March 2013 / Issue 18

The Global Cyber Advisor

Invensys Critical Infrastructure & Security Practice

this issue

Who's attacking our ICS networks?

In January, we looked at the increase in attacks on our ICS networks, with ICS-CERT responding to and investigating 198 cyber incidents in 2012, up from 130 in 2011. As focused as we can be on numbers sometimes, the real question is who is behind the attacks? To begin to understand this, we must first understand who they are and what their goals are.

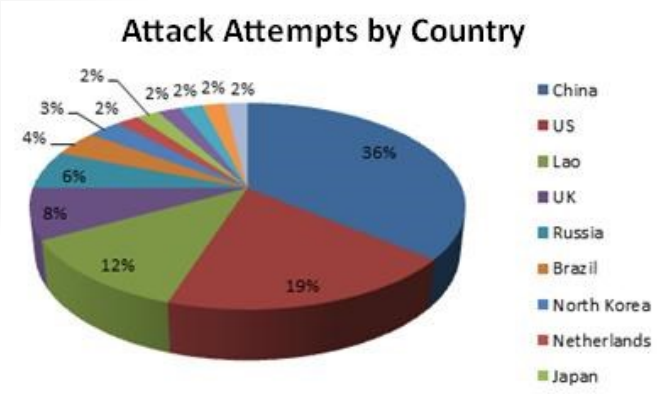
Who they are:

- Nation-States, who probably will not launch major cyber attacks against one another, even though they have the greatest capability
- Terrorists—groups seeking to expand their capability in this area
- Terrorist Sympathizers—the most likely group to launch a cyber attack
- Thrill Seekers—a minor threat driven by a desire to show skills rather than a desire to destroy

What their goals are:

- Information Theft—stealing of data, whether it is personal or corporate intellectual property
- Information Disruption—defacement for the purpose of sabotage or vandalism, rendering critical operating systems incapable of performing their essential functions
- Information Denial—destruction via floods of automated hits, capable of bringing down whole networks, companies, and even countries

Recently, Trend Micro did some research by setting up a honeypot with servers named "SCADA-1" and "SCADA-2." Within 18 hours, they had their first attacks, and according to the following chart, most originated from China and the United States.



What is not shown in the figures above is the number of repeat offenders, with China again at the lead. The report indicates that these repeat offenders often came back at dedicated times on a 24-hour basis and attempted to not only exploit the same vulnerabilities present on the devices but also attempted additional exploitation if they did not succeed with prior attempts. This shows that these particular actors were likely interested in gaining access to the devices or causing further damage or exploitation. Although this was just a test scenario, the results are all too real. The only thing that we won't know is who was a nation-state out to do harm and who was a thrill seeker out to show off.

Mar. 2013
Cyber Attack Statistics
- **Hackmageddon.com**

Attack Motivations
- 49% Cyber Crime
- 48% Hacktivism
- 1% Cyber Espionage

Top 3 Attack Targets
- 27% Finance
- 26% Government
- 14% News

Top 5 Attack Techniques
- 50% DDoS
- 13% SQL
- 8% Defacement
- 7% Unknown
- 6% Account Hijacking

Industry News

U.S. gas pipelines at risk after Chinese military attack

Beforeitsnews.com, 3/1/2013

Independent cyber security researchers have traced the digital signatures of attacks back to an espionage group that has close links with the Chinese military. The information stolen from the companies provides everything necessary for someone with the knowledge to blow up, not just one, but hundreds or thousands of gas compressor stations simultaneously, effectively giving that person the power to hold the U.S.'s gas infrastructure hostage, and in turn the whole of the U.S., as it now relies on natural gas for nearly 30% of its power grid.

Pentagon forming cyber teams to prevent attacks

m.monroenews.com, 3/12/2013

The Defense Department is establishing a series of cyber teams charged with carrying out offensive operations to combat the threat of an electronic assault on the United States that could cause major damage and disruption to the country's vital infrastructure, a senior military official said Tuesday. Gen. Keith Alexander, the top officer at U.S. Cyber Command, warned during testimony that the potential for an attack against the nation's electric grid and other essential systems is real and more aggressive steps need to be taken by the federal government and the private sector in order to improve digital defenses. Alexander told the Senate Armed Services Committee that foreign leaders are deterred from launching cyber attacks on the United States because they know such a strike could be traced to its source and would generate a robust response.

Critical infrastructure at risk of cyber attack

www.industryweek.com, 3/12/2013

Citing "increasing risk to U.S. critical infrastructure," National Intelligence Director James Clapper said in an annual report to Congress that "unsophisticated" attacks could penetrate poorly protected computer networks for power grids or similar systems. The threat of a large-scale digital assault that could cripple a regional power network was genuine but remained a "remote" possibility, the report said. "We judge that there is a remote chance of a major cyber attack against U.S. critical infrastructure systems during the next two years that would result in long-term, wide scale disruption of services, such as a regional power outage," it said. But "there is a risk that unsophisticated attacks would have significant outcomes due to unexpected system configurations and mistakes, or that vulnerability at one node might spill over and contaminate other parts of a networked system."

Cyber attack leaves natural gas pipelines vulnerable to sabotage

www.csmonitor.com, 3/1/2013

Cyber spies linked to China's military targeted nearly two dozen U.S. natural gas pipeline operators over a recent six-month period, stealing information that could be used to sabotage U.S. gas pipelines, according to a restricted U.S. government report and a source familiar with the government investigation. From December 2011 through June 2012, cyber spies targeted 23 gas pipeline companies with e-mails crafted to deceive key personnel into clicking on malicious links or file attachments that let the attackers slip into company networks, says the Department of Homeland Security (DHS) report.

BP fights off up to 50,000 cyber attacks a day

www.CNBC.com, 3/6/2013

As part of CNBC's ongoing special "Hacking America," top CEOs and cyber security experts are being asked about the potential damage of cyber attacks and what businesses and governments can do to protect themselves—and you. At the IHS CERAWeek Conference in Houston on Wednesday, CNBC spoke to BP CEO Bob Dudley about the persistent cyber threats that companies like his receive. "Cyber security is a growing issue around the world, not only with companies but with governments," Dudley observed. "We see as many as 50,000 attempts a day like many big companies... to my knowledge we haven't had an incident that's taken away data from us, but we're incredibly vigilant."

Cyber News

"MiniDuke" malware takes aim at Euro government via Adobe

news.cnet.com, 3/1/2013

A new attack is targeting European governments through flaws exploited in Adobe's Reader software, according to security researchers. Kaspersky Lab and CrySys Lab today detailed a new malicious program in the wild, called "MiniDuke," that has been attacking government entities and institutions across Europe. Government entities in the Ukraine, Portugal, Romania, and others have also been targeted.

Security breaches remain undiscovered and unresolved for months

www.net-security.org, 3/1/2013

At RSA Conference 2013 in San Francisco, Solera Networks announced the results of the Ponemon Institute's 2013 report, "The Post Breach Boom," which revealed that organizations are unprepared to detect data breaches and contain them. The Ponemon Institute polled 3,529 IT and IT security professionals in U.S., Canada, UK, Australia, Brazil, Japan, Singapore, and United Arab Emirates to understand the steps they are taking in the aftermath of malicious and non-malicious data breaches. All participants in the study represent organizations that had one or more data security breaches in the past 24 months.

Corporate data loss hit highest levels since 2008

www.net-security.org, 3/1/2013

Recent incidents of corporate data loss hit the highest levels since 2008 as companies work to improve data security strategies against a greater variety of more sophisticated IT attacks that can pose severe enterprise and reputational risks. Data loss attacks affected more than one billion people in the last five years and more than 60 percent of those incidents were the result of hacking, says The Data Loss Barometer report from KPMG that analyzed incidents since 2005 across industries, types of data loss, and global regions.

U.S. National Vulnerability Database hacked

www.regoster.co.uk, 3/14/2013

The U.S. government's online catalog of cyber vulnerabilities has been taken offline—ironically, due to a software vulnerability. The National Institute of Standards and Technology's National Vulnerability Database's (NVD) public facing website and other services have been offline since March 8 due to a malware infection on two web servers. The Register received an anonymous tip about the infection on the following Wednesday, which led to a Google+ post containing information from NIST. "On Friday, March 8, a NIST firewall detected suspicious activity and took steps to block unusual traffic from reaching the Internet," Gail Porter of NIST's public inquiries office told a concerned chief security officer in an email, according to the post.

South Korea traces cyber attack to IP address in China

news.cnet.com, 3/26/2013

The cyber attack that targeted banks, TV broadcasters, and an Internet service provider in South Korea yesterday originated from an IP address in China, but the identities of the people responsible remain unknown, South Korean regulators say. "We've identified that a Chinese IP has connected to the organizations affected," a spokesman for South Korea's Communications Commission told a press conference on March 21, according to a Reuters account of the event. The revelation comes a day after a massive coordinated attack on servers in South Korea led officials to raise the alert status for the nation's army amid concerns that the attacks were initiated by its neighbors in North Korea.

Officials worried about cyber attacks on U.S. nuclear command control

news.foxnews.com, 3/13/2013

Anonymous U.S. strategic nuclear weapons and the command systems that control them are vulnerable to cyber attacks, although most are hardened against many types of electronic attacks, the commander of the U.S. Strategic Command said on March 12.

Consultant's Corner

Patch Management

Patch management is a critical part of maintaining the security posture of your systems and network. The patches that operating system and application vendors release help mitigate the known vulnerabilities of a continuously evolving threat landscape that malicious malware exploits. Unfortunately, patching vulnerabilities is often treated in an inconsistent manner. In many networks, systems are patched once before they are brought online and are rarely updated, if at all, as new patches become available. In these environments, there is no clear patch management strategy. Systems are manually updated one at a time. Sometimes update schedules are missed or systems are ignored. As a result, systems will be at different patch levels with different threat vulnerabilities. It's only a matter of time before one of these systems becomes compromised and shuts down a critical process, or worse, causes an entire facility to go offline. Most security breaches are the result of a vulnerability caused by a missing patch on any given system in the network. With this in mind, it is critical that a unified patch management strategy should be set in place.

Listed below are 4 key elements to look for when deciding on the application control of your patch management solution:

- **Single administrative point-of-contact for hosts:** The only way to have an effective patch management program is by choosing an application that can automate as much of your required host scans and patching as possible. This application will reside on a single server that all hosts in your network will have access to and provide a single unifying interface for interactions within the network.

- **Customization:** While no patch management application will cover 100% of your needs, it should provide some degree of customization to where you can make it perform the task you need it to do. You should be able to customize what type of scans you need to perform, whether it's by OS type, systems in a particular location or function, select vulnerability scans, or only to deploy certain patches.

- **Robust reporting:** An effective patch management application should provide robust reporting so you always know what your security posture is on any system or groups of systems on your network. Whether you are dealing with internal policies, or external requirements like PCI, HIPPA or NERC-CIP, a good patch management solution makes it easy to remain in compliance, making certain all systems are up-to-date.

- **Vulnerability scanning and remediation:** The primary reason to have patch management is to keep up with security updates. Patch management applications should be able to scan for and report vulnerabilities. From a centralized interface, administrators should be able to remediate these vulnerabilities by quickly pushing the updates to a single system or a group of systems and receive real-time feedback whether the updates have been successfully deployed or if there were installation failures.

By having the right patch management solution in place, systems are kept up-to-date with relative ease. But as critical as patch management is to the function of any business, it should not be your only line of defense; it should be part of a layered vulnerability management framework. With this framework in place, your business is safe from most threats.

This month's contributor to Consultant's Corner is
Todd Wheeler
Consultant, Critical Infrastructure & Security Practice, Invensys
todd.wheeler@invensys.com

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
March 2013 / Issue 18

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.

Industry Knowledge

CISP has a number of resources that understand the demands of Controls 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 active participation 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 Assessments, Development, Implement 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.

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**