April 2012 / Issue 07

The Cyber Advisor

Invensys Critical Infrastructure & Security Practice

this issue

Who's Attacking the Networks? Nation-States

A 2010 survey of 200 industry executives from the Power, Oil, Gas, and Water sectors in 12 Western countries, China, and Russia indicates that 85% of respondents experienced network intrusions that were government sponsored sabotage and espionage was the most often cited cyber threat.

"Foreign Spies Stealing U.S. Economic Secrets by the Office of the National Counterintelligence Executive
Oct-2011

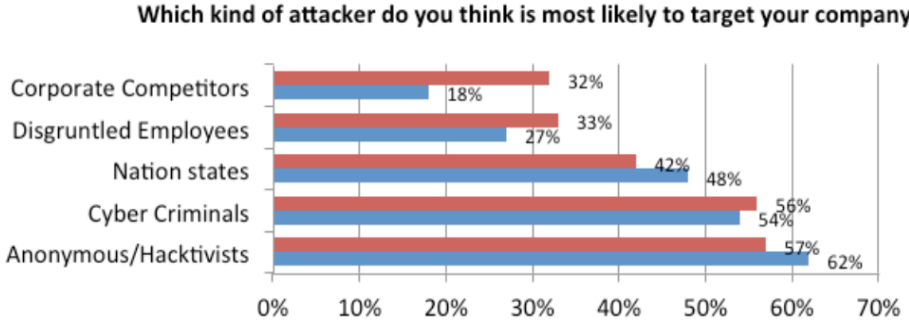
Who is attacking your network? Nation-states like China, Russia, and India all have their own motivations for launching cyber attacks. You do not have to look far to read reports titled like "U.S. forces vulnerable to Chinese cyber attack" (Washington Times). Reports like these are on nearly every newspaper and magazine these days. Why? The answer is money. Consider the following:

- Defense Industry—cost to develop stealth fighter: $2 billion
- Pharmaceutical Industry—cost to take a new drug to market: $1 billion
- Energy Industry—global cost has increased 200% since 2002 (IMF), drive production improvement and cost associated with intellectual property
- Food Industry—global cost increased 70% since 2002 (IMF), improvement in fertilizer and seed technology
- Cyber Weapon development cost: $300–$1,000

As the sophistication required for hacking has decreased over recent years, so has the cost associated with the tools and accessing those tools. This has made cyber attacks the new weapon of choice for developing countries or nation-states. Cyber weapons provide nation-states with the lowest cost means by which to easily get access to the information needed to "short cut" development cycles and to get to market faster. In today's global economy, speed to market is critical. In many of these nation-states, providing just the basic utility infrastructure (i.e. power, oil, gas, and water) is critical to gain a manufacturing foothold and in some cases, to help level the playing field. The ability to disrupt a competitor's infrastructure is just as effective. Who are these nation-states? Let's first look at the countries who have fallen prey; in almost all cases they are western nations with a well-developed economic industrial base. An October 2011 article titled "Foreign Spies Stealing U.S. Economic Secrets by the Office of the National Counterintelligence Executive" reported the following:

- The U.S. referenced McAfee's Global Energy Cyber Attacks in a February 2011 report about theft of data from Oil and Energy firms.
- Germany lost $28–71 billion to foreign economic espionage.
- S. Korea lost $82 billion to industrial espionage (more than 50% from China).
- In Japan, 35% of companies surveyed reported technology losses (more than 60% from China).
- In Canada, 86% of large firms reported being hit with cyber espionage.

While many of today's headlines focus on the military threat and political implication that these cyber attacks may lead to, there is also the flip side to these stories, as pointed out by FBI Director Robert Mueller: "nation-states are beginning to use a 'cyber one-two punch' method, first stealing intellectual property and then using it to interrupt daily operations." The interruption that Director Mueller is referring to is that larger SCADA landscape that controls the nation's power utilities, oil and gas industries, water systems, and manufacturing. In a recent report posted by TMCnet.com on April 23, 2012, nation-states are ranked in the top three threats by IT Professionals in both North America and Europe.



Nation-States

FBI: Cyber attacks grow as national security menace *From Networkworld, 4/3/12*

Cyber attacks are starting to eclipse terrorism as a threat to the country, says top officials from the Federal Bureau of Investigation, speaking before an audience of security professionals at the GovSec Conference.

Potential for digital Pearl Harbor is real *From CNET, 4/18/12*

How serious is the Internet-borne threat to critical infrastructure?
It's absolutely serious. The backbone of what we do every single day, the essence of what we do—our lives are dependent on critical infrastructure. There are groups that are intent on penetrating that infrastructure and it's a matter of either acquiring or developing the capability. And the networks are inherently vulnerable. The technology is vulnerable. The technologies deployed to run the infrastructure is very complex. The reason we see the level of attacks we see is because there are a lot of vulnerabilities, whether they be software, hardware, human vulnerabilities, or application layer vulnerabilities. You can't protect it all.

Iran switches to the offense in cyber war, panel says *From Defense Systems, 4/26/12*

Iran has demonstrated a willingness to attack the US and the intent to develop a cyber war capability, eclipsing Russia and China as a threat to the nation, a panel of policy and technical experts told House lawmakers. "Iran appears to be moving from defensive to offensive in the way it thinks about cyberspace," said Ilan Berman, VP of the American Foreign Policy council.

Report details successful China -based cyber espionage *From CNET, 4/1/12*

Hackers based in China have carried out 90 attacks on targets in Japan, India, and Tibetan activists in a cyber espionage campaign started last year, according to a report. Trend Micro released an analysis of the Luckycat campaign, which it traced back to a command-and-control center in China. The attacks are part of an organized effort, rather than random hacks, and have compromised 233 computers, according to the report. The New York Times reported the attacks can be traced back to a specific individual, a former graduate student in China who may have recruited others to work on the Luckycat campaign. The attackers targeted a number of Japanese and Indian industrial sites working in aerospace, enginery, engineering, shipping, and military research.

Can the US prevent a digital sneak attack *From CNET, 4/19/12*

In the Digital Era, espionage is a shadowy game of rapidly changing affiliations where the attacks are swift, anonymous, and devastating. So how can the U.S. stay ahead? Experts gathered here at Bloomberg's 2012 Cyber Security Conference to discuss exactly that. Northrup Grumman's Christopher Valentino, Raytheon's Jeff Snyder, former U.S. Air Force military intelligence officer Cedric Leighton, and Trend Micro vice president Tom Kellermann discussed how secure American companies really are (not really), discussed where the threats will come from next (where you least expect) and what can be done about it.

Threat intensity of cyber aggression to rise in 2012 *From Defense Systems, 2012*

It's the new year, and with it comes the tradition of predictions. And this year is no different. Looking at a healthy cross section of cyber security reports, it appears almost everyone is in agreement that 2012 will be a banner year when it comes to the threat of cyber attacks. Technolytics began tracking acts of cyber aggression in 2007. Acts of cyber aggression are defined as the unlawful or threatened use or acts of cyber aggression (i.e. cyber attacks) designed and conducted to intimidate, compel targets to comply with the perpetrator's demand, or to disrupt, defame, or destroy the online operations or data of the target. Threat intensity is defined at the vigor, force, energy, strength, or concentration associated with the use of threatening cyber activities.

Russian Million Dollar Hackers *From Forbes, 4/24/12*

Few nationalities are as good at making money from hacking than the Russians. Their share of the global cyber crime market, an estimated $12.5 billion black market, doubled last year to $4.5 billion, according to Moscow-based Group-IB, a cyber security services firm working mainly with the Russian government and banks to help reduce online fraud.

Industry News

DHS: America's water and power utilities under daily cyber attack *From Networkworld, 4/4/12*

America's water and energy utilities face constant cyber espionage and denial-of-service attacks against industrial control systems, according to the team of specialists from the U.S. Department of Homeland Security who are called to investigate the worst cyber-related incidents at these utilities.

These ICS-based networks are used to control water, chemical, and energy systems; the emergency response team from DHS ICS-CERT based at the DHS in Washington, D.C. will fly out to utilities across the country to investigate security incidents they learn about. ICS-CERT typically doesn't name the utilities they try to assist, but this week they did provide a glimpse into how vulnerable America is. In a panel at the GovSec Conference, ICS-CERT's leaders candidly presented a bleak assessment of why America's utilities have a hard time maintaining security, and why it's getting worse. "On a daily basis, the U.S. is being targeted," said Sanaz Browarny, chief intelligence and analyst for the control systems security program at the U.S. Department of Homeland Security as she presented some statistics from fly-away trips taken last year by the ICS emergency response team to utilities, most in the private sector.

Out of the 17 fly-away trips taken by the ICS-CERT team to assist in network and forensics analysis, it appeared that seven of the security incidents originated as spear-phishing attacks via e-mail against utility personnel. Browarny said 11 of the 17 incidents were very "sophisticated," signaling a well-organized threat. If only the compromised utility had been able to practice the most basic type of network security for corporate and industrial control systems, they would likely have detected or fended off the attack. One of the basic problems observed at utilities is that "a lot of folks are using older systems previously not connected to the Internet," she said. "The mindset is the equipment would last 20 or 30 years with updates. These systems are quite vulnerable."

Cyber-Security Czar Tells Utilities Companies to Keep Alert of Cyber Threats *From Secureworldpost, 4/12/12*

President Obama's top cyber security official said on Wednesday that utilities must pinpoint security gaps in their electricity delivery systems on a regular basis. The Energy Department, in cooperation with the White House, Homeland Security Department, and power companies, this month is expected to test a voluntary reporting model that assesses an individual utility's security posture to identify where safeguards are needed most. As of March 30, the Office of Management and Budget was finalizing information -collection procedures for the trial. The nation's energy sector must perform "active risk-management performance evaluations, continuous monitoring, exercises, and simulations to determine on a regular basis how we're doing," White House cyber security coordinator Howard Schmidt told industry and government leaders at McAfee's annual public sector conference. As the industry moves toward smart meters with Internet-connected sensors that help utilities and customers economize, it is becoming a hacker target. The government plans to make a template available to the electric sector this summer.

US battles rising cyber threats. Energy, water companies growing vulnerable to computer hackers *From Durango Herald, 4/23/12*

The mysterious caller claimed to be from Microsoft and offered step-by step instructions to repair damage from a software virus. The electric power companies weren't falling for it. The caller, who was never traced or identified, helpfully instructed the companies to enable specific features in their computers that actually would have created a trapdoor in their networks. That vulnerability would have allowed hackers to shut down a plant and thrown thousands of customers into the dark. The power employees hung up on the caller and ignored the advice. The incident from February, documented by one of the government's emergency cyber response teams, shows the persistent threat of electronic attacks and intrusions that could disrupt the country's most critical industries. The House this week will consider legislation to better defend these and other corporate networks from foreign governments, cybercriminals and terrorist groups. But deep divisions about how best to handle the growing problem mean that solutions are a long way off.

Consultant's Corner

SCADA Cyber Security and your smartphone

Security of your smartphone affecting your Industrial control system?

I have become dependent on my smart phone. I suspect you have too? Have you considered the possible attack vectors we open up while leveraging all these great features on these important little devices.

I know with my Blackberry, I download music, movies, files, email, pictures, apps, etc. It connects to Cellular wireless networks along with Wi-Fi and Bluetooth. If not configured correctly it could associate with rogue Cellular base stations that "bad actors" prop up to either steal your information or send malware to your phone. You can also become a carrier of malware from downloading apps, files, music and pictures of Cellular or Wifi networks. How about access via Bluetooth?

So, how does this affect other systems? While not overlooking the risk of losing your own data on the phone, having accounts hijacked etc, you also risk every system that you connect your phone to. While I travel, I was using my laptop as my charger. Using the supplied USB cable I connect my phone to my laptop and let it "Charge" but ignoring the fact that I'm connecting a USB drive to my system that could possibly infect it. I suspect this could be an overlooked practice on any system with the USB connector exposed. Not only do we need to manage our thumb drives we have to consider everything we connect to these systems even when in the past we consider them benign.

Some things to consider for your smartphone:

1. Configure your phone to only join trusted networks
2. Beware of Apps and any file downloads.
3. Keep your phones OS up to date
4. Set a screen lock and password ….and use it.
5. Don't hack your phone…ie Jail Break it.
6. Consider some of the phone locator apps to locate your lost phone.

Does it sound like a stretch? Maybe it is…but I would hope this might make you consider these little overlooked attack vectors.

This months contributor to Consultant's Corner is
Doug Clifton
Director, Critical Infrastructure & Security Practice
Invensys
Doug.Clifton@Invensys.com

The Cyber Advisor
Invensys Critical Infrastructure & Security Practice
April 2012 / Issue 07

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**