Schneider Electric

The Global Cyber Advisor

Invensys Critical Infrastructure & Security Practice

June 2014
Issue 33

this issue

Hackers found controlling malware and botnets from the cloud

From www.nertworkworld.com, 6/26/2014

In what is considered to be a natural evolution of tactics used by cyber criminals to infiltrate corporate networks, security firm Trend Micro has new evidence that more botnets and malware are being not only hosted in the cloud, but controlled remotely from cloud servers. The goal of hackers is to disguise their malicious software as regular traffic between corporate end points and cloud-based services. Trend Micro reported through a blog post that it has observed the first instance of hackers using DropBox to host the command and control instructions for malware and botnets that have made it past corporate firewalls.

Energy Sector at High Risk of Cyber Attacks

The energy infrastructure encompasses many things—heat, water, and refrigeration, to name a few—and they all rely on the power grid. Not surprisingly, this makes the energy sector a popular target among hackers, including hostile insiders, political hacktivists, and nation states looking to steal information. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) reported over 200 incidents between October 2012 and May 2013, 53 percent of which were aimed at the energy sector, a 13 percent increase from the previous reporting period. With the energy sector at such high risk of cyber attacks, a voluntary initiative called the Oil and Natural Gas Information Sharing and Analysis Center was formed this month that is aimed at protecting energy infrastructure from computer-based attacks because data breaches, cyber threats, and cyber espionage campaigns [are] becoming more commonplace, according to the group (InfoSecurity).

Recently, security researchers discovered a new form of malware called Havex that has been used in a number of cyber attacks against the energy sector, namely European SCADA systems. Similar to the Stuxnet worm that was designed to attack industrial PLCs (Programmable Logic Controllers) and reportedly ruined almost one-fifth of Iran's nuclear centrifuges, Havex is also programmed to "infect industrial control system software of SCADA and Industrial Control Systems, with the capability to possibly disable hydroelectric dams, overload nuclear power plants, and even shut down a country's power grid with a single keystroke" (thehackernews.com). And with the energy sector at such high risk of attacks, insurance agencies generally do not provide coverage due to the billions of dollars at stake if major events like explosions are triggered remotely by hackers.

According to Symantec, "The energy sector has become a major focus for targeted attacks and is now among the top five most targeted sectors worldwide."

With that in mind, it is important to have a plan, take action, monitor, and be vigilant.

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
June 2014 / Issue 33

Industry News

Middle East hackers target Europe and US

From www.ft.com, 6/2/2014

A group of Middle Eastern hackers has targeted European national governments and a major US financial institution in a recent cyber espionage campaign, according to research by FireEye, the US cyber security company. The group—known as molerats—has previously been linked with attacks on the US and UK governments as well as former UK prime minister Tony Blair, in his role as Middle East peace envoy, and the BBC. The latest cyber attacks took place between April 29 and May 27 of this year, with the hackers sending "phishing" emails that aim to get employees of the European national governments and the US financial company to click on links and attachments, which then download malicious software, known as malware. Ned Moran, senior malware researcher at FireEye, which specializes in detecting "advanced persistent threats," said the attacks were an example of the global proliferation of cyber espionage as the hackers were probably trying to obtain strategic intelligence and sensitive information about their enemies.

Hackers warn of cyber attacks on oil companies in Saudi, UAE, Qatar

From www.livetradingnews.com, 6/20/2014

A Middle East-based group of hackers has issued a threat warning of cyber attacks against Crude Oil, Natural Gas, and Energy companies in the Middle East, security firm Symantec reported. The threat, made by Anonymous, a politically motivated group of hacktivists, states that they are planning to attack before, during, and after June 20, 2014. This is due to Anonymous disagreeing with the USD being used as the currency to buy and sell Crude Oil, Symantec said. According to the security firm, governments that may be attacked include those in Saudi Arabia, Kuwait, and Qatar.

Energy makes prime target in cyber threat infrastructure

From www.ft.com, 6/5/2014

In May, the US Department of Homeland Security revealed that the industrial control system of a public utility had been hacked by a "sophisticated threat actor." The department—or rather its industrial control systems cyber emergency response team (ICS-CERT)—did not reveal the type of utility. But access to the control system of a power company could give hackers the ability to switch off parts of the electrical grid, while access to a water utility's control system could allow them to interrupt water supplies. In 2012, the agency said hackers had waged a campaign to break into the systems control of US natural gas pipelines. The method used on the utility was rudimentary: a "brute force" attack that compromised the system's remote access connection to the internet by trying a variety of password combinations.

Sustained threats to oil and gas infrastructure boost need for security solutions

From www.frost.com, 6/3/2014

New infrastructure development in the oil and gas industry and the growing threats to the security of critical oil and gas assets are encouraging end users to invest in security solutions. Plant owners are particularly interested in security products, services, and solutions that can detect and delay threats and are able to employ cutting-edge innovation and technology. Acknowledging these requirements, market participants are offering user-friendly security solutions that create superior customer value. New analysis from Frost & Sullivan, Global Oil and Gas Infrastructure Security Market Assessment, finds that the market earned revenues of $19.63 billion in 2013 and estimates this to reach $24.68 billion in 2021. The study covers the segments of security services, command and control, screening detection, surveillance, access control, perimeter security, and cyber security.

As Stuxnet anniversary approaches, new SCADA attack is discovered

From www.darkreading.com, 6/26/2014

Nearly four years since Stuxnet broke onto the scene, F-Secure has discovered another series of attacks against industrial control systems—this time aiming at mostly European organizations. The attackers' ultimate motives are unclear. Researchers suspect they are simply gathering intelligence in preparation for a more serious attack. The attackers are infecting SCADA and ICS systems with the HAVEX remote access tool mostly used for information gathering, using a unique infection vector. In addition to the usual phishing messages and exploit kits, the attackers compromised the websites of three industrial application vendors and swapped their legitimate installers with ones that would also install HAVEX when downloaded and run.

Schneider Electric

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
June 2014 / Issue 33

Cyber News

Cyber security is fastest growing market

From gulfnews.com, 6/9/2014

For several years, the Middle East region has been targeted by wide-scale cyber attacks, for espionage or sabotage means, resulting in serious damage caused to companies and facilities. “Cyber security is the fastest growing market at 8-10 per cent per year and the market is worth around $66 billion this year,” said Guy Meguer, General Manager in Middle East for Cyber Security at Airbus Defence and Space. The Middle East’s energy sector is rapidly adopting smart devices and cloud computing to enhance business, but this is also creating a larger landscape for cyber security threats. Malware can cripple an energy company’s IT infrastructure and halt business operations, and potentially disrupt the world’s energy supplies,” said Rabih Dabboussi, General Manager of Cisco UAE. As connectivity increases, he said the energy sector faces a malware encounter rate of more than 400 per cent, or more than 300 per cent higher at risk than the median industry.

US to ask China to restart cyber working group

From www.businessweek.com, 6/27/2014

The United States wants to restart a cyber security working group that China shut down after the U.S. indicted five Chinese military officers on charges of hacking into American companies' computers to steal trade secrets. After the indictments against the five officers were unsealed in May, Beijing pulled the plug on the group. It had been set up a year ago in what Washington viewed at the time as a diplomatic coup after President Barack Obama and China's President Xi Jinping held a summit in California aiming to set relations between the two global powers on a positive track.

Witness protection scheme hacked

From www.hampshirechronicle.co.uk, 6/26/2014

Self-confessed phone hacker Glenn Mulcaire accessed the new identities of individuals put under witness protection but Scotland Yard took no action, it has been claimed. BBC Panorama reported last night that the Metropolitan Police had evidence in 2006, during a previous investigation into phone hacking, that Mulcaire had accessed the highly secret information. Ex-Metropolitan police officer Brian Paddick told the program: "The Witness Protection Scheme is a very expensive operation to give people who've been convicted of very serious offenses and people who are very vulnerable witnesses—to give them a completely new identity, so they can have a completely fresh start. For that information to get into the hands of journalists is potentially putting people's lives at risk."

Iran’s Bushehr reactor resumes operations after earthquakes, cyber attacks

From www.worldtribune.com, 6/2/2014

Iran has reported the renewal of operations at its only nuclear energy facility. The Iranian Atomic Energy Organization said the Bushehr nuclear energy reactor complex has resumed operations after a suspension of several months. Bushehr, completed by Russia, has been shut down several times since reaching full capacity in August 2012. Iran has reported suspected Western cyber attacks on Bushehr and other nuclear facilities. Atomic Energy Organization spokesman Behrouz Kamalvandi said Bushehr would be relinked to the national electricity grid over the next few days. He said this first required the warming of the reactor core.

Self-propagating SMS worm Selfmite targets Android devices

From www.computerworld.com, 6/27/2014

A rare Android worm that propagates itself to other users via links in text messages has been discovered by security researchers. Once installed on a device, the malware, which was dubbed Selfmite, sends a text message to 20 contacts from the device owner's address book. Most malware programs for Android are Trojan apps with no self-propagation mechanisms that get distributed from non-official app stores. Android SMS worms are rare, but Selfmite is the second such threat discovered in the past two months, suggesting that their number might grow in the future. The text message sent by Selfmite contains the contact's name and reads: "Dear [NAME], Look the Self-time," followed by a goo.gl shortened URL.

Schneider Electric

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
June 2014 / Issue 33

Cyber Security Return on Investment

In today's business environment, implementation of a cyber security program is a necessity. Many people correlate cyber security with an insurance policy, which is incorrect. Implementing a cyber security program is better related to risk management. Insurance provides compensation after an incident has happened. The idea of risk management prevents or minimizes the incident occurrence.

A cyber security program has many facets. In most cases, adding a firewall to a computer system does not constitute implementation of a cyber security program. The many facets of cyber security include addition of hardware, installation of security software, and training personnel in cyber security policies. Implementing the program may have significant costs. Minimizing the cost and meeting the appropriate cyber security requirements is the challenge.

Decisions for many facility or company improvements are based on Return on Investment (ROI) analysis to implement changes. Determining the ROI should be done based on factors associated with the risk of a cyber security incident. The impact of a cyber security incident could have a significant negative perception, impact the reputation, and potentially cause a financial impact to the company or facility. Examples of the negative impact have been seen from recent cyber security attacks on Target, Marshalls, and the Stuxnet attack. If the company or facility is perceived as a risk to personal financial information, environmental contamination of the surrounding area, potential of significant explosion by mixing inappropriate materials, or general safety, the company or facility will sustain a financial impact. This impact may be from fines or penalties and can also be from additional costs associated with a hazardous facility or company. The perception of risk from a cyber security intrusion may affect stock prices, personnel wages, insurance costs, and future potential for plant or company improvements or expansion.

When planning to implement or improve a cyber security program, the following criteria needs determined:

- Identify the regulatory requirements, both future and pending
- Establish current system status and planed upgrades
- Assess the risk associated with implementation of various levels of the cyber security program
- Determine current personnel capabilities and any need for external support

Cyber security implementation should reduce and minimize the risk of a cyber security attack. A cyber security program should not be thought of as insurance. Insurance compensates after the incident. Once the incident has occurred, damage to the facility or company reputation and perception will continue. The intent of insurance does not provide restoration to a loss of reputation or perception. A determination of the cost to the company or facility's loss of reputation should be a significant factor in determining the cost of implementing a rigorous cyber security program.

This month's contributor to Consultant's Corner is Bernie Pella, GIAC GSLC
Consultant, Critical Infrastructure & Security Practice, Invensys
bernie.pella@schneider-electric.com

Schneider Electric

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
June 2014 / Issue 33

Most Popular Blog Posts This Month

ATM Hacking (April 3, 2013)
Read about how a new type of malware being planted in ATMs can lift card information, compile the data in a document, and send it straight to the hacker.

Public-private survey finds cybercrime on the rise (May 30, 2014)
The hackers are winning, according to a survey of 500 executives of U.S. businesses, law enforcement services and government agencies.

Personal Information Compromised After AT&T Data Breach (June 16, 2014)
Two big companies have been hit by cyber attacks and now your information may be up for sale.

Anonymous plans global cyber attacks on energy firms on Friday (June 19, 2014)
AnonGhost, a politically motivated group of hacktivists, is planning to launch cyber attacks on energy companies globally, including Adnoc and Enoc in the UAE, on Friday for using the dollar in oil trades.

Hackers Warn Of Cyber Attacks On Oil Companies In Saudi, UAE, Qatar (June 24, 2014)
A Middle East-based group of hackers has issued a threat warning of cyber attacks against Crude Oil, Nat Gas and Energy companies in the Middle East, security firm Symantec reported. The threat, made by Anonymous, a politically motivated group of hacktivists, states that they are planning to attack before, during, and after June 20, 2014.

Featured Post: 5 Wi-Fi Security Myths

Wi-Fi has evolved over the years, and so have the techniques for securing your wireless network. An Internet search could unearth information that's outdated and no longer secure or relevant, or that's simply a myth. Read this article for information on the most current and effective means of securing your Wi-Fi network.

Visit us on Blogger!

Schneider Electric

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
June 2014 / Issue 33

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,

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!

Schneider Electric

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

1820 Preston Park Blvd. Suite 1900 Plano, TX 75093 ▪ P 469.365.6400 ▪ F 888.758.7675 ▪ **iom.invensys.com**