

THE STATE OF THE STATION

A report on attackers in the energy industry



CONTENTS

Introduction	3
Outmoded and out there	4
Changing the game	4
The names	5
The profiles	5
Two groups, one spillover	9
A plethora of opportunity	10
Attack targets and the reasons behind them	10
The 'How'	11
Investigating and naming	12
Still succeeding	12
Mitigating	13
Conclusions	15

INTRODUCTION

Interconnected systems in the energy industry increase cyber vulnerabilities, with cyber attacks often going undetected for some time. Malicious actors are increasingly targeting critical infrastructure (CNI) sites and distribution facilities for energy, and cyber attacks have real-world effects. As energy companies save costs against the backdrop of a lower oil price, consolidating operations can weaken business resilience and redundancy levels. This gives rise to new, single critical points of failure, with any disruption across the supply chain potentially having increased consequences.

Cyber attacks using individual vulnerabilities and exploits have, and always will be directed against the vast number of Programmable Logic Controllers (PLCs) in existence. However, connecting Industrial Control Systems (ICS) to the Internet and enterprise business networks is increasing. These factors, plus fewer backups in place with an increased dependency on fewer facilities, are only part of the picture.



OUTMODED AND OUT THERE

Many Operational Technology (OT) components have built-in remote operation capabilities, but are partly or entirely lacking in security protocols such as authentication. These concerns are not new, but many have recognized the need for increased cyber security around CNI for years.

Critical infrastructure is unique in the threat landscape, however. It is one of few sectors to be tied to private and public infrastructure, with a wide spread of physical and mobile assets. Consequently, there are a number of different factors that influence who, how, and why attackers target CNI.

A considerable number of CNI systems in use were installed before the advent of Stuxnet. Many of them were built decades ago before a 24/7 internet

connection was usual. Cyber security was not a realistic threat when they were manufactured, and legacy protocols and systems never had built-in security controls that we take for granted today. Transitioning these systems to the Internet has opened them up to attacks from a myriad of angles.

Updates and security patching further complicate the issue – especially when a system needs to be “on” all the time. This leaves little-to-no time for critical security improvements. Moreover, any system costing millions and designed to work for decades is not going to be readily discarded and replaced by a new one, even if it is deemed to be insecure. Together, these factors allow attackers to successfully penetrate ICSs.

CHANGING THE GAME

A variety of different adversaries, each with their own motivations and tradecraft, constantly strive to compromise organizations that operate critical infrastructure. Nation-state sponsored Advanced Persistent Threat (APT) groups continue to seek network foothold positions on CNIs and espionage opportunities in the interests of exercising political leverage. A realistic worst-case scenario is a type of DoS attack against a power plant’s ICS infrastructure, driving the facility down and making it unavailable for a long time. Potential outcomes include destroying the industrial control devices and systems. As a rule, the segregation between operational and business IT assets (e.g. programmable logic controllers versus a corporate user’s laptop) means that attacks of this type are unlikely to impact a power plant’s operational capability. They would impact a power plant’s

ability to carry out other normal business functions, however.

Appropriating APTs to just nation-state groups belies the fact that the threat landscape has moved on, however. Nation-state capabilities trickle down and become more widely available, giving other hacking groups the ability to be as advanced and persistent as APTs. Cyber criminals, who are generally after money, have acquired sophisticated tools as a result of the Shadow Brokers and Vault7 data breaches and modified their operating procedures. Money laundering techniques have also changed considerably, fueling ever-greater ransomware demands.

THE NAMES

Determining the number of attackers/malwares/techniques targeting the energy industry is not an exact science, but 9 different ones stand out. These are:

- Operation Sharpshooter (Lazarus Group)
- APT33
- GreyEnergy (the successor to the BlackEnergy group)
- BlackEnergy 1, 2 and 3 Malware
- Industroyer Malware – also known as CrashOverride
- Dragonfly/Dragonfly 2.0
- Havex Malware
- ICS side-channel attack
- TRITON/TRISIS Malware

THE PROFILES

Operation Sharpshooter: a name given by McAfee for a campaign which started on October 25, 2018. Additional evidence uncovered recently strengthens suspicions that this campaign is operated by the Lazarus Group. Its current focus seems to be on cyber espionage and reconnaissance. Using spear phishing, threat actors approach their targets disguised as recruiters via a social media service using English-language job description titles for

positions at unknown companies

The job titles are: Strategic Planning Manager, Business Intelligence Administrator, and Customer Service Representative. These are distributed by an IP address in the United States through the Dropbox service. The group does not commonly attack the energy industry, but the operation touching this sector might have been collateral.

Initial access: Spear phishing via service

Execution: Scripting, user execution, command-line interface

Persistence: Registry Run Keys / Startup Folder

Defense evasion: Process injection, obfuscated files or information, file deletion, hidden files and directories

Discovery: Account discovery, file and directory discovery, process discovery, system network configuration discovery, system network connections discovery, system time discovery, query registry

Collection: Data from local system, automated collection

Exfiltration: Automated exfiltration, exfiltration over command and control channel, data encrypted

Command and control: Commonly-used port, remote access tools, web service, data encoding

APT33: believed to be supported by the government of Iran focusing on cyber espionage and reconnaissance. The malware has been tied to an Iranian persona who may have been employed by the Iranian government to conduct cyber threat activity against its adversaries.

It has shown increased activity since the US nuclear deal withdrawal in May 2018. The latest attack, against Italian oil and gas company Saipem in

December 2018, used a new variant of the Shamoon disk wiper – a tool that wipes data on computers and can cause energy companies significant costs – called Shamoon 3, which built on the capabilities of the previous versions.

Industry targets include mainly aviation and energy, though it appears to be overall less advanced than some other actors targeting the energy sector. It has two aliases: Magic Hound, and Timber Worm.



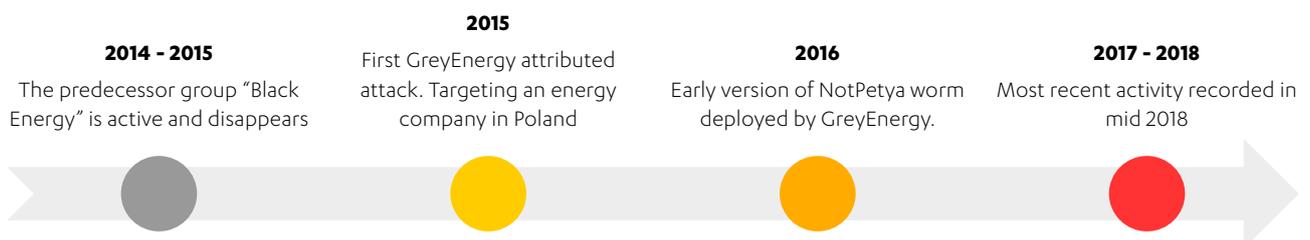
Initial access: Spear phishing link, spear phishing service
Execution: Mshta, PowerShell, user execution, scripting, exploitation for client execution
Persistence: Registry Run Keys / Startup Folder
Privilege escalation: Valid accounts
Defense evasion: Obfuscated files or information, de-obfuscate/decode files or information
Credential access: Credential dumping, brute force
Command and control: Data obfuscation

GreyEnergy: the successor to BlackEnergy malware still affecting Ukraine. Directed against energy and other high-value industry targets, the malware is used to attack ICS control workstations running Supervisory Control and Data Acquisition (SCADA) software and servers.

The group focuses on cyber espionage and reconnaissance, with a high focus on stealth and leaving minimal footprints and traces. Initial access, like the majority of the groups/malware we have

examined, is via a spear phishing attachment.

The adversary uses decoy word documents with malicious macros used to download and execute the GreyEnergy Mini Backdoor before escalating privileges and installing the main one. Malware modules are encrypted or fileless in nature. Any tools used are securely wiped from the target systems. The most recent activity is traced to mid-2018.



Initial access: Exploit public-facing application, spear phishing attachment
Execution: Scripting, service execution, user execution, PowerShell
Persistence: Registry Run Keys / Startup Folder, modify existing service, Web Shell
Privilege escalation: Valid accounts
Defense evasion: Code signing, file deletion, masquerading, indicator removal on host, process injection, timestomp, deobfuscate/decode files or information, obfuscated files or information
Credential access: Credential dumping, input capture, credentials in files, credentials in registry
Discovery: Query registry, system information discovery (via WMI), network service scanning
Lateral movement: Windows admin shares
Collection: Screen capture, input capture
Exfiltration: Over command and control channel
Command and control: Connection proxy, multi-hop proxy, standard application layer protocol, commonly-used port, standard cryptographic protocol

The BlackEnergy Group: has used a backdoor to deploy a KillDisk component to overwrite firmware in substation breakers and make the host OS unbootable. It contains functionality to target serial-ethernet connection services to attack SCADA systems.

The Group has deployed additional persistence via a backdoored SSH server on the system. The SSH server accepts authentication with a specific certificate or a specific hardcoded password. This makes attacks more potent. Wipers are used to sabotage systems and destroy forensic evidence.

The most conspicuous APT, tied to **BlackEnergy 2/3**, is the Sandworm Team. They have compromised a wide array sectors including power generation and distribution companies by utilizing an easily exploitable Microsoft Windows vulnerability.

Industroyer Remote Access Trojan (RAT) malware (aka CrashOverride): targets ICS systems which support the IEC 60870-5-101, the IEC 60870-5-104, the IEC 61850 protocols, or the Microsoft-developed proprietary Object Linking and Embedding (OLE) technology for process control data access (OPC DA) control protocols.

It can control electricity substation switches directories, effectively turning off power via substations' remote terminal units. The malware

developers have knowledge of industrial control systems and the protocols used for control and management in power grids, and can disrupt operations.

ESET security community researchers view Industroyer as being the biggest threat to ICS since Stuxnet – one of [the most famous cases](#) in malware history, which uses techniques similar to [Conficker](#).

Dragonfly/Dragonfly 2.0: attributed to the Russian Government. It has the potential for sabotage, but has not caused notable damage. This actor's campaigns have affected multiple organizations in the energy, nuclear, water, aviation, construction, and critical manufacturing sectors.

Latest observed operations are very similar to Dragonfly but are tracked separately as Dragonfly 2.0. It targets multiple critical infrastructure sectors including energy (according to US-CERT), and is used for espionage and sabotage of systems. ICS and SCADA infrastructure, workstations / servers with control access over the systems are at risk.

It has 11 aliases: Berserk Bear, Energetic Bear, Anger Bear, Dymalloy, Havex, PEACEPIPE, Fertger, IRON LIBERTY, Group 24, Crouching Yeti, and Koala Team.

2011 Dragonfly

First sightings when targeting defense and aviation companies in the U.S. and Canada.

2013 - 2014 Dragonfly

Target shift into energy sector across U.S. and Europe.

2016 - 2017 Dragonfly 2.0

Increased activity in 2017, targeting energy organizations in the U.S., Turkey and Switzerland with some traces outside these countries.

Initial access: Spear phishing attachment, drive-by compromise, valid accounts, trusted relationship
Execution: Scripting, PowerShell, service execution, scheduled task
Persistence: Valid accounts, registry Run Keys / Startup Folder, shortcut modification, Web Shells
Privilege escalation: Valid accounts, Web Shells
Defense evasion: Valid accounts, indicator removal on host, file deletion, masquerading, template injection
Credential access: Brute force, forced authentication, credential dumping
Discovery: Network service scanning, account discovery, network share discovery, system network connections discovery, system owner / user discovery, remote system discovery, file and directory discovery
Lateral movement: Remote desktop protocol, Windows admin shares, remote file copy
Collection: Screen capture, data from local system
Exfiltration: Data compressed
Command and control: Commonly-used port, standard application layer protocol

Havex Remote Access Trojan (RAT): operated by the Dragonfly group. It has been used against a variety of ICS operators and functions chiefly as an espionage tool.

The Havex RAT is delivered via spear phishing, exploits, and 'watering hole' attacks – a classic supply chain attack method in the ICS/SCADA sector. Viewers of legitimate websites are redirected to Dragonfly-controlled sites that delivered the Havex malware to them.

Havex contains functions for network enumeration, aimed at establishing network assets, firmware, and software editions by targeting OLE for Process Control (OPC), commonly used to interface with ICS applications. It communicates out to attackers via C2 command and control channels.

ICS side-channel attacks: are a specific category of attack technique, as are DDoS or supply chain compromises. They can extract system data based on physical implementation information. Timing and power analysis attacks rely on analysis of how long executing various computations takes and the measurable changes in power consumption.

Attackers can extract the encryption key and use it to make configuration changes with serious consequences, as ICS are used to protect the power grid. A malicious actor could cause the system to fail or to send false data back to its operator. An attacker could also change non-immediately obvious configuration changes, such as seasonal ones.

TRITON/TRISIS: developed for use against Schneider Electric's Triconex Safety Instrumented Systems (SIS), which is how it got its name, and is not dependent on any vulnerability within their products. It leverages the architecture of the safety systems themselves, in cases where they have been set up in a fashion allowing sysadmins (and by extension, attackers) to roll out changes.

Intended outcomes have included deliberately causing explosive damage and potential loss of life. Attackers need highly-specialized knowledge of the target environment in order to launch it against their targets, which makes TRITON/TRISIS difficult to scale. These types of attacks will continue to be highly-focused in their targeting. Past attacks have included a petrochemicals organization in Saudi Arabia.

The malware has never been fully-attributed, but ongoing research reveals that the originators are continuing to develop and test it. It currently sits

alongside an array of malware developed to cause physical damage such as Stuxnet, Havex, and CrashOverride.

TWO GROUPS, ONE SPILLOVER

Infrastructure companies are chiefly vulnerable to attacks by either profit-seeking criminals or nation-states with geopolitical motives. Cyber criminals use a combination of Tor Hidden Services and cryptocurrencies to extract money. Who pays the money does not matter to them.

The Dark Net is used to provide instructions and even customer support to victims in a way that makes it difficult to trace back to the perpetrators. Cryptocurrencies are used to funnel and launder the criminal proceedings to a (semi-) anonymous entity before cashing out money in the real world.

CryptoLocker, active around 2013, was one of the most 'successful' of ransomware campaigns. The ransomware infected more than 250,000 computers in the last four months of that year. Those who spread it netted over USD 3M before the Gameover Zeus botnet used for its distribution was taken down.

The campaign's success spawned a number of successors, such as CryptoWall and TeslaCrypt. LockerGoga is the most recent example of a ransomware campaign, [encrypting everything](#) on infected systems belonging to Norsk Hydro, a Norwegian aluminum producer. The attack in March this year did not affect the international firm's

renewable energy arm, however.

Most of the attacks on CNI do not have a financial motive, as they are more political. Advanced Persistent Threat (APT) actors are very professional in what they do and will get into an organization, even if it takes them years.

One of a nation-state's motives for targeting another country's energy sector is to exploit critical systems when required. They do this by establishing a foothold in the network, maintaining it without being discovered. This gives actors a cyber weapon, convenient for disrupting industrial assets, amongst other things.

Governmental attacks involving espionage and spying are extremely targeted and directed against very specific organizations. Attackers might conduct campaigns on various countries and specific targets where they want to gain access – either at different times, or concurrently. Nation-states can use country codes, IP ranges, network topology, or even MAC address combinations, as we have learned recently regarding [ShadowHammer](#), to figure out where they are, and only activate when they are in the right place. A cyber attack is the IT equivalent a sleeper in the real world.

A PLETHORA OF OPPORTUNITY

Ransomware's popularity amongst criminals for use is declining, but nobody was expecting the 2017 global [WannaCry ransomware](#). The cryptoworm exploited a vulnerability in Windows OS. WannaCry was an attack attributed to the Government of North Korea and targeted pretty much the rest of the world.

The Taiwan Semiconductor Manufacturing Company, one of the world's largest semiconductor and processor chip fabricators, was among those organizations affected. TSMC suffered at least one full day of production down-time, and costs associated with the attack were estimated at hundreds of millions of dollars.

North Carolina's Onslow Water and Sewer

Authority (ONWASA) was the victim of a [multi-stage ransomware attack](#) in late 2018. An initial RAT compromise was followed by deploying Ryuk, a ransomware variant, to the corporate domain. It caused extensive disruption to normal business activities for several weeks, but did not impact water treatment and distribution.

Russia is thought to be behind the 2017 NotPetya attack against Ukraine. The believed cyber weapon caused billions worth of unintended collateral damage in the West. Companies in Europe, North America, and Asia were hit by the same attack just because they happened to be running a piece of software which was used to launch it. People did not die, but the principles were the same.

ATTACK TARGETS AND THE REASONS BEHIND THEM

Energy sector supply chains, organizations, or facilities that work with energy use a lot of IT infrastructure and possibly cloud service providers. In addition to traditional IT infrastructure, these energy sector organizations use a lot of ICS hardware which makes them unique from other sectors such as the financial or technology ones. Commonly used ICS components are built by companies such as Siemens and can be a target in an attack, as we saw happen with Stuxnet.

Energy sector organizations share a similar kind of supply chain scheme, but the hardware that is specific to power plants, for example, has a unique touch. However, these installations are primarily lacking cyber security resilience, with misconfigurations, insufficient segmentation, or poor company awareness of the issues.

There are also companies which build nuclear power plants as turnkey systems to order, though nuclear power is quite unique in the energy sector, and is very mandated by the government. They build legal frameworks around how nuclear power plants

must implement their IT, access controls, or other parts of their supply chain. It is possible, but unlikely that a cyber attack would result in a nuclear power plant exploding. This is because current techniques that we see would be inadequate to counter the redundancies in place.

People are the weakest link in production, however, with company employees seemingly being criminals' go-to target. 2018 saw malware being delivered via malicious links instead of traditional e-mail attachments. Users would either have to download malware or use [login pages utilized for phishing](#). Another notable trend was malware delivered to smartphones via e-mails. This gave attackers access to a company's internal networks or otherwise sensitive data through people's mobile devices.

Nation-states conduct extensive reconnaissance of their targets. Attackers have more time than their targets and will take months to plan their attack, determining which employees fall for social engineering targets, testing for whether or not known vulnerabilities have been patched.

THE 'HOW'

Email phishing (spear phishing) is attackers' (APT) compromise vector of choice against CNI operators. The traditional phishing attack compromises the human element first, gaining access to the production network before moving on to get into the ICS network. Techniques vary between the malicious actors. Here is an example of a typical spear phishing email:



Message  CV Controls Engineer.docx (19 KB)

Hello

Over 10 years Controls/Software Experience

Software development for PLC based control systems:
SIEMENS S5, S7-200, S7-300, S7-400 series,
Rockwell 5000, 500 series.
SCADA, HMI configuration.

Various Conveyor system experiences
Networking with PLC's: Ethernet, PROFIBUS-DP, PROFINET MPI, ASi, DeviceNet, DH+
EPLAN

Multi Å skilled controls engineer with experience in hands on project based work. Experience ranges from budget estimate and managing electric engineering projects to developing and commissioning software for PLC - SCADA control systems.

I Look forward to hearing back.

Best Regards,

Attackers usually start with the easiest technique to gain access, as they do not wish to show all of their cards. Failed attempts at this juncture will give rise to advancing levels of sophistication until they are successful.

They would almost always escalate their privileges to steal more information from the local host unless the higher/required privileges exist from the start of the attack. The next stage might include some type of collection, where information is searched for then aggregated. The final stage is exfiltration, where the file would be zipped up, protected, encrypted, and sent with the least size to avoid detection.

A nation-state could use a variety of techniques together and / or combine attack methods. They would likely have to engage in almost all of the attack techniques in order to go deeper into the network to where they want. Attacks and tools are more carefully planned in the energy sector because they have to overcome obstacles.

What separates the energy sector from others is the motivation of the attacker, and the ICS network and devices. Energy sector facilities usually have their ICS network separated from their production

network, but sometimes they are not. In this case, it means that gaining access to the control facility is fairly easy. Moreover, the third-party that doesn't specialize in IT services but provides them to the target organization is probably the weakest link in a supply chain attack.

One of the favorite techniques of threat actor APT10 (also known as Stone Panda), thought to be a Chinese cyber espionage group, is gaining entry to a network via a trusted third-party IT service provider. Network traffic between the organization and the service provider is normal. APT10 would first compromise the service provider, which they will then use as a proxy to get access to the target organization.

APT10 targeted at least three companies in the United States and Europe between November 2017 and September 2018 as part of the CloudHopper espionage campaign. One of them was Norwegian IT and business managed service provider (MSP) [Visma](#), a billion-dollar company with at least 850,000 customers globally.

INVESTIGATING AND NAMING

Tying cyber incidents to adversaries involves looking into the attack events and how it was accomplished. Attackers usually develop their own combination of techniques and have countless different ones. Putting this together with which ones were used is essentially how an adversary is identified by comparing the observed artifacts, infrastructure, techniques, tactics, and procedures of the attacker with previous incidents.

Many criminal groups, individuals, and hacktivists eventually deploy the same tactics, techniques, and procedures (TTPs) as APTs, with variants of nation-state malware and zero days being deployed throughout the threat landscape. This trickle-down effect also motivates nation-state groups to innovate in order to stay under the radar.

The picture then tends to look like a specific adversary, but anyone can read about TTPs online and make an attack based on those and try to look

like someone else. This makes attribution more difficult. Attackers stealing from each other to bring costs down and improve effectiveness also provides plausible deniability, or at least the capability to muddy the waters even more regarding attribution. Furthermore, any practical advantage will be sought when it comes to improving the odds of success and diminishing the chances of being caught.

Certain techniques will be preferred more than others. For instance, attackers will favor keeping their people and infrastructure in countries that do not extradite. This could make them easier to detect. Nation-states use each other's attacks because they work, and almost everything about repurposing attacks works to the advantage of online criminals. This is true whether they are backed by a nation-state or not. The constant switching up of attacks and tactics makes attribution an everlasting cat and mouse game.

STILL SUCCEEDING

The fundamental reason for this is organizations' lack of mature cybersecurity practices. The undersupply of dedicated qualified staff to handle cybersecurity related incidents / monitoring is well-known. A normal organization's attack surface is so large, that the security team needs to make a major contribution as well. A firewall/NIPS/AV and a sysadmin as operator are just not enough anymore. This particularly applies to a business of interest for a nation-state or otherwise advanced attacker.

From a business point of view, cyber security is often considered as being a necessary evil. It is an endless cost. It boils down to threat modelling and appropriate investment in security taking the risk and possible loss of revenue into account. Now, if you put two armies against each other, one without limitations on resources or time and the second with

a strict budget and slow pace, it is not even a fair fight. Attackers only need one hit. Defenders, by contrast, need to succeed at every move.

The concept of totally air-gapped operational networks has always been posited as the best way to avoid a compromise of Operational Technology (OT) assets. This is almost impossible to achieve in reality, however. Some files must be transferred from the production to the corporate estate occasionally, and updates cannot be applied to operational assets without transferring data into the air-gapped network using some method. Many companies have historically kept their OT data secure by cutting it off from any internet connectivity. This this is becoming increasingly difficult to maintain, however, as several still physically transfer the data on USB drives.

MITIGATING

Identifying how to move data from the OT to the IT in the most secure way is one of the energy industry's biggest challenges. How does data from IoT devices affect the security of this information transfer? It is sometimes easier for a malicious actor to target the organization's supply chain with the security protocols in place sufficient to resist targeted attacks – or even when they don't. Equipment providers, managed IT service providers, and websites for hosting software updates have all been targeted.

Organizations should assess the risk they face and measure their ability to identify malicious actors inside their networks concurrently, segregating critical networks away from traditional IT environments and making sure there are no connections between these systems.

Accurately-defined DMZs and network segregation should ensure that a targeted attack will always begin with the corporate IT network. It is easier to establish detection and response controls here, and defenders win if they are quicker in responding to the breach than the attacker is in completing their goal.

Operational Technology and Information Technology have different mindsets and priorities. Building bridges between these two departments before an incident occurs, however, is crucial in making sure there is no duplication of efforts which could ultimately cause a hindrance to stressful incident situations. Keeping the 'unsecurable' away from what you can control will increase the security of any infrastructure.

Another method is to implement the most advanced endpoint detection and response (EDR) solution. EDR is a quick way to set up capabilities to detect and respond to advanced threats and targeted attacks which might bypass traditional endpoint solutions. The most advanced EDR solutions can automate monitoring to cover the needs 24/7. This means organizations' IT teams can operate during business hours to review the detections while automation takes care of the rest. Managed EDR is a more cost-effective solution for organizations that don't want to implement fully-qualified cybersecurity teams. EDR provides visibility and intelligence.



VUCA is an acronym coined by the U.S. Army to describe the **v**olatility, **u**ncertainty, **c**omplexity, and **a**mbiguity of the post-Cold War era. Firms in the energy and other sectors are battling an unseen and stealthy enemy with wide-ranging objectives deploying unseen tactics, techniques, and procedures (TTPs). VUCA has been adopted in the corporate setting as a framework for preparing, leading, and even thriving in an unpredictable business, economic, and geopolitical environment.

Businesses need to understand the threat landscape and where their organization sits within it. In brief, the VUCA framework involves identifying:

- **Volatility:** what external factors affect the risks to an organization. It applies to the changing motivations and shifting components of the threat landscape and how they affect security posture
- **Uncertainty:** who might target it and why. This also includes what the impact of an attack would be, and what or who within an organization would be of value to nation-state hacker or criminal groups
- **Complexity:** where business goals and growth objectives affect security strategy. It details the entirety of an organization’s IT estate and the people that rely upon it, identifying the crucial assets in order to craft strategies and how to protect them using security
- **Ambiguity:** how a business might be targeted. This factor attempts to break down how attacker TTPs including phishing, social engineering, and malicious attachments manifest across multiple cyber attacks



CONCLUSIONS

Breaches are, in some ways, unavoidable. No matter how tight your controls, threat actors – especially nation-state ones – have proven they have the resource and the patience to achieve their objectives. Organizations that operate with critical national infrastructure face a set of unique challenges against the threat landscape.

Keeping a small attack surface in the energy industry – while often pitched as the best way to mitigate the risk of a cyber attack – is simply not possible. Between an IT estate that needs to support multi-national business operations and the increased use of IoT devices in both IT and OT, the attack surface of companies and organizations that deal with critical infrastructure is only set to increase.

Tracking all of the devices connected to the OT alone is a mammoth task. For the immediate future, these technologies are unlikely to see use in any but the newest production environments, as the lifetime of OT devices such as PLCs frequently run into decades. It is also not possible to quantify exactly when the next sophisticated exploit or vulnerability will be disclosed, but we can be sure that they will be quickly weaponized for use in targeted attacks or unspecific campaigns – within days or hours.

All organizations need to make sure they are familiar with their incident response plans and procedures.

This is particularly important when considering that not every problem is a technology issue. Human factors such as communication, organizational structures and ways of working are often more important to ensure effective incident detection and containment.

This is based on the three cs of Continuous Response: collaboration, context, and control. An emerging concept in cyber security that is central to boosting response capabilities, it is the art and science of having the right people, in the right place, at the right time, armed with the information they need to take control of the situation.

The aim is to combine elements of the three cs into a fluid process. Treating response as a continuous activity means that team members will be in constant communication and collaboration with one another, able to discuss suspicious events happening anywhere within their infrastructure.

Basic Infosec is also important, and the same mitigations that work in the energy sector apply to any industry. Properly-implemented, mature passive and active cybersecurity will block most of the attacks, quickly detect the ones which go through the defenses, and make it very hard for attackers.

ABOUT F-SECURE

F-Secure is a European cyber security company with decades of experience in defending enterprises and consumers against everything from opportunistic ransomware infections to advanced cyber attacks. Its comprehensive set of services and award-winning products use F-Secure's patented security innovations and sophisticated threat intelligence to protect tens of thousands of companies and millions of people.

F-Secure's security experts have participated in more European cyber crime scene investigations than any other company in the market, and its products are sold all over the world by over 200 operators and thousands of resellers.

