Volume 3, Issue 2

INFRAGARD – NORTH CAROLINA

ncinfragard.org

Inside This Issue

Electrical Grid Sunscreen

By: Torry Crass, Charlotte Board Member

Warm, sunny days are on their way once again. Hopefully, with everyone's share of vacations. Don't forget to pack your sunscreen! SPF 15 or above (93%+ protection) is the American Cancer Society recommendation. The Sun is a great resource that we simply could not do without. It gives us energy in so many different ways, some of which we need to block while at the beach to help preserve our health.

All the great benefits also come with risks. Without getting into too much detail, the Sun runs on a cycle of activity spanning approximately 11 years. In this time, sunspots come and go based on what's happening with the Sun. During peaks in the solar cycle, the activity, and thus spot occurrence, tends to increase significantly. While sunspots are not themselves the danger (only a balmy ~3500K vs ~6000K), they are an indication of other activity that is dangerous since most solar flares and coronal mass ejections (CMEs) originate around groups of sunspots.

Every now and then, those solar flares and CMEs erupt and head on an intercept path with Earth. When they arrive, they interact with the upper atmosphere, concentrating around the poles first to create what can be an awe-inspiring sight in the extreme northern and southern latitudes, the Aurora Borealis or Northern Lights.

Typically, the Earth's magnetic field protects us from these charged particles by absorbing and deflecting them. Once the amount of particles reaches a threshold where the magnetic field can no longer keep up, the particles begin to affect things that we rely on, radio communications and the electrical grid to start. In extreme cases, this causes damage to equipment and outages such as the 1989 blackout of the Canadian province of Quebec (http://www.nasa.gov/topics/earth/features/sun_darkness.html).

Let's go back to those sunny days on the beach for a moment, and very importantly applying your recommended sunscreen. Unfortunately, our electrical grid and much of what makes our nation function on a daily basis goes without its sunscreen. As studies have shown, still today we simply don't have protection in place for much of this critical infrastructure.

This risk, and that of nuclear and non-nuclear EMP burst, poses a tangible threat to our infrastructure and day-to-day lives. Over the past few months, we've been working hard to help extend the mission of the InfraGard National EMP-SIG to regional and local involvement in efforts to raise awareness, promote education, legislation, and any other activities which might help provide some sunscreen for this gap.

Are you interested in learning more? Great! Make sure to visit the Charlotte InfraGard May 2015 meeting for a talk presented by the author of "One Second After", William Forstchen, followed by a panel presentation and discussion on this topic. In addition, as we continue to work through our local and regional efforts, we invite you to visit our new website www.empcenter.org which will continue to be developed and used as a central repository for long term, high-impact threats which includes a focus on EMP threat.

CHARLOTTE INFRAGARD CYBERCAMP

Scheduled for July 27-31

Still looking for applicants, volunteers, speakers and sponsors. Interested?

Contact one of the Board Members or click here for more details:
Charlotte Cyber Camp

What can Critical Infrastructure Learn from Retail Data Breaches?

BY ALEXIS LAVI, Cybersecurity Analyst, Fortalice Solutions, LLC

As the critical infrastructure owners and operators of the US, you are responsible for delivering the essential services and functions needed for the US economy and population. Cybersecurity is tied to your business processes, mission, plus national and economic security. For many critical infrastructure owners, cybersecurity is a thought-through and integral element of an enterprise risk management and business continuity, whether due to market demands or existing regulations, guidance, or compliance.

Despite existing practices, regulations and compliance bodies, all sectors are susceptible to cyber attacks. Unfortunately, this past year was the worst ever for data breaches across all communities—banking, the US government, healthcare, and especially retail. As a critical infrastructure entity, you may have become immune to the score of retail breaches: Supervalu, Home Depot, Kmart, and Bebe, just to name a few. Because, well, how much can an electricity utility have in common with Dairy Queen? More than one may first think.

1. **Timing for an Attack:** The recent hack against Sony took place during a change in management.[1] The transition between Chief Information Security Officers (CISOs) could have created a vacuum that enabled an unauthorized user to enter the computer systems. During leadership turnover, operations may become disjointed or processes may be altered; however, security and monitoring should always remain at a company and industry standard to reduce the damage of a breach.
2. **Internet-facing Systems:** The Point of Sale (POS) terminal attacks are analogous to SCADA and Industrial Control Systems (ICS)—both are internet facing; both are key systems to the business; disruptive to operations to patch; and, both normally have legacy software involved. POS attacks due to malware scrapping the RAM of the terminals was one of the greatest causes of the retail breaches this year. Critical infrastructure owners and operators must face similar decisions as retailers when SCADA systems are potentially compromised, to take them offline and sacrifice business or continue to operate knowing the incurring damage to profit, consumer loyalty, and business function. Learning when retailers decided to take POS terminals offline may be helpful for SCADA operators.
3. **Vendor Security Risk:** Companies' supply chains complexity breeds areas of risks. Regrettably, most organization do not know their tier three or greater vendors. Vendor security proved to be one of the most significant causes for the largest data breaches in the past year. For example, Target's HVAC vendors were responsible for the malicious malware; similarly, vendors were used in the Home Depot attacks. Critical infrastructure is encouraged to implement a complete and robust vendor management program to mitigate risks and monitor for abnormal behavior.
4. **Repetitive Attacks:** Many of the retail data breaches this past year were point of sale (POS) attacks that used the same or similar malware – the amount of breaches vis-à-vis the known malware is disproportional. For example, this past year, one malware that resurfaced multiple times was the infamous Backoff, variants of Backoff that appeared in attacks included 211G1; other repetitive malware was Mayhem and BlackPOS. The repetitive attack should alert critical infrastructure owners and operators. If the cyber criminals can use a limited number of malware strains and the similar attack kill chains to inflict damage on retailers, then it would not be surprising if cybercriminals targeting the water sector, for example, would employ the same techniques repetitively. , then why take the time and resource to develop additional strains.
5. **Vulnerability Management Challenges:** The 2014 string of exploits, Shellshock, Heartbleed, or POODLE, did not discriminate between sectors. Patch management is a challenge for most organizations, for example, there are timing, prioritization, testing, inventory management, implementation verification considerations. The most robust of vulnerability management programs includes application white listing and enterprise patch management technologies. The National Institute for Standards and Technology 800-43 Revision 3 provides additional guidance for patching and vulnerability management.

6. **Cyber Insurance incorporated into Risk Management:** The frequency and sophistication of attacks against the retail sector are helping to drive the insurance market. Across industries, cyber insurance or self-insuring is becoming a necessary element in a cyber security and risk management plan to protect against of a breach. While the price for insurance has decreased, review what the policy covers and ensure that your organizations needs in the time of a breach are being met. For instance, forensic assistance and crisis communications are valuable benefits during and post breach. Plus, a full review of the policy requirements is crucial in order to maintain compliance. For example, many policies have a notification requirement. While notification of a breach is normally determined by state law, the policy may have its own requirements; there are certain cases where public disclosure has to be made to the carrier 24 hours prior to public disclosure. Critical infrastructure entities objectives for a policy may be different than retailers, but the need is the same.

7. **Insider Threat Reality:** Due to heightened security threats from insiders across all industries, organizations are leveraging their own knowledge and expert resources such as the Carnegie Mellon CERT to build out more robust and comprehensive insider threat programs.[1] An insider can be a disgruntled employee, vendor, or business partner --- entities that all critical infrastructure organizations have, as well. All organizations are encouraged to have some degree of an insider threat detection capability. The following elements are important to mitigate the risk of an insider (employee or business partner/contractor). Key elements of an insider threat program includes: screening process, convenient and anonymous method to report activity, comprehensive termination procedures, determination of a baseline of "normal" behavior, vigilance over social media postings, anticipating and managing negative issues in the work environment, clear ownership of intellectual property.

8. **Business Trends and Impact of Cyber Attacks:** Many compromised companies' profits and sales were impacted from data breaches this year. Examples include: Supervalu who announced a 23% decrease in their quarterly earnings. The second quarter profit fell from $40 million to $31 million dollars, with $1 million covering the immediate cost of the breach.[1] This decline in profit, according to the supermarket chain, is directly linked to the recent data breaches. Another prominent example was Target. Following their widespread breach, profit declined by 46%.[1] This decline is due to the overwhelming number of lawsuits, investigations, credit monitoring, and call centers to field customer inquiries. The direct expenses associated with the breach cost Target $148 million.[1] Many small businesses that rely on eBay to sell products were greatly impacted by eBay's breach. According to a small business owner, who conducts 70% of business transactions via eBay, the breach "changed everything overnight".[1] In one weekend, the business owner lost $5,000 in sales. In order to redirect consumers back to eBay, additional resources are being directed to marketing initiatives; however, only two-thirds of eBay users have reset their passwords, per eBay's counsel and "Google Inc. changed its search results, curbing visits to eBay's website from potential shoppers".[1] Needless to say, eBay and the business that rely on eBay are in for a long road ahead to recovery, as evident by the following figures: Net income in the third quarter fell 2.3 percent to $673 million, or 54 cents a share, from $689 million, or 53 cents, a year earlier.[1] The shares of EBay fell 4.7 percent to $47.88 at the close in New York. The stock is down roughly 13 percent this year.[1] The potential profit loss and financial consequences of a breach should be alarming to any business owner.

9. **Incident Response Plans:** There are two types of companies – those that know that they were hacked and those who don't know they were hacked. For many of the critical infrastructure owners there are specific notification requirements and regulations, even beyond the state laws. In order to effectively 1) know about the cyber incident, 2) respond, and 3) recover from the incident, a tested and developed incident response framework is essential. The framework and respective process includes internal and external support to coordinate a response to the public, contain the incident, and resume operations as soon as possible. Many risk owners lack the processes and technologies to maintain awareness of potential incidents and have the knowledge to respond effectively. All critical infrastructure owners should establish a trusting relationship wither their internet service provider (ISP) and various data management personnel associated with business functions.

10. **Big Data and Analysis:** The term "big data" is a buzz word, but there is significant meaning, purpose, and future for big data. The key to leveraging big data for threat detection is incorporating an analytic solution. According to a recent SANS survey of companies, "36% feel that the concept of big data is key for detection and investigation, and another 25% see the growing importance of big data and analytics in event management and security intelligence".[1] However, many companies are struggling to use big data for threat detection, because they are struggling to conduct analysis. In order to truly see the power of big data for cyber security purposes, "Analytics solutions will need to integrate with numerous internal detection platforms in an effort to increase visibility and improve security intelligence".[1]

11. **New Information Sharing Platforms:** The Retail Cyber Intelligence Sharing Center (R-CISC) is only four months old but with more and more retailers joining, the maturity, capabilities, and purpose of the group is growing. The Retail Industry Leaders Association (RILA) is behind the creation of the R-CISC, which now includes top names in the community, such as: Walgreens, Gap, Lowes, Target, and Nike. The membership extends beyond those in the RILA. As a member of the R-CISC, one gains: training opportunities, cyber threat information from the Secret Service, FBI, and US-CERT. The ultimate goal of the R-CISC, like many other ISACs, is to establish an intelligence sharing mechanism in near real time, so retailers can learn about pending attacks. While the critical infrastructure communities have their existing ISACs, reinvigorating and reevaluating the objectives and projects to ensure that cyber threat information is being shared as quickly and efficiently as possible.

12. **Compliance- Necessary but Not Sufficient**: The retail companies breached this year all had one thing in common: they were compliant with the payment card industry (PCI) requirements. PCI compliance is necessary but not sufficient in this current environment. Compliance to industry standards, baselines, or regulations does not stand in the way of a dedicated attacker. While each industry will tirelessly check the box for security requirements, conducting a holistic risk assessment is essential to proactively manage the risk of a cyber incident. Companies that have been breached dedicate more time and resources for cyber security, specifically the IT budgets which are now reaching 6-15% of a company's total budget. In many cases, Boards are instructing their companies to conduct risk assessments, penetration testing, and threat assessments in order to align budgets with company IT risks. In fact 70% of companies surveyed in an IANS study[1] indicated that they are using risk assessments to drive their IT security budgets. A budget for critical infrastructure entities should be risk-based, in addition to compliance-based.

Upcoming Events

Eastern Carolina Chapter Meeting
Date/Time: Wednesday, April 15th from 1-4 pm
Location: Cisco, #5, 1025 Kit Creek Rd,
Morrisville, NC.
Register at www.ncinfragard.org

Charlotte Chapter Evening Meeting
Date/Time: Tuesday, April 21st from 6-8 pm
Location: Ballantyne Hotel, Charlotte, NC.
Register at www.ncinfragard.org

Charlotte Chapter Meeting
Date/Time: Wednesday, May 20th from 1-4pm
Location: Microsoft, 8050 Microsoft Way,
Charlotte, NC.
Register at www.ncinfragard.org

Eastern Carolina Chapter Meeting
Date/Time: Wednesday, June 17th from 1-4 pm
Location: Cisco, #5, 1025 Kit Creek Rd,
Morrisville, NC.
Register at www.ncinfragard.org

SA James Granozio
InfraGard Coordinator
7915 Microsoft Way
Charlotte, NC 28273
704-672-6351
james.granozio@ic.fbi.gov

InfraGard Helpdesk/Tech Support
(877)861-6298
infragardteam@leo.gov