Blueliv. NEUROsoft

The Electric Avenue

An Overview of the Energy Sector's Threat Landscape

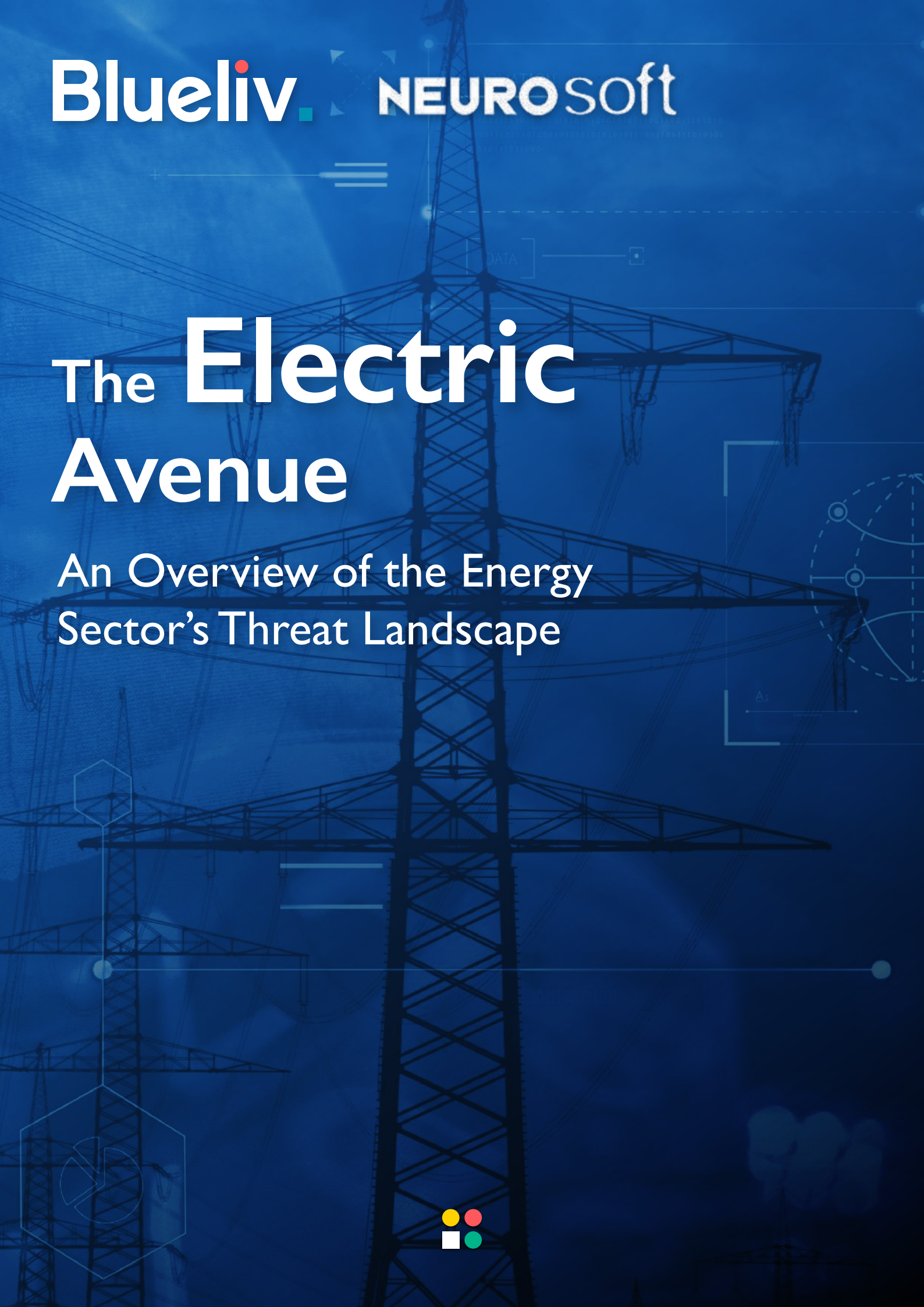


Table of Contents

Introduction

Like many sectors in recent years, the energy sector is currently going through an immense period of digital transformation, thanks to the widespread use of increasingly sophisticated technology such as artificial intelligence (AI), the Internet of Things (IoT), blockchain, and the use of big data. Leveraging these technologies, the energy sector is able to link its practices and communications in a way that has never before been possible, leading to new and innovative ways to streamline operations.

As the energy sector's digital footprint widens, however, so too does its vulnerabilities. By heavily, and suddenly, leaning on these new technologies to improve business operations, the industry has exposed itself to threat actors looking to cause ruin or achieve financial gain by compromising these systems.

One such example of this is the Stuxnet Worm, a virus that first emerged and began infiltrating computer systems in 2010. The Stuxnet Worm targeted Windows networks and systems infiltrating the host machines, before continually replicating itself. One system to fall victim to this was the Windows-based Siemens Step7 software favored by, and prevalent in, the energy sector, such as nuclear facilities. By compromising the system, the worm stole access to the industrial program logic controllers. The Stuxnet Worm compromised over 15 Iranian energy facilities, including the Natanz nuclear facility. After several months, and a series of broken uranium enriching centrifuges, Natanz sought help from an outside security firm, which ultimately discovered a series of malicious files on the facility's system. Ten years later, Natanz is yet to disclose the full extent of the attack, though it is widely believed that the Stuxnet Worm destroyed roughly 1,000 uranium enriching centrifuges, equating to an estimated 30% decrease in the facility's efficiency and holding the country's nuclear program back by a number of years.

The energy sector is a vital component of our global infrastructure and, in order to defend itself and the countries, organizations, and civilians it serves, this newly digitized industry must look to new security practices and threat defenses that are on par with the newly deployed kit. In addition, the industry must further its holistic understanding of cyber and physical security measures as whole, rather than two siloed sides of the same coin, if it is to clearly analyze and understand the motivations of its attackers. This includes a fresh appreciation for the political and geopolitical factors that affect and motivate these actors.

Why is the energy sector targeted?

Since the emergence of the Stuxnet Worm, the energy sector has only become more targeted.

Intellectual property (IP) is one of the leading reasons actors target organizations, and the energy sector is rich in this commodity due to the competitiveness of the industry and the need to stay agile, innovative, and disruptive. The energy sector is also an attractive target for actors with a political or socioeconomic agenda: stealing IP could put one nation vastly ahead of the competition when it comes to energy or technological advantages.

Another factor which makes this sector appealing to actors is its role - and impact should it collapse - in many nation's security and economy. By compromising energy facilities, cybercriminals with an understanding of the facility's economic value can rest assured they will likely get paid for whatever ransom they demand as the victim group will be desperate to restore order for its facility and dependents.

Finally, as the energy sector has grown, so too has its attack surface, largely due to its geographic complexity, organizational needs, and physical size. Electric and gas suppliers in particular strike a unique balance between physical and cyber infrastructures, meaning they are more vulnerable to exploitation from attackers looking to capitalize on specific exploitations, such as commandeering operational technologies to cause physical damage.

Going full circle, Natanz reported a fire and large explosion at its facility in July of 2020, likely the result of a devastating cyber-attack, proving that the energy sector is highly sought after – and that actors are more focused on exploiting the industry than ever, whatever the cost, or collateral damage.

Threats to the Energy Sector

The energy sector is not exempt from the threats that plague most industries, be it data theft or ransomware, but, given the very nature of the power this sector deals with, the fallout of successful cyber-attacks has the potential to be extremely destructive. Potential threat impacts include disruption of services and outputs from power and clean energy plants, disruption of power via remote transmission services, outages for substations that would lead to regional disruption, and of course the theft or fraud of customer information. Such outages would slow down or completely stop the supply of energy, resulting in immeasurable impacts on not only the economy but the functionality of society.

Advanced Persistent Threat Actors (APTs)

Often working with a nation-state, APTs target foreign energy organizations with a view to stealing IP, gaining leverage, or seizing control of operations. One such example comes from DragonFly (assessed in further detail later in this whitepaper), a Russian APT group known to target US and European energy providers. In 2017, DragonFly stole access to US power grid controls, granting them the power to initiate instant blackouts should they feel like doing so.

In this and other cases, DragonFly broke into platforms used by energy engineers to issue commands to equipment that supplied energy to homes and organizations alike. The group is known to achieve access through phishing attacks in which it steals credentials from compromised devices.

Cybercriminals

Motivated solely by financial gain, cybercriminals target the energy sector for its revenue - either by holding data at ransom or issuing Distributed Denial of Service (DDoS) attacks - and have no qualms about attacking energy companies in a time of need. North Carolina energy provider ONWASA can testify to this, having fallen victim to the Emotet malware in 2018 whilst dealing with Hurricane Florence, and then being targeted by Ryuk just ten days later.

The Emotet virus quickly made its way through ONWASA's systems, though the company refused to pay any ransom and instead worked with the FBI to manage the situation. In the end, ONWASA's utility service remained untouched by the attack, though, had this not been the case, millions of residents within the region would have lost access to clean water, sanitation operations, and a stop to waste treatment. Today, ONWASA is still recovering from the ill-timed attack on its operations.

Hacktivists

Though a large-scale attack at the hand of activists is yet to be recorded against the energy sector, it is widely believed to be a matter of time before this takes place: many energy companies are known for immoral and anti-eco business practices which are likely to make them a target for green-minded hacker groups.

Nation-state actors

Unlike hacktivists or other cybercriminals, nation-state actors are known for creating and utilizing custom attack vectors, typically through the incorporation of previously unknown software vulnerabilities, a.k.a. zero-day attacks. Usually, when an attack takes place that cannot easily be identified or associated with a single group, it is believed to have been the work of nation-state groups.

Nation-state attacks are subtle, secretive, and rarely create enough noise to warrant suspicion or detection, allowing the attackers to easily find and hold a foothold in the target network for an increased duration. In turn, this allows them to access and see communications or sensitive data over a matter of weeks, months, or longer. While they're at it, they typically plant hidden malware in the network, which can remain dormant for years to come.

Attacks from these groups are more considered when compared to other actors on this list: each attack has a single goal in mind and is executed methodically to ensure success. Nation-state groups favor the aerospace, public sector, financial, and energy industries, due to the sensitive nature of each sector's data, intellectual property, or geopolitical position.

Ransomware

2020 is positioning itself as the year Ransomware grew up and, just like every other industry, the energy sector is not exempt from these mature, devastating attacks. In fact, according to a VMware report from earlier this year, hackers looking to deploy ransomware to extort businesses will most likely target energy and manufacturing sectors, as well as local governments. This, and newer methods like wiper attacks, are favored by individual criminals and state-sponsored groups alike due to its "purely destructive" nature.

Energy provider Energias de Portugal (EDP) fell victim to such methods earlier this year when it was attacked with the Ragnar Locker ransomware. EDP has operations in 19 countries globally, as well as a workforce of 12,000 and, at peak energy production, an 11 million strong customer base.

The fallout of this breach saw the attackers access and steal over 10TB of sensitive data, comprised of employee login information, names, accounts, URLs, notes, and the KeePass password manager database. To confirm their success, the hackers included samples and screenshots of the stolen files in their ransom note, which they threatened to publish – and share with EDP competitors - if the ransom of $11 million was not paid swiftly. EDP spoke to Bleeping Computer about the attack in April of this year, though was unwilling to discuss if it had paid the high ransom.

State of the industry

As the average cost of a breach has grown (estimated at $3.92 million at the time of writing), so too has the target on the energy sector's back. In an analysis of 1,000 domains, Hornetsecurity Security Lab found the energy sector to be one of the most sought-after targets for cybercriminals.

Energy suppliers have widely adopted digitization – allowing for remote-controlled machines via the internet, interconnected networks, rapid information sharing, among other benefits – but this shift has only left the industry more vulnerable, and even the narrowest of security gaps can lead to fatal fallout and costly and damaging ramifications for a nation's critical infrastructure.

Considering the importance of keeping these facilities secure from outside forces, it's vital that energy C-suite teams develop a firm understanding of the threat landscape that faces them, and invest in robust strategies, tools, and partners to bridge any gaps in skills or knowledge.

Recent attacks

India's nuclear power

Earlier this year officials in India confirmed that part of its core critical infrastructure – its latest nuclear power plant - had fallen victim to a cyber-attack from a nation-state group. The Kudankulam nuclear plant hack was announced by the Nuclear Power Corporation of India Limited (NPCIL), and was reported to be the result of malware designed for data extraction deployed by the North Korean actor Lazarus Group, according to the Financial Times, and was only discovered when Google's virus scanner site VirusTotal noticed a suspicious data dump related to the malware. Fortunately, the plant systems were not affected, and thorough investigations revealed that an infected PC belonging to a user on the plant's connected network introduced the malware to the system. Though the critical internal network was not affected on this occasion, this is a frightening example of just how swiftly a core component of a nation's energy infrastructure can be compromised. Following an investigation by DAE specialists, security experts warned that the power plant's cybersecurity is far from robust, and much work needs to be done to stop an infection like this from happening again.

Russia's electric grid

In an example of nation-states interfering with other nations, this year saw the US ramp up its digital presence in Russia's electric power grid. This follows warnings from the Department of Homeland Security and the FBI that Russia had inserted malware into America's power, oil, and gas infrastructure that could one day be used to sabotage the nation's energy access. In retaliation, the Trump administration deployed a range of undisclosed tools to gain access to Russian infrastructure. Though either nation has yet to make significant use of its foothold, the result of both nations tampering with the other's critical infrastructure could lead to a new digital cold war, and result in serious power outages for both regions. Reporting on the development, the New York Times cited that the US had "shifted more toward offense, with the placement of potentially crippling malware inside the Russian system at a depth and with an aggressiveness that had never been tried before" suggesting that this is only the beginning of a potentially destructive exercise in infiltrating and utilizing critical infrastructure. In the months since this was reported, former President Donald Trump declared foreign cybersecurity threats to the US as a national emergency.

The UK's electricity market

Elexon, the organization responsible for facilitating payments on the UK electricity market, fell victim to a cyber attack in May of this year. Elexon works alongside Great Britain's National Grid Electricity System Operator (ESO) to ensure constant power to the nation's residents. This attack did not cause outages for British civilians, though internal IT systems and devices were compromised. Elexon is highly targeted by criminals and nation-states due to its role in managing finances for the energy sector, a market estimated to turn over $2.07 billion annually according to The Telegraph. The nature of the attack is believed to be ransomware, with Elexon admitting to being unable to send or receive emails, and that its internal IT systems had been impacted by the attack, though this is yet to be confirmed. The cybersecurity specialist Jérôme Robert of Alsid noted that "if it is ransomware, Elexon could face a long and expensive road to recovery."

Threat Actors Targeting the Energy Sector

The threat landscape facing the energy sector has grown exponentially in recent years, leading to more actors - from nation-state groups to sophisticated individuals - and more tools at their disposal than ever before. This sudden rise in attack vectors led a US government source to alert critical infrastructure providers that these criminals are "capable, at a minimum, of carrying out attacks with temporary disruptive effects against critical infrastructure" earlier in 2020, in a bid to make the sector understand the gravity of the challenges ahead of them.

This section will identify key threat actors targeting the energy sector, as well as their motivations, area of operations, and preferred tactics, citing in-depth knowledge gathered from Threat Context, Blueliv's powerful threat intelligence enrichment tool.

TEMP.Veles

Figure 1 - Map of countries targeted by TEMP.Veles

Aliases

ATK 91, TEMP.Veles, XENOTIME, Trisis, and Central Scientific Research Institute of Chemistry and Mechanics.

Targeted countries

Saudi Arabia.

TEMP.Veles is known for its interest in sensitive environments where it seeks to deploy malware and gain remote access, though the end goal of these attacks is currently unknown. That being said, Blueliv analysts assess with a moderate degree of confidence that the aim is likely disruptive.

In August 2017, a Saudi Arabian petrochemical plant fell victim to a cyberattack seeking to manipulate industrial control systems (ICS) at the plant. The malware was subsequently dubbed TRITON by researchers. The attack is particularly noteworthy as malware attacking ICS or other industrial processes is relatively rare. In this instance, the attacker first gained remote access to a workstation at the plant before deploying the malware. The attack was eventually detected after the adversary accidentally shut down the industrial process.

The researchers who reported on this new threat actor – referring to this "activity set" as TEMP.Veles – published a report in October 2018 indicating that Russia may be behind the activity. The report focused specifically on the Russian government-owned Central Scientific Research Institute of Chemistry and Mechanics (known by its transliterated Russian initials CNIIHM) and the links between that institute, TEMP.Veles, and TRITON.

On October 23, 2020, the US Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned the Central Scientific Research Institute of Chemistry and Mechanics for the development and deployment of the Triton malware against the Middle East.

Energetic Bear

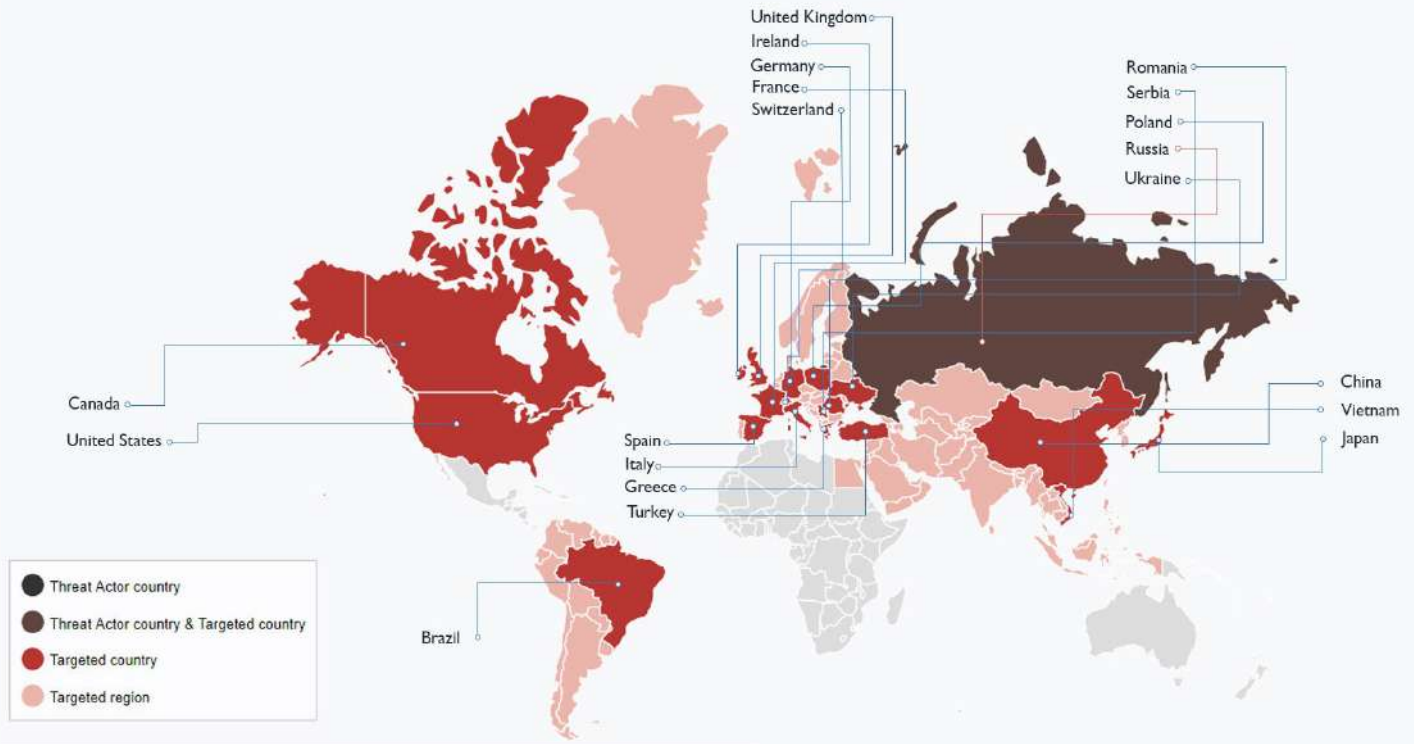


Figure 2 - Map of countries targeted by Energetic Bear

Aliases

DragonFly, Crouching Yeti, Group 24, Iron Liberty, Koala Team, Electrum, TEMP.Isotope, TeamSpy Crew, and IRON LYRIC.

Targeted countries

Brazil, Canada, China, France, Germany, Greece, Ireland, Italy, Japan, Poland, Romania, Russia, Serbia, Spain, Switzerland, Turkey, the United Kingdom, Ukraine, the United States, and Vietnam.

Energetic Bear is a cyberespionage group that heavily targets the energy sector. The group is linked to the Russian government, and often compromises targets through the use of phishing emails or watering hole attacks. Energetic Bear's interests appear to lie with understanding the operations of energy facilities as well as gaining access to the actual operational systems.

Energetic Bear has targeted a wide variety of organizations across sectors and around the world. Many of the group's targets are located in Europe and the US, though other countries have been targeted by the group as well. In 2016 and 2017, for example, the group's targeting of Turkish entities noticeably increased. According to Kaspersky reporting, Energetic Bear has also targeted Russian entities.

While energy and industrial entities are the frequent targets of Energetic Bear, the group has also focused their efforts on the education, pharmaceutical, manufacturing, construction, and IT sectors. The US-CERT observed that Energetic Bear's targeting appeared to be very selective, as opposed to purely opportunistic. The US-CERT specifically mentioned targeting of "U.S. Government entities as well as organizations in the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors."

Energetic Bear typically makes use of phishing emails and watering holes in their attacks. The US-CERT noted that Energetic Bear often identifies and compromises "staging targets," or third-parties with less secure networks that are likely to be trusted by the ultimate "intended target." Some of the malicious emails were generated using the Phishery toolkit, a publicly available tool used to steal credentials through a template injection attack. Many of the watering holes identified by the US-CERT were "trade publications and informational websites" with information about "process control, ICS, or critical infrastructure." The group also makes use of Trojanized software updates and overall has an extensive malicious toolkit.

The group's actions inside compromised networks suggested that they seek to collect information. According to Symantec, Energetic Bear's interests appear to lie with understanding the operations of energy facilities as well as gaining access to the actual operational systems. According to the US-CERT, once Energetic Bear gained access, they moved laterally to steal information from Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems. No sabotage efforts associated with these intrusions has been publicly reported. To avoid detection, the attackers cleared the following Windows event logs: System, Security, Terminal Services, Remote Services, and Audit.

The Netwalker Group

Figure 3 - Map of countries targeted by Netwalker Group

Aliases

Mailto Group, Kazkavkovkiz, Kokoklock, Netwalker Group, Bugatti, and CIRCUS SPIDER.

Targeted countries

Australia, Austria, Argentina, Canada, Chile, Colombia, France, Germany, Greece, India, Italy, Japan, Pakistan, Romania, Saudi Arabia, South Africa, Spain, Sweden, Thailand, the United Arab Emirates, the United Kingdom, and the United States.

The Netwalker Group is the threat group behind the Netwalker or Mailto ransomware and is driven purely by financial gain. Their first known activity is from August 2019, and it has since been established that the group's modus operandi is compromising RDP systems or using malspam campaigns to distribute ransomware, including the use of malicious attachments and fake impersonations of Glary Utilities and Sticky Password software.

The Australian Cybersecurity Centre observed a campaign in February 2020 where the threat group likely used phishing and password spray attacks to compromise email accounts. Then, the attackers would have sent further phishing emails to emails in the compromised accounts' address book.

Netwalker operates using a ransomware-as-a-service model. As a result, the group behind Netwalker seeks to recruit affiliates who can assist in distributing the malware, with revenues being shared. The threat actor operating under the alias "Bugatti" appears to be the representative of the Netwalker group on the cybercriminal underground.

Bugatti registered on the top-tier Russian-language forum Exploit on February 25, 2019. Their first post was on March 19, 2020, seeking to recruit Netwalker affiliates. Bugatti has made a deposit of 1 BTC to the forum; if there are disputes and Bugatti is found to be at fault, this money will be used to provide restitution. Deposits like this are typically indicators that the threat actor is more likely to be legitimate.

On May 13, 2020, Bugatti posted a Tor site created to leak data from victim companies that refused to pay the Netwalker ransom. Some analysts hypothesize that the threat actor "eriknetwalker" might be active in the Netwalker gang due to eriknetwalker's inclusion of the name "netwalker" in their alias as well as eriknetwalker's prior activity as a vendor of a ransomware builder. eriknetwalker was active on the Russian-language underground from July 2016 until 2019. Blueliv analysts did not conclusively establish a connection between eriknetwalker and the Netwalker gang.

Here below is a list of CVEs with their associated score related to Netwalker Group's attack tracked by Blueliv Threat Context solution.

SCORE	NAME	EXPLOITS	MALWARE	MENTIONS	PLATFORMS	MS BULLETINS	PUBLICATION DATE
9.9	CVE-2019-18935	1	81	135	59	×	11/12/2019
8.2	CVE-2020-0796	3	323	1782	12	×	12/03/2020
7.8	CVE-2019-11510	1	×	1124	153	×	08/05/2019
7.7	CVE-2019-1458	×	8	147	11	×	10/12/2019
7.7	CVE-2015-1701	11	553	69	44	1	21/04/2015
6.5	CVE-2017-0213	2	1690	67	24	1	12/05/2017

Figure 4 - List of CVEs with their associated score related to Netwalker Group

Sandworm Team

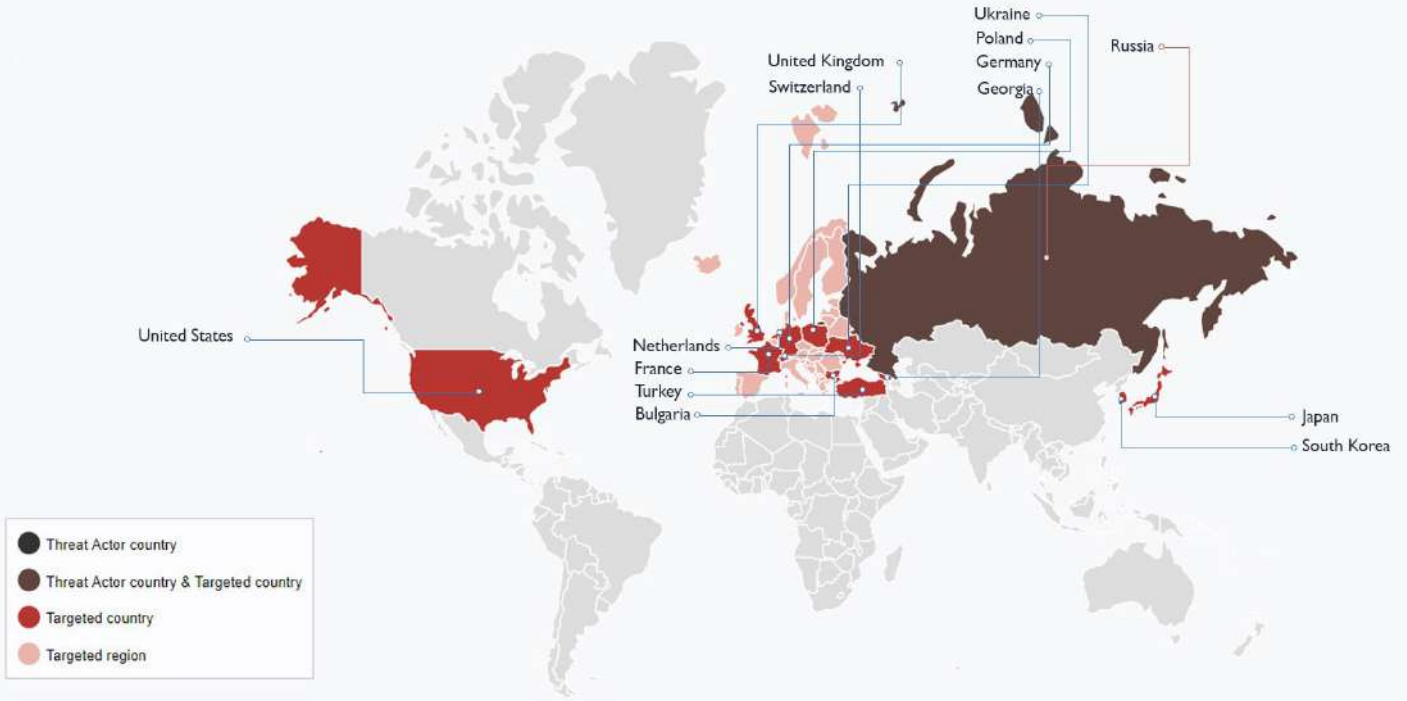


Figure 5 - Map of countries targeted by Sandworm Team

Aliases

Sandworm Team, Quedagh, TEMP.Noble, VOODOO BEAR, Iron Viking, BlackEnergy, TeleBots, GreyEnergy, Unit 74455, GRU Main Center for Special Technologies (GTsST), and Hades.

Targeted countries

Bulgaria, France, Georgia, Germany, Japan, the Netherlands, Poland, Russia, South Korea, Switzerland, Turkey, Ukraine, the United Kingdom, and the United States.

Sandworm Team is a cyber-espionage group that has operated since approximately 2009, attributed to the Unit 74455 of the Russian Main Intelligence Directorate (GRU). Sandworm Team targets mainly Ukrainian entities associated with energy, industrial control systems, SCADA, government, and media, looking to cause sabotage and destruction by distributing emails containing malicious attachments, or distribution of malicious code via Trojanized updates to widely used software.

Sandworm Team has been linked to the 2015 attack on Ukraine's electric power grid, Ministry of Finance, and State Treasury Service, utilizing the destructive malware BlackEnergy, Industroyer, and KillDisk.

In 2017, the Sandworm Team spread the NotPetya wiper malware, disrupting at least 300 Ukrainian companies and important international companies such as Merck, TNT Express, and Maersk. Ukrainian authorities estimated the 10% of all computers in the country were wiped as a result of NotPetya. Sandworm Team distributed NotPetya through a Trojanized version of the M.E. Doc software.

The Sandworm Team was also responsible for Olympic Destroyer malware, which disrupted thousands of computers used to support the 2018 PyeongChang Winter Olympics. The reason behind the attack is that the International Olympic Committee had banned Russian athletes representing Russia from participating after a state-sponsored doping program was uncovered.

SunCrypt Group

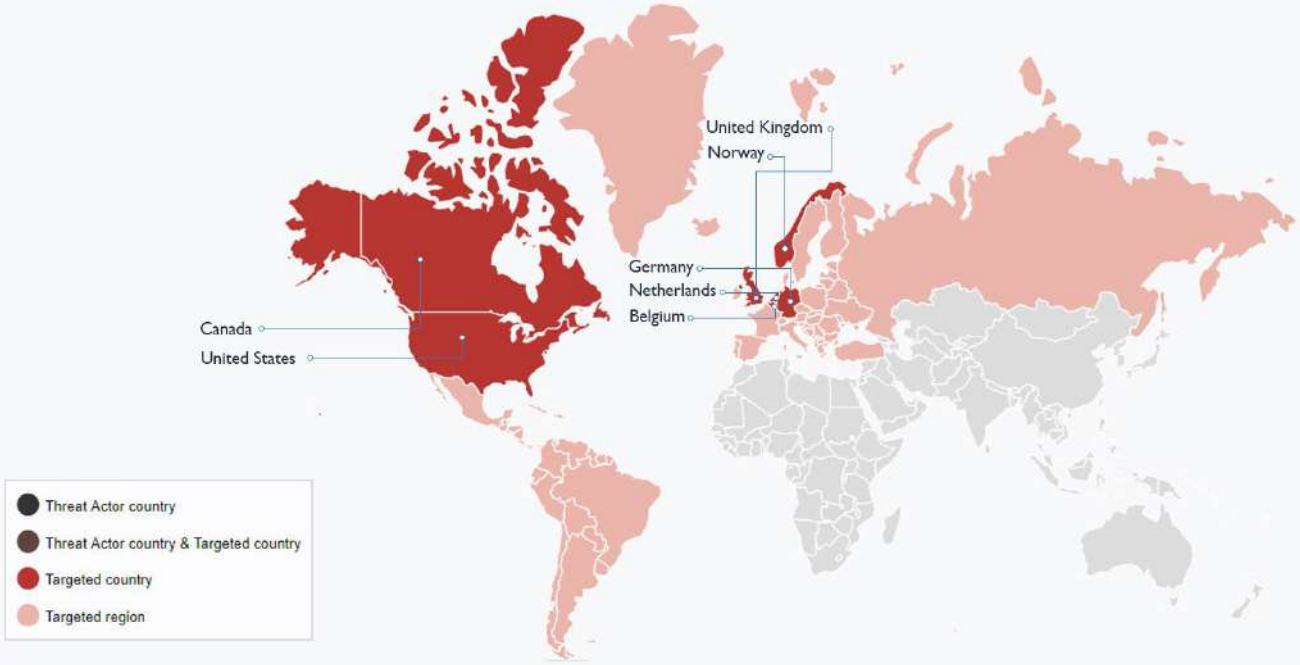


Figure 6 - Map of countries targeted by SunCrypt Group

Aliases

SunCrypt Group.

Targeted countries

Belgium, Canada, Germany, the Netherlands, Norway, the United Kingdom, and the United States.

SunCrypt Group is the financially-motivated threat group behind the SunCrypt ransomware and claims to be part of the Maze cartel, a conglomerate of ransomware gangs that threaten to leak confidential information stolen from victims. The SunCrypt ransomware shares similarities to Maze and Netwalker ransomware.

SunCrypt Group seeks to gain access to company networks to install ransomware and threaten the victims to release confidential company data if the ransom is not paid.

The SunCrypt Group began operating their custom ransomware dubbed SunCrypt in October 2019 but went largely unnoticed until they created a leak site to publish information stolen from their victims in August 2020: hxxp://nbzzb6sa6xuura2z[.]onion/

SunCrypt Group ransomware uses 5 operation modes that are almost identical to Maze ransomware ones, suggesting both ransomware could have been developed by the same individuals. The SunCrypt ransomware is installed via a heavily obfuscated PowerShell loader, as Netwalker Group has likewise done. Interestingly, eSentire analysts observed that after an unsuccessful attempt to infect a victim with SunCrypt ransomware, the attackers tried to execute Netwalker ransomware, failing to successfully execute the attack again. The modes are the following:

- **log:** logs ransomware's activity
- **noshares:** disables network shares encryption
- **path:** indicates a directory to be encrypted
- **noreport:** disables user data transfer to the server
- **nomutex:** enables running multiple copies of the ransomware

In August 2020, SunCrypt Group contacted security news outlet Bleeping Computer claiming to be part of the Maze cartel, which was created in June 2020, to share information and techniques about extorting victims amongst ransomware gangs. The threat group stated that they joined the Maze cartel because they needed help in handling their high volume of operations.

Maze Team may be providing compromised network access to SunCrypt in exchange for a revenue share. However, Maze operators denied any collaboration with SunCrypt to Bleeping Computer. Given, however, that ransomware belonging to both groups have communicated with the IP 91.218.114[.]31, there is likely a connection between these gangs.

Furthermore, in October 2020, SunCrypt Group expanded the impact of its campaigns by disrupting the victims' operations with DDoS attacks.

OilRig Group

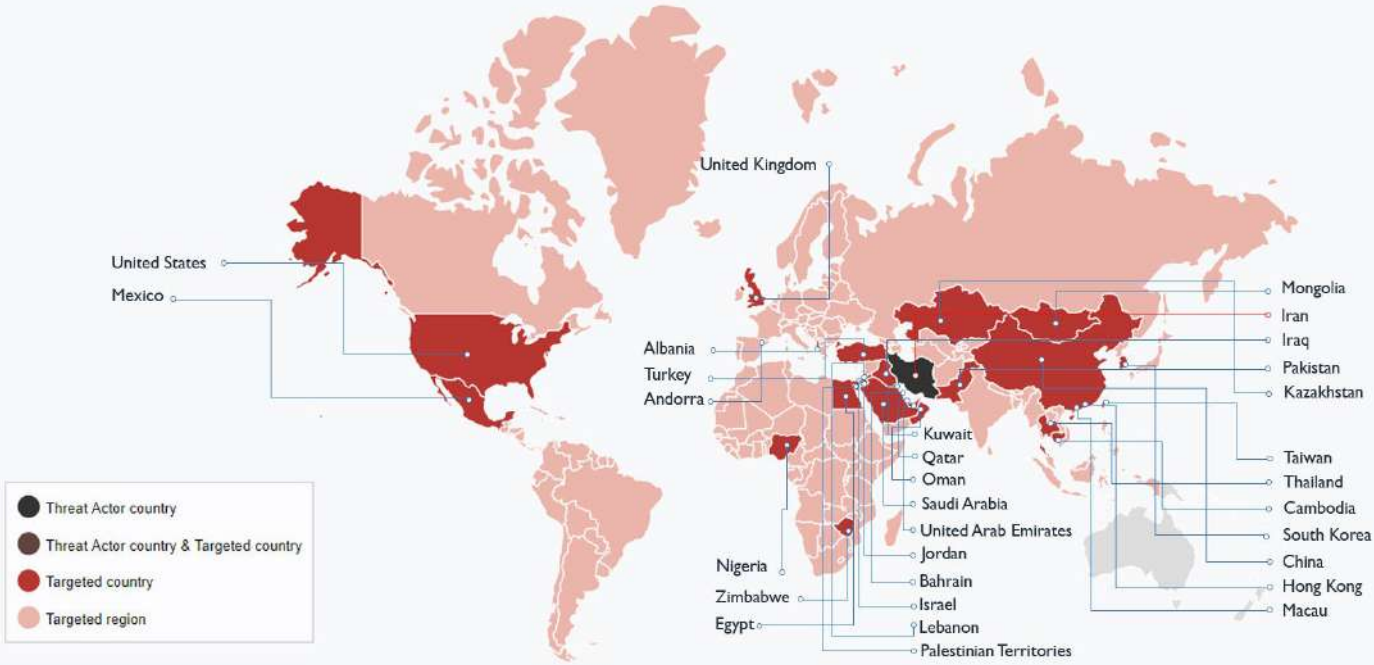


Figure 7 - Map of countries targeted by OilRig Group

Aliases

Greenbug, APT 34, Helix Kitten, Chrysene, IRN2, Helminth, Cobalt Gypsy, Crambus, PIPEFISH, and ITG13.

Targeted countries

Albania, Andorra, Bahrain, Cambodia, China, Egypt, Hong Kong, Israel, Iraq, Jordan, Kazakhstan, Kuwait, Lebanon, Macau, Mexico, Mongolia, Nigeria, Oman, Pakistan, Palestinian Territories, Qatar, Saudi Arabia, South Korea, Taiwan, Thailand, Turkey, the United Arab Emirates, the United Kingdom, the United States, and Zimbabwe.

"OilRig" is a threat actor with noteworthy abilities and resources; there is speculation that this hacking organization is sponsored by the Iranian government, and is known to collect high-value internal information related to both the public and private sector organizations in the Middle East and the United States.

The group commonly uses spear-phishing with malicious documents or a link to a malicious website where the user is requested to download an executable. In both cases, the objective is to install a backdoor in the victim's computer.

OilRig has targeted Middle Eastern industries and financial institutions since at least 2014. The group commonly uses spear-phishing with malicious documents or a link to a malicious website where the user is requested to download an executable. In both cases, the objective is to install a backdoor in the victim's computer.

In late 2018 it was discovered that OilRig was using a new Trojan called BONDUPDATER, which is a PowerShell-based Trojan that is installed by a malicious macro in a Microsoft Word document. The threat group also started using a new payload called OopsIE and replaced the previously used QUADAGENT.

In April 2019, a leak of tools and credentials allegedly associated with APT34 was uploaded to GitHub and shared widely. It is important to keep in mind that while these tools may actually be those used by APT34, this leak could also be part of a counterintelligence operation and may not reflect APT34's targeting and capabilities. Blueliv analysts did not independently assess these tools, their capabilities, nor the veracity of the GitHub repository.

Here below is a list of CVEs with their associated score related to OilRig group's attack tracked by Blueliv Threat Context solution.

SCORE	NAME	EXPLOITS	MALWARE	MENTIONS	PLATFORMS	MS BULLETINS	PUBLICATION DATE
8.5	CVE-2017-11882	3	13238	936	8	1	15/11/2017
8.5	CVE-2017-0199	25	6580	1066	18	2	12/04/2017
7.8	CVE-2019-11510	1	×	1124	153	×	08/05/2019
7.2	CVE-2019-1579	×	×	107	205	×	20/07/2019
7.0	CVE-2017-11774	×	×	28	8	1	13/10/2017
6.1	CVE-2018-13379	2	×	336	20	×	04/06/2019

Figure 8 - List of CVEs with their associated score related to OilRig Group

APT 33

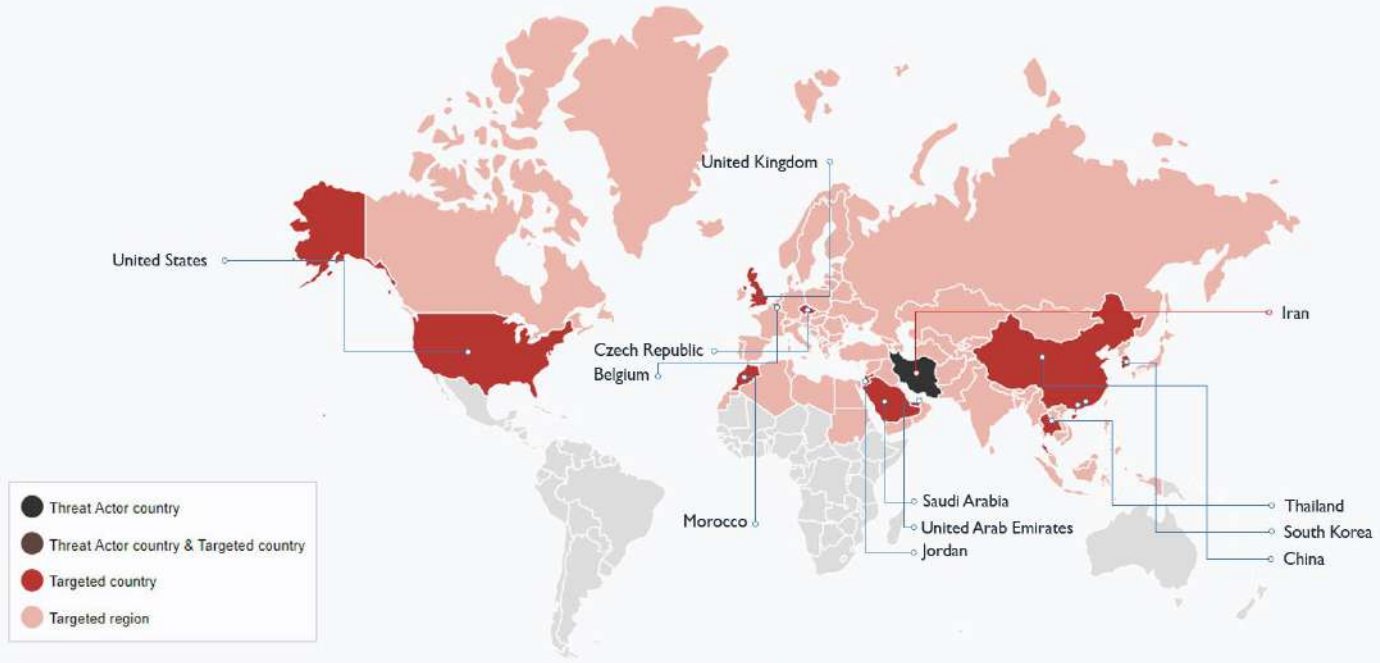


Figure 9 - Map of countries targeted by APT 33

Aliases

Elfin, Magnallium, Refined Kitten, COBALT TRINITY, and Holmium.

Targeted countries

Belgium, China, Czech Republic, Jordan, Morocco, Saudi Arabia, South Korea, Thailand, the United Arab Emirates, the United Kingdom, and the United States.

APT33 is a threat group believed to be sponsored by Iran. This threat group has carried out cyber-espionage operations since at least 2013.

APT33 has targeted organizations and industries headquartered in the United States, Saudi Arabia, and South Korea, among others, with a particular interest in organizations in the aviation sector involved in both military and commercial capacities, as well as organizations in the energy sector with ties to petrochemical production.

In December 2018, Symantec revealed that one of the victims of the destructive wiper Shamoon 3.0 had been previously infected by APT33's Stonedrill malware, raising the possibility of cooperation or coordination between the APT33 and the threat actors behind Shamoon. Shamoon is sometimes believed to be an Iranian threat group.

Furthermore, researchers at McAfee published an analysis following the December 2018 attacks also linking Shamoon to APT33 (or, interestingly, "a group masquerading as APT33"). Despite these claims, McAfee refers only vaguely to shared TTPs and domains linking the two groups. It's unclear what evidence McAfee is basing these claims on; Blueliv analysts cannot independently verify the analysis conducted by Symantec or McAfee.

In November 2019, researchers at Microsoft unveiled evidence that APT33 may be shifting their focus towards targeting industrial control systems (ICSs). The evidence presented by Microsoft is largely circumstantial and hypothetical.

Most relevant TTPs to defend against

Here are the ATT&CK TTPs used by threat actors targeting the energy sector. The darker the color red, the more actors use that technique.

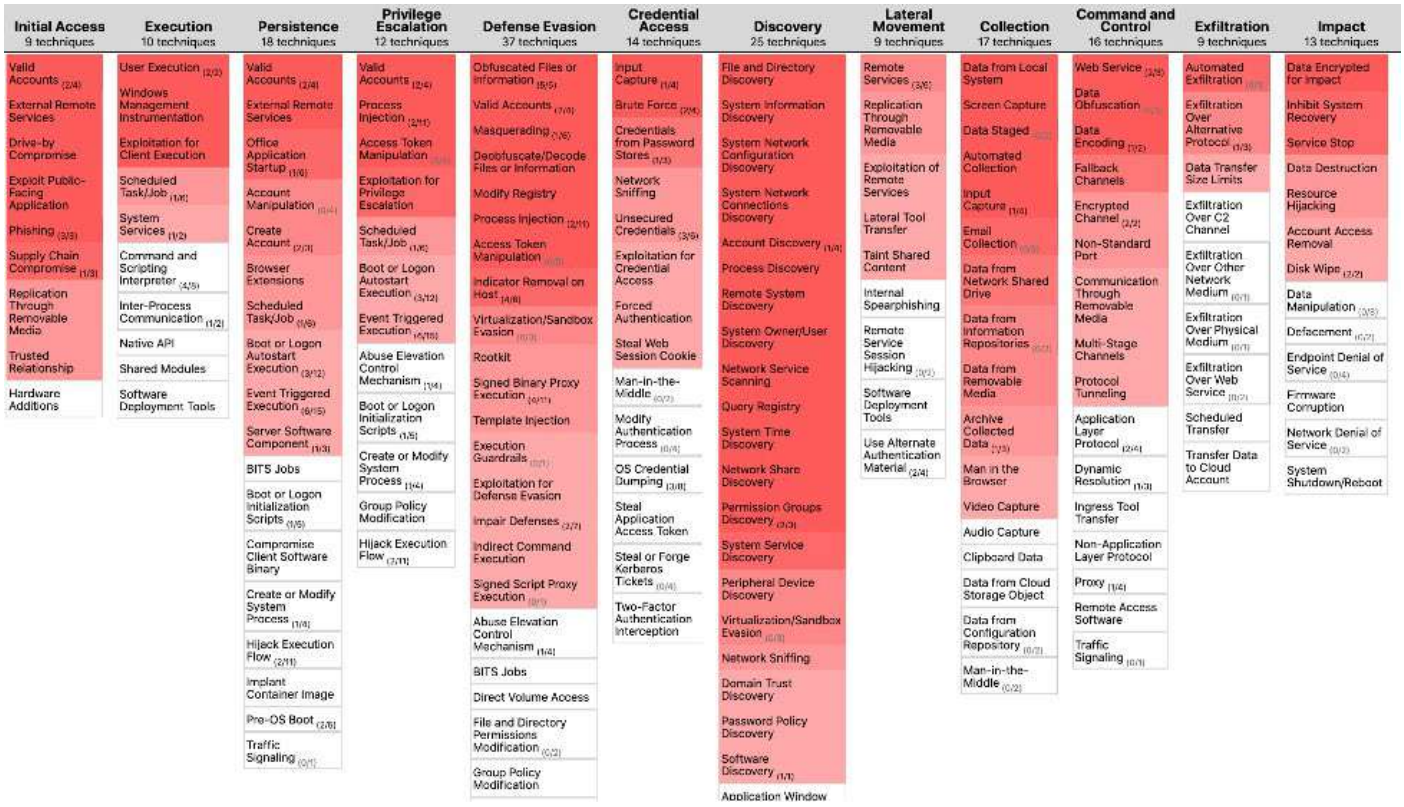


Figure 10 - ATT&CK TTPs used by threat actors targeting the energy sector

Threat actors targeting the energy sector usually seek to target third-parties with less secure networks in a supply chain attack (T1195) in order to reach the intended organization. Spear-phishing (T1566) and watering hole attacks (T1189) leveraging decoys about energy or critical infrastructure are also a popular path to gain initial access to a network. From there, depending on the attack objective, the threat actor can install a Remote Access Trojan (RAT) to quietly spy and exfiltrate data (TA0010) from the victims' network, or perform more destructive actions, such as data destruction (T1485) or disk wipe (T1561), among others.

How the energy sector can manage cyber-risk

As each industry digitizes and becomes increasingly dependent on data, software, shared networks, and other developments that allow for increased efficiency, they are increasingly vulnerable to cybercriminals willing and able to exploit these technologies. Every industry must build proactive security measures to mitigate this risk, though this is especially pertinent for the energy sector, which, if infiltrated, could spell destruction and loss of critical infrastructure for entire nations. This section details how organizations in the energy industry can manage rising cyber-risk.

Greater infrastructure visibility

Energy is a complex environment, and as such having complete visibility across all IT and OT systems is a difficult goal for security teams who can't afford to have blind spots in their defenses. To overcome these gaps, security teams must better understand their network and the devices, protocols, configurations, and traffic operating on it. This can be achieved through the use of continuous monitoring, real-time threat detections, and one-panel platforms that provide an accessible umbrella view.

Integrated intelligence

Thanks to the prevalence of IoT, organizations can now gather deep analysis of their production data and more. This means IT and OT can be easily integrated for intelligence and insights that were previously unavailable to the c-suite. In turn, IT teams can be far more informed, and prepared for the range of attacks before them, be it spear phishing, social engineering, infected devices, or another source.

Developed skills

The ability to understand IT and OT network security aspects, both common in the energy sector, is hard to come by among security professionals. To combat this, organizations would be wise to invest in training their staff to identify, understand, and remediate the varied threats that face both computer and physical systems.

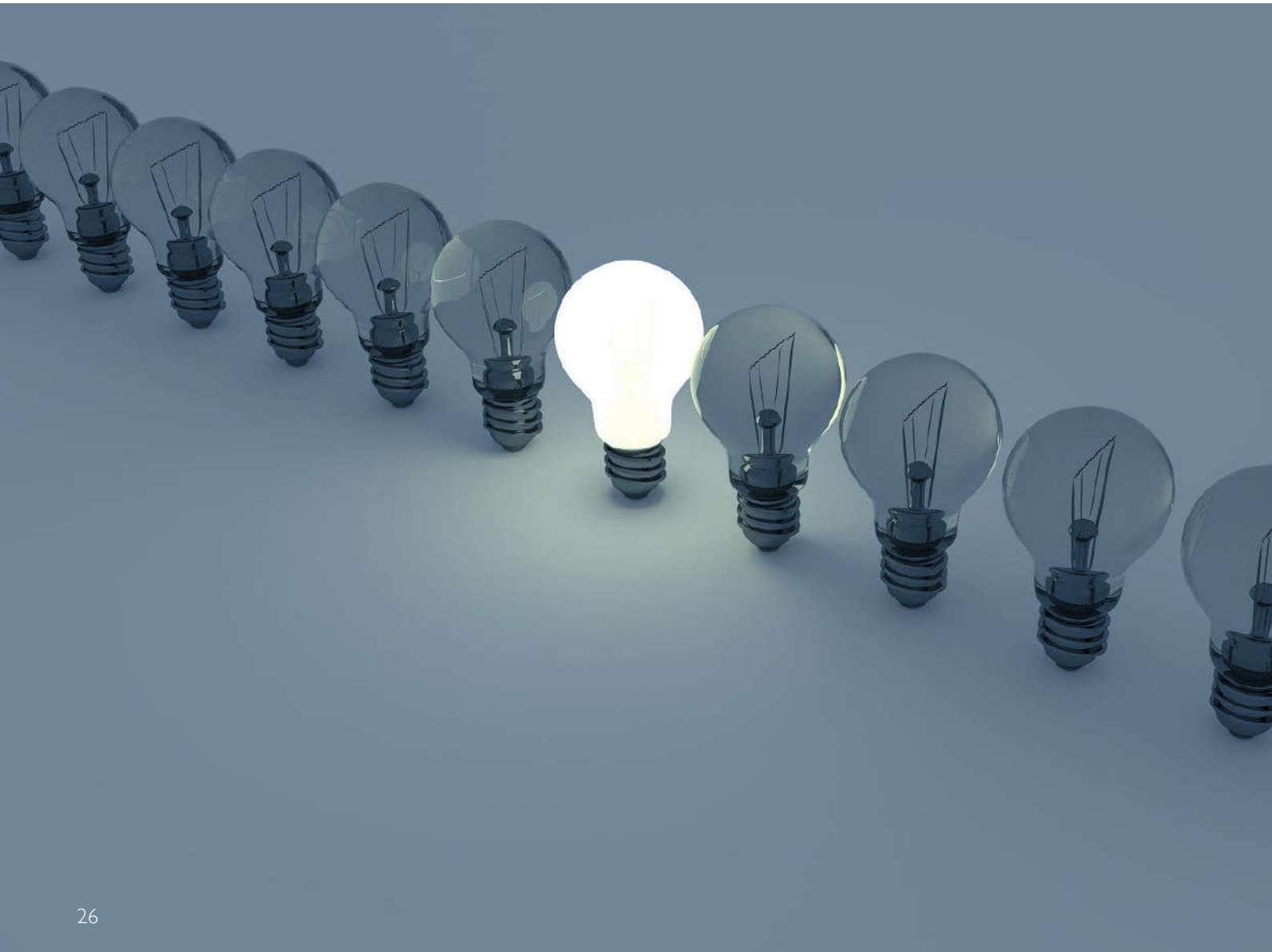
A cyber blueprint

To ensure resiliency to whatever may come, those operating in the energy sector must have a roadmap in place for when, not if, they fall victim to a cyber-attack. This includes steps and tools to follow to identify and contain a breach, and a route to restoring mission-critical operations. This is best achieved through an incident response platform, ideally with the ability to automate security automation from a single, easy to access a dashboard that can be integrated with third-party security solutions.

Ensure compliance

A sure-fire way to bolster security posture is to ensure your organization is compliant with standard best practice for your region. In Europe, EEU EUROPA acts to encourage best practice in the energy sector, facilitating European energy legislation, enhancing cooperation among regional and national authorities

and governments, and establishing an effective, efficient and transparent energy market in line with the EU's energy regulations. Similarly, the European Union Agency for Cybersecurity (ENISA) acts to create a cybersecurity standard throughout the region through the use of knowledge sharing, capacity building, awareness, and training, with a view to driving cyber resilience among Europe's businesses and civilians alike. By working to comply with such bodies, organizations will see huge benefits to their cyber resiliency.



The role of threat intelligence

Whilst organizational efforts to better understand and therefore mitigate cyber risks can go some way in building better cyber resilience and driving a security culture, this is no substitute for a robust threat intelligence platform. Only by harnessing true intelligence can energy organizations tackle the challenges outlined throughout this paper, accelerating the detection, management, and recovery from these aforementioned threats, and providing actionable, dynamic insights in the process. Threat intelligence is easily actionable, is autonomous, and is equipped to detect threats both inside and outside the network and execute their responses accordingly, and provides energy IT teams with the following:

Vulnerability management

Considering the large and typically complex architecture energy organizations have to secure, there is a real need for the ability to identify and patch vulnerabilities as swiftly as possible. A good threat intelligence solution will do this and more, categorising the most dangerous vulnerabilities in need of patching first, based on their perceived level of risk and other factors.

Rapid Incident response times

As well as genuinely malicious alerts, security teams spend a significant portion of their time assessing false positive alerts. Threat intelligence eliminates this process, not only freeing up the valuable time of the security expert but guaranteeing swift and efficient differentiation between genuine threats and false positives, ultimately resulting in a radical improvement in threat response times.

Proactive threat monitoring

Throughout this paper, we have established that the energy sector is highly sought after by the world's cybercriminal community, which is why proactive security measures are a must for any organization operating in this space. A good threat intelligence solution will offer truly modular real time detection, red teaming, internal hunting, and other proactive measures to ensure security remains at its best - and most impenetrable.

Anti-hacktivism

Considering its role as critical infrastructure, as well as it's at times perceived immoral eco standing, the energy sector remains a top target for hacktivists looking to convey a political message through a cyber-attack. Using threat intelligence, organizations can benefit from an early-warning system and active geolocator that continuously creates targeted and specific insights that can be used to predict and defend against expected attacks of this nature.

Breach containment

Infected systems can stay that way for several years before being detected, allowing criminals to gain a foothold in their victim's network and wreak havoc and steal sensitive data and credentials over a long period. The energy sector cannot afford for this to happen, considering what it could mean for millions of civilians and entire nations, as cited throughout this report. By leveraging threat intelligence, this industry can immediately identify its compromised assets and contain them in real-time.

Blueliv's Credentials module is one solution to stopping credential theft as a result of such a breach. We can provide actionable intelligence around leaked, stolen, and sold user credentials, and are equipped to locate the compromised credentials in real-time on the open, deep, or Dark Web. This includes relevant information on the malware used to steal it, and leverages Blueliv's honeypots, crawlers, and sensors to continuously hunt for stolen credentials.

Threat hunting

By leveraging threat hunting organizations can improve team productivity with simple, qualified, contextual threat intelligence in the form of continuous, intuitive, and intelligent updates on current actors, campaigns, malware indicators, attack patterns, tools, signatures, and CVEs. Blueliv's threat intelligence means teams benefit from significantly increased incident triage and response times, can harness strategic intelligence before, during, and post-incident, and are able to prioritize relevant IOCs for orchestration and run highly realistic attack simulations in preparation.

Red teaming

Beyond strengthening your perimeter, threat intelligence can also help develop and run realistic 'red team' attack scenarios that are unique to your business context in order to test and ultimately bolster your incident response processes. By running rigorous red team attacks, teams can ensure they are primed and ready to respond in the event of a real attack and are confident in how they leverage the threat intelligence available to them.

Brand protection

Despite what other losses may occur in the wake of a successful breach – financial, operational, or otherwise – brand reputation will always take significant damage, and could affect current and future customer loyalty and intake, ultimately impacting any future earnings. Blueliv seeks to protect brand reputation and preserve customer loyalty using real-time social media, domain, and mobile marketplace monitoring, protecting online presence and identifying malicious entities impersonating or compromising your staff and organization. We identify news channels, social accounts, and websites where your organization is being discussed, and can discover sites and mobile apps that are abusing your brand or luring your customers to fake portals.

Asset allocation

Although energy companies rightly allocate a larger portion of their budget to security measures compared to other industries, security resources are still finite and must be managed accordingly to ensure they are being maximized. Threat intelligence solves this conundrum, helping CIOs better manage their assets depending on maturity and the threat landscape before them, allowing them to invest their resources where they're most needed, and not waste valuable time or efforts elsewhere.

Information sharing

The fight against threat actors is industry-wide and as such organizations should unite and share their knowledge, skills, and experiences with their peers. An often-overlooked route to robust security, sharing insights from comprehensive threat intelligence can lead to radically reduced breach response times, improved preventative measures, and can help to create an altogether safer industry.

There are many bodies working to encourage information sharing in the energy sector. In the US, the Cybersecurity Risk Information Sharing Program (CRISP) and Electricity Information Sharing and Analysis Center (E-ISAC) work to better inform the energy sector of the cyber threats before them using advanced sensors and threat analysis. In Europe the European Electricity Information Sharing and Analysis Center (EE-ISAC) plays a similar role, driving cyber resilience information sharing across a network of private, public, and non-profit energy organizations in the region

Conclusion

In order to secure its critical assets and avoid large scale disruption or destruction, be it at the hands of an individual or established nation-state group, the energy sector must commit to improving its current security measures, creating a strong security culture and a better top-to-bottom understanding of its unique threat landscape in the process.

Blueliv is uniquely equipped to aid organizations in this journey to better security health, having long and lasting ties with leading companies in this sector, as well as a tried and tested understanding of the threats before it, the actor groups targeting it, and the specific vulnerabilities and blind spots it must overcome – and most importantly, how to meet these challenges head-on. Though, compared to many industries, the energy sector understands the severity of what could happen should it become compromised, there is still much to do on a grassroots level to ensure professionals at every level of the organization are equipped and educated to execute security awareness in their day-to-day operations.

Blueliv hosts a global community of thousands of cybersecurity experts and encourages them to share news, views, IOCs, and more – the Blueliv Threat Exchange Network. It gives members access to our free proprietary elastic sandbox, a close-to real-time cyberthreat map and it encourages information sharing. The growing global community is free to join – the fight against cybercrime is an ongoing and collaborative effort.

About Neurosoft

Founded in 1994, Neurosoft began as an in-house software development company with the vision of providing quality solutions and services to its clients both in Greece and abroad. Since then, Neurosoft has evolved into a fully integrated ICT company with Software Development, System Integration and Information Security capabilities, offering its products and services in SEE and MENA. The staff headcount currently exceeds 200 highly skilled employees with in-depth experience in their fields.

neurosoft.gr

info@neurosoft.gr

linkedin.com/company/neurosoft

About Blueliv

Blueliv is Europe's leading cyberthreat intelligence provider, headquartered in Barcelona, Spain. We look beyond your perimeter, scouring the open, deep and dark web to deliver fresh, automated and actionable threat intelligence to protect the enterprise and manage your digital risk.

Covering the broadest range of threats on the market, a pay-as-you-need modular architecture means customers receive streamlined, cost-effective intelligence delivered in real-time, backed by our world-class in-house analyst team.

Intelligence modules are scalable, easy to deploy and easy to use, maximizing security resource while accelerating threat detection, incident response performance and forensic investigations.

Blueliv is recognized across the industry by analysts including Gartner and Forrester, and has earned multiple awards for its technology and services including 'Security Company of the Year 2019' by Red Seguridad, Enterprise Security and Enterprise Threat Detection 2018 category winners by Computing.co.uk, in addition to holding affiliate membership of FS-ISAC for several years.

blueliv.com

info@blueliv.com

twitter.com/blueliv

linkedin.com/company/blueliv

Computing Security Excellence Awards 2018 Winner Enterprise Threat Detection Award

Computing Security Excellence Awards 2018 Winner Enterprise Security Award

Cybersecurity Breakthrough Award 2018