WHITEPAPER

Growing CyberSecurity Threats to the Energy & Industrial Sectors

The damage hackers and malware present to our energy and industrial sectors

www.nopsec.com | info@nopsec.com

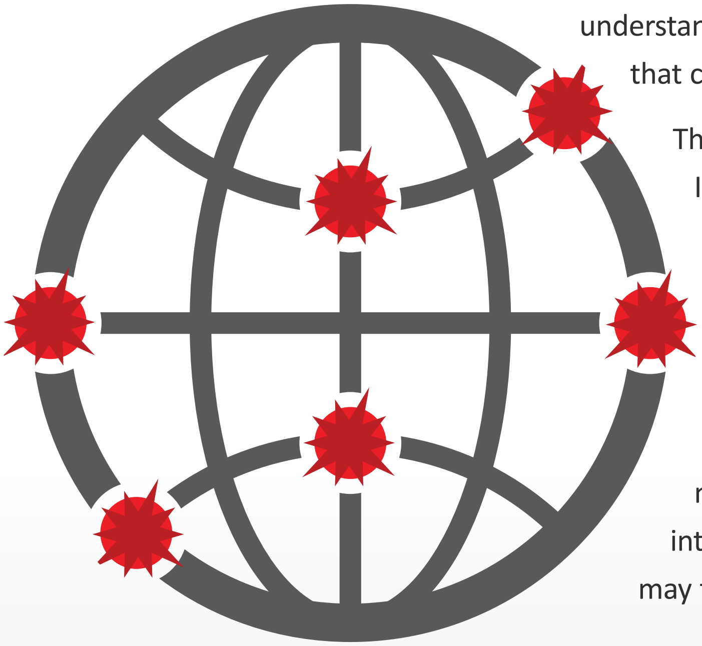
NOPSEC

Even superficially, we are aware of the digital threats we face on a daily basis. We read about them in our newspapers and online. We hear about them on Twitter and at conferences. Whenever a new dangerous ransomware emerges, or a major business or government agency gets hacked, it is inevitably front page news.

Except, of course, when it comes to our industrial and energy sectors. Most of us are blissfully unaware of the threats they face on a daily basis. This is possibly because they aren’t the most immediately exciting verticals, and won’t be front page news unless the grid is taken down by one of these attack vectors and impacts lives.

But this obscures the fact that they are attacked on a daily basis by actors as diverse as hacktivists and nation states, using digital weaponry ranging from open source, to tools that cost millions of dollars to produce or procure.

This white paper will examine the threats faced by the industrial and energy sectors on a daily basis. It will look at the attack vectors used, and the actors that perpetrate them. By the conclusion, the reader will gain an understanding of the management and technological tools that can defeat them.



Those working in the roles of CISO (Chief Information Security Officer), CIO (Chief Information Officer), CRO (Chief Risk Officer), and CTO (Chief Technology Officer) may find this paper most useful, especially if working in the industrial or energy sectors.

It may also be useful to those working in a management or procurement role. Similarly, those interested in security issues in these two verticals may find this paper of interest.

INTRODUCTION

In order to understand how we can remedy the threats posed to organizations based in the energy and industry sectors, it helps to have a historical perspective.There have been a number of high profile hacking and malware attacks aimed at companies in these two verticals. Many differ in execution.

It’s logical to start with the most high-profile attack on energy infrastructure ever recorded. This is, of course, Stuxnet.

Stuxnet

This was a malicious computer worm identified in 2010. Although not confirmed by either party, most researchers believe that this was a joint effort between the American and Israeli intelligence services.

Stuxnet targeted the programmable logic controllers (PLCs) that are ubiquitous in the SCADA systems used in industrial and energy contexts. It exploited four zero-day flaws found in the Siemens SCADA system used in order to force Iran’s nuclear centrifuges to spin wildly out of control, whilst innocently appearing to be an industrial accident.

It’s believed that Stuxnet was responsible for the destruction of 1000, or 10 percent, of Iran’s nuclear centrifuges between November 2009 and January 2010.

Shamoon

It’s not just rogue nations that have been targeted. In 2012, an attack against Saudi Aramco, one of the world’s largest oil companies, wiped or disabled 35,000 computers and propelled the company into a technological dark age, forcing it to rely on typewriters and faxes while it recovered. Had it failed to do so, 10% of the world’s oil supply would have been in jeopardy.

Had the Shamoon attack succeeded, 10% of the world’s oil supply would have been in jeopardy.

The attack occurred during the Islamic holy month of Ramadan, when most Saudi Aramco employees were on vacation, spending time with family, and sheltering from the blistering heat of the Arabian summer.

The skeleton crew that remained noticed that some computers were acting strangely. According to CNN, screens started flickering and files began to disappear. It wasn’t long until total devastation had been wrecked against the company.

A group that called itself the “Cutting Sword of Justice” claimed responsibility. It opposed the Saudi royal family, which Saudi Aramco is intrinsically linked to.

According to the US CERT, The Cutting Sword of Justice used a virus called W32.DistTrack, which is also known as “Shamoon”. The way it worked was not terribly sophisticated. It’s simply wiped over essential parts of the hard drive with zeroes – the files, the Master Boot Record (MB), and the partition record.

But despite its simplicity, it brought one of the biggest companies in the world to its knees.

DragonFly

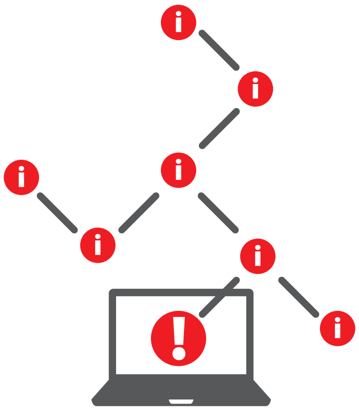
Dragonfly wasn't a specimen of malware, but rather a hacking group that infected literally hundreds of business computers using their own bespoke malware.

While this isn't a lot, especially when compared to ransomware specimens like Cryptolocker, it had a profound and damaging impact on the energy, defence, and aviation sectors.

It is believed that the operators of the Dragonfly malware intended to collect information on industrial control systems used across the United States and Europe. These are computer systems that are used to monitor, control, and automate processes used in industrial and manufacturing contexts.

SANS notes that Dragonfly wasn't part of a hacktivist or organized crime initiative, as we have come to expect. Rather, it was a "cyber-espionage campaign" that was perpetrated by actors with "ample funding and technical know-how". The campaign began in late 2010, and was only discovered by security researchers in 2013.

Dragonfly was spread through spear-phishing attacks that targeted companies that were overwhelmingly based in the United States, Spain, France, Italy, Germany, Turkey, and Poland. Among its victims were energy grid operators, electricity generation firms, petroleum pipeline operators, and energy industry industrial equipment providers.



Dragonfly malware intended to collect information on industrial control systems used to monitor, control, and automate processes used in industrial and manufacturing contexts.

BlackEnergy 3

In December, 2015 a power outage plunged the Ukraine into darkness for hours. The cause was not faulty equipment or human error, but rather a sophisticated cyber attack based on the BlackEnergy malware package, which was first identified in 2007.

The initial strain was a run-of-the-mill Trojan with distributed denial of service capabilities. In the years that have followed it has been upgraded to have better deployment tools, and more obfuscation and defensive features.

The attack happened at a time when the Ukraine was embroiled in a conflict along it's eastern border. It is currently fighting to regain territory that has been lost to separatist movements in Donbass and Luhansk. As a result, many researchers suspect that BlackEnergy 3 was politically driven. However, as McAfee points out, this conclusion is all but certain.

The Israeli Electricity Authority Attack

A more recent example of electricity infrastructure being disrupted by malware comes from January, 2016. Israel's electricity authority was hit by ransomware attack which paralyzed some computers for more than two days. This led many to suspect that Israel's electrical grid had been compromised.

Yuval Steinitz, Israel's minister of Infrastructure, Energy, and Water told the Times of Israel:

"Yesterday we identified one of the largest cyberattacks that we have experienced. The virus was already identified and the right software was already prepared to neutralise it. We had to paralyse many of the computers of the Israeli electricity authorities. We are handling the situation and I hope that soon, this very serious event will be over... but as of now, computer systems are still not working as they should."

Fortunately, Israel's power network didn't go down. However if it did, it would have been disastrous as the attack happened during two consecutive days of record-breaking winter electricity consumption.

THE IMPACT OF CYBER ATTACKS ON ENERGY AND INDUSTRIAL INFRASTRUCTURE

It's hard to understand the damage that can happen as a result of a successful cyber attack on energy and industrial infrastructure. At the most benign end, companies only have to deal with a loss of productivity as staff are diverted to resolve the problem.

But not all energy and industrial companies are as lucky. A cyber attack can disrupt business functions, which has an impact on end-users. It can lead to a loss of intellectual property, which has the potential to have long lasting effects on the business as it becomes less competitive.

There are financial losses. Not just from replacing broken equipment, but from compensating customers, lost earnings, and regulatory penalties.

Finally, there is the potential of physical harm to people – even death. Whilst this may seem alarmist to some, an uncontrolled explosion in a nuclear station, contamination in a water plant, or extended loss of heat or electricity could have serious repercussions.

A cyber attack can disrupt business functions and lead to a loss of intellectual property, which has the potential to have long lasting effects on the business.

EMERGING THREATS

In recent years, these threats facing industrial and energy sector companies have diversified.

Companies no longer have to simply worry about insider threats, where a disgruntled employee uses their position to damage the firm. The list of potential actors is no longer limited to just hacktivists and organised criminals. The attack vectors have broadened past spear phishing and vulnerable software.

Nation State Campaigns

Some of the biggest cyber criminals aren't the stereotypical adolescents working from their mother's basement, or gangsters working from a boiler room. They can be well funded, well trained, and well equipped employees of nation states.

The recent Yahoo attack is believed to be from a nation state actor. Likewise it's believed that Guccifer 2.0 is actually Russian intelligence.

There are countless examples of nation state actors targeting the energy and industrial sectors. We previously mentioned the Stuxnet malware, which is believed to be from the American and Israeli intelligence services. Many also suspect that the BlackEnergy 3 attack that targeted the Ukrainian power grid was the product of the Russian government.

There are many reasons why a country would target another's industrial and energy sector. Perhaps the biggest is that it causes immense disruption and panic. In the case of Stuxnet, it set back Iranian nuclear efforts without a shot being fired.

It can also be for technological acquisition. It's widely believed that Chinese intelligence was able to breach the computer systems used to design the F22 and F-35 fighter jets. This was then used to develop their own indigenous designs.

Ransomware

Ransomware is another contemporary threat that the industrial and energy sectors are facing right now. Ransomware can best be described as a type of virus that impairs the use of a computer, or damages the files stored on it, unless a ransom is paid.

Modern variants of ransomware, called crypto ransomware, entombs the files stored on a hard drive using strong encryption. If the victim wishes them back, they will have to pay a ransom. The cost is often in the hundreds of Dollars per infected machine.

When Israel's electricity board was infected with ransomware, it almost brought the entire country to a halt.

Ransomware can be spread through campaigns that target specific individuals or companies. More often though, it is spread indiscriminately via spam networks.

The SAaaS model is ideal for hacktivists and terrorists because it allows them to inflict staggering amounts of damage and destruction to infrastructure with a degree of anonymity.

SCADA Access As A Service (SAaaS)

Cybercrime is a business. Like any business, the proprietors are always looking for new opportunities. One is called SCADA Access as a Service, or SAaaS. This is a perverse kind of business model, where an actor sells access to a SCADA system to another unauthorised third party.

According to Booz Allen Hamilton, this is a growing sector. It defines SAaaS services as entities that identify zero-day flaws in industrial controls networks and build exploits for them. These are then sold onto third-parties.

It notes that many of the vendors in this field aren't actually cybercriminals, but rather legitimate businesses selling a product to governments and police forces. It gives the example of Hacking Team, based in Italy, and Vupen Security, based in France.

But it also points out actors in this field who do not have the best of intentions. According to the information security giants, there is one known criminal that uses the handle of Bonito, and has been identified as selling access to SCADA systems.

The SAaaS model is ideal for hacktivists and terrorists. It allows them to inflict staggering amounts of damage and destruction to infrastructure. It also allows them to do this at a safe distance, and with a degree of anonymity.

Supply Chain Compromise

Very few companies, if any, are entirely self-contained. Most have to depend on third party suppliers and manufacturers to function.

As a result, many malicious actors target smaller companies downstream in order to target a larger organisation that may prove to be difficult to penetrate. It is for this reason why it is crucial to protect the supply chain.

One of the most stark examples of this does not come from the industrial or energy sectors, but rather from the American Dental Association (ADA). In April 2016, it sent out USB flash drives to its 37,000 members. These had been manufactured by a subcontractor in China, and were infected with code that would have allowed an attacker to remotely control the machine.

Compromised USB drives are a common attack vector, and one that requires vigilance in order to avoid a supply chain attack, or an attack that exploits social engineering tactics.

In 2008 the United States Department of Defence was compromised by an unknown foreign Intelligence Agency when an employee inserted a compromised USB flash drive into a government laptop computer.

A later example of supply-chain compromise comes from November 2014. When an unknown actor had compromised devices used for scanning items at shipping distribution centres. These devices were also sold to a manufacturing firm.

And between 2013 and 2014, a Russia-backed group alternatively known as Dragonfly and Energetic Bear launched targeted attacks against energy sector companies by targeting suppliers and service providers used by these companies.

A Russia-backed group launched targeted attacks against energy sector companies by targeting suppliers and service providers used by these companies.

Perhaps most troubling, attackers occasionally target the device firmware of industrial control systems. The best examples of these are the two aforementioned Dragonfly malware specimens, namely Backdoor.Oldrea and Trojan.Karagany.

These were distributed via spearphishing attacks and watering hole attacks. Perhaps crucially, they targeted the underlying Windows operating system that's typically used in ICS contexts.

CONCLUSION

Attacks that target ICS systems are a niche, albeit one that is constantly growing. Threats are being discovered all the time, and the actors behind them are often dangerous, well funded, and skilled.

But it is by no means hopeless. There are ways to mitigate against them.

For those in the Industrial or energy sectors, it's crucial that you have an ongoing security strategy. You should constantly be taking advantage of threat intelligence in order to determine who the actors targeting your sector are, what tactics and approaches they employ, and whether it's likely that your company would be targeted by them.

You should also have a remediation strategy that will allow you to resolve any compromise with a minimum of disruption for your customers and for your business. But this should not be a top down approach. It should not merely involve management and C-suite level staff. Every employee has a role to play in protecting the business. Every employee should have the security training that would allow them to do their part.

A unified vulnerability management solution, such as NopSec's Unified Vulnerability Risk Management SaaS platform, will allow these sectors to take advantage of enriched prioritization data through threat intelligence feeds, database exploits, patches, social media, and organizational context. Attack vectors and trends unique to the organization are tracked, and helps IT Teams to harden their security posture and remediate the risks accordingly, all within one platform.

It is vital that employees are aware of social engineering attacks. It should be emphasized that these manifest themselves in various different ways, from dropped USB sticks, to phone calls, and emails. Constant vigilance is required.

Similarly, good management is required in order to ensure that employees do not fall victim to watering hole attacks.

In addition to an ongoing security strategy, it's vital that businesses in the energy and industrial sectors have an active vulnerability risk management program.

It's vital that businesses in the energy and industrial sectors have an active vulnerability risk management program.

This would examine how both an internal and external threat could damage the business, and include both penetration testing and social engineering testing in order to identify weak spots before an attacker does. Given the sensitivity of the energy and industrial sectors, this should be an ongoing process which is complimented by a strategy for vulnerability remediation.

ABOUT NOPSEC

NopSec operates with one mission: to help people make better decisions to reduce security risks. Our team is passionate about building technology to help customers simplify their work, manage security vulnerability risks effectively, and empower them to make more informed decisions. Our software-as-a-service approach to vulnerability risk management offers an intelligent solution to dramatically reduce the turnaround time between identification of critical vulnerabilities and remediation.

For additional information or to schedule a demo, visit www.nopsec.com or email info@nopsec.com.