Femtosecond®
www.femto-second.com

In the News

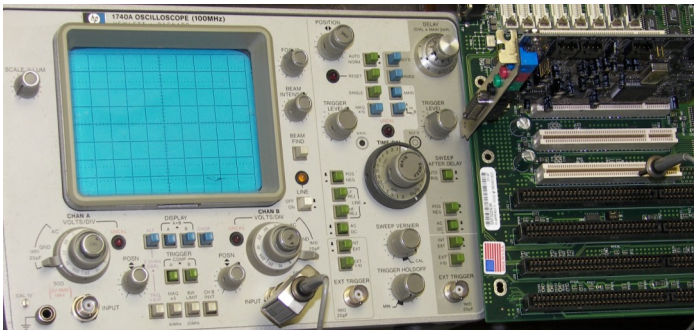
Volume 1 Issue 6

May 4, 2008

Cybercrime Tools

Cybercrime tools can be categorized as supporting law enforcement, state intelligence gathering, or nefarious bad actors. Microsoft has developed a USB tool for law enforcement that allows quick extraction of computer information for the purpose of computer forensics [1]. The tool includes software that as long as the computer is left on, encrypted data can be extracted [2]. However, if the computer is shut down, encrypted data can't be opened. Microsoft has denied that they are providing a backdoor to circumvent Vista encryption capabilities including BitLocker [3]. This tool illustrates how malicious software could effectively perform the same function and decrypt encrypted files. Microsoft is also helping law enforcement with a bot-busting tool that uses data from the 450 million users that installed the malicious software removal tool [4].

Looking at intelligence gathering tools, the U.S. does not have a monopoly. One Senator has suggested that the Chinese Government plans to install hotel filters to monitor Olympic visitor Internet access [5]. Sometimes governments do not cooperate in efforts to abate cyber attacks. This was evidenced in the case of Estonia which suffered weeks of cyber attacks, while Russia refused to help [6]. As Government intervention in abating cyber attacks becomes more prevalent some of the current intelligence exploits will be sacrificed. For example, intelligence analysts exchanged information with our allies following observed active exploits on their networks [7]. This makes perfect sense for if an exploit cripples the domestic or allied economies, where will funding for intelligence gathering operations originate?



Yesterday's Tool

In a unique twist, malicious software (malware) writers are trying to protect their interests. One approach used is threatening to turn in violators to anti-virus companies [8]. Hackers have been successful in developing malware that exploits vulnerabilities. Recently, hundreds of thousands Microsoft web servers were subjected to an SQL injec-

(Continued on page 2)

More Bank Losses

In the latest wave of bank losses for this quarter, the Deutsche Bank swung to a 141 million euro loss and the Allianz will write-down around 900 million euros [1]. Germany is bailing out the Düsseldorf-based WestLB bank to the tune of $7.8 billion [2].

As western banks continue their slide, three of the top four banks are now in China [3]. This illustrates the shift from U.S. financial institution to international banks. Similarly, the Kuwait Investment Authority is planning to increase its current $3 billion in Citigroup and $2 billion in Merrill Lynch [4]. At the same time, the oil rich Gulf States are considering pegging the price of oil on currencies other than the U.S. Dollar [5]. These events signal the decline in U.S. economic power.

(Continued on page 2)

Inside this issue:

Cybersecurity	3
States	3
Hedge Funds	4
Backscatter SPAM	4
30 years of SPAM	4

Special points of interest:

- 3 of the 4 largest banks in the world are now in China

CybercrimeTools

(Continued from page 1)

tion attack [9].

1. Romano, Benjamin J., Seattle Times, *Microsoft device helps police pluck evidence from cyberscene of crime*, April 29, 2008.
2. Gohring, Nancy, IDG News Service, *Microsoft Helps Law Enforcement Get Around Encryption*, April 29, 2008.
3. Vamosi, Robert, cnet, *Microsoft serves law enforcement free COFEE*, April 30, 2008.
4. McMillan, Robert. IDG News Service, *Microsoft Botnet-hunting Tool Helps Bust Hackers*, April 29, 2008.
5. Hananel, Sam, Associated Press, *Senator: China plans to spy on Olympic hotel guests*, May 1, 2008.
6. Bain, Ben, FCW, *Cybersecurity's new world order*, April 28, 2008.
7. Krebs, Brian, Washington Post, *White House Plans Proactive Cyber-Security Role for Spy Agencies*, May 2, 2008.
8. Robertson, Jordan, Associated Press, *Criminals try to "copyright" malware*, April 30, 2008.
9. Krebs, Brian, Washington Post, *Hundreds of Thousands of Microsoft Web Servers Hacked*, April 25, 2008.

It is common sense to take a method and try it. If it fails, admit it frankly and try another. But above all, try something.–Franklin D. Roosevelt

More Bank Losses

(Continued from page 1)

Helping mitigate bank losses has become a global effort. The Federal Reserve is coordinating with central European central banks, boosting reserves supplied to banks [6].

Closer to home, a CEO of two Philadelphia companies pleaded guilty to defrauding Wachovia Bank and First Union banks of $1.45 million from 2001 to 2005 [7].

1. Kennedy, Simon, Market Watch, *Deutsche Bank, Allianz take fresh write-downs*, April 29, 2008.
2. Casert, Raf, Associated Press, *EU bails out German bank for $7.8 billion*, April 30, 2008.
3. AFP, *Three Chinese banks in world's top four: study*, April 30, 2008.
4. Westbrook, Jesse, and Cook, Peter, Bloomberg, *Kuwait Sovereign Fund May Boost Citi, Merrill Stakes*, May 1, 2008.
5. MacDonald, Fiona, and Brown, Matthew, Bloomberg, *Gulf States May End Dollar Pegs, Kuwait Minister Says*, May 1, 2008.
6. Crutsinger, Martin, Associated Press, *Fed joins with European banks to battle credit crisis*, May 2, 2008.
7. Philadelphia Business Journal, *Former CEO of Phila.-area companies admits bank fraud*, May 2, 2008

Next Administration Cybersecurity

Preparations for the next administration's cybersecurity agenda are picking up steam. One group, the Commission on Cyber Security for the 44th Presidency met for a second time. Among their assertions was cybersecurity is not a technical issue [1]. However, it is unlikely that solutions that do not include technology will be successful.

The next president will be confronted with cybersecurity issues as our potential adversaries gain a competitive edge. There is a growing gap in the U.S. competitiveness [2]. For example, China's military has made cybersecurity one of its topmost priorities [3]. We can expect China to continue to its march toward dominance in other technology. Consider that China has 200,000 engineers and technicians involved with Space R&D [4].

The White House

1. Jackson, William, GCN, *Experts struggle with cybersecurity agenda*, April 29, 2008.
2. Mervis, Jeffrey, ScienceNOW Dailey News, *Has U.S. Science Lost its Competitive Edge?*, April 29, 2008.
3. UPI (New Delhi), *Indian army to boost cybersecurity*, May 2, 2008.
4. Covault, Craig, Aviation Week & Space Technology, *China's military secrecy clouds its value as exploration partner to Moon and beyond*, May 5, 2008.

Find out just what any people will quietly submit to and you have the exact measure of the injustice and wrong which will be imposed on them.– Frederick Douglass

States

Following 9/11 there have been many changes that impact daily life. These changes are similar to a tax that costs time at airports and reduced foreign travelers [1].

Other domestic security enhancements continue. One theme is stronger identification credentials. In a 6-3 decision, the Supreme Court recently upheld the right for states to demand photo identification for voting [2]. A statutory attempt at requiring a stronger uniform identification is addressed in the Real ID Act of 2005 (P.L. 109-13) that requires improvements to states driver's licenses. However, as the dates for implementing Real ID approach, senators are faulting the DHS for pressuring states [3]. One state, Arizona, has gone so far as to start the legislative process to basically ignore Real ID [4].

Arizona State Flag

1. Joffe, Josef, Washington Post, *Fear Is a Tax, and We're Eagerly Paying it*, May 4, 2008.
2. Sherman, Mark, Associated Press, *Supreme Court says states can demand photo ID for voting*, April 28, 2008.
3. Layton, Lyndsey, Washington Post, *Senators Fault DHS Pressure on Real ID*, April 3, 2008.
4. Pitzl, Mary Jo, The Arizona Republic, *Bill barring state from new U.S. ID plan gets initials ok*, May 2, 2008.

Backscatter

Have you ever received a returned message that you did not send? One trick hackers and spammers do is to use other people's email addresses. By using a real email address, the likelihood of getting through SPAM blockers increases. Cases where the email is rejected and returned to the sender is referred to as backscatter. It is estimated that 2—3 percent of all SPAM uses this technique and it is on the rise [1]. When the message is bounced back, many email products (mail transfer agents) will include a copy of the original message [2]. The danger is that the unsuspecting receiver of the bounced back email may open the message to see what they did wrong. This illustrates that email received may not have been sent by the party that is listed on the from line.

1. McMillan, Robert, IDG News Service, *100 E-mail Bouncebacks? You've Been Backscattered.*, May 2, 2008.
2. Prince, Brian, eWeek, *Backscatter Spam Is Back*, April 4, 2008.

It is a very sobering feeling to be up in space and realize that one's safety factor was determined by the lowest bidder on a government contract .— Alan Shepherd

Thirty years of SPAM

Another milestone was reached this week. May 3 was the 30th anniversary of the first SPAM email [1]. The original SPAM message was an advertisement for the DEC-SYSTEM-20 and the cost for fighting SPAM has grown to an estimated at $42 billion this year [2]. SPAM has come a long way in thirty years. Bad actors now hijack personal computers to use university and military systems to relay junk mail [3].

Law enforcement is trying to shut down SPAM. One Spammer who made $ millions by issuing penny stock advisories, has been sentenced to 21 months in jail and a fine of $714,000 [4].

1. Zeitvogel, Karin, AFP, *For 30 years now, you've been getting spam*, May 2, 2008.
2. Musgrove, Mike, Washington Post, *On Spam's Birthday, Three Cheers for 'Delete'*, May 3, 2008.
3. Broersma, Matthew, Techworld, *Botnet attacks military systems*, May 2, 2008.
4. McMillan, Robert, IDG News Service, *Colorado Penny Stock Spammer Gets Jail Time*, April 30, 2008.

Hedge Fund News

There are a number of incidents of hedge fund fraud that are surfacing in the news. In response, the treasury envisions giving the Fed authority to collect and analyze data from institutions, including hedge funds [1].

Some examples of hedge fund fraud follow. Operating two virtual offices to appear larger, a fund manager is alleged to have bilked investors out of over $1.5 million [2]. The co-founder of the Bayou Group hedge fund was sentenced for his role in cheating investors out of over $400 million [3]. A hedge fund partner in San Diego has been sentenced to 6 year in federal prison and must pay $49 million in restitution [4].

1. Tett, Gillian, and Guha, Krishna, Financial Times, *Treasury eyes stronger powers for Fed*, April 29, 2008.
2. Goldstein, Matthew, Business Week, *Regulators: 'Fund Manager' was a Fraud*, April 30, 2008.
3. New York Times, *Hedge Fund Founder Given 20 Years for Investment Fraud*, April 16, 2008.
4. Associated Press, *Partner in San Diego hedge fund fraud gets 6 years*, April 10, 2008.