A Note From The Editor

With the completion of Tim Hoffman’s series “Get a Job” I completely forgot to ask (until it was too late) the ISSA-COS board members for a short article for the front page. Please forgive me while I prattle on. Hopefully, next month you will hear from someone who knows what they are talking about.

Speaking of the “Get a Job” articles. Tim and I have been discussing reprinting the articles as a single booklet. Our plan is to make them available in a compact format to chapter members so that, if the need arises, they may be more easily shared with those (in and out of the Chapter) who are either actively engaged in looking for employment or considering making a change. The articles will be updated and expanded with additional information that didn’t fit within the newsletter format. Until then, at the next meeting I’ll bring in a few copies of the articles as they appeared in the newsletter (in case someone truly needs them now.) Let me know if you would like for me to e-mail it to you.

Please note on Page 15 that the schedule for 2013 meetings is posted and that the day of the week for the meetings has changed. It will now be on the second Thursday of each month except in December. This new schedule will begin with the first meeting in 2013: January 10th.

Elections for Chapter vacancies are upon us. Details are also on Page 15 of this newsletter. If you know someone (including yourself) who would be a good candidate, please contact one of the Board members.

I need for members to step up with articles, because I know that all of you have something to share. We are all professionals in one of the more exciting fields out there. Share some of that excitement with the rest of us. You have experiences from which others may learn. You have done things in your professional environment that others are considering but don’t know how to accomplish. Or what you have to say may make someone else realize that they had not looked at a problem that way before. I have spoken with many of you at Chapter meetings and know that I can learn from all of you. Are you a reader of IA books? Please provide reviews of books you have read. We could call it the IA Professional’s Bookshelf. These are just a few of the ideas for future articles. Details on how to get them to me are on Page 14.

If you know IA professionals who are not currently members, bring them to one of the meetings. They will get to meet others who are not part of their immediate circle. They can share experiences with those who are in a completely different field of work (defense, non-defense government, banking, medical, infrastructure, etc.)

Don Creamer
RATs and Poison: Can Cyber-espionage Victims Counterhack?

By Stewart Baker • October 13, 2012

More good news for network security: It turns out that the tools attackers use to control compromised computers are themselves full of security holes. A couple of undergrads interning for Matasano Security have reverse-engineered the Remote Access Tools (RATs) that attackers use to gain control of compromised machines.

According to Dark Reading (http://www.darkreading.com/threat-intelligence/167901121/security/vulnerabilities/24008942/popular-rats-found-riddled-with-bugs-weak-crypto.html), Jesse Hertz and Shawn Denbow found numerous flaws in commonly used RATs, including SQL injection, arbitrary file reading, and weak encryption.

“This shows that it is possible, and that it’s not hard, to pick apart attacker tools and come up with proactive defenses against them,” says John Villamil, senior security consultant with Matasano, who served as Denbow and Hertz’s adviser for the project. “If nothing else, it can help forensics companies analyzing traffic from compromises ... and help build tools that analyze these Trojans, and provide signatures [to detect them].”

Vulnerability research into attacker tools is rare, but not unheard of. “It’s very rare to see this type of research,” Villamil says.

RATs, which typically conduct keylogging, screen and camera capture, file management, code execution, and password-sniffing, for example, basically give the attacker a foothold in the infected machine as well as the targeted organization.

This is great news for cybersecurity. It opens new opportunities for attribution of computer attacks, along lines I’ve suggested before: “The same human flaws that expose our networks to attack will compromise our attackers’ anonymity.”

In this case, the flaws identified by Hertz and Denbow could allow defenders to decrypt stolen documents and even to break into the attacker’s command and control link – while the attacker is still on line. That opens up the possibility of a true counterhack, in which the defender exploits a flawed attack to gain control of the attacker’s machine.

It’s only a matter of time before counterhacks become possible. The real question is whether they’ll ever become legal. Both the reporter and the security researcher agree that, “legally, organizations obviously can’t hack back at the attacker.”

I think they’re wrong on the law, but first let’s explore the policy question. Should victims be able to poison attackers’ RATs and then use the compromised RAT against their attacker?

We’ll start with the obvious. Somebody should be able to do this. And, indeed, it seems nearly certain that somebody in the U.S. government — using some combination of law enforcement, intelligence, counterintelligence, and covert action authorities — can do this. (I note in passing, though, that there may be no one below the President who has all these authorities, so that as a practical matter RAT poisoning may not happen without years of delay and a convulsive turf fight. That’s embarrassing, but beside the point, at least today.)

Asking government to do the job has some drawbacks, though. Counterhacking is likely to work best if the attacker is actually on line, when the defenders can stake out the victim’s system, ready to give the attacker bad files, to monitor the command and control machine, and to copy, corrupt, or modify exfiltrated material. Defenders may have swing into action with little warning.

Who is going to do this? Put aside the turf fight. Does anyone think that NSA or the FBI or the CIA have enough technically savvy counterhackers to stake out the networks of the Fortune 500, waiting for the bad guys to show up?

Read the rest here: http://www.volokh.com/2012/10/13/rats-and-poison-can-cyberespionage-victims-counterhack/
Are You Missing Your Coin?

Here is the list of current and former ISSA members that Deborah Johnson has at least one coin for. Please take a look at the list to see if you know any of these folks. The coins can be picked up by proxy, or she can mail them to folks if they can be located. Deborah’s email address is djohnson@swcp.com and her telephone number is 719-329-4495 (voicemail) if folks want to contact her directly. Thank you!

<table>
<thead>
<tr>
<th>A</th>
<th>Corlew, Michael</th>
<th>Hughes, Paul</th>
<th>Mohl, Darrick</th>
<th>Slavick, Mike</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adams, Tim</td>
<td>Coultrap, Michael</td>
<td>Hutchison, James</td>
<td>Moll, Joseph</td>
<td>SMALLEY, JACKIE</td>
</tr>
<tr>
<td>Aguryanov, Sergey</td>
<td>Crout, John</td>
<td>Ingram, Louis</td>
<td>Mondello, Mark</td>
<td>Smith, Harry</td>
</tr>
<tr>
<td>Alexeev, Eugene</td>
<td>Dailey, Shane</td>
<td>Jones, Bryant</td>
<td>Moore, Kathryn</td>
<td>Spencer, Dawn</td>
</tr>
<tr>
<td>Anders, Christopher</td>
<td>de la Garza, Enrique</td>
<td>Jordan, Erin</td>
<td>Morrison, Richard</td>
<td>Spinney, Byron</td>
</tr>
<tr>
<td>Anderson, Richard</td>
<td>Donjon, Dan</td>
<td>Killroy, Margaret</td>
<td>Myers, Ryan</td>
<td>Staggs, Michael</td>
</tr>
<tr>
<td>Andrus, Thip</td>
<td></td>
<td>Kolb, Garrett</td>
<td>Neely, Richard</td>
<td>Stoddard, Lewis</td>
</tr>
<tr>
<td>Archer, Cliona</td>
<td></td>
<td>Krzywonski, Branden</td>
<td>Nieman, Joann</td>
<td>Sullivan, Michael</td>
</tr>
<tr>
<td>Arrington, Charles</td>
<td>Egert, Dan</td>
<td>Laborwit, Al</td>
<td>Norquist, Bruce</td>
<td>Swinnich, David</td>
</tr>
<tr>
<td>Bailey, Craig</td>
<td></td>
<td>Lanham, Michael</td>
<td>Novak, Heath</td>
<td>Tang, Freddy</td>
</tr>
<tr>
<td>Beasley, Marke</td>
<td>Fanberg, Kevin</td>
<td>LeFebvre, Brad</td>
<td>O'Neil, Michael</td>
<td>Taylor, Jeremy</td>
</tr>
<tr>
<td>Bilyeu, Raymond</td>
<td>Farrow, Chris</td>
<td>Levesque, Robert</td>
<td>Oswald, John</td>
<td>Tesch, John</td>
</tr>
<tr>
<td>Birkeland, Rolf</td>
<td>Fernandez, Damian</td>
<td>Lohndorf, Jon</td>
<td>Palm, Scott</td>
<td>Treslin, Manuel</td>
</tr>
<tr>
<td>Bond, David</td>
<td>Frankovich, Dawn</td>
<td>Lorenc, Chad</td>
<td>Paynter, Stephen</td>
<td>Trussell, Terry</td>
</tr>
<tr>
<td>Bone, Regina</td>
<td></td>
<td>Lund, Tim</td>
<td>Peralta, Rex</td>
<td>Tugade, Medarlo</td>
</tr>
<tr>
<td>Borer, Arthur</td>
<td>Freeman, James</td>
<td>Lundmark, Dennis</td>
<td>Playle, Greg</td>
<td>Turner, Deborah</td>
</tr>
<tr>
<td>Bowers, Mark</td>
<td>Fry, Josh</td>
<td></td>
<td>Puryear, Scott</td>
<td>Tyree, George</td>
</tr>
<tr>
<td>Brown, Clark</td>
<td>Guzman, Henry</td>
<td>Malone, David</td>
<td>Ray, Lori</td>
<td>Underwood, Ralph</td>
</tr>
<tr>
<td>Brown, George</td>
<td>Garate, Reynaldo</td>
<td>Mance, Howard</td>
<td>Regan, Joseph</td>
<td>Van Cura, Robert</td>
</tr>
<tr>
<td>Brown, Jason</td>
<td>Gates, Ryan</td>
<td>Mann, John</td>
<td>Rodrigues, Rory</td>
<td>Vulcan, Leland</td>
</tr>
<tr>
<td>Brown, Josh</td>
<td>Gobea, Michael</td>
<td>Marchand, Hummer</td>
<td>Rogelio, Raymond</td>
<td>Walth, Sarah</td>
</tr>
<tr>
<td>Buckley, Lisa</td>
<td>Gonzales, Mark</td>
<td>Martens, Pamela</td>
<td>Ross, Clark</td>
<td>Walls, Todd</td>
</tr>
<tr>
<td>Buehler, Scott</td>
<td>Gosnell, Steven</td>
<td>Martin, Jeremy</td>
<td>Roth, Lee</td>
<td>Weatherford, Mark</td>
</tr>
<tr>
<td>Bull, Justin</td>
<td>Hulman, David</td>
<td>Martinez, Mitch</td>
<td>Saparito, Tia</td>
<td>Weiss, Brian</td>
</tr>
<tr>
<td>Burns, R.</td>
<td>Hardin, David</td>
<td>Masincup, Danny</td>
<td>Sawyer, Jim</td>
<td>White, Steve</td>
</tr>
<tr>
<td>Burton, James</td>
<td></td>
<td>Matthews, Clint</td>
<td>Schierholz, Andrew</td>
<td>Williams, Jarold</td>
</tr>
<tr>
<td>C</td>
<td>Callaghan, John</td>
<td></td>
<td></td>
<td>Wright, Christopher</td>
</tr>
<tr>
<td>Callaway, Ernest</td>
<td>Harper, Brian</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Carlson, George</td>
<td>Hennings, Fred</td>
<td>Martin, Jeremy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chisesi, Dan</td>
<td>Herod, Dan</td>
<td>Martinez, Mitch</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ciampa, John</td>
<td>Herrera, Steven</td>
<td>Masincup, Danny</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Coffman, Darrell</td>
<td>Hill, Butch</td>
<td>Matthews, Clint</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Collier, Andrew</td>
<td>Hinz, Kevin</td>
<td>Menkhus, Mark</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Collins, David</td>
<td>Hoefelmeyer, Ralph</td>
<td>Mercer, Samuel</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Copeland, Brian</td>
<td>Hooper, William</td>
<td>Miles, Tracy</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hughes, Jeff</td>
<td>Modisette, Mark</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
News Ripped From the Headlines

October 17, IDG News Service – (International) **High bandwidth DDoS attacks are now common, researcher says.** Distributed denial-of-service (DDoS) attacks with an average bandwidth over 20Gbps have become commonplace in 2012, according to researchers from DDoS mitigation vendor Prolexic. In 2011, such high-bandwidth attacks were isolated incidents, Prolexic’s president said October 16. Very few companies or organizations have the network infrastructure to handle such attacks. Prolexic released its global DDoS attack report for the third quarter October 17. According to the report, there is an 88 percent increase of attacks from the same quarter of 2011. However, compared to the second quarter of 2012, the number of attacks actually declined by 14 percent. The average attack bandwidth during the third quarter of 2012 was 4.9Gbps, which represents a 230 percent increase compared to 2011, and an 11 percent increase compared to the previous quarter. The average attack during the third quarter of 2012 lasted 19 hours, slightly longer than in the second quarter. The majority of attacks — over 81 percent — targeted the infrastructure layer, while 18.6 percent of attacks targeted the application layer. The top three countries where DDoS attacks originated were China with 35 percent of attacks, the United States with 28 percent, and India with 8 percent. Source: [http://www.computerworld.com/s/article/9232487/High_bandwidth_DDoS_attacks_are_now_common_res_searcher_says](http://www.computerworld.com/s/article/9232487/High_bandwidth_DDoS_attacks_are_now_common_res_searcher_says)

October 8, The Register – (International) **Bing is the most heavily poisoned search engine, study says.** Bing search results are more affected by poisoning than those of other search engines, according to a study by SophosLabs. Search engine poisoning attacks are designed to skew results so that dodgy sites — anything from malware infected Web sites to payday loan sites — appear prominently in the index of sites related to popular search terms. In many cases, the tactic is so successful that malware sites appear in the first page of results for popular search terms, sometimes much higher than legitimate Web sites. More recently, miscreants began trying to manipulate image search results. Source: [http://www.theregister.co.uk/2012/10/08/bing_worst_search_poisoning/](http://www.theregister.co.uk/2012/10/08/bing_worst_search_poisoning/)

October 25, Softpedia – (International) **Advanced malware allows cybercriminals to empty a bank account in one go.** Security firm AVG released its Community Powered Threat Report for the third quarter of 2012. The study focuses on the 2.0 version of the Blackhole exploit kit, the evolution of malware and other threats that marked the past quarter. According to AVG, the Blackhole exploit kit leads both the toolkit and the malware markets with a share of almost 76 percent, respectively 63 percent. Considering that the crimewit’s authors launched the 2.0 version, experts say its market share will grow even further and the attacks it utilizes in will become even more “aggressive” because of the advanced evasion techniques recently integrated into it. “Blackhole is a sophisticated and powerful exploit kit, mainly because it is polymorphic and its code is heavily obfuscated to evade detection by anti-virus solutions. The rapid update capabilities of the kit have also made it challenging for traditional anti-virus vendors to track, which are the main reasons it has a high success rate,” said the CTO at AVG Technologies. “Through our multi-layered security approach with real-time analysis at the endpoint, AVG has been detecting a much higher rate of Blackhole Toolkit-based attacks than other toolkits, as Blackhole’s creator seeks to stay ahead of their competition,” he added. Source: [http://news.softpedia.com/news/Advanced-Malware-Allows-Cybercriminals-Empty-a-Bank-Account-in-One-Go-302135.shtml](http://news.softpedia.com/news/Advanced-Malware-Allows-Cybercriminals-Empty-a-Bank-Account-in-One-Go-302135.shtml)

October 15, Ars Technica – (National) **Solar panel control systems vulnerable to hacks, feds warn.** DHS is warning of critical vulnerabilities in a computerized control system that attackers could exploit to sabotage or steal sensitive data from operators of the solar arrays that generate electricity in homes and businesses, Ars Technica reported October 15. A slew of vulnerabilities in a variety of products, including the Sinapsi eSolar Light Photovoltaic System Monitor and the Schneider Electric Ezylog Photovoltaic Management Server, allow unauthorized people to remotely log into the systems and execute commands, warned the Industrial Controls Systems Cyber Emergency Response Team in a recent alert. Other vulnerable devices include the Gavazzi Eos-Box and the Astrid Green Power Guardian. Proof-of-concept code available online makes it easy to exploit some of the bugs. The advisory is based on a report published in September that disclosed SQL injection vulnerabilities, passwords stored in plain text, hard-coded passwords, and other defects that left the devices open to tampering. According to researchers, the vulnerable management server is incorporated into a photovoltaic products from several manufacturers. “All the firmware versions we analyzed have been found to be affected by these issues,” the researchers wrote. “The software running on the affected devices is vulnerable to multiple security issues that allow unauthenticated remote attackers to gain administrative access and execute arbitrary commands,” the researchers said. Source: [http://arstechnica.com/security/2012/10/solar-panel-control-systems-vulnerable-to-hacks/](http://arstechnica.com/security/2012/10/solar-panel-control-systems-vulnerable-to-hacks/)
FBI Expands Cybercrime Division

Federal Bureau of Investigation will hire computer scientists, build new tools and boost collaboration to help catch malicious hackers.

By J. Nicholas Hoover, InformationWeek
October 30, 2012

The Federal Bureau of Investigation is adding resources, building new tools, increasing hiring and expanding collaboration with local groups as part of its Next Generation Cyber Initiative, an effort to overhaul the FBI’s Cyber Division, the agency announced last week.

The FBI has long been a force in combating cybercrime. In the last year alone, the agency has busted dozens involved in the online trafficking of credit card and bank account data, arrested key members of the Anonymous and LulzSec hacktivist groups, broken up a sophisticated gang of online bank fraudsters, taken down a small-town mayor for hacking a website calling for his recall and worked closely with international officials to disrupt a botnet that had stolen $14 million.

However, the FBI still wants to get better, especially in its ability to attribute attacks to the hackers behind them. Attribution of cybercrime has long been the bane of law enforcement due to the nature of the Internet and the ability of hackers to spoof their IP addresses and rely heavily on proxies. As the adage says, on the Internet, nobody knows you’re a dog.

Over the course of the last year, the law enforcement agency has launched an effort to “uncover and investigate Web-based intrusion attacks and develop a cadre of specially trained computer scientists able to extract hackers’ digital signatures from mountains of malicious code,” the FBI said in a press release. For example, the FBI has increasingly hired computer scientists to work alongside agents as part of cyber investigations.

The question the FBI is attempting to resolve is "who is conducting the attack or the exploitation and what is their motive," FBI assistant director of criminal, cyber, response and services Richard McFeely said in a statement. "In order to get to that, we’ve got to do all the necessary analysis to determine who is at the other end of the keyboard perpetrating these actions."

Such an effort requires not only new talent and better tools, but also ongoing collaboration with organizations that get hacked and other government agencies. To that end, the FBI said that its agents are working to build relationships with critical infrastructure companies in industries like finance and transportation. The FBI is also sharing a lot of information with the Department of Defense, Department of Homeland Security and National Security Agency as part of the National Cyber Investigative Joint Task Force.


---

Quote of the Month

“The reader must remember that if he defends against everything, he defends nothing. It is not possible to stop all the badness.

“Organizations should determine what is critical to their business operations. In other words, what systems must be secured versus just observed. Some systems must be expendable with an understanding that they will be best efforts to secure but not essential. Security professionals must get used to the idea that there are casualties in cyberspace. They must focus their efforts on securing critical business operations in cyberspace and use intelligence preparation of the operational environment to focus their efforts to that end.”

Matthew Stern
Security Week

If you wish to read the article from which this quote was taken, go here: [http://www.securityweek.com/cyber-intelligence-identifying-threat-and-understanding-terrain-cyberspace](http://www.securityweek.com/cyber-intelligence-identifying-threat-and-understanding-terrain-cyberspace)
The Russian Mob Shows Chinese Hackers How It's Done

Strategy Page October 4, 2012

China's Cyber War hackers are getting cocky and careless. Internet security researchers have found identical bits of code (the human readable text that programmers create and then turn into smaller binary code for computers to use) and techniques for using it in hacking software used against Tibetan independence groups and commercial software sold by some firms in China and known to work for the Chinese military. Similar patterns have been found in hacker code left behind during attacks on American military and corporate networks. The best hackers hide their tracks better than this.

It's also been noted that Chinese behavior is distinctly different from that encountered among East European hacking operations. The East European hackers are more disciplined and go in like commandos, and get out quickly once they have what they were looking for. The Chinese go after more targets with less skillful attacks and stick around longer than they should. That's how so many hackers are tracked back to China, often to specific servers known to be owned by the Chinese military or government research institutes.

The East Europeans have been at this longer and most of the hackers work for criminal gangs, who enforce discipline, select targets, and protect their hackers from local and foreign police. The East European hacker groups are harder to detect (when they are breaking in) and much more difficult to track down. Thus the East Europeans go after more difficult (and lucrative) targets. The Chinese hackers are a more diverse group. Some works for the government, many more are contractors and even more are independents, who often slip over to the dark side and scam Chinese. This is forbidden by the government and these hackers are sometimes caught and punished, or simply disappear. The Chinese hackers are, compared the East Europeans, less skilled and disciplined. There are some very, very good Chinese hackers, but they often lack adult supervision (or some Ukrainian gangster ready to put a bullet in their head is they don't follow orders exactly.)

For Chinese hackers that behave (don't do cybercrimes against Chinese targets) the rewards are great. Large bounties are paid for sensitive military and government data taken from the West. This encourages some unqualified hackers to take on targets they can't handle. This was seen recently when one group of hackers were caught trying to get into a high-security network in the White House (the one dealing with emergency communications with the military and nuclear forces.)

http://www.strategypage.com/htmwb/htiw/articles/20121004.asp

New security threat at work: Bring-your-own-network

By Lucas Mearian, October 11, 2012, Computerworld

Even as IT pros wrestle with the bring-your-own-device (BYOD) trend, corporate security is being further complicated by another emerging trend: bring your own network (BYON).

BYON is a by-product of increasingly common technology that allows users to create their own mobile networks, usually through mobile wireless hotspots. Security professionals say BYON requires a new approach to security because some internal networks may now be as insecure as consumer devices.

Jim Kunick, an attorney with the Chicago law firm Much Shelist, said BYON represents a more dangerous threat to data security than employees who bring their own smartphones or tablets into the office. "The network thing blows this up completely, because it takes the data out of the network the company protects," he said. "There's no way to ensure the security of that data. People are running corporate apps and processing corporate and client data using networks that may or may not be secure.

"I mean, no one is sure the Boingo network is secure," he said.

Kunick, an intellectual property attorney, said BYON is cropping up in start-ups, particularly at software development firms and entities that rely on cloud services.

"[BYON] allows people to run applications in three different cloud-based environments at one time because they're on their own network, they're on a network that they contracted with and they're on the corporate network," he said.

Initially, BYON should be seen as a policy issue where a company sets rules that ban employees from running private networks. Employees who use hotspots also have contracts with network service providers, he said, and they need to understand how data on that network may be used or further disclosed.

Read the rest here:
http://www.computerworld.com/s/article/9232302/New_security_threat_at_work_Bring_your_own_network
Government Agencies Get Creative In Advanced Persistent Threat Battle

By Kelly Jackson Higgins, Oct 03, 2012

SANS National Cybersecurity Conference -- BALTIMORE, MD. -- A handful of security professionals at the U.S. Department of Energy's laboratories were getting weary of trying to repel advanced persistent threat (APT)-type attacks and keep up with the latest threats. So they decided to roll their own tool to automate intelligence-sharing among the agency's national labs and scores of smaller labs.

"A couple of us were basically tired of losing [the race to keep up with new threat intelligence], so we decided we were going to do something about it. We were tired of getting together in little rooms" to share information, said Matt Myrick, senior cybersecurity engineer at DOE's Lawrence Livermore Laboratory, in a presentation here today. So Myrick and a handful of colleagues from Sandia Labs, Los Alamos Labs, and DOE's Pantex plant wrote a Python-based tool to block malicious websites, hashes, spear-phishing attacks. The so-called Master Block List (MBL) runs on an Apache server and can be integrated with any application to share real-time threat data.

Myrick says the tool is simple -- not XML-based, like some open-source tools -- and has helped unite the various labs so they can share attack information quickly. "It's nothing fancy: It's less than 300 lines of code," he says. "Talking about indicators of compromise is hard, and so is parsing PDFs, Office, and XML, for most [people]," he said. The goal was to make it easy for anyone to use.

Federal agencies like Lawrence Livermore Labs are attractive targets for cyberespionage attackers looking for valuable research and other intelligence. But federal budgets are tight, so amid a constant battle to fight back APTs, some agencies are opting to build their own solutions using existing tools and resources.

Debora Plunkett, information assurance director at the National Security Agency (NSA), in a keynote address here today pointed to the recent breaches of major financial institutions as an example of how even the most security-conscious organizations are getting hit. "We can all agree that all of these targeted companies are among the best at security, yet they were still vulnerable to attack," Plunkett said. Given the value of these organizations, the attacks are "truly highway robbery," she said.

"There is no person or business network that is immune," Plunkett said.

Some 10 DOE organizations in addition to Lawrence Livermore employ its MBL tool, which incorporates threats detected by the various agency sites, as well as from various threat intelligence sources.

"There have been a couple of cases where we've been protected against attack campaigns that others have fallen victim to because they are not" using the list, Myrick told Dark Reading. The breach suffered by Oak Ridge Laboratory last year that forced the lab to temporarily shut down Internet access originated from a convincing-looking spear-phishing email that Myrick says Lawrence Livermore had blocked later that day, after the East Coast-based Tennessee lab had gone home.

U.S. government agencies aren't the only ones with tight budgets. The Australian Defence Signals Directorate (DSD) in 2011 identified some 327 different APT-type attacks, more than 200 of which were not detected by traditional security controls. As part of an effort to roll out the agency's designated top mitigation strategies (including better patching, among other things), Australia's Department of Industry, Innovation, Science, Research and Tertiary Education (DIISRTE) employed a combination of existing tools to whitelist applications.

"We didn't have a budget for whitelisting, so we looked for existing" features in our security products, said David Cottingham, who helped spearhead the project at DIISRTE. Cottingham and his team took the whitelisting feature in the agency's Symantec Endpoint Protection software and now block all new applications that aren't preapproved by the agency.

Cottingham, who is now with Foresight Consulting, says a combination of the agency's now-automated patching process and whitelisting has basically stopped most APT-type attacks from escalating. "We found 200 threats and passed them over to DSD," he said.

Those are the attacks that the agency sees, however. Cyberespionage attacks are often camouflaged to maintain their foothold in the victim's network.

"We know APTs are a danger to all organizations. And they are not actually that advanced at all: It's more like targeted, persistent threats," said David Cottingham, who helped spearhead the project at DIISRTE. "If you're lucky to detect them, you'll be continually battling them and cleaning them up."

Read the rest here:
Computer Viruses Are "Rampant" on Medical Devices in Hospitals

By David Talbot, technology Review, October 17, 2012

A meeting of government officials reveals that medical equipment is becoming riddled with malware.

Computerized hospital equipment is increasingly vulnerable to malware infections, according to participants in a recent government panel. These infections can clog patient-monitoring equipment and other software systems, at times rendering the devices temporarily inoperable.

While no injuries have been reported, the malware problem at hospitals is clearly rising nationwide, says Kevin Fu, a leading expert on medical-device security and a computer scientist at the University of Michigan and the University of Massachusetts, Amherst, who took part in the panel discussion.

Software-controlled medical equipment has become increasingly interconnected in recent years, and many systems run on variants of Windows, a common target for hackers elsewhere. The devices are usually connected to an internal network that is itself connected to the Internet, and they are also vulnerable to infections from laptops or other device brought into hospitals. The problem is exacerbated by the fact that manufacturers often will not allow their equipment to be modified, even to add security features.

In a typical example, at Beth Israel Deaconess Medical Center in Boston, 664 pieces of medical equipment are running on older Windows operating systems that manufacturers will not modify or allow the hospital to change—even to add antivirus software—because of disagreements over whether modifications could run afoul of U.S. Food and Drug Administration regulatory reviews, Fu says.

As a result, these computers are frequently infected with malware, and one or two have to be taken offline each week for cleaning, says Mark Olson, chief information security officer at Beth Israel.

"I find this mind-boggling," Fu says. "Conventional malware is rampant in hospitals because of medical devices using unpatched operating systems. There's little recourse for hospitals when a manufacturer refuses to allow OS updates or security patches."

The worries over possible consequences for patients were described last Thursday at a meeting of a medical-device panel at the National Institute of Standards and Technology Information Security & Privacy Advisory Board, of which Fu is a member, in Washington, D.C. At the meeting, Olson described how malware at one point slowed down fetal monitors used on women with high-risk pregnancies being treated in intensive-care wards.

"It's not unusual for those devices, for reasons we don't fully understand, to become compromised to the point where they can't record and track the data," Olson said during the meeting, referring to high-risk pregnancy monitors.

Fortunately, we have a fallback model because they are high-risk [patients]. They are in an IC unit—there's someone physically there to watch. But if they are stepping away to another patient, there is a window of time for things to go in the wrong direction."

The computer systems at fault in the monitors were replaced several months ago by the manufacturer, Philips; the new systems, based on Windows XP, have better protections and the problem has been solved, Olson said in a subsequent interview.

At the meeting, Olson also said similar problems threatened a wide variety of devices, ranging from compounders, which prepare intravenous drugs and intravenous nutrition, to picture-archiving systems associated with diagnostic equipment, including massive $500,000 magnetic resonance imaging devices.

Olson told the panel that infections have stricken many kinds of equipment, raising fears that someday a patient could be harmed. "We also worry about situations where blood gas analyzers, compounders, radiology equipment, nuclear-medical delivery systems, could become compromised to where they can't be used, or they become compromised to the point where their values are adjusted without the software knowing," he said. He explained that when a machine becomes clogged with malware, it could in theory "miss a couple of readings off of a sensor [and] erroneously report a value, which now can cause harm."

Often the malware is associated with botnets,

Read the rest here:
Small Town in Ohio Learns Lessons of Unintended Consequences


Elyria school safety system shuts down phone, Internet

Elyria City School’s phone lines and Internet access bit the dust yesterday. Dust on a sensor set off a chain reaction that took down computerized systems for the majority of yesterday’s school day.

While the district could still dial 911 in the event of an emergency, a non-existing emergency perceived by a state-of-the-art safety system crippled most land line communications in the district.

The outage affected all of the district’s buildings, except for the middle school, which had yet to be updated to a new phone system. Problems started when dust set off an advanced smoke alarm system’s sensor tucked into the peak of the bell tower at the old Washington building at the new high school. The system, seeing the speck, believed it was detecting smoke and reacted as programmed, Superintendent Paul Rigda said.

In the early morning hours, it set off a series of silent alarms and shut down systems in the building to protect them from possible smoke or heat damage. It took the school’s air conditioning and heating offline to avoid spreading “smoke” throughout the building.

With the air conditioning off, the school’s server room — responsible for keeping the district’s network and voice over Internet protocol phone lines operating — heated up quickly, reaching as high as 140 degrees, Rigda said.

“The temperatures reaching those heights set off another trigger system,” he said. “It is programmed that when it gets too hot, it shuts down.”

If the server room had not powered down, the high temperatures could have caused a large amount of damage.

The outage lasted for nearly eight hours, ending at about 2 p.m.

The district at no point lost the ability to call for emergency help, Rigda stressed, as the phones are still connected for such services in the event of network failure.

The advanced system is designed to be hard to override because it is a life saving system, Rigda said.

“It is extremely hard to override by design,” he said. “It would not relinquish control of the system because it thought we were in danger.”

The sensor in the bell tower posed a problem. It was high up in the peak of the tower, out of sight and out of mind. It was installed so high up that a standard ladder could not reach it.

“Everybody forgot about it,” he said. “They couldn’t get to it right away, they had to build a scaffold and then they got a ladder on top of that. As soon as they cleaned it, it saw, ‘I guess that you guys are alright’ and turned everything back on.”

“It was reacting as it was programmed to do, you can’t really blame it,” Rigda said.

An auxiliary system will need to be instituted to keep the air conditioning working in the server room in the event of an actual emergency, Rigda said.

“You can only imagine how many meetings we are going to have to have now,” Rigda said. “We can’t have the air conditioning going off and the servers heating up like that. We need those servers to do the function that we have become so dependent on.”

Discussions of possible auxiliary systems have already begun, he said. The sensors will also get more attention with a more permanent fixture built so it can be cleaned regularly.

No damage was done to any of the school’s systems, he said.

http://morningjournal.com/articles/2012/10/19/news/doc5080c79c57b68919820920.txt?viewmode=fullstory
Eye Movements Could Be Next PC Password

Francie Diep, TechNewsDaily, 12 October 2012

No two people look at the world in the same way — literally. When looking at a picture, different people will move their eyes among points of interest in different sequences, researchers have found. Even if two people trace the same paths, the exact way they move their eyes differs. That’s why Oleg Komogortsev, a computer scientist at Texas State University-San Marco, is looking to create a system that can identify people by the way they flicker their eyes while looking at a computer screen.

"We are seeing there are enough differences so we can talk about this as a biometric," Komogortsev told TechNewsDaily. A biometric is a measurement of something on the body — fingerprints, for instance — used to identify people. Computer scientists all over the world are studying biometrics for crime solving, for border security, and just as a high-tech way to sign into smartphones, tablets and other devices.

Komogortsev’s research is in its earliest stages and needs years of work before it might show up at airports, high-security workplaces or even home computers. However, he thinks eye movements could be part of the next generation of more established biometric, iris scans, which are already used in some airports and private companies, and in a countrywide ID effort in India.

Previously, researchers showed that crooks can fool an iris scanner with printed contacts, or by holding up a high-quality printout of the correct person’s eye in front of the scanner. Komogortsev hopes adding an eye-movement sensor could prevent this type of counterfeiting. "The strength of our method is it can work together with iris [scanning]," he said.

"They appear to be making progress in refining and perfecting the idea," Kevin Bowyer, an iris-scanning researcher at the University of Notre Dame, wrote to TechNewsDaily in an email. Bowyer reviewed papers for a recent conference in which Komogortsev presented his research, but was not involved in Komogortsev's work.

If the Texas State University research goes well, Komogortsev’s team could field test an eye-movement security machine in "the next year or two or three," Bowyer said.

Komogortsev’s system records eye movements and analyzes two features. In one, the system measures "fixations," the times when people linger their gaze over a point on screen. In another, it measures "saccades," the swift movements the eye makes when it flies between points. Komogortsev’s system considers both the exact path that people's gazes take and the fixations and saccades they make along the way. [SEE ALSO: Eye Movements Control New Laptop Computer]

From those movements, the system calculates unique properties about people’s eyes, including the force their eye muscles use and other properties about the fat and flesh around the eye and the eyeball itself, Komogortsev explained.

In research they recently presented, Komogortsev and his team recorded people's eyes as the subjects read part of a poem ("The Hunting of the Snark" by Lewis Carroll), looked at Rorschach inkblots and watched a black screen on which white dots suddenly appeared. All three images worked well. "If you collect enough eye-movement information, no matter the type of stimulus, it's pretty reliable," Komogortsev said.

Eye movements alone have an "equal error rate" of about 34 percent, he and his colleagues found. The equal error rate is a standard measure in security research that takes into account both false positives, letting someone through who doesn't belong, and false negatives, locking someone out who does belong. Smaller rates mean the system works more effectively, and rates for market-ready technologies are generally in the single digits.

The equal error rate of eye movements combined with low-cost iris scans is much better, at about 5 percent. Komogortsev found. The low-cost iris scans alone have an equal error rate of about 6 percent.

Further in the future, eye-movement scans could also help security officials determine if someone is ill or emotionally distressed, conditions that can affect eye movements according to some research. Komogortsev said. "Do we want to accept people into, let's say, some secure facility, if they are emotionally unstable?" Komogortsev asked rhetorically. If future iris scanners incorporate movement sensors, he said, "you are able not only to identify the person, but also to talk about his emotional state."

However, there's still plenty to do before people will check in with an eye-movement scanner at work or an airport. Komogortsev still needs to answer some basic questions, such as whether people's eye-movement patterns stay the same over time, or if they'll need to update their ID systems as they age.

Read the rest here:
Former DHS official says U.S. should go on cybersecurity offensive

Homeland Security News Wire, 1 October 2012

Stewart Baker the first assistant secretary for policy at DHS under President George W. Bush, has a straightforward theory when it comes to cyber security in the United States: “To prevail in the cybersecurity war, defense is not enough”; not all cyber experts agree with him.

Stewart Baker, the first assistant secretary for policy at DHS under President George W. Bush, has a straightforward theory when it comes to cyber security in the United States: “To prevail in the cybersecurity war, defense is not enough.”

PC Advisor reports that Baker will elaborate on his position in a testimony before the House Homeland Security Committee on cybersecurity.

“Probably the most important point I’ll be making is a simple one,” Baker wrote in a blog post. “We will never defend our way out of the current cybersecurity crisis. That’s because putting all the burden of preventing crime on the victim rarely succeeds.”

“The obvious alternative is to identify the attackers and punish them.”

Baker was quoted in an article earlier this year saying that an increasing number of U.S. companies are retaliating against cyber-attacks with so-called “active defense” or “strike-back” technology including unusual measures like “hiring contractors to hack the assailant’s own systems.”

This is because “current defenses have failed against a cadre of state-sponsored attackers ....” Baker said.

Baker also acknowledged that counterattacks by companies can violate state and federal laws, including those against computer fraud and trespassing, but he believes that taking such actions is no different than self-defense of one’s property.

Baker said in a recent blogpost, that it is much easier to track and identify hackers than it was in the past. “Investigators no longer need to trace each hop the hackers take,” Baker wrote. “Instead, they can find other ways to compromise and then identify the attackers, either by penetrating hacker networks directly or by observing their behavior on compromised systems and finding behavioral patterns that uniquely identify the attackers.”

Jeremiah Grossman, founder of WhiteHat Security, does not agree with Baker, saying that the government and private sector “Absolutely have not gotten better at identifying and tracking hackers. It’s gotten harder, particularly because if the bad guys how to hide, they can.”

Grossman does agree with Baker in that defending against a cyber-attack is not enough. According to Grossman, the best way to protect a network is to use the “hack yourself first” approach; hiring hackers to expose vulnerabilities within your system.

“This is the same method Google, PayPal, Facebook, Mozilla, etc. used as part of their security program,” Grossman told PC Advisor. “For a few hundred to a few thousand dollars, you can take some serious vulnerabilities in your system off the market and avoid a damaging breach.”

“The concept that [Baker] is proposing has been a topic of discussion for some time in the security community but still has yet to be fully realized,” Grossman said. “This is how everyone already treats every other crime, such as those in the physical world, and we should try to do the same with the digital world, as the line between two continues to blur.”

Amir Orad, CEO of NICE Actimize, which specializes in financial crime, risk and compliance, thinks in order to start talking about taking an offensive to cyber attacks, we have to define what is meant by offense.

If it is simply just to take down a bad guy’s computer, “that will only slow down an attack by a few minutes,” Orad told PC Advisor. “While that has some value as a tactical move, it doesn’t win the battle, I can hijack 10,000 computers and have them attack a Fortune 500 company.”

According to Orad, deterrence is a better solution than attacking in retaliation. “Instead of blocking an attack, you make them not want to attack you,” Orad said. “You make them turn to somebody less painful to attack.”

One of the issues when it comes to cybersecurity is when private U.S. companies are attacked; they do not report it because they feel the government is not going to investigate the situation thoroughly.

“Complaining to the FBI and CCIPS (Computer Crime and Intellectual Property Section of the Department of Justice) about even a state-sponsored intrusion is like complaining to the DC police that someone stole your bicycle,” Orad told PC Advisor. “You might get a visit from the local office; you might get their sympathy; you might even get advice on how to protect your next bicycle. What you won’t get is a serious investigation. There are just too many crimes that have a higher priority.”

http://www.homelandsecuritynewswire.com/dr20121001-former-dhs-official-says-u-s-should-go-on-cybersecurity-offensive
Preparing for Cyber War, Without a Map

TOM SIMONITE, October 16, 2012, Technology Review

The U.S. government has pledged to retaliate quickly if power grids or other critical elements of infrastructure are hacked—but the technology needed to do so is lacking.

Last week U.S. defense secretary Leon Panetta warned that critical infrastructure such as power grids or chemical plants could be inactivated or destroyed by a cyber attack, and he pledged that the U.S. would “defend the nation in cyberspace” as it does on land and sea, in air and space.

But with the art of cyber detection and defense lagging far behind the sophistication of attacks (see "Hey, Hackers: Defense Is Sexy, Too"), the U.S. and other nations appear largely unprepared to rapidly detect and respond to an attack on critical infrastructure. That would make it difficult to respond with “decisive action” as Panetta promised, or even to know whom to retaliate against.

Working out the nature and source of an attack is particularly challenging for critical infrastructure systems, which are operated by tried, trusted, and consequently outdated software (see “Old-Fashioned Control Systems Make U.S. Power Grids, Water Plants a Hacking Target”)


“We don’t have technology to secure these systems [and] don’t even have technology to do cyber forensics or logging at the control layer,” says Joe Weiss, managing director of the International Society of Automation’s efforts to create security standards for industrial control systems. Through his consulting firm, he is working with both the Defense Department and infrastructure companies on security efforts.

Read more here:

Security holes enable attackers to switch off pacemakers, rewrite firmware from 30 feet away.

BY DARREN PAULI, OCT 17, 2012, SC MAGAZINE

IOActive researcher Barnaby Jack has reverse-engineered a pacemaker transmitter to make it possible to deliver deadly electric shocks to pacemakers within 30 feet and rewrite their firmware.

The effect of the wireless attacks could not be overstated — in a speech at the BreakPointsecurity conference in Melbourne today, Jack said such attacks were tantamount to “anonymous assassination”, and in a realistic but worse-case scenario, “mass murder”.

In a video demonstration, which Jack declined to release publicly because it may reveal the name of the manufacturer, he issued a series of 830 volt shocks to the pacemaker using a laptop.

The pacemakers contained a “secret function” which could be used to activate all pacemakers and implantable cardioverter-defibrillators (ICDs) in a 30 foot -plus vicinity.

Each device would return model and serial numbers.

“With that information, we have enough information to authenticate with any device in range,” Jack said.

In reverse-engineering the terminals – which communicate with the pacemakers – he discovered no obfuscation efforts and even found usernames and passwords for what appeared to be the manufacturer’s development server.

That data could be used to load rogue firmware which could spread between pacemakers with the “potential to commit mass murder”.

“The worst case scenario that I can think of, which is 100 percent possible with these devices, would be to load a compromised firmware update onto a programmer and … the compromised programmer would then infect the next pacemaker or ICD and then each would subsequently infect all others in range,” Jack said.

Read the rest here:
World of Warcraft hit by hacking massacre!

08 October 2012

Apocalypse has come to World of Warcraft: whole cities have been massacred in the online adventure game, leaving nothing but smoking wreckage.

The game, which features an elaborate world made up of mystical creatures, magical abilities and a complex set of settings, including cities and towns, is one of the largest online gaming communities in the world. More than 10 million subscribers play World of Warcraft (WoW) online, with half of those residing in China. Hackers were able to massacre swaths of virtual characters via a virtual plague (or possibly a homicidal Level 1 character—an investigation is ongoing) in two of the main cities in the world, Stormwind and Orgrimmar, eliminating thousands of players.

The players can resurrect, but it caused a serious disruption nonetheless.

"Certain realms were affected by an in-game exploit, resulting in the deaths of player characters and non-player characters in some of the major cities," wrote Nethaera, community manager for game creator Blizzard Activision, in the game’s online forum. "As with any exploit, we are taking this disruptive action very seriously and conducting a thorough investigation. If you have information relating to this incident, please email hacks@blizzard.com,"

Nethaera added, “We apologize for the inconvenience some of you experienced as a result of this and appreciate your understanding...This exploit has already been hot-fixed, so it should not be repeatable.”

Even though the exploit was fixed, some users complained that the hackers responsible have been attacking the game in various ways for quite some time, and urged action from Blizzard.

Debris, a 62 Night Elf Druid, had this to say: "Well... The people who were responsible for this attack are the same people who crashed the servers a few weeks ago and have been messing around with the game for quite some time now. I wouldn't be surprised if they were the ones who stole all the account information a while back. I really wish you would do something about them..."

Some pointed out that tracking down the perpetrators is far from difficult. "This exploit, along with crashing the servers, the DoT being cast on friendlies bug, and a couple of others have seen the same people be involved in them, if you’re so serious about it maybe it’s time to start handing down permanent bans?" said Shalanias in the forum. "I see the same people who I know are responsible still running around in org. It’s ridiculous."

And some users alerted Blizzard to the existence of YouTube videos spotlighting what appears to be in-game progression of the hack. "There is a video on YouTube of a guy that isn't affected by the hack, is laughing with someone else while he runs around, and they laugh harder as each person dies,” noted Vasparian. “You should check into YouTube videos."

Article for the Newsletter?
If you would like to submit an article...

Are you a budding journalist? Do you have something that the Colorado Springs ISSA community should know about? Can you interview one of the “movers and shakers”? Tell us about it!

We are always looking for articles that may be of interest to the broader Colorado Springs security community.

Send your article ideas to Don Creamer at doncreamer-issa@q.com or william.creamer.ctr@us.af.mil

Ensure that “Newsletter” is in the subject line.

Looking forward to seeing you in print!

Upcoming ISSA Events

2012 November Conference, Friday, Nov 16, Crowne Plaza Hotel 7:30 – 5:00

2013 Spring Conference, Friday, Mar 8, Crowne Plaza Hotel 7:30 – 5:00

2013 Fall Conference, Friday, Nov 15, Crowne Plaza Hotel 7:30 – 5:00

Training

From Harry Smith: Here is one that may interest ISSA-COS members:

Information Security and Risk Management in Context

https://www.coursera.org/#course/inforiskman

At the very least it is good for some CPEs. (And it’s free!)
2013 - 2014 ISSA-COS Elections

Executive Vice President
Recorder
Member-at-Large

These are two-year positions.
Elections at December luncheon (Carrabba’s). For nominations contact any Board member (see the back page of this Newsletter. For their contact information)

Chapter Meetings: *Note that the meetings will be on the 2nd Thursday of the month in 2013. (except Dec.)*

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nov 14</td>
<td>5:30 to 7:30</td>
<td>Bambino's</td>
</tr>
<tr>
<td>Dec 14</td>
<td>11:00 to 1:00</td>
<td>Carrabba’s North</td>
</tr>
<tr>
<td>Jan 10</td>
<td>5:30 to 7:30</td>
<td>Bambino's</td>
</tr>
<tr>
<td>Feb 14</td>
<td>11:00 to 1:00</td>
<td>Bambino's</td>
</tr>
<tr>
<td>Mar 14</td>
<td>5:30 to 7:30</td>
<td>Bambino's</td>
</tr>
<tr>
<td>Apr 11</td>
<td>11:00 to 1:00</td>
<td>Bambino's</td>
</tr>
<tr>
<td>May 9</td>
<td>5:30 to 7:30</td>
<td>Bambino's</td>
</tr>
<tr>
<td>Jun 13</td>
<td>11:00 to 1:00</td>
<td>Bambino's</td>
</tr>
<tr>
<td>Jul 11</td>
<td>5:30 to 7:30</td>
<td>Bambino's</td>
</tr>
<tr>
<td>Aug 8</td>
<td>11:00 to 1:00</td>
<td>Bambino's</td>
</tr>
<tr>
<td>Sep 12</td>
<td>5:30 to 7:30</td>
<td>Bambino's</td>
</tr>
<tr>
<td>Oct 10</td>
<td>11:00 to 1:00</td>
<td>Bambino's</td>
</tr>
<tr>
<td>Nov 14</td>
<td>5:30 to 7:30</td>
<td>Bambino's</td>
</tr>
<tr>
<td>Dec 6</td>
<td>11:00 to 1:00</td>
<td>Carrabba’s North</td>
</tr>
</tbody>
</table>
The Information Systems Security Association (ISSA)® is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications, and peer interaction opportunities that enhance the knowledge, skill, and professional growth of its members.

The primary goal of the ISSA is to promote management practices that will ensure the confidentiality, integrity, and availability of information resources. The ISSA facilitates interaction and education to create a more successful environment for global information systems security and for the professionals involved. Members include practitioners at all levels of the security field in a broad range of industries such as communications, education, healthcare, manufacturing, financial, and government.

Hackers crack hotel room locks with tool disguised as a dry erase marker.

October 2, Forbes (International) A trio of hackers built a tool that appears to be a dry erase marker, but when inserted into the port on the bottom of a common form of hotel room keycard lock triggers the lock’s open mechanism in a fraction of a second.

I guess we wanted to show that this sort of attack can happen with a very small, concealable device,‖ said one of the three hotel lock hackers and a security researcher with the consultancy Trustwave.

Someone using this could be searched and even then it wouldn’t be obvious that this isn’t just a pen.


Published at no cost to ISSA Colorado Springs by Sumerduck Publishing™, Woodland Park, Colorado