The Global Cyber Advisor

by the Cyber Security Services Group

Schneider Electric

February 2015
Volume 41

"Desert Falcons" hacking group devastate Middle Eastern targets

From www.itproportal.com, 2/20/2015

A group using self-developed targeted attack tools has hit 3,000 targets in the Middle East and carried out espionage actions across the region. Named the Desert Falcons, according to the report by Kaspersky Lab the 30-strong Palestine, Egypt and Turkey-based group carries out its actions with its own "homemade malware tools and techniques to execute and conceal its campaigns on PC and Mobile OS".

this issue

2015: The Year for a Change in Our Cyber Security Behavior

We are only a couple of months into 2015 and already there's news of increased targeted cyber attacks. Unfortunately the cyber threat forecast for 2015 is no better than last year. All one has to do is look at the numbers from Mandiant's recent report, "Cyber Security's Maginot Line." The current landscape shows that nearly 97% of all organizations have been breached. This means an attacker has bypassed all layers of a company's defense.

Other findings include:

- More than a fourth of all organizations experienced events known to be consistent with tools and tactics used by advanced persistent threat (APT) actors.
- Three-fourths of organizations had active command-and-control communications, indicating that attackers had control of the breached systems and were possibly already receiving data from them.
- Even after an organization was breached, attackers attempted to compromise the typical organization more than once per week (1.59) on average.

So how can the number of companies impacted be so high at 97 percent? In part, it is a reliance on ineffective point solutions in addition to poor network monitoring. Only 31 percent of companies detected the breach internally and 69 percent had to be notified by an external source! There is an even more disturbing trend behind these numbers—how long the attackers dwell on a victim's network. The median number is 205 days, with the longest presence at 2,982 days as reported by Mandiant's report, "View from the Front Lines."

As we go forward into 2015 with the looming reality of cyber threats, we must make a resolution to change our behavior and our cyber security posture. Gone are the days of point solutions that are not kept in check by internal staff. Instead, we must look at company needs and evaluate a cyber security strategy based on risk assessment. We must identify what is critical and how we can best defend those critical items as part of a comprehensive cyber security strategy that is unique to each facility's needs, moving away from the "one size fits all" point solutions and finally focusing on managed security services that monitor the network for any change.

Cyber Security Services by Schneider Electric

February 2015 / Volume 41

Cyber Central

How We Do It: Cyber Security Lifecycle Methodology

Part 1 of 4

Last month, we introduced who we are and what we do. The focus was primarily on our cyber security methodology and how that makes us platform-independent and product-agnostic. This brings us to How We Do It. The answer is our unique lifecycle approach, which consists of four key stages: Assess, Develop, Implement, and Manage. These four steps are not only critical to developing a holistic cyber security solution, but they also outline critical points of our client engagement. This approach allows us to engage any customer at any point in their own cyber security program.

Stage 1: Assess

The starting point for any engagement is the assessment. This is where CISP works closely with the client to assess their current network to help identify problems and develop requirements. The goal of the assessment stage is to define a risk-based assessment of the client's network in order to develop what the true needs of the client are. As an example, if a client wants three firewalls installed, the first questions are:

- Why are firewalls determined to be the best approach?
- How was the quantity of three determined?
- Who determined the locations of the firewalls?

In many cases, this is putting the perverbial cart in front of the horse. A risk-based assessment determines what the client needs to protect and the level of risk is appropriate for the network asset in question. Keeping control room connectivity is probably a higher priority than keeping power to the break room. This type of assessment helps the client to determine what their actual needs are versus their wants.

The assessment is also an important element of most regulatory programs and plays a crucial role in most companies in determining budgeting.

Next month, we will discuss Stage 2 of our Cyber Security Lifecycle Methodology: Development.

Schneider Electric

The Global Cyber Advisor
Cyber Security Services
February 2015 / Volume 41

Industry News

Mideast tops world in cyber security priority (MENA)

From www.tradearabia.com, 2/23/2015

More than half of business and government leaders in the Mena region identify cyber security as a strategic priority, compared to only 23 per cent in the US and 36 per cent in UK/Europe, a report said. Boards of directors in 35 per cent of Mena organizations have been briefed on strategic cyber security issues in the last 12 months, as compared to 22 per cent globally, added the survey titled "Global Megatrends in Cybersecurity 2015" commissioned by US-based Raytheon Company, a technology and innovation leader. "You don't have to wait until you're attacked to take cyber security seriously," said Jack Harrington, vice president of cyber security and special missions at Raytheon Intelligence, Information and Services.

Nautilus Minerals falls victim to cyber scam, prepays $10m into wrong account (NA)

From www.miningweekly.com, 2/2/2015

Canada's Nautilus Minerals and Dubai-based marine solutions company Marine Assets Corporation (MAC) report having been the victims of a cyber attack, which resulted in Nautilus paying a $10-million deposit intended for MAC into an unknown account. The deposit was part of an $18-million charterer's guarantee that was to be provided at the start of a charter of a vessel that would first be deployed for use at the Solwara 1 project, offshore Papua New Guinea. However, in December, Nautilus discovered that an unknown third party had launched a cyber attack on it and MAC, resulting in Nautilus paying the deposit into a bank account it believed to be MAC's, but which MAC had subsequently advised was not its account.

16 nuclear reactors vulnerable to terrorist drone attacks (EU)

From rt.com, 2/23/2015

Britain's aging nuclear power plants are vulnerable to terrorist attacks by unmanned drones that could kill thousands of people, a government adviser has warned. John Large, an engineer for Britain's Atomic Energy Authority, says ministers are ignoring risks posed by nuclear terror assaults. Nuclear power stations around the UK suffered 37 security breaches in 2014 – the highest number since 2011. Large is calling for urgent security reforms. He is also demanding the government set up a major operation to test the resilience of Britain's power plants against prospective attacks.

US oil and gas cyber security market sees global cyber attacks rise by 179% (NA)

From www.companiesandmarkets.com, 2/16/2015

With the increasing prevalence of devices that are connected to the Internet, cyber attacks have become commonplace in the vast majority of industries across the world. The US oil and gas market in particular has seen the number of cyber attacks shoot up over the past two years. With the number of attacks against oil and gas companies in 2013 reaching 6,500, which was an almost 180% increase on 2012.

UVI to help secure nation against cyber attacks (CALA)

From virginislandsdailynews.com, 2/16/2015

In an era of mass information breaches and identity theft, the territory's university is working to train a new workforce to combat cyber attacks. The University of the Virgin Islands has received a $1.3 million grant from the U.S. Energy Department's National Nuclear Security Administration. The grant funding is part of a presidential initiative to boost the level of cybersecurity expertise in America, according to a UVI statement.

Cyber security remains a top concern in the Middle East (MENA)

From www.zawya.com, 2/26/2015

As news reports are abuzz with cyber criminals having reportedly succeeded in stealing USD1 billion from over 100 banks globally within a span of two years, the Market Forecasts and Analysis Report (2014 -2019) by MarketsandMarkets predicts that the global cybersecurity industry will be worth USD155.74 billion in 2019. Also, with the 2014 Global Economic Crime Survey by PricewaterhouseCoopers (PwC) having identified cybercrime as the second most common form of economic crime reported in the Middle East, the same MarketsandMarkets report has indicated that the region's cybersecurity market will grow by 84 per cent from USD5.17 billion in 2014 to USD9.56 billion in 2019.

Schneider Electric

The Global Cyber Advisor
Cyber Security Services
February 2015 / Volume 41

Cyber News

Evolving threats demand an evolving national security strategy

From www.forbes.com, 2/19/2015

The highly publicized cyber-attack on Sony Pictures Entertainment in November 2014 is the type of greatly feared computerized catastrophe that all individuals and institutions face. Although a personal cyber attack can be overwhelming, attacks at the corporate or government level can have dire consequences. In addition to financial losses, cyber attacks have the ability to shut down or manipulate energy infrastructure, weapons defense systems, medical devices, financial markets, and transportation networks.

Companies 'must see cyber attacks as inevitable'

From www.newsweek.com, 2/15/2015

A top executive from the firm whose forensic experts investigated the Sony Corporation cyber hack last year says we "shouldn't be surprised" by the recent cyber robbery of up to $1bn - deemed one of the world's biggest cyber heists to date - and that companies should plan for the worst and see attacks as an inevitability. A report by Kaspersky Lab, a cyber security company, revealed on Monday that up to 100 banks and financial institutions in 30 countries, including Russia, France, Germany, the UK, Spain, Poland, Norway and Switzerland, have been attacked in an unprecedented cyber robbery. The gang responsible, dubbed 'Carbanak' and comprising of members from Russia, China and Ukraine, is believed to have been taking up to $10m at a time from banks over periods of two to four months since 2013, using various techniques including 'spearfishing' - the sending of malware-infected emails to individual employees which activate once opened.

Record number of cyber attacks hit Lockheed Martin in 2014

From mil-embedded.com, 2/18/2015

Lockheed Martin President and CEO Marillyn Hewson, announced that Lockheed Martin was hit by 50 cyber attacks during 2014, the most the company has ever seen directed against it and Hewson says she expects the number to only increase. She made her remarks during an address to journalists at Lockheed Martin's corporate media day in Arlington, Va. The company's cyber leadership said the number of 50 attacks was up significantly from 28 in 2010 when there only 10 attacks.

Israel spared two major cyber attacks

From www.timesofisrael.com, 2/22/2015

Israel has managed to dodge two massive cyber attacks, according to data collected by Kaspersky Lab, the Russia-based cybersecurity firm that discovered the mega Flame and Stuxnet viruses several years ago. This past week, Kaspersky Lab's Global Research and Analysis Team (Great) reported a major cross-border hacking attack called the Equation Group, which Kaspersky said was worse than any attack ever encountered. A spokesperson for Kaspersky Israel said the malware operation missed Israel, particularly its banks, but hit nearly every other country in the Middle East.

Arabic cyberespionage group attacking Middle Eastern, other targets

From www.networkworld.com, 2/17/2015

An Arabic cyberespionage group has attacked thousands of high-profile targets in Egypt, Israel, Jordan and other countries for the past two years, cybersecurity vendor Kaspersky Lab said. The cyber mercenaries, which the vendor dubbed the Desert Falcons, has stolen more than 1 million files from 3,000 victims in more than 50 countries, Kaspersky Lab said Tuesday. The group, likely native Arabic speakers, began in 2011, with the first infections coming in 2013, the company said. Targeted countries include Algeria, Lebanon, Turkey and the United Arab Emirates in the Middle East, and the U.S., Russia, France and Sweden beyond the region, Kaspersky said.

Schneider Electric

The Global Cyber Advisor
Cyber Security Services
February 2015 / Volume 41

Oversharing in Social Media

While watching the recent Allstate Insurance-sponsored college football playoff game, Mr. Mayhem commercials sparked some thoughts about social media and cyber security. The popularity of social media has prompted many to share significant aspects of people's lives. For the Mr. Mayhem commercials, a couple shared they were spending the weekend at the playoff game on social media. In the commercial, Mr. Mayhem used that information to break into the couple's house and have a "during the game" auction of their household contents. Although the commercial was an over-the-top exaggeration, the concept has some elements of reality.

People share information about their lives with the intent of allowing friends the ability to keep up with family and personal events. This shared information provides insight into the lives of the individuals sharing the information. Much of this shared information can be used for more unethical purposes. The individuals sharing the information are naïve to the concept of nefarious individuals using the information.

If you think like a hacker, significant information is easily obtained from the shared information. The individual doesn't share direct information, but does provide clues to assist in gaining personal information. Using passwords as an example, many clues are supplied in social media. The clues provided in social media can provide passwords, resetting password questions, and other common criteria for account validation. Many password reset questions pertain to personal information as a validation to reset a lost or forgotten password. Most people use common personal information for passwords or the answer to the reset questions. If sharing on social media includes some of this personal information, it is much easier to guess the password or password reset. An example of this is someone that posts information about their pets, sports team, parents, their mother's maiden name, and other personal information. This provides the malicious individual significant assistance in accessing someone's account.

An example of how to use the social media information is as follows: John posts he is the network administrator for the ABC corporate network. He loves the Green Bay Packers and his dog Sparkles, as shown by his pictures and posts on social media. He is enamored with the Packers and Sparkles; he uses them for his passwords. His sharing on social media has potentially placed the ABC corporate network in jeopardy to a hacking attack. Another example is an individual posts he is single, available, and travels frequently for work. The individual always tweets his travel information. This information may not be useful from a computer security perspective but is useful for someone like Mr. Mayhem. If a single individual travels frequently and tells his friends or followers where he is, there is a high probability no one is at his home. This is an ideal situation for Mr. Mayhem or a real burglar. Upon return from the travel, the individual may be missing household contents and additional information, allowing something like identity theft.

Much of this may seem like common sense; however, I continue to be amazed at how much information individuals share on social media. Significant thought is required before sharing information on social media.

This month's contributor to Consultant's Corner is Bernie Pella
Consultant, Cyber Security Services, Schneider Electric
bernie.pella@schneider-electric.com

Schneider Electric

The Global Cyber Advisor
Cyber Security Services
February 2015 / Volume 41

Cyber Security Services

Schneider Electric's Cyber Security Services organization has the 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 Cyber Security Services include:

Hardware Independence

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

Regulation Knowledge

Cyber Security Services 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 Cyber Security Services 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

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

Proven Methodology

Cyber Security Services follows a proven life cycle methodology to support the implementation of a comprehensive successful cyber security program. Attributes of the lifecycle approach are Assessments, Development, Implementation, and Management.

Schneider Electric

For additional information please visit us at
http://software.invensys.com/services/security-and-compliance-services/cyber-security-services/

1650 West Crosby Road, Carrollton, TX 75006 ▪ P 972.323.1111 ▪ F 888.758.7675 ▪ www.schneider-electric.com