 8, 2008.
5. McMillan, Robert, IDG News Service, *Four Microsoft Security Patches Due Next Week*, May 8, 2008.
6. Espiner, Tom, ZDnet (UK), *Defend against patch-based exploits, warns Sans*, May 6, 2008.
7. Tung, Liam, ZDNet Asia, *Multiple flaws found in HP Software Update tool*, April 29, 2008.
8. Lawton, George, IEEE Computer, *Is It Finally Time to Worry about Mobile Malware?*, May, 2008.
9. DoD 5200.28-STD, *Department of Defense Trusted Computer System Evaluation Criteria*, 1985
10. Mills, Elinor, Cnet News Blog, *Antivirus holes, browser spies are highlights at Microsoft's BlueHat hacker sessions*, May 2, 2008.
11. Keizer, Gregg, Computerworld Security, *Adobe breaks silence on February's PDF bugs*, May 7, 2008.
12. Grimes, Roger A., ComputerWorld, *Zero-second exploits*, May 10, 2008.
13. McMillan, Robert, PC World, *Hackers Find a New Place to Hide Rootkits*, May 9, 2008.

Secrecy, once accepted, becomes an addiction.—Edward Teller

Malicious Attacks

(Continued from page 1)

generating 50% of all SPAM operating from approximately 300,000 zombie computers [4].

As we consider various attacks, it is worth examining new controls. In one case, the owner of a stolen Mac used a remote control program to take a picture of a suspect [5]. There is no reason such controls couldn't be applied to other computers, perhaps limiting the incentive for criminals considering stealing computers. It also highlights the risk of having a built in camera should the computer be compromised. Bad actors could have a remote audio visual monitoring capability culminating in loss of privacy.

1. Robertson, Jordan, Associated Press, *Hackers' posts on epilepsy forum cause migraines, seizures*, May 7, 2008.
2. Harris, Sheryl, Newhouse News Service, *Scams target payers, tax pros*, April 13, 2008.
3. Savvas, Antony, Computer Weekly, *Major media malware attack breaks out on file-sharing networks*, May 7, 2008.
4. Pauli, Darren, Computerworld Australia, *Parasitic botnet spams 60 billion a day*, May 8, 2008.
5. Foderado, Lisa W., The New York Times, *Stolen Laptop Helps Turn Tables on Suspects*, May 10, 2008.

DHS in the News

The Department of Homeland Security (DHS) National Cyber security Division drew criticism from senators for not providing enough information to the public [1]. DHS will withhold information as seen in the response to the 2002 snmp ASN.1 vulnerability [2]. At the same time, the Transportation Worker Identity Credential (TWIC) compliance goal has slipped from September 25, 2008 to April 15, 2009 [3]. The TWIC and other smart card initiatives are critical for establishing strong identification and authentication.

In related news, the Senate Committee on Homeland Security and Governmental Affairs is calling for ideological communications to counter the messages originating from terrorist [4]. On the House side, Rep. James Langevin (D-R.I.), introduced Homeland Security Network Defense and Accountability Act of 2008 which would require DHS to determine contractor cybersecurity capabilities before signing a contract [5]. The bill, if enacted, would also place qualifications on the DHS CIO.

1. Lipowicz, Alice, FCW, *DHS cybersecurity strategy draws fire*, May 5, 2008.
2. Lemos, Robert, ZDnet, *SNMP bugs put Net traffic at risk*, February 13, 2002.
3. Chan, Wade-Hahn, FCW, *DHS delays TWIC deadline*, May 5, 2008.
4. Bain, Ben, *Internet strategy said needed to limit terrorism*, May 8, 2008.
5. Lipowicz, Alice, Washington Technology, *House bill targets DHS cybersecurity efforts*, May 9, 2008.

China

Microsoft broke ground on a new R&D campus in Beijing that will employ 1,500 researchers (growing to 3,000) [1]. China has also established a company to manufacture their own jumbo jets [2]. This at a time when currency continues to flow into China. The March trade deficit with China fell 12.4 percent to $16.1 billion, the smallest level in two years [3]. In contrast with the US Federal Reserve lowering interest rates, China is opting to maintain a tight money policy [4].

In addition to an economic giant, China continues to modernize and expand its military capabilities. For years, there were rumors of a nuclear submarine base and now there is photographic evidence of the base at Hainan Island [5].

China continues making news in other parts of the world. There are reports that China has mounted cyber attacks against India, looking for network and computer weaknesses [6]. Perhaps this is one reason that India plans to expand its cybersecurity capability [7].

Closer to home, the FBI broke up a counterfeit distribution network that sold fake Cisco equipment (made in China) to government agencies [8]. If Government customers are purchasing counterfeit hardware, how difficult would it be for including malicious back doors? Failure to contain these problems could be catastrophic in any future military engagement. Perhaps this is one reason that DARPA is funding research into ways to identify hardware back doors [9].

1. Lenon, Sumner, IDG News Service, *Microsoft Breaks Ground on $280M Beijing R&D Center*, May 6, 2008.
2. Associated Press, China establishes company to make its own jumbo jets, May 11, 2008.
3. Crutsinger, Martin, Associated Press, *March trade deficit drops by bigger-than-expected amount*, May 9, 2008.
4. Yanping, Li, Bloomberg, *China to Stick With Tight Monetary Policy, Wang Says*, May 9, 2008.
5. Northam, Jackie, National Public Radio, *China's Underground Submarine Base Scrutinized*, May 9, 2008.
6. Bagchi, Indrani, *The Times of India, China mounts cyber attacks on Indian sites*, May 5, 2008.
7. Middle East Times, *Indian army to boost cybersecurity*, May 2, 2008.
8. Lawson, Stephen, and McMillan, Robert, IDG News Service, *FBI Worried as DoD Sold Counterfeit Networking Gear*, May 9, 2008.
9. Adee, Sally, IEEE Spectrum, *The Hunt for the Kill Switch*, May 2008.

I hear and I forget. I see and I remember. I do and I understand. –Confucius

Financial Landscape

The ANB Financial National Association banks with approximately $2.1 billion in assets was closed by Federal regulators [1]. However, the good news is that former Fed Chairman, Alan Greenspan predicts the worse of the credit crisis is over [2]. In the interim, Fannie Mae [3] and UBS [4] are reporting multibillion dollar quarterly losses. Furthermore, Citigroup plans to cut their assets from $2.2 trillion down to $1.7 trillion [5].

The March trade deficit fell 5.6 percent to a mere $58.2 billion [6]. Given the high cost of oil imports, this implies that imports of other goods and services fell by a higher percentage.

1. Associated Press, Bentonville, *Federal regulators close Arkansas bank ANB Financial*, May 9, 2008.
2. Reuters, *Greenspan upbeat on credit crisis-sources*, May 9, 2008.
3. Gordon, Marcy, AP, *Fannie Mae loses $2.2B in 1Q, warns of severe weakness*, May 6, 2008.
4. Abegg, Ernst E., AP, *UBS reports 1Q net loss $11 billion*, May 6, 2008.
5. Read, Madlen, Associated Press, *Citigroup to shed nearly $500B in assets*, May 9, 2008.
6. Crutsinger, Martin, Associated Press, *March trade deficit drops by bigger-than-expected amount*, May 9, 2008.

Success is to be measured not so much by the position that one has reached in life as by the obstacles which he has overcome.–Booker T. Washington

Phony email

Phony email or phishing attacks are targeted against most Internet users. A number of executives are being targeted with fake subpoenas and many have fallen for the scam [1].

Perhaps the widest concern are those attacks against customers of financial institutions. These attacks are targeting not only the large banks but smaller ones. For example, for a $90 bonus, First Tennessee Bank customers are asked to enter their private bank information [2]. Attacks such as these are many times successful because the content seems reasonable. In contrast the, *you won a million dollar prize,* message is more suspect. One could reasonably expect a $90 bank bonus.

The quality of phishing attacks is such that consumers may find it difficult to discern legitimate from bogus email. In short, if an email is not properly digitally signed by a source you trust, then caution should be used.

1. Chapman, Glenn, AFP, Hackers harpoon US executives with phony email subpoenas, May 5, 2008.
2. WVLT, *First Tennessee Bank trying to cast off phishing scammers*, April 9, 2008.

Identity Theft

A former contractor for the US Navy admitted selling military personnel identify information to an undercover FBI agent [1]. Before wide-scale bot-net attacks, insiders were considered the greatest risk.

In the past, financial institutions have absorbed customer losses due to Internet fraud. In the United Kingdom (UK), the financial institutions are taking a harder line and may not reimburse customers for losses [2]. The UK has had its share of identity theft problems. For example, last November, civil servants lost sensitive information on 25 million people [3].

1. Kaplan, Dan, SC Magazine, *Military contractor pleads guilty to ID theft*, May 5, 2008.
2. Thompson, Lauren, The Times Online, *How to get safe online*, April 24, 2008.
3. Ellson, Andrew, The Times Online, *Cyber crime: bigger than drugs and aimed at you*, November 23, 2007.