ACME POWER GRID COMPANY DIGITAL FORENSICS INCIDENT RESPONSE REPORT

Siggi Bjarnason

InfoSecHelp Consulting

https://www.infosechelp.net

siggi@infosechelp.net

Table of Contents

Disclaimer

This report is a complete work of fiction, any resemblance to anything else fictional or real is a pure coincident. As a fictional incident report, this report lacks all real data, and as such is more generic than a real incident report. If this were a real incident report, it would contain specific and detailed finding along with specific and actionable recommendations. Also, it most likely would contain less history. In other words, this is science fiction and completely bogus. I hope though that you enjoy reading this fictional report

Executive Summary

InfoSecHelp Consulting Company specializes in cyber operations, defensive tactics, cybersecurity, online safety and strategies for companies large and small as well as the individual. We have been retained to evaluate ACME Power Grid Company and report on our findings.

We will start this report with some background on cyber warfare and cyber threats to drive home why good cyber defense strategy and operational security is important

Then we'll go into what we found followed by our recommendations across three main aspects: people technology and operations.

Evolution of Cyber Warfare

There has been a huge leap in the evolution of cyber-related capabilities and technologies in warfare since the late 1990s. In the late 1990s, Internet proliferation was taking off. According to IETF RFC2235 by July 1992, there were less than a million hosts on the Internet. By July 1997, there were between nineteen and twenty million hosts on the Internet (Zakon, 1997). Things were much simpler back then; there was little worry about malware of any kind. Maybe the lack of worry was more based on ignorance than facts as there was little to no monitoring capabilities in the early days of the Internet. This is evident by multiple patent filings in 1998 for network monitoring systems such as the "Method and apparatus for automated network-wide surveillance and security breach intervention" (Patent No. 5,796,942, 1998). Due to this lack of monitoring any attacks largely went unnoticed. There were few viruses around, which were mostly for intellectual challenge and notoriety (Symantec Security Response, 2017). There were few exceptions, but by large the hackers of the early 1990s did not have criminal intent. Hacking pretty must started as a challenge, "how far can I get" kind of a thing, so more of an unauthorized access kind of an issue. From there it evolved into surveillance thing and theft, both in terms theft of information, software and unauthorized bank transfers. An example of that is the well-known hacker, Kevin Mitnick, who at age 16 hacked Digital Equipment Corporation and stole a copy of their proprietary operating system. (Chapple & Seidl, 2015)

This adolescence intellectual game soon evolved into full fledge espionage (i.e., reconnaissance and surveillance) as the cyber kill chain developed and organized groups started to get into this game.

At the turn of the 21st century, we started to see a drastic increase in attacks, and their sophistication was drastically improving. Many different attach vectors were discovered, and computer worms started to become prevalent and stepped up the reconnaissance effort. One of the most prevalent worms that

swept the world at the beginning of the 21st century was SQL Slammer. According to a paper published by SANS Institute in 2003, SQL Slammer started to spread on January 25, 2003 and infected more than 75,000 hosts. The paper goes on to say that slammer was doubling in size every 8.5 seconds having scanned approximately 55 million IP address within 3 minutes, causing huge disruption of the internet. The authored claimed this was the worst worm ever to hit the world at the time the paper was authored. (SANS Institute, 2003)

Not only has sophistication, frequency, and techniques drastically increased, the threat actors have also diversified significantly. Originally, threat actors acted largely alone. These days, they are often part of a group. These group can be loosely formed, such as the hacktivist group Anonymous, or more tightly organized such as nation-states or organized crime syndicates. Also, large corporations are engaging in cyber warfare for purposes of corporate espionage. These large groups are often well funded, very advanced and very persistence threat actors, whereas solo threat actors, as well as loosely formed federations, are none of those.

One pivotal point in cyber warfare came in the spring of 2007 when there was a politically motivated denial of service attack against the Estonian Government. The Russian government was attributed to this attack but denied any knowledge. Experts labeled this “Future of warfare” (Bruno, 2008)

Another pivotal point came in 2010 when the world saw the first case of a destructive cyber incident. The computer worm, now named Stuxnet, took down an enrichment centrifuge at the Natanz nuclear facility in Iran by infecting their SCADA and PLC. (Singer, 2015).

After the success of Stuxnet, cyber threat agents realized that they weren’t limited to just information gathering. Since then, there has been a cyber arms race. Threat actors are finding new ways to get in and finding new and creative ways to be destructive as fast as security professional can patch holes and putt up defenses.

In December 2015, we saw yet another highly destructive malware targeting three energy distribution companies in Ukraine. This attack resulted in substation shutdown and power customers by the hundreds and thousands left without power (Symantec Security Response, 2017)

Characteristics of an APT

APT stands for Advanced Persistent Threat and refer to the sophisticated threat actor groups which are often well funded and with large resources to draw from. They tend to have a very specific mission with specific objectives that often includes a very specific target, be that target a specific company, specific branch of government or military, or a specific person.

APT use various tools, depending on the mission and what was found during the reconnaissance phase of the mission. For example, they may have found an exploitable vulnerability in Internet-facing system, allowing remote code execution (RCE), which then allows them to pivot and compromise other systems directly. Most of the time, they utilize social engineering tactics such as phishing or pretexting to trick an employee at the target organization into giving them access. In some cases, the APT get the employee to give them their login credentials, other cases they trick them into installing malware such as remote access trojan (RAT) and then pivot from there. (Symantec Corporation, 2011)

Effect of the Internet on Attacks

Before the advent of the Internet, back before 1998, technology was much more primitive. Back then, most systems were isolated standalone computers. Personal computers were starting to make inroads in some companies, and few computer enthusiasts had them in their homes. More advanced companies had few computers connected into a LAN, but a connection to the outside was pretty much unheard of. Some companies with large mainframe had dial-up connections. Educational and research institutions, for the most part, made up what constituted the Internet at the time. Pretty much the only "hacking" that took place was more of unauthorized access than hacking per se. These were folks that would discover the dial-up number for say a military installation or a bank and brute force the login (if there even was a login) and poke around. Some did this for an intellectual challenge, others for bragging rights, some for personal gain where they would access a bank and make unauthorized transfers. The movies "War Games." (War Games (1983) - IMDB, n.d.) and Sneakers (Sneakers (1992), n.d.) illustrate this trend.

When the Internet became popular, and everyone and everything was connected to it, things changed drastically. This wasn't solely due to Internet proliferation as there was also incredible technology advancements at the same time. Whether the Internet caused technology advancements, advances in technology made the Internet, or a bit of symbiotic relationship is hard to say with any certainty. It is however highly likely that it was advances in technology that propelled advancements in the Internet which then spurred more technological advancements. With all the technological advances and the Internet becoming an essential utility created a whole new landscape with a host of issues that were not foreseen by most people in the 20th century, Winn Schwartau being a notable exception. (Schwartau, 1994)

These days the threat landscape is ever-changing, and the human factor is the biggest challenge as the APT favorite tool is Social Engineering. While history of PLC, DCA and SCADA systems at ACME Power Grid (APG) isn't readily available it is safe to bet that any computers at APG prior to 1998 were not connected to anything on the outside and the only way to get anything on or off those computers in a digital format was via floppy disks. Any connections these computers might have to the PLC would have been through an RS-232 serial connection. There were no viable attach vector during those days. Even if the systems at APG had an outside connection, it would have been through a dial-up modem, and any incursion would have been extremely labor intensive with a limited payoff.

Now you have systems that are interconnected as well as connected to the internet. Even if systems are air-gapped, malware can spread through USB drives as we saw with Stuxnet.

Internet-connected workstations are everywhere at APG, and there is a heavy reliance on SCADA and PLC systems, which are all interconnected, to reduce the workload on the operators at APG. The downside of that is that in case of a breach workload of a threat actor is also largely reduced.

Attack Origination and Perpetrator

APG does have good perimeter security setup and appear to have all the right technology solutions in place. We, however, found that there was a lack of focus on the human factor. What I mean by that is there wasn't enough focus on security training for employees, what proper operational security is, etc.

After forensically analyzing the security information and event management (SIEM) systems at APG, it appears that the attack originated through a phishing attack. What we found is that this all started when an operator on a control station with Internet access was checking their email and clicked on a link in a sophisticated phishing email that installed a Remote Access Trojan (RAT) on the control station. This gave the perpetrator full control over the control station. With this, they performed reconnaissance to map out the systems and network at APG. From there they installed a worm on the supervisory control and data acquisition (SCADA) system which then spread to the Programmable Logic Controllers (PLC) providing the threat actor complete control over the systems at ACME Power. We were able to catch this before the threat actor did anything destructive.

Profile of the Attacker

The attacker is most likely an APT group known as Waterbug which was first known to operate in 2005. They are very likely a state-sponsored group, however pinpointing exactly which nation-state might be sponsoring them has been a challenge. They are known to operate an attach network nicknamed Venom which consists of 84 compromised websites used for watering-hole attacks as well as hosting malware used in phishing attacks. Majority of servers that make up Venom appear to be split up across many European countries, mainly France, Germany, and Romania.

A watering-hole attack is when a threat actor infects a site or group of sites that are known to be popular amongst the intended target so that when the target comes to the web site, they unknowingly install the threat actor's malware. This term can also be a part of social engineering tactic, where the threat actors have a generic server farm that they then lure their prey to.

The Venom network appears to be very sophisticated and targeted, much more so than other watering-hole attacks which indiscriminately infect everyone who comes to the site.

Waterbug is known to target Government institutions, Embassies, and research facilities, so a utility such as APG seems right up their alley. They are known to use whatever attack methods that suites their mission, be it Zero-day exploits, phishing, etc. (Martin, 2016) (Symantec Corporation, 2016)

There appears to have been no physical access used in the attack on APG; they seem to have relied exclusively on logical access through RAT and other malware.

Analysis and Findings

Reconnaissance

This is the phase where the APT gathered their intel. There are two types of information gathering techniques. The first type is called passive and consists of any information gathered without contacting the target. This includes collecting information from public domain such as new articles, press releases, regulatory statements (e.g., SEC filings), postings on public forums, information on company web site, etc. The second type of information gathering is called active gathering and includes pretty much anything else, any actual contact with the target of any sort. (InforSec Institute, 2016) (Offensive Security Ltd, 2016)

Based on our forensic analyses, we have concluded that the Waterbug agent was able to find names and email addresses of employees of APG using passive intel gathering. The exact details of how they accomplished this are not yet known. However, they likely used tools such as harvester to gather this information. Waterbug then used this intel to switch to active reconnaissance and launch a phishing attack against APG.

When the operator clicked on that link in the phishing email, malware known as a remote access trojan (RAT) got installed on the operator's computer. This RAT communicated back to the command and control server for Waterbug, giving them full remote access to the operators' workstation. With full access to a computer inside the APG network, Waterbug could now conduct full active intelligence gathering, and fully mapped out the network and all systems involved. They could have done this using common tools such as nmap, tcpdump, and netcat. However, considering the resources Waterbug appears to have, it is more likely they have their own reconnaissance toolset that conducts network sweeps and port scans to identify, fingerprint OS and map out the network at APG.

Weaponization and Delivery

During the reconnaissance phase, Waterbug was able to harvest email address for APG employees from various internet sites and launched a phishing attack using those harvested emails. Additionally, public information about the employees was collected along with public information about APG. The email addresses were compiled into an email list. This email list along with other relevant data was fed into a standard malware platform that Waterbug developed in house, which then generated a custom believable phishing email target at the emails in the email list

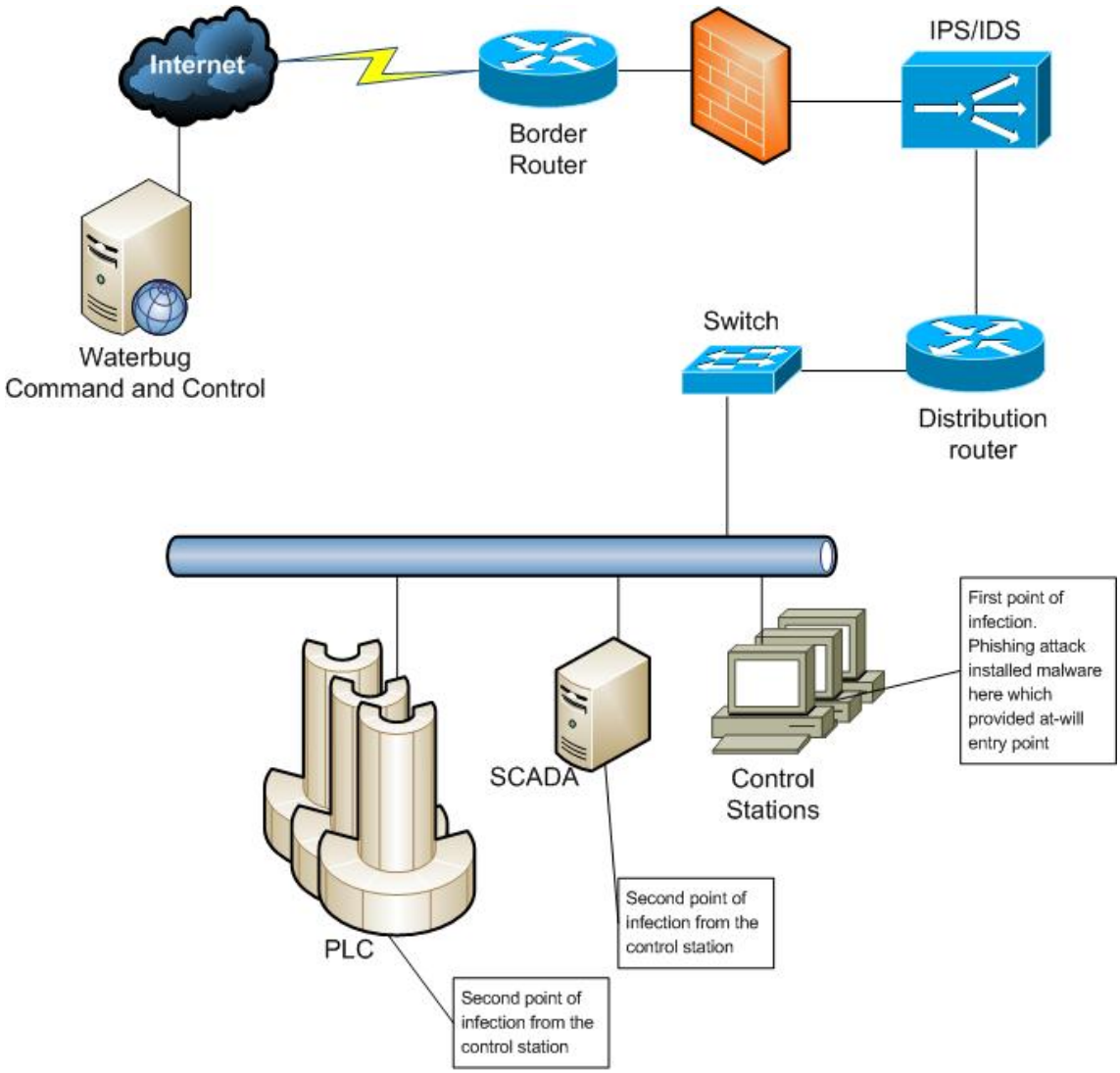
One of those phishing emails got a control station operator to click on a link that installed malware on the control workstation. This malware was a remote access trojan (RAT)

Exploitation and Installation

Because the control operators station was running an original and unpatched version of Windows XP (no service pack) and had an outdated malware scanner, when the operator clicked on the link to the malware, the malware installer was able to evade detection and install itself on the control station without anyone noticing. From there the malware would self-replicate onto other stations and report success back to the Command and Control servers back at Waterbug network.

Command and Control

The RAT installed by Waterbug communicates back to their Command and control server over port TCP 443 simulating HTTPS communication. The communication appears to be fully compliant with the HTTP 1.1 protocol and REST API where each command is a get, put, post, etc. The payload inside those commands appears to be proprietary command language utilizing a simple cipher to mask their true purpose. Furthermore, the RAT will rotate the IP address of the Command and Control server it is utilizing, presumably to avoid detection. Through this communication channel, the Waterbug group has an "at will" entry point for sending and receiving information, conducting surveillance, delivering a malicious payload, and compromising additional systems. Since all the TCP connections are initiated from a control station, aka engineering work station, and they are always going to a TCP port 443 utilizing what appears to valid HTTPS neither the firewall or the IPS detected anything as it is quite common for a control station operator to access websites on the internet.



Simplified overview of the APG Network to demonstrate components in the attack

Actions

Through the Waterbug's command and control server, utilizing their covert communication protocol, the ATP can exfiltrate all the data they wish. This includes both system information as in how things are set up, connected, etc., as well as operational status data, what systems are operational, what the load was on each system, what the backup systems are, etc.

With this information, they could shut down any automated failover systems, disconnecting failsafe systems, then start shutting down active systems causing power outages. If their goal was to be destructive, they could use their newfound understanding of the systems to transition load from underutilized systems over to the highly loaded system. This would cause overload situations, possible burning out critical components, and causing long term outages.

Defense in Depth Recommendations

People

People are usually the weak link when it comes to information security, and that is no exception here. Our investigation revealed a lack of training regarding appropriate information security. This team recommends that APG establishes new policies and educates their operators as well as all staff in proper operational security; this will raise information assurance levels significantly. Here are specific items that should be included based on common information security industry best practices.

- Links to all critical systems will be pushed into bookmarks and desktop short cuts by APG IT department
- Monitor traffic to the internet with a proxy and only allow traffic to pre-approved sites.
- Internal communications will only refer to those bookmarks and will never include an actual clickable link.
- All files will be shared using file-sharing services, such as SFTP servers, Microsoft OneDrive, Google Drive, etc., and never sent via email.
- Train all employees, never click on any links in any emails and never open any attachments in emails, ever under any circumstances
- Only visit trusted web sites stored in your computer's bookmarks by the IT department
- Any email from unknown sources should be immediately reported to Information security for investigation
- Any email that appears to be from a known source but doesn't feel right should result in a call or instant message to the source to verify.
- Prohibit the use of company email when posting something publicly, in forums, etc. None of the public information on the web site or other sources contains email addresses.
- All official company publication should be done from a special email account monitored by information security.
- Prohibit release of any information over the phone
- APG IT department is the only one that installs any software

By establishing these processes, training all employees in them at least once or twice a year, and enforcing them, you can cut off the social engineering attack vector which was utilized in this case. By only allowing access to known and trusted links, never clicking on links in email or opening attachments in emails, your information assurance will be raised significantly over where they are today. Reducing your attack surface, whether its people, facilities, or systems always raises information assurance levels. When folks aren't falling for phishing attacks or other social engineering attacks, information assurance levels are raised. Perform phishing simulations can also assist with this.

As far as facilities go, physical security is critically important as well. If a threat actor can gain physical access to the facilities, and therefore the APG systems by extension, unchecked, they can eventually bypass all security measures. Therefore to increase information assurance levels from a physical/facilities point of view, we recommend the following:

- All personnel authorized to access APG facilities shall be issued an ID badge with a recent picture on it.

- Institute a policy that badges much be worn in a highly visible manner, around the middle of upper torso picture & name facing out, while on site.
- Ensure all doors are equipped with a badge reader, replacing any lock where you must punch in a number to get access.
- All physical locks should be rekeyed, and the key's stored in a safe which only high-level on-site management has access to.
- For extra sensitive areas equip the badge reader with a pin pad for two-factor authentications. That is, to gain access, personnel would need to swipe their badge and enter in a PIN that is at least six digits long.
- Establish a roving security team that patrols all APG facilities, every nook and cranny should be patrolled. Patrols should be frequent, and predictable rounds should be avoided.
- Any personnel found not wearing a badge in a prominently visible manner, shall be stopped, questioned, and escorted to the security office for remediation unless they can rectify the issue on the spot. Security shall keep a log of those that are found in violation of the badge-wearing policy, which should be incorporated in human resources performance records.
- Security officers should carry portable wireless badge readers and randomly ask personnel they encounter to verify the badge is valid. This includes other security officers.
- All external entry points should have turnstiles with badge readers to stop tailgating problem.

Technology

It is import for APG to evaluate their supply chain and make sure they are only doing business with trusted suppliers. Establish a contract with these trusted suppliers requiring them to perform background checks per your specifications on all employees that work on systems being delivered to APG. Ensure only those with the need to know to have knowledge of what you are procuring from who and have them go through all the same checks as internal APG employees. By only doing business with trusted suppliers and keeping an eye on their employees you reduce the risk of threat actors leveraging the supplier for their attacks by planting malware, for example, backdoors, RAT, etc., on APG systems before it ever reaches APG facilities.

Once the equipment is received, it goes through exhaustive malware scan by information security before being put in use. This includes looking for infection at the BIOS or master boot record level for computers. For software, the installation media is put on a server and extensively scanned for malware, then installed on an isolated test system and scanned again. This will help identify any malware that might have gotten installed in the supply chain despite human monitoring efforts. With this double check, you raise your information assurance levels by detecting any malware that might have slipped through at the supplier side.

Operations

In terms of day to day operations, we make the following recommendation based on common information security industry best practices.:

- Ingrain in operators and engineers the importance of following the established policies.
- Ensure all systems are always patched to the latest available patches.
- Any systems for which no patching is available due to lack of available support you must replace those systems with systems for which support is available and for which regular patches are made available
- Ensure all systems have an up to date malware scanner on it with the most current definition files. As for the reasons, why this is important, consider these:
    - No system is immune to malware, doesn't matter the make, model or operating system
    - If a product vendor claims their system is immune to malware or that they have a system that is 100% guaranteed to prevent all malware 100% of the time, be assured you are talking with a snake oil salesperson.
    - All systems have vulnerabilities in them; most have not been discovered yet. Or they have been discovered by an adversary, and their existence keeps private. These are called 0-day vulnerabilities.

One of the specifics on how this will raise information assurance levels is that human factor continues to be the number one cybersecurity issue. Per a report by RSA Security LLC, a new phishing attack is launched every 30 seconds at the annual cost of $9.1 Billion to organizations globally. That report also states that 1 in 20 malware attacks are ransomware at the average cost of $300 per victim. (RSA Security LLC, 2017). So, by reducing your human factor element, you raise information assurance levels.

Another specific example of how this will raise information assurance levels is that most if not all, malware outbreaks happen due to unpatched systems without an up to date malware defense. For example, the recent Petya and WannaCry Ransomware outbreaks have been traced back to windows vulnerability for which patches had been available for months before the outbreak. (O'Brien, 2017)

Safeguards

Recommended Safeguards

It is common knowledge in the information security business that the most secure computer is a powered off a computer that is locked in a Faraday cage inside of a high-security bank vault with no connections and no way to get any information on or off said computer. It is also acknowledged that such a computer would be utterly useless, and useless computers have little need for security. So, all useful computers and system have some level of security concerns or outright issues. Therefore it is the general goal of information security specialists like InfoSecHelp to find the optimum balance between usability and security. We recommend that, in the case of APG and their critical infrastructure, balance means no remote access to APG networks. To access the APG system, you must be on-premise and using pre-approved APG owned and managed systems, preferably hard-wired workstations. All network systems should be authenticated with IEEE 802.1x authentication protocol before them gaining access to anything, to prevent unauthorized devices access to the network. By not allowing devices not owned and managed by APG to connect to APG networks, and by requiring all connections originate from on-premise, you reduce your scope, reduce your attack surface and protect APG critical infrastructure. Without those measures in place, you would have to figure out how to apply your supply chain management measures (malware scanning, etc.) to devices that you do not control.

Evolution of Safeguards

At this point, there does not appear to be enough business justification to outweigh the cost (both capex and opex) of setting up a secure remote access solution and solution that can securely allow “bring your own device” (BYOD) on the network. If that changes, this would need to be looked at again. If a VPN or other remote access solutions are deemed to be business critical in the future it is critical that a second-factor authentication is implemented for all level of authentications, both for the VPN system as well as other critical systems. Two factor means that the user proves possession of something in addition to knowing the username and password. Examples of this include a cryptographic smart card that a user needs to insert into a smart card reader in addition to providing username and password. Other examples are One-Time Password Algorithm (OTP) systems, where a user has a six-digit number that changes every 60 seconds and gets prompted for this number after providing username and password. SecureID from RSA and VIP from Symantec were the initial commercial application of this sort of a system which has now been updated and published by IETF as RFC 4226. Google Authenticator is a popular open source implementation of this protocol.

If it becomes business critical to allow systems not owned or managed by APG (aka BYOD) then an additional safeguard will have to implemented to ensure that those systems are free of malware and have the proper security posture to not pose a threat to the APG systems. BYOD should only be allowed to connect once this has been validated.

Recommended Functions or Systems

While APG has a firewall, IPS/IDS and a hodgepodge of SIEM systems, they are by large severely outdated. The firewall and IPS/IDS systems manufacturer has been out of business for years, so support is not possible. Because the current SIEM setup is a disjointed mismatch of unrelated systems, it is barely useful for forensic purposes and not much else. For APG Security Operation Center (SOC) to be able to timely detect, respond and block cybersecurity threats all these systems need to be replaced with current systems that can receive security update, signature, and heuristic database subscription, etc. These newer systems would allow timely detection of cybersecurity threats as well as do a better job of blocking issues to begin with. While InfoSecHelp does not endorse any particular vendor, products like those offered by Palo Alto Networks are getting high ratings from other customers with critical infrastructure. https://www.paloaltonetworks.com/products/secure-the-network/next-generation-firewall

APG needs to evaluate several vendors before deciding on the product that will work best for their use. One feature to look is the ability to automatically block traffic from networks known to be watering holes or operated by threat actors.

Another recommendation is to install a data leak prevention (DLP) system. This is a monitoring system that integrates into other infrastructure systems to monitor for data leaving the network that should never be allowed outside. Example of data you may want to monitor is confidential documents, operations details, and customer information to name a few. This would allow for timely detections of cybersecurity threat by notifying the SOC that this is going on so they can take appropriate actions.

Evolution of Functions or Systems

It is important to stay informed as to the developments in the cybersecurity space as it is hard to predict what the future is going to look like. As your systems grow to make sure you scale the existing system appropriately. Keep all systems at the most current operating system revision and patch vulnerability as soon as a patch is released. If a system is discontinued plan to replace them with the next-gen systems.

References

Bruno, G. (2008, February 27). *Backgrounder: The Evolution of Cyber Warfare*. Retrieved from The New York Times: http://www.nytimes.com/cfr/world/slot1_20080227.html?_r=0&pagewanted=print

Chapple, M., & Seidl, D. (2015). Cyberwarfare: Information Operations in a Connected World. Jones & Bartlett Learning, LLC.

Esbensen, D. (1998). *Patent No. 5,796,942.*

InforSec Institute. (2016, June 23). *Information Gathering*. Retrieved from InfoSec Institute: http://resources.infosecinstitute.com/information-gathering/

Martin, S. (2016, April 16). *8 Active APT Groups To Watch*. Retrieved from Dark Reading: https://www.darkreading.com/endpoint/8-active-apt-groups-to-watch/d/d-id/1325161?image_number=9

O'Brien, D. (2017, 6 28). *How software updates help keep you safe*. (Symantec Security Response) Retrieved 7 9, 2017, from Medium. Com Threat Intel: https://medium.com/threat-intel/software-updates-petya-wannacry-b99c932fdfef

Offensive Security Ltd. (2016). Penetration Testing With Kali LInux V1.1.5. *Offensive Security Professional Information Security Training and Sevices*, 375.

RSA Security LLC. (2017). *Global Fraud and Cybercrime Forecast.* RSA Security LLC. Retrieved from https://www.rsa.com/content/dam/pdfs/5-2017/3956-infographic-fri-2017-global-fraud-forecast.pdf

SANS Institute. (2003). *MS SQL Slammer/Sapphire Worm*. Retrieved from https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=21&ved=0ahUKEwj2m-uc3uTUAhXs54MKHYqvBS4QFgiUATAU&url=https%3A%2F%2Fwww.giac.org%2Fpaper%2Fgsec%2F3091%2Fms-sql-slammer-sapphire-worm%2F105136&usg=AFQjCNH8Z1GEldBRY7k0ya_fsieizjrvyw&cad=rjt

Schwartau, W. (1994). Information Warfare: Chaos on the Electronic Superhighway. Thunder's Mouth Press.

Singer, P. W. (2015). STUXNET AND ITS HIDDEN LESSONS ON THE ETHICS OF CYBERWEAPONS. *Case Western Reserve Journal of International Law, 47*(3), 79-86. Retrieved from https://wgu.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=eft&AN=108307851&site=eds-live&scope=site

Sneakers (1992). (n.d.). Retrieved from IMDB: https://www.imdb.com/title/tt0105435

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015). Guide to Industrial Control Systems (ICS) Security. *NIST Special Publication 800-82 Revision 2*, 247. Retrieved from http://dx.doi.org/10.6028/NIST.SP.800-82r2

Symantec Corporation. (2011). *Advanced Persistent Threats*. Retrieved from Symantec: https://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf

Symantec Corporation. (2016). *The Waterbug attack group.* Mountain View CA: Symantec Corporation .

Symantec Security Response. (2017, March 23). *Destructive malware: an ever-evolving threat*. Retrieved from Medium.com: https://medium.com/threat-intel/destructive-malware-evolution-392d3f8ef9d2

War Games (1983) - IMDB. (n.d.). Retrieved from IMDB: https://www.imdb.com/title/tt0086567/

Zakon, R. (1997, November). *RFC2235*. Retrieved from IETF: https://tools.ietf.org/html/rfc2235