December 2012 / Issue 15

The Cyber Advisor

Invensys Critical Infrastructure & Security Practice

this issue

2012 Year in Review

2012 was a busy year for cyber security. We saw the reoccurrence of Stuxnet and the Stuxnet-related worm Duqu, which attacked Microsoft Windows systems using a zero-day vulnerability. We also saw the return of Flashback, malware that infected close to 700,000 Macs and was the largest MacOS X breach to date, thanks to a Java vulnerability. Flame also appeared in the first half of 2012, having breached networks at oil platforms in the Middle East. Allegedly developed by U.S. and Israeli governments to target Iran's oil ministry, Flame has become known as the most sophisticated piece of malware ever identified, forcing its way onto computer systems disguised as a fake Microsoft certificate that attacked the Windows Update feature.

LinkedIn and Dropbox fell victim to a massive data breach that leaked 6.4 million password hashes, confirming that hackers were targeting valuable user credentials. In the second half of the year, Shamoon infected Saudi Aramco, one of the world's largest oil suppliers, destroying more than 30,000 computers. Gauss targeted personal details such as banking information, passwords, browser history, cookies, and system configurations. And the Mini-Flame virus carried out more precise attacks on companies in the Middle East. 2012 also saw a growth in Android malware, and will likely continue to grow in the next year.

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) warned of cyber attacks in the form of spear-phishing against U.S. natural gas pipeline companies as well as attacks on utilities systems as hackers were trying to gain remote access by guessing login credentials.

Symantec predicts that with 2013, cyber espionage will become "more and more popular among nation-states" and that mobile adware (madware) instances will continue to increase. In addition to mobile platforms and cloud services, social networks could also become the target of cyber attacks as real money comes into play for various add-ons and apps.

2012 introduced many new types of cyber warfare; let's begin 2013 armed with new knowledge and a plan of action.

Dec. 2012
Cyber Attack Statistics
- **Hackmageddon.com**

Attack Motivations
- 69% Cyber Crime
- 28% Hacktivism
- 2% Cyber Espionage

Top 3 Attack Targets
- 19% Industry
- 18% Government
- 15% Torrent Sites

Top 5 Attack Techniques
- 52% SQL
- 21% Defacement
- 11% Unknown
- 2% DNS
- 2% Targeted

Industry News

European renewable power grid rocked by cyber attack

EurActiv.com 12/10/2012

A German power utility specializing in renewable energy was hit by a serious cyber attack in late November that lasted five days, knocking its internet communications systems offline in the first confirmed digital assault against a European grid operator. EurActiv has learned that the security breach has already been discussed at an assembly meeting of the European Network of Transmission Systems Operators for Electricity (ENTSO-E), which brings together bosses of the continent's transmissions industry operators (TSOs). The association is understood to be communicating closely and regularly with the European Commission about potential cyber-security threats to Europe's grids. However, beyond flagging their critical systems protection working group, ENTSO-E will not comment on the details of particular incidents like the 50hertz attack, or even whether similar attacks have occurred before.

Utilities' cyber survey may be model for other industries

www.federaltimes.com 12/11/2012

A White House effort to improve the cyber security of the nation's commercial power grid could soon be expanded to other critical sectors, such as transportation and water. The Energy and Homeland Security departments kicked off the initiative (known as the Electricity Sector Cyber Security Capability Maturity Model) this year as an effort to assess and improve the security of thousands of utility companies. A key component of the initiative is a self evaluation survey of more than 300 questions that helps utilities evaluate their cyber security, identify gaps, and plan how to mitigate risks and implement necessary changes.

UK Officials: Our Critical Infrastructure Has Already Been Hit by Cyber Attacks

news.softpedia.com 12/11/2012

Although they haven't pinpointed the attacked networks, it's likely that they belong to organizations responsible for supplying water, gas, and electricity, The Guardian reports. The announcement came just before Francis Maude, Minister for the Cabinet Office, released a written statement to Parliament regarding the progresses made since the National Cyber Security Strategy was launched one year ago. According to the statement, in the past year, 93% of corporations and 76% of small businesses from the UK suffered data breaches. Maude warned that government departments were not immune to cyber attacks. He also listed the country's four main objectives as far as the Cyber Security Strategy was concerned. The National Cyber Security Program—responsible for the objectives—provides 650 million GBP ($1 billion / 800 million EUR) to improve the UK's cyber security capabilities.

Aramco Hack Aimed at Curbing Oil Production

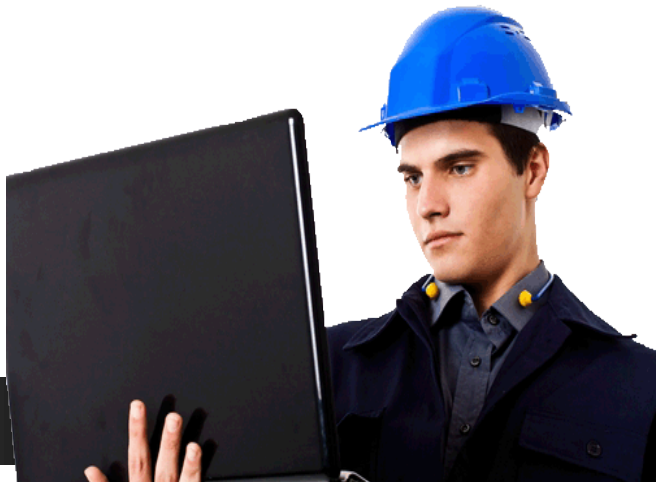
threatpost.com 12/10/2012

An August attack on the Saudi Arabian national oil company, Aramco, was reportedly launched in order to hinder oil production at the world's most valuable company, according to a report published in the New York Times on December 9. The attack damaged some 30,000 company workstations but failed to achieve its primary goal, which, according to Abdullah al-Saadan, the company's vice president of corporate planning, was to stop the flow of oil and gas from Aramco to local and international markets. Despite causing no perceptible interruption to Aramco's output, which accounts for a tenth of the world's oil supply according to the Times, the attack was destructive enough that it prompted the company to take its internal network down and its main website offline. These were restored after more than a week of downtime.

Natural Gas Industry's Cyber Concerns

Politco.com 12/4/2012

Cyber threats are a clear danger to the natural gas industry, but even top industry officials aren't sure how big. "We know they can get into our systems," said Ron Jibson, incoming chairman of American Gas Association, told reporters. "What we don't have a good feel for is why do they want to? To prove they can, or is it truly to do damage?"



Cyber News

80 Percent of Attacks in 2012 Were Redirects From Legitimate Sites

www.darkreading.com 12/4/2012

Sophos today released its Security Threat Report 2013, a detailed and interactive assessment of what's happened in IT security for 2012 and what's expected for 2013—from the ever-growing Bring Your Own Device (BYOD) movement to the increasing adoption of (and uncertainty around) the cloud to countless other security challenges faced by organizations of all sizes. 2012 was a year of new platforms and modern malware—what was once a homogeneous world of Windows systems is now a landscape made up of diverse platforms. Modern malware is taking advantage of these trends, creating new challenges for IT security professionals. The increasing mobility of data in corporate environments has forced IT staff to become even more agile. 2012 was also a retro year driven by resurgence in traditional malware attacks, specifically malware distributed via the web. For example, more than 80 percent of attacks were redirects, the majority of which were from legitimate websites that were hacked.

9 out 10 hospitals lost personal data in last two years

www.scmagazine.com 12/7/2012

Take out a quarter and flip it four times. It's unlikely the coin will land on heads (or tails) four times in a row—a one-in-16 chance to be exact. Yet tossing four consecutive heads or tails is a likelier outcome than being a hospital that hasn't been breached over the past two years. That's the finding from a new study from the Ponemon Institute and security firm ID Experts, which surveyed 80 health care organizations and found that 94 percent had experienced a data-loss incident in the past two years. Another 45 percent sustained more than five breaches during that period. According to the study, which was released in early December, lost devices, worker- or third-party-induced errors, and hacker attackers were the most common reasons for the breaches. Scaled out, the incidents cost the U.S. health care industry about $7 billion per year.

No password is safe from this new 25 GPU computer cluster

news.cnet.com 12/10/2012

Your really, really strong password just became a little bit easier to break. Jeremi Gosney, founder and CEO of Stricture Consulting Group, a company that handles password cracking, has unveiled a computer cluster boasting 25 AMD Radeon graphics cards. The cluster's horsepower allows it to make 350 billion password guesses per second against the NT Lan Manager (NTLM) security protocol Microsoft has used in Windows Server since 2003. Ars Technica was first to report on the cluster. Speaking to Ars in an emailed statement, Gosney said that his company's technology "can attack hashes approximately four times faster" than it previously could. Using a brute force method, the cluster is capable of guessing every single eight character password containing letters, numbers, and symbols in 5.5 hours. If companies use LM, an earlier password option for Windows Server, the cluster can figure out a password in six minutes.

GhostShell claims breach of 1.6M accounts at FBI, NASA, and more

news.cnet.com 12/10/2012

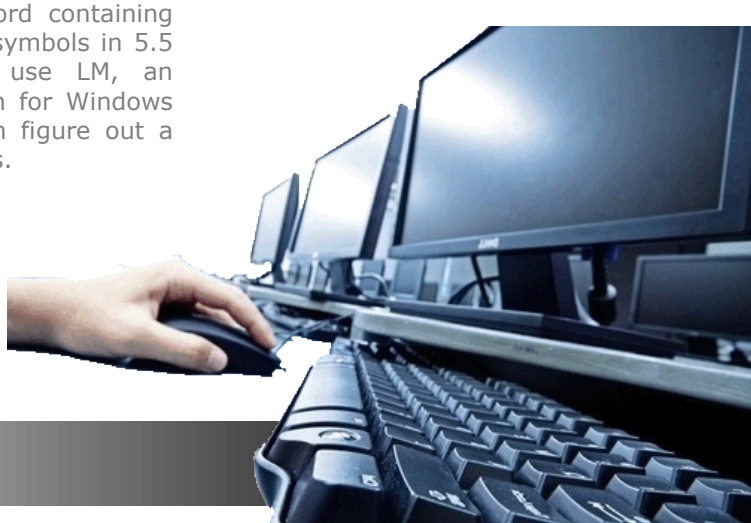
Team GhostShell, the hacktivist collective, said today that it has stolen accounts from a large number of government agencies, contractors, and security firms, posting information from 1.6 million accounts online. Dubbed Project White Fox, the hacking project appears to have affected NASA, the FBI, the Pentagon, and Interpol, among many others. The hackers announced their work in a file posted on Pastebin.

Who's using "password" as a password? TOO MANY OF YOU

theregister.co.uk 12/3/2012

A study to find the top 25 leaked passwords of 2012 has revealed too many people are still using extremely weak passwords for their login credentials. Here's are the top 3 most common leaked web passwords, with the change in position from last year in brackets:

1. password [unchanged]
2. 123456 [unchanged]
3. 12345678 [unchanged]



Consultant's Corner

SQL Server Hardening

Server Hardening is one of the most important tasks to be done on your servers, once you understand just how vulnerable servers are "out of the box." The default configuration of most operating systems are not designed with security as the primary focus. Instead, default setups focus more on usability, communications, and functionality. To protect your servers, you must establish solid and sophisticated server hardening policies for all servers in your system's network.

One best practice solution is SQL Server Hardening, and as with all servers, once connected to the Internet, they are vulnerable to cyber attacks. What sets the SQL server apart from other servers is the function it performs. SQL servers are a relational database management system. These databases and the information contained are what make SQL servers a target for hackers and the reason that all SQL servers should be hardened at install and continually monitored for updates and changes.

Hardening the SQL servers is a fundamental first step in a cyber security program. SQL servers are ICS critical assets, and any compromise to one of these servers can have a devastating impact on business. Most successful SQL server cyber attacks can be tracked back to a basic lack of best practices: badly configured user accounts, missing patches, and weak passwords resulting from lack of password policies.

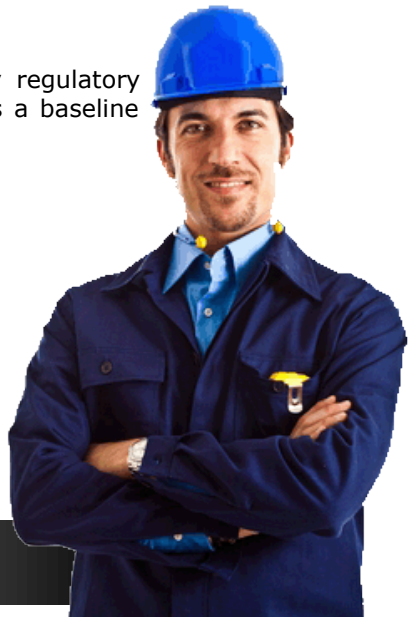
The main threats to a SQL server are:

- Indirect attack—SQL injection
- Direct—exploit attack
- Cracking SA Password
- Google hacks

Understanding the nature of these threats is critical in developing a SQL Server Hardening solution. Developing a best practice SQL hardening solution must first address the required remediation steps, ensuring that common threat vectors are addressed and mitigated. The CISP hardening solution addresses these issues:

- Remote access policies
- Server authentication mode(s)
- Server account policies
- System privileges policies
- SA account policies
- Server services accounts
- Patch management
- Security logging

SQL Server Hardening is critical to any cyber security initiative and is part of many regulatory compliance program. Server hardening not only provides security, but also establishes a baseline for all server platforms assisting with maintenance, patching, and planning.



This month's contributor to Consultant's Corner is
Tom Jackson
Principal Consultant, Critical Infrastructure & Security Practice
Invensys
tom.jackson@invensys.com

Consultants 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 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 actively participate 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.

Join us on Blogger

Industry Knowledge

CISP has a number of resources that help them understand the demands of Control 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 Assessment, Development, Implementation, and Management.

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**