invensys

January 2013 / Issue 16

The Global Cyber Advisor

Invensys Critical Infrastructure & Security Practice

this issue

Jan. 2013
Cyber Attack Statistics
- Hackmageddon.com

Attack Motivations

51%	Hacktivism
46%	Cyber Crime
46%	Cyber Espionage

Top 3 Attack Targets

25%	Finance
24%	Government
13%	Industry

Top 5 Attack Techniques

35%	SQL
26%	DDoS
12%	Unknown
11%	Defacement
4%	Malware

Looking Ahead at 2013

Before we look ahead to the new year, let’s pause and review the some of the findings from this past year. As the famous philosopher George Santayana said, “Those who cannot remember the past are condemned to repeat it.”

2012 saw an increase in targeted attacks on the country’s critical infrastructure such as power generation plants, water systems, and nuclear facilities as reported by the U.S. Department of Homeland Security. 2013 will bring more of the same events that occurred in 2012.

- ICS-CERT responded to and investigated 198 cyber incidents (compared to 130 in 2011)
- The Energy sector was the most targeted industry in 2012, accounting for 41% of events
- The Water sector was the second most targeted industry in 2012, accounting for 15% of events
- The cyber security response team helped with incident responses for 23 oil/natural gas sector events
- Chemical organizations reported 7 incidents to ICS-CERT
- The Nuclear sector reported 6 incidents to ICS-CERT

It is clear that cyber incidents are global, on the rise, and becoming industry specific and targeted.

The Human Factors / Policies & Procedures

Employee mistakes that are due to a lack of security awareness and/or training is still a top threat. Weak passwords continue to be one of the single largest security weaknesses. One has to look no further than the data breach of Yahoo! in July 2012—the top 3 passwords were *123456*, *Password*, and *Welcome*.

USB drives are ubiquitous in the work place. Did you know that USB drives account for over 25% of malware (Panda)? A recent report by the U.S. Army concluded that 70% of viruses were the result of USB drives. In December 2012, the ICS-CERT Monitor reported that a U.S. power company was brought down by malware traced back to a USB drive.

Targeted Attacks

Targeted attacks have become prevalent in the past few years, using engineered malware to attack specific industries like Stuxnet. Hacktivist organizations continue to thrive with a single-minded goal of making a political or social point. Look no further than the August 2012 malware attack on Saudi Aramco that took out 30,000 servers. A group calling themselves the “Cutting Sword of Justice” took credit. Nation-states are a growing area of concern, with a focus on cyber espionage, cyber weapons, cyber theft, and sabotage, lead by one nation-state against another or many.

As always with cyber security, have a plan, take action, monitor, and be ever vigilant.
Happy New Year!

Industry News

US power company shut down by USB transmitted viruses

www.scmagazine.com, 1/18/2013

A U.S. power company was shut down for three weeks by a virus brought in by an infected USB stick. According to media reports, a U.S. Department of Homeland Security report did not identify the plant but said that the virus was introduced last October by an employee of a third-party contractor that does business with the utility, according to Reuters. The U.S. Department of Homeland Security's Industrial Control Systems-Cyber Emergence Response Team (ICS-CERT), which helps protect critical U.S. infrastructure, described the incident in a quarterly newsletter that was accessed via its website. It also described a second incident, in which the CERT said it had recently sent technicians to clean up computers infected by common as well as "sophisticated" viruses on workstations that were critical to the operations of a power generation facility.

DHS: Industrial controls systems subject to 200 attacks in 2012

www.homelandsecuritynewswire.com, 1/14/2013

Forty percent of those attacks were on energy firms, according to the Industrial Control Systems (ICS) and Cyber Emergency Response Team (CERT), which reviewed every incident. Water utilities came in second, with 15 percent of the attacks focused on them. Some of the incidents occurred by security researchers using the Sentient Hyper Optimized Data Access Network (SHODAN), a regularly updated directory of ports, to find exposed industrial control systems, but the majority were serious breaches, the report stated. EWeek reports that SHODAN responded to more than twenty attacks on oil and natural gas firms and discovered that sensitive information on the supervisory control and data analysis (SCADA) systems was accessed by the attackers.

ICS-CERT: Responses to cyber "incidents" against critical infrastructure jumped 52 percent in 2012

www.securityweek.com, 1/10/2013

Attackers increasingly targeted the country's critical infrastructure such as power grids, water systems, and nuclear facilities in 2012, according to a recent Homeland Security report. The department's Industrial Control Systems-Cyber Emergency Response Team (ICS-CERT) responded to and investigated 198 cyber incidents against critical infrastructure in fiscal year 2012, compared to 130 in 2011, according to the latest ICS-CERT Monitor report. The energy sector was the most targeted industry in 2012, accounting for 41 percent of reported events, followed by water with 15 percent. This rise in attacks against critical infrastructure systems is hardly surprising given many of the headlines and reports that emerged during 2012. Spearphishing and Internet-facing systems with weak or default credentials were the most common incidents in the water sector. In fact, control systems devices that could be directly accessed from the Internet were an "area of concern" in fiscal year 2012.

Oil and gas infrastructure vulnerabilities drive security spending

www.securityweek.com, 1/16/2013

Recent analysis from Frost & Sullivan shows that the security of critical facilities remains the topmost priority for the global oil and gas industry. Accordingly, these markets are increasing the amount spent on security offerings, including those integrated and flexible solutions with rounded protection. Escalating demand for oil and gas, the construction of new facilities, and physical and cyber threats to these installations have led to growth in the oil and gas infrastructure security market, the report explains. The market earned revenues of $18.31 billion in 2011 and estimates this to reach $31.27 billion in 2021.

Critical infrastructure vulnerable to simple cyber attacks

www.salon.com, 1/18/2013

Spearphishing, the technique by which hackers gain access to computer networks through sending misleading, malicious emails which users click on, is a risk to more than just small computer networks. According to the New York Times' "Bits" blog, critical infrastructure like "watersheds, power grids, oil refineries, and nuclear plants" are vulnerable to spearphishing attacks. Spearphishing is so easy to deploy and so effective that 91 percent of targeted attacks start with malicious e-mails, according to TrendMicro, a computer security firm with headquarters in Tokyo. But that same method could be used to harm utilities, power plants, gas pipelines and watersheds.

Industry News

Top five hurdles for security and compliance in industrial control systems

www.net-security.org, 1/24/2013

For many decades, Industrial Control Systems (ICS) have been the operational systems relied upon to safely and reliably deliver the essentials of daily life. Sometimes referred to as a critical infrastructure, they are the backbone of a modern economy. With these systems generally working well, there has been little need to make major changes to them. There has been innovation and some incremental changes, but in the ICS world, it has largely been "business as usual." That's very different than other industries and sectors, such as enterprise IT, where seismic technology shifts seem to occur about every two years. Change in industrial control environments has been handled at a more measured pace and with a lot more caution.

U.S. government warns of hack threat to network gear

news.yaonoo.com, 1/20/2013

The Department of Homeland Security urged computer users on Tuesday to disable a common networking technology feature after researchers warned that hackers could exploit flaws to gain access to tens of millions of vulnerable devices. The U.S. government's Computer Emergency Readiness Team advised consumers and businesses to disable a feature known as Universal Plug and Play or UPnP, and some other related features that make devices from computers to printers accessible over the open Internet.

ICS Diary: What can happen within a cyber terrorist attack to the electrical grid of a country?

isc.sans.edu, 1/23/2013

Management systems involve a new spectrum of risks which, if materialized, can cause incalculable losses to the population in terms of money and even human lives. The electrical system is controlled by SCADA systems, which manage the three core subsystems. The most common facilities used to generate energy are thermo electrical plans, nuclear plants, and hydro electrical plants. Inside these facilities, the SCADA platform is vital to perform the following when generation takes place: ensure turbines are not having revolutions more than supported, generators are not overloaded, and energy being generated matches the amount of energy that the transmission line can handle.

Securing SCADA systems still a piecemeal affair.

www.networkworld.com, 1/23/2013

For several years now, security researchers have warned that SCADA software is riddled with serious vulnerabilities and often lacks the most basic security controls. Adding to this problem is the fact that many industrial control system owners are increasingly exposing SCADA management interfaces to the Internet for the convenience of remote administration. Many security researchers would like SCADA systems to be re-engineered with security in mind, but that's a long term goal at best.

Cyber attacks against oil & gas infrastructure to drive $1.87 billion in cyber security spending by 2018

www.abiresearch.com, 1/29/2013

As a highly critical sector, the oil and gas infrastructure should be one of the most secure, both physically and digitally. This is not the case. A multibillion dollar industry trading one of the most valuable commodities on the market is connecting its industrial control systems full of unpatched vulnerabilities to the Internet, where cybercriminals roam in all impunity. These systems are poorly protected against cyber threats; at best, they are secured with IT solutions that are ill adapted to legacy control systems such as SCADA. "The lack of appropriate security has already allowed a number of destructive cyber attacks to lay waste to some of the most high profile companies in the industry," says senior cyber security analyst Michela Menting. From Night Dragon to Shamoon, oil and gas companies have been the victims of sophisticated cyber threats since 2009.

Cyber News

Inside the 1,000 Red October cyber espionage malware modules

threatpost.com, 1/17/2013

The Red October espionage malware campaign is providing security researchers with a deep dive into the complexity of targeted attacks, which in this case made use of more than 1,000 malware modules for everything from reconnaissance on targets to exfiltration of data to command and control servers. The moving parts behind Red October are vast and have been under wraps for the better part of five years, Kaspersky Lab researchers revealed this week. The attackers behind this campaign targeted victims in 39 countries, primarily diplomats, researchers. and military facilities, among other institutions since August 2007.

Iran said to be responsible for cyber attacks on U.S. banks

www.cnet.com, 1/5/2013

Several U.S. banks were hit with online attacks over the past few months, but it's been unclear who was responsible. Now, government officials and security researchers are saying Iran was waging these cyber attacks, according to a report by the New York Times. "There is no doubt within the U.S. government that Iran is behind these attacks," James A. Lewis, a former official in the State and Commerce departments and a computer security expert at the Center for Strategic and International Studies in Washington, told the Times. The attacks were aimed at several major banks, including Wells Fargo, J.P. Morgan Chase, Bank of America, Citigroup, HSBC, and others. They involved inundating the banks' Web sites with bogus traffic, known as distributed denial-of-service attacks.

Android botnet infects over 1 million phones

Mobile.slashdot.org, 1/18/2013

Up to a million Android users in China could be part of a large mobile botnet according to research unveiled by Kingsoft Security, a Hong Kong-based security company, this week. The botnet has spread across phones running the Android operating system via Android.Troj.mdk, a Trojan that researchers said exists in upwards of 7,000 applications available in the Google Play marketplace, including the popular Temple Run and Fishing Joy games.

65% of firms fear a cyber attack in 2013, according to BCI research

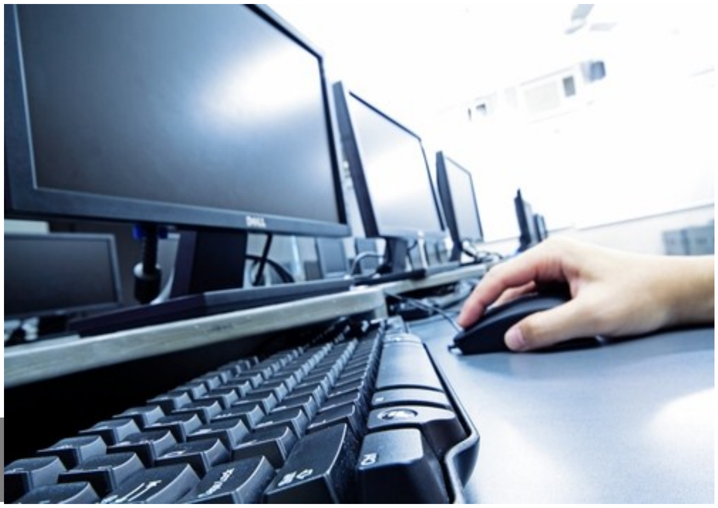
www.ameifnocom, 1/20/2013

BSI has revealed that 65% of organizations are extremely concerned or concerned about a cyber attack in 2013. The survey also reveals that 71% see the use of the Internet for malicious attacks as a major trend that requires a business continuity response with 42% seeking to manage the prevalence and high adoption of Internet dependent services, such as the cloud, within their preparedness activities. The Horizon Scan 2013 Survey Report concludes that the level of concern across sectors and geography over a cyber attack is a major challenge for public policy makers and board rooms. More needs to be done to gain a better understanding of the threat and underlying trends that drive the vulnerability to ensure that a proportionate business continuity approach is in place.

90 percent of passwords "vulnerable to hacking"

www.independent.ie, 1/15/2013

Even passwords that are considered strong are vulnerable because users can't remember them, new research says. Global consultancy Deloitte claimed that over 90 percent of user–generated passwords, even those considered strong by IT departments, will be vulnerable to hacking in 2013. Jolyon Barker, global lead for Deloitte's technology, media, and telecommunications industry, said "Whilst moving to stronger, longer passwords means greater levels of security, people understandably find these harder to remember." He added that so-called "two-factor authentication," using additional methods, could improve security. "Instead, an additional bit of identification can be used. It could be a password sent to a cell phone or smartphone, a physical device that plugs into a USB slot, or possibly be a biometric feature of the user," Mr. Barker said.



Cyber News

Two-thirds of banks hit by cyber attacks in past 12 months

www.darkreading.com, 1/22/2013

More than two-thirds (64%) of IT & IT security practitioners reported that their banks have suffered at least one Distributed Denial-of-Service (DDoS) attack in the last 12 months, according to independent research commissioned by Corero Network Security (CNS: LN), a leading provider of network and application layer DDoS defense products. The research of 650 IT and IT security professionals at 351 banks, including from some of the largest in the world, also revealed that 78% of those surveyed believed that DDoS attacks will continue or significantly increase in 2013, leaving them vulnerable to cyber attacks that could lead to downtime and compromised data. Conducted by the Ponemon Institute, almost half of respondents (48%) said their banks had suffered multiple DDoS attacks in the past 12 months.

Most exploit kits originated in Russia, say researchers

www.ner-security.org, 1/23/2013

58 percent of the vulnerabilities targeted by the most popular exploit kits in Q4 were more than two years old and 70 percent of exploit kits reviewed were released or developed in Russia, reveals Solutionary SERT's Q4 2012 Quarterly Research Report. In reviewing 26 commonly used exploit kits, SERT identified exploit code dating as far back as 2004, serving as evidence that old vulnerabilities continue to prove fruitful for cyber criminals. The fact that 58 percent of the vulnerabilities exploited are over two years old further supports SERT findings that the number of newly discovered and disclosed vulnerabilities has declined since 2010.

Android malware could reach the 1 million mark by year's end

www.securitytube.net, 1/30/2013

Security firm Trend Micro's predictions for 2013 include one potentially concerning consideration: The post-PC malware threat has truly arrived, and Android will take the brunt of the targeted attacks throughout this year. According to the security giant and anti-malware maker, 2012 showed that malware writers, spammers, and hackers have begun to capitalize upon the mobile market, with a particularly keen eye for attacking the Android platform. Not only does Google-owned Android have the greatest market share, therefore making it an easier target, it also has a more open platform to work with, compared to Windows Phone or the iOS-based platforms.

Denial-of-Service attacks: It's a problem, bro

www.gcn.com, 1/30/2013

It isn't just your imagination or media hype—denial-of-service attacks were more common in 2012 than ever before. Prolexic Technologies logged a 53 percent increase in the attacks for last year over the year before, and the largest single culprit seems to be the itsoknoproblembro DDOS toolkit. According to the security company's most recent quarterly report on DDOS activity, the attacks not only are becoming more common but also more powerful, and the botnets that support them are more resilient. Itsoknoproblembro was used to launch high-profile distributed attacks against banking companies in late 2012 and had a role in most of the attacks analyzed by the company in the fourth quarter. A number of government agencies also were among the organizations targeted.

Security team fails to check logs, lets man goof off by outsourcing own job for years

nakedsecurity.sophos.com, 1/17/2013

It's getting a fair bit of coverage, and it goes like this:

- IT checks the VPN logs after neglecting them for years.
- IT spots a connected session from China, right before their eyes.
- IT sees the login was done with the authentication token of an employee.

IT notices the employee sitting calmly at his desk. At this point, the story descends into conspiracy theories. The bloke has outsourced his own job! He's found someone in China who'll do his work for him at 20% of his salary, so he's taken a 20% paycut in return for a 100% cut in effort.

Consultant's Corner

Cyber Security Defense-in-Depth: Mobile Media

Cyber security defense in-depth is a concept of protecting digital assets from cyber attacks by placing multiple defensive mechanisms in a series to prevent or detect a cyber attack. Common defense in-depth practices include using multiple brands of firewalls to protect network layers. This example deals with vulnerabilities within a certain brand or type of firewall. If the first firewall, brand X, has a vendor-specific vulnerability, then the second firewall, brand Y, should not contain the same vulnerability. But what if the attack originates on the inside of the network? What if a mobile media device such as a flash drive is used to launch an attack knowingly or unknowingly?

The Nuclear Regulatory Commission (NRC) recognizes the need for defense in-depth as it pertains to mobile media. Part of NRC Regulations Title 10, Code of Federal Regulations (CFR) 73.54 is to address mobile media. As this type of attack has become more prevalent in recent years with malware launching from flash drives behind defensive layers, multiple defensive mechanisms should be put in place to prevent or detect these types of attacks. Let us look at the multiple defense mechanisms that can be put place:

Policies and Procedures
Organizations should provide policies to their employees, vendors, and contractors that provide detailed information that governs the proper use of mobile media. In addition to use, policies and procedures should also direct procurement of mobile media.

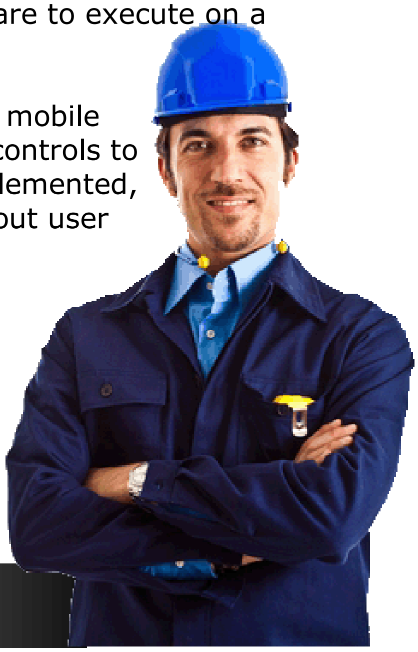
Training
Job-specific training concerning the use of mobile media will bring awareness and understanding of the risks associated with mobile media use.

Scanning
Dedicated scanning workstations to scan and detect malware. These workstations should run malware software that is different from malware software in use on the business network or Distributed Control System (DCS) network.

Whitelisting
Whitelisting software is a last line of defense that prevents unauthorized software to execute on a workstation or server.

These types of defensive mechanisms can prevent or detect a cyber attack from a mobile media device, and it is important to implement both administrative and technical controls to have the most robust defense. However, even with multiple types of controls implemented, the most important part of these defensive mechanisms is user compliance. Without user compliance, most types of defensive mechanisms will fail.

This month's contributor to Consultant's Corner is
Stephen Santee, CISSP, PMP
Consultant, Critical Infrastructure & Security Practice, Invensys
Stephen.Santee@invensys.com



Consultant's Corner

Tim Johnson, CISSP —CISP Principal Consultant

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

Doug Clifton, CISSP — Dir. CISP

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

Steve Batson, CISSP — 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

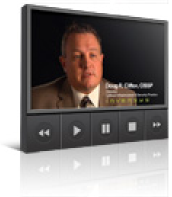
"According to Kaspersky Labs, applications like Adobe are primary targets for hackers to deliver viruses. Implementing patch management and update services is an effective fix."

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.

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 Critical Infrastructure Consulting include:

Hardware Independence

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

Regulation Knowledge

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

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.

Industry Knowledge

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

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 Assessments, Development, Implement and Management.

invensys™

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