August 2012 / Issue 11

The Cyber Advisor

Invensys Critical Infrastructure & Security Practice

this issue

August 2012
Cyber Attack Statistics
- Hackmageddon.com

Attack Motivations
- 49% Hacktivism
- 43% Cyber Crime
- 6% Cyber Espionage
- 2% Cyber Warfare

Top 3 Attack Targets
- 33% Industry-Tech
- 33% Industry-Trans
- 17% Industry-Oil

Top 5 Attack Techniques
- 32% DoS
- 21% SQL
- 17% Unknown
- 10% Defacement
- 5% Account Hijacking

IT security companies miss the mark in Industrial Security implementations

By now, a number of you have read the news story about Matt Honan, a senior writer for Gizmodo and, by all accounts, a tech guy. On August 3, 2012, Honan went from technology observer to technology casualty when he was hacked. Matt was subjected to the perfect storm—he was targeted by a group that wanted to hack his Twitter account and in doing so, worked their way through his Amazon and Apple accounts to get his Twitter information. His social media accounts were taken over along with his email addresses, iPhone, and MacBook data. He wrote an article for Wired magazine that gives an excellent accounting of his nightmare.

Matt's article spawned a number of subsequent articles all discussing what should have been done or could have been done to prevent this. Most of the solutions offered were point solutions such as the software or hardware products sold by almost every IT security company. Common software products are anti-virus and malware or hardware products like firewalls, to name a few. On their own, these products are point solutions that target a specific threat and work autonomously. Miss the threat and miss the target.

However, just integrating these products into a network does not constitute a defense-in-depth strategy:

- How will the anti-virus software and other critical files be updated?
- How will the firewall rules be created?
- How will updates be done?
- How will logs be kept and monitored?

A comprehensive cyber security solution takes into account the uniqueness of the client's networks, regulatory compliance, and internal requirements and addresses these issues and many more, ensuring that security best practices are met and kept.

Industry News

Saudi Arabia's national oil company kills network after cyber attack

SecurityWeek.com, 8/16/2012

Arabia's national oil company (the largest in the world) has confirmed that it has been hit by a cyber attack that resulted in malware infecting user workstations, but did not affect other parts of its network. On Wednesday, August 15, 2012, an official at Saudi Aramco confirmed that the company has "isolated all its electronic systems from outside access as an early precautionary measure that was taken following a sudden disruption that affected some of the sectors of its electronic network," the company wrote in a statement. "The disruption was suspected to be the result of a virus that had infected personal workstations without affecting the primary components of the network." The company did not comment on the vector of attack or who may be behind it, but insists its core operations have not been impacted as a result of the security breach. "Saudi Aramco confirmed the integrity of all of its electronic network that manages its core business and that the interruption has had no impact whatsoever on any of the company's production operations," the statement said.

Saudi Aramco oil producer's 30,000 workstations victim of cyber attack

TheHackerNews.com, 8/27/2012

Saudi Aramco, the world's biggest oil producer, has resumed operating its main internal computer networks after a virus infected about 30,000 of its workstations in mid-August. Immediately after the August 15 attack, the company announced it had cut off its electronic systems from outside access to prevent further attacks.

Saudi Aramco said the virus "originated from external sources" and that its investigation into the matter was ongoing. There was no mention of whether this was related to this month's Shamoon attacks. "The disruption was suspected to be the result of a virus that had infected personal workstations without affecting the primary components of the network," Saudi Aramco said.

Some signs point to Shamoon as malware in Aramco attack

TheThreatpost.com, 8/27/2012

While researchers continue to dig into the Shamoon malware looking for its origins and a complete understanding of its capabilities, a group calling itself the Cutting Sword of Justice is claiming responsibility for an attack on the massive Saudi oil company Aramco, which some experts believe employed Shamoon to destroy data on thousands of machines. The attack on Aramco occurred on August 15, taking the main Web site of Saudi Aramco offline. Officials at the company said that the attack affected some of the company's workstations, but did not have any effect on oil production or on the main Aramco networks. The attackers claiming responsibility for the incident dispute that, saying that they deployed a destructive piece of malware that erased data on infected machines and then made them unusable. "As previously said by hackers, about 30,000 (30k) of clients and servers in the company were completely destroyed. Symantec, McAfee and Kaspersky wrote a detailed analysis about the virus. Hackers published the range of internal client IPs which were found in the internal network and became one of the phases of the attack target," the group said in a post on Pastebin shortly after the attack.

Cyber attacks using PDFs target industries (Chemical)

gsnmagazine.com, 8/18/2012

A new kind of targeted cyber attack against defense, chemical, and technology industries is slipping into networks under the guise of PDF files, said cyber security experts. FireEye Malware Intelligence Lab and Kaspersky Labs noted on August 15 that the new malware has the makings of a targeted attack campaign against several high-value industries, including the defense, chemical, technology, and aerospace industries that uses a Trojan program rigged to PDFs to deliver its payload. The MyAgent Trojan is primarily spreading through email as a zipped .exe file or PDF attachment, according to researchers writing on FireEye's blog site.

DOE wants electric utilities to create "cyber security governance board"

Networkworld.com, 8/10/2012

The DOE has issued a call for proposals to electric-power companies that encourages them to make cyber security a top priority by setting up a "cyber security governance board" to oversee an internal cyber security program for protection and share information with the DoE.

Cyber News

Gauss virus: Stuxnet-like cyber weapon hits Middle East banks

Guardian.co.uk, 8/9/2012

A new cyber surveillance virus has been found in the Middle East that can spy on banking transactions and steal logins and passwords, according Kaspersky Lab, a leading computer security firm. Dubbed Gauss, the virus may also be capable of attacking critical infrastructure and was very likely built in the same laboratories as Stuxnet, the computer worm widely believed to have been used by the U.S. and Israel to attack Iran's nuclear program, Kaspersky Lab said on Thursday. The Moscow-based firm said it found Gauss had infected more than 2,500 personal computers, the bulk of them in Lebanon, Israel and the Palestinian territories. Targets included Lebanon's BlomBank, ByblosBank, and Credit Libanais, as well as Citibank and eBay's PayPal online payment system. Officials with the Lebanese banks said they were unaware of the virus.

With Gauss tool, cyber spying moves beyond Stuxnet, Flame

News.cnet.com, 8/9/2012

Gauss, a new "cyber-espionage toolkit," has emerged in the Middle East and is capable of stealing sensitive data such as browser passwords, online banking accounts, cookies, and system configurations, according to Kaspersky Lab. Gauss appears to have come from the same nation-state factories that produced Stuxnet. According to Kaspersky, Gauss has unique characteristics relative to other malware. Kaspersky said it found Gauss following the discovery of Flame. The International Telecommunications Union has started an effort to identify emerging cyber threats and mitigate them before they spread. In a nutshell, Gauss launched around September 2011 and was discovered in June. Gauss, which resembles Flame, had its command and control infrastructure shut down in July, but the malware is dormant, waiting for servers to become active.

Gauss cyber threat targeting Lebanon has interesting relation to Flame, Stuxnet

Defensesystems.com, 8/10/2012

Moscow-based Kaspersky Lab said August 9 that it had discovered what it believed was the fourth state-sponsored computer virus to appear in the Middle East in the last several years, reports the New York Times. The Gauss virus, which was apparently aimed at Lebanon and gets its nickname from a name found in its code, appeared to have been written by the same programmers who created the Flame virus that was found to be spying on computers in Iran in May, the story said. Furthermore, the latest virus might also be linked to Stuxnet. The Gauss virus, which has been detected on 2,500 computers, seems to have as its purpose the acquisition of logins for e-mail and instant messaging accounts, social networks, and certain bank accounts—the last being a function typically found in malicious programs used by profit seeking cybercriminals. Gauss is best-described as "a nation state sponsored banking Trojan," reports Information Week. It's code framework is related to the Flame virus, and therefore is an extension of Duqu and Stuxnet.

Gauss espionage malware phones home to same servers as Iran-targeting Flame

Arstechnica.com, 8/23/2012

A packet capture showed a Gauss -infected computer accessing a command and control channel. The IP address corresponding to the domain name is also used to host Flame command servers. The Gauss malware recently found spying on thousands of machines located mostly in the Middle East recently began connecting to command servers previously accessed by the state-sponsored Flame Trojan that's targeting Iranian computers, providing more proof that the two are linked, a security researcher said.

Consultant's Corner

Can a password ever be fully secure?

Is your password really secure? As recent news articles have shown, it probably isn't. Just over the last few months, LinkedIn, Yahoo, Blizzard Games, and others have been hacked and customer passwords stolen. Last year, Sony's Playstation Network was hacked and not only were passwords captured, but also other personal customer information.

What can be the impact of having your personal information stolen? Many hacker groups are no longer concerned about capturing passwords and instead thrive on personal information. They use this information to perform a "social engineering" attack on people by impersonating someone from a company the victim does business with. They are usually prepared with some information they have already stolen to convince victims that they are legit, and then they will attempt to gather more information such as a credit card number, social security number, or something like a "secret question answer." This allows them to access private accounts and recover or change passwords. They can use this information to wreak havoc on people's online lives just as if they had originally stolen someone's password.

What can you do to protect yourself if a vendor does not adequately protect your personal information? There are three things you can do:

1. Use complex, yet easy-to-remember passwords, as Tom Jackson stated in Issue 8 of the Cyber Advisor (May 2012).
2. Do not link your online accounts together. Sites such as Yahoo now allow you to sign in using your Facebook username and password. While it may be tempting to link accounts to reduce the number of passwords to remember, if one account gets hacked, then all of your accounts can get hacked. If you must link accounts, only link non-secure accounts together. For example, you might link two social media accounts as long as they aren't linked to your email or an account with credit card information (like eBay or Amazon).
3. Use two-factor authentication. Two-factor authentication is where you use "something you know" and "something you have" to log in to your account. If you work for a large company and have VPN access, then you may already be using two-factor authentication if you have a key fob in addition to your network password.

Yahoo now offers the option of having a code sent via text message to your cell phone to access your account. You use this feature by entering your username and password online, and then Yahoo will send a code to your cell phone that must be entered before you can access your account. In this case, even if a hacker has stolen your password, they cannot access your account unless they have physically stolen your cell phone as well. Two-factor authentication isn't offered by every online service yet, but it is gaining popularity. Click here for more information on two-factor authentication.

If you follow the three key points above, then your information will be much more secure in today's online world.

This months contributor to Consultant's Corner is
Charles Smith
Consultant, Critical Infrastructure & Security Practice
Invensys
charles.smith@invensys.com

Consultant's Corner

Tim Johnson, CISP Principal Consultant

"Centralized Anti-Virus DAT repository deployments enable quick and reliable Anti-Virus updates for Stand Alone Control Systems."

Doug Clifton, CISP Dir.

"It's significantly less expensive to purchase Managed Security Services than to hire new staff with Security Experience."

Steve Batson, CISP Principal Consultant

"Implementing common security controls across disparate systems can greatly reduce the cost of security and maintenance."

Michael Martinez, CISP Principal Consultant

"Being regulatory compliant does not ensure being secure. Cyber Security is a ongoing life cycle."

Tom Jackson, CISP Principal Consultant

"According to Kaspersky Labs, applications like Adobe are primary targets for hackers to deliver viruses. Implementing patch management and update services is an effective fix."

Meet the CISP team and learn more about cyber security at

http://www.real-time-answers.com/cyber-security/

Cyber Security for the Nuclear Industry »
Focusing on 10 CFR 73.54 and NEI 08-09 Reg. guide 5.71, learn more about cyber security in the nuclear industry.

Cyber Security for Power Generation »
As more and more electric power plants begin their NERC CIP compliance plan, many are left trying to understand where to start. See which areas require special attention.

Cyber Security Compliance »
Cyber compliant does not necessarily mean cyber secure. Identify the keys common to both.

Cyber Security Threats »
Cyber attacks are increasing. A continuous state of preparedness is required.

Cyber Security Life Cycle »
Cyber security cannot be maintained from a one-time initiative. Learn about a methodology designed to keep your site cyber secure well into the future.

Cyber Security Consulting Advantage »
Security and compliance take a tremendous amount of effort. Help is available to get secure and compliant … and stay that way.

The Cyber Advisor
Invensys Critical Infrastructure & Security Practice
August 2012 / Issue 11

Invensys Critical Infrastructure and Security Practice (CISP)

Invensys CISP has capability in establishing, implementing, and maintaining industry best practices to meet the demands for government regulations (NERC-CIP, NEI 08-09, CFATS), industry requirements, and company compliance requirements. Attributes of Invensys CISP include:

Hardware Independence

CISP can work with any type of control system or type of technology a customer prefers for the security environment.

Industry Knowledge

CISP has a number of resources that help them understand the demands of Control Networks and the requirements for continued uptime.

Regulation Knowledge

CISP has a number of subject matter experts who understand a whole host of regulatory requirements as well as actively participate in a number of industry and government groups.

Proven Methodology

CISP follows a proven life cycle methodology to support the implementation of a comprehensive successful cyber security program. Attributes of the life cycle approach are Assessment, Development, Implementation, and Management.

Technical Knowledge

The same CISP personnel who have regulatory knowledge are also well versed in the latest security policies, procedures, and technologies for intrusion detection and prevention, firewalls, DCS, and network architecture.

Join us on Blogger

invensys™

For additional information, please visit us at
http://iom.invensys.com/CyberSecurity

5601 Granite Pkwy. Suite 1000 Plano, TX 75024 ▪ P 214.295.6365 ▪ F 888.758.7675 ▪ **iom.invensys.com**