Trustwave SpiderLabs

2025 Trustwave Risk Radar Report

Energy and Utilities Sector

Trustwave®

Contents

Energy and Utilities' Unique Threat Landscape 6

Notable & Prominent Trends in Energy & Utilities Sector 10

Ransomware Trends 11

Ransomware Threat Groups 15

IT/OT Convergence 18

Evolving Regulatory Pressures 21

Threat Actor Techniques by Attack Stage 24

Conclusion & Key Takeaways 28

For the past two years, Trustwave SpiderLabs has released research analyzing industry-specific attack flows, offering insights into threat actors, actionable intelligence, and recommended mitigations for each attack stage. In this report, we delve into the unique cybersecurity challenges facing the energy and utilities sector, which is increasingly targeted due to its critical role in supporting national and global infrastructures.

In this research, we've categorized energy and utilities to include the production, distribution, and storage of oil and gas, renewable energy, and nuclear energy, as well as the generation and distribution of electricity, gas, and water. This broad scope reflects the sector's complexity and the interconnectedness of its diverse systems, each presenting its own unique security challenges.

The Trustwave SpiderLabs team highlights significant trends shaping the industry, including the rise of ransomware, the convergence of operational technology (OT) and information technology (IT), and evolving regulatory pressures. We also address the growing sophistication of threat actors and provide a comprehensive overview of the tactics, techniques, and procedures (TTPs) they employ, categorized by attack stage. This intelligence empowers energy sector organizations to better prepare, detect, and mitigate potential attacks.

Additionally, Trustwave SpiderLabs has produced two in-depth analyses focusing on critical areas of concern: notable trends in ransomware attacks and detailed profiles of the most active and dangerous ransomware groups. These reports offer extensive research and actionable strategies for mitigating risk. For example, ransomware attacks targeting the energy and utilities sector have increased by 80% year over year, underscoring the growing urgency of addressing this threat.

The sector faces several unique challenges which makes it particularly vulnerable to a diverse range of threats, from ransomware targeting critical infrastructure to spear-phishing campaigns aimed at exploiting human vulnerabilities. These challenges include the prevalence of aging infrastructure, reliance on legacy systems, and the complexity of OT systems. Coupled with the sector's geopolitical significance and the potential for widespread societal impact, these factors make the energy and utilities industry a prime target for malicious actors.

The increasing reliance on digital technologies, remote operations, and cloud-based systems has expanded the attack surface, creating new vulnerabilities that must be addressed through robust cybersecurity measures. For example, earlier this year, the North American Electric Reliability Corporation (NERC) warned that US power grids are becoming increasingly vulnerable to cyberattacks, with "the number of susceptible points in electrical networks increasing by about 60 per day." This fact highlights the urgency for energy providers to bolster their cybersecurity defenses.

While the average cost of a data breach in the energy sector is $5.29 million, higher than the overall cross-industry average of $4.8 million, the potential consequences extend far beyond financial loss. A cyberattack can lead to operational disruptions, physical damage, and reputational harm. Given the critical role of the energy sector in society, a cyberattack can have significant societal implications, including power outages, supply chain disruptions, and national security risks. As a result, energy and utility providers must prioritize cybersecurity to ensure the reliability and resilience of their operations.

Key Report Findings for the Energy & Utilities Sector

80%

increase in ransomware activity YoY

47%

of ransomware attacks in the United States

19%

of ransomware attacks were conducted by Hunters International in H2 2024

84%

of attacks originated from phishing

96%

of attackers relied on remote services to move laterally

67%

of credential access techniques were brute force

Energy and Utilities' Unique Threat Landscape

IT/OT Convergence

- The energy and utilities sector heavily relies on the integration of physical infrastructure/OT (power plants, pipelines, etc.) with cyber systems/IT (SCADA, IoT devices). The integration of these two domains has created a more efficient and responsive energy ecosystem, but it has also introduced a complex and expanded attack surface for cybercriminals. Traditionally, OT systems were isolated or "air-gapped" from the Internet to prevent remote cyberattacks. However, the need for real-time data exchange, remote monitoring, and automation has led to the increased connection of OT systems to IT networks. This convergence allows for greater operational efficiencies and enables cybercriminals to exploit vulnerabilities in previously isolated systems.

- A successful cyberattack on an OT system can result in not just data breaches, but physical damage to infrastructure, disruptions in service, or even safety incidents that put human lives at risk. As IT/OT boundaries continue to blur, organizations must adopt a holistic cybersecurity approach that addresses both domains simultaneously.

Critical Infrastructure

- Energy and utility systems form the backbone of modern society, making them a prime target for cyberattacks with potentially devastating consequences. A cyberattack targeting a critical energy infrastructure—such as a power grid, oil pipeline, or water supply system—can cause widespread disruptions that ripple across multiple sectors.

- For instance, a breach that takes down the electrical grid can disable communication systems, halt manufacturing processes, and disrupt transportation networks. In more severe cases, such an attack can compromise healthcare services by incapacitating hospitals that rely on electricity for medical equipment and patient care. Furthermore, because the energy sector is also interconnected with other essential services like telecommunications and finance, an attack on one industry can have cascading effects, jeopardizing public safety and national security.

- The convergence of physical and digital systems in energy operations means even localized disruptions can have far-reaching consequences, making cybersecurity in this sector a matter of national interest. Governments and regulators recognize the importance of securing these systems, and attacks on critical infrastructure are often treated as matters of national security.

Regulatory Compliance

- The energy and utilities sector is subject to rigorous and evolving cybersecurity regulations designed to protect national and economic security. Regulatory frameworks like NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection) in the US and NIS2 (Network and Information Security Directive 2) in the EU establish mandatory cybersecurity requirements for critical infrastructure operators.

- These regulations include guidelines for securing networks, monitoring vulnerabilities, and ensuring data integrity in both IT and OT environments. Compliance is not just about adhering to best practices; it also includes requirements for reporting cyber incidents in a timely manner, often with strict deadlines. Non-compliance can lead to significant financial penalties, litigation, and reputational damage that could undermine consumer trust and investor confidence. As cybersecurity threats evolve, these regulations continue to become more stringent, pushing organizations to invest in advanced cybersecurity technologies, processes, and employee training to stay ahead of potential risks. Given the high stakes involved, the ability to demonstrate compliance has become a critical component of corporate governance in the energy sector.

Aging Infrastructure and Legacy Systems

- A significant challenge facing the energy and utilities sector is the widespread reliance on aging infrastructure and legacy systems. The average age of electrical infrastructure in the US is 40 years— with 25% of the grid being 50-plus years old — and many systems still use decades-old IT systems. Many critical systems, particularly in the OT domain, were designed decades ago and were not built with modern cybersecurity threats in mind. These legacy systems often lack the necessary patches, updates, and support to address evolving vulnerabilities. Additionally, they may run on outdated software and hardware that is incompatible with newer security solutions, making it difficult to implement necessary cybersecurity upgrades without disrupting critical operations.

- Many energy companies are also wary of making large investments in overhauling aging infrastructure due to the high costs and potential disruptions to service. As a result, legacy systems remain a significant security risk, particularly when connected to modern networks or IoT devices that may have stronger, but different, security features. Ensuring the protection of legacy systems while transitioning to more secure, modern technologies requires careful planning, increased investment, and collaboration between IT and OT teams to ensure a seamless integration of security measures without compromising operational continuity.

American Water, Largest Water Utility Company in the U.S. Targeted in Cyberattack

October 2024, **CNBC**

OT Complexity

- OT systems are often more complex and specialized than traditional IT systems, requiring a unique approach to cybersecurity. These systems are responsible for controlling and monitoring industrial operations—everything from power generation and distribution to water treatment and gas pipeline management. Unlike IT systems, which are built around general-purpose software and hardware, OT systems often rely on proprietary software, specialized control systems (like SCADA—Supervisory Control and Data Acquisition), and customized hardware.

- Securing OT systems requires professionals to possess specialized knowledge in cybersecurity and the specific industrial processes they support. Cybersecurity teams need to understand the underlying engineering and operations of OT systems, as vulnerabilities in these systems can have immediate, tangible consequences on physical infrastructure.

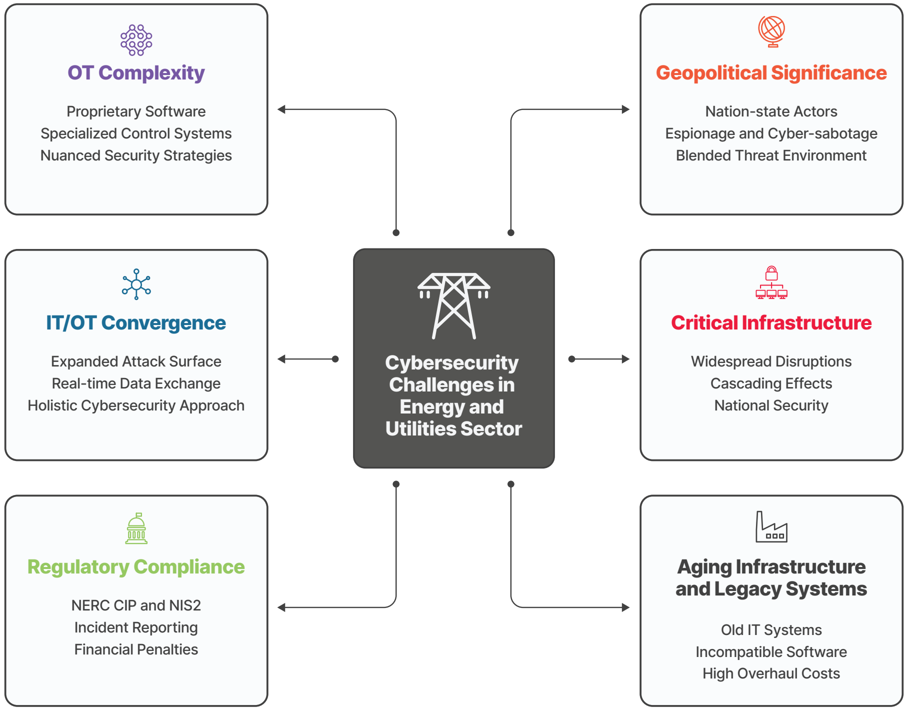
- The traditional "patch-and-update" approaches used in IT security are often not feasible in OT environments due to concerns over system downtime and operational disruption. As a result, OT cybersecurity requires a more nuanced strategy that balances the need for security with the need for continuous, uninterrupted operations.

Geopolitical Significance:

- The energy sector holds immense geopolitical significance, and as such, is a frequent target for nation-state actors. Energy infrastructure is often viewed as critical not only for economic stability but also for national security. Disrupting or sabotaging energy systems can destabilize a country's economy , hinder military operations, and disrupt the functioning of key sectors like healthcare, transportation, and communications.

- Nation-state actors may target energy infrastructure for various reasons, including espionage (gathering intelligence), cyber-sabotage (disrupting operations), or even as part of hybrid warfare strategies designed to weaken or destabilize a rival nation. For example, state-sponsored cyberattacks can target power grids or pipeline systems with the intent of causing blackouts, fuel shortages, or broader systemic chaos.

- The threat landscape is further complicated by the potential for cyberattacks to be used in conjunction with physical attacks, creating a "blended" threat environment where cyber incidents can amplify the impact of traditional kinetic attacks. As a result, energy organizations must be prepared to defend against highly sophisticated, well-funded adversaries with both cyber and geopolitical motives, making the cybersecurity challenge in this sector one of the most complex and critical facing the global economy today.



Cybersecurity Challenges in Energy and Utilities Sector

OT Complexity

Proprietary Software
Specialized Control Systems
Nuanced Security Strategies

Geopolitical Significance

Nation-state Actors
Espionage and Cyber-sabotage
Blended Threat Environment

IT/OT Convergence

Expanded Attack Surface
Real-time Data Exchange
Holistic Cybersecurity Approach

Critical Infrastructure

Widespread Disruptions
Cascading Effects
National Security

Regulatory Compliance

NERC CIP and NIS2
Incident Reporting
Financial Penalties

Aging Infrastructure and Legacy Systems

Old IT Systems
Incompatible Software
High Overhaul Costs

Trustwave SpiderLabs

With more than 250 cybersecurity experts across the globe, the Trustwave SpiderLabs team puts its resources to task researching the top threats in today's landscape. We are uniquely positioned to do so, as we perform over 200,000 hours of penetration tests and uncover tens of thousands of vulnerabilities annually. We also have a dedicated email security team analyzing millions of phishing URLs validated daily, including 10k per day that are uniquely identified by Trustwave SpiderLabs. Our diverse coverage of infosec disciplines, including Advanced Continuous Threat Hunting, Digital Forensics and Incident Response, Malware Reversal, and Database Security, give us insight into identifying how these breaches occur, as well as mitigations and controls that your organization can put in place to prevent these compromises.

This report examines the myriads of threats facing the energy and utilities industry. In addition to supplemental reports focused on notable trends in ransomware attacks and detailed profiles of the most active and dangerous ransomware groups, Trustwave SpiderLabs will offer recommendations to help providers mitigate risks and safeguard their operations.

Notable & Prominent Trends in Energy & Utilities Sector

Ransomware Trends

The Threat

We explore ransomware trends in the energy and utilities sector in depth in our accompanying report. At a high level, here are some key points to consider:

The rising frequency of ransomware attacks against the energy and utilities sector underscores the need for robust cybersecurity resilience strategies, designed to proactively identify, mitigate, and respond to breaches and ransomware attacks. There are a few reasons why this sector is often targeted by attackers:

- It consists of prosperous organizations with considerable revenues, making them lucrative targets
- The interconnected nature of SCADA systems, including IoT devices and remote access points, provides multiple entry points for cyber attackers
- Recovery time is longer compared to other sectors
- Disruption has high operational costs

What Trustwave Is Seeing

The number of ransomware attacks, which is based on claims published on group's extortion websites for the energy and utilities sector, was significantly higher in H2 2023 and H1 2024.

The below data shows more than an 80% increase in ransomware activity in H1 2024 and H2 2023 than the same time period one year prior.

Ransomware Attacks in Energy and Utilities

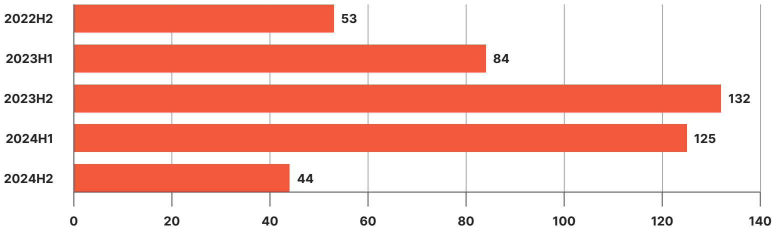


Figure 1. The number of ransomware attacks waged against the energy and utilities sector since H2 2022

Top Ransomware Groups Since H2 2022

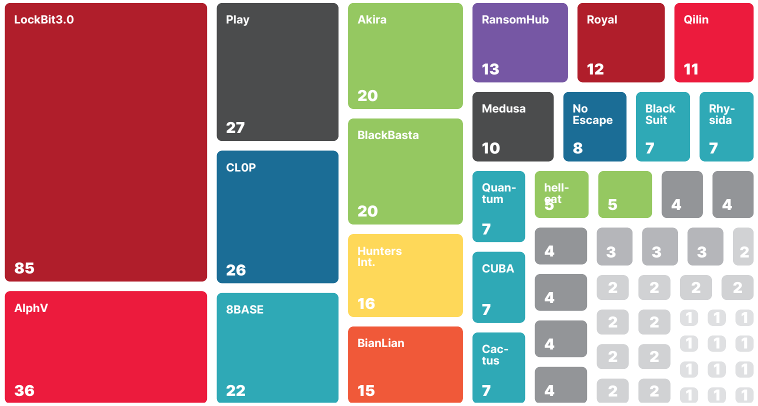


Figure 2. Ransomware groups targeting energy and utilities and count of attacks since H2 2022

When looking at the trends since H2 2022, LockBit and AlphV are the most active groups, with Play, Cl0P, and 8Base following.

However, in the chart below, in the second half of 2024, **Hunters International** and **Qilin** took a lead in launching attacks against the energy and utilities sector compared to other groups. Hunters International accounted for 19% of attacks (8 total), Qilin accounted for 14% (6 total), and Akira accounted for 10% (4 total).

Top Ransomware Groups in H2 2024

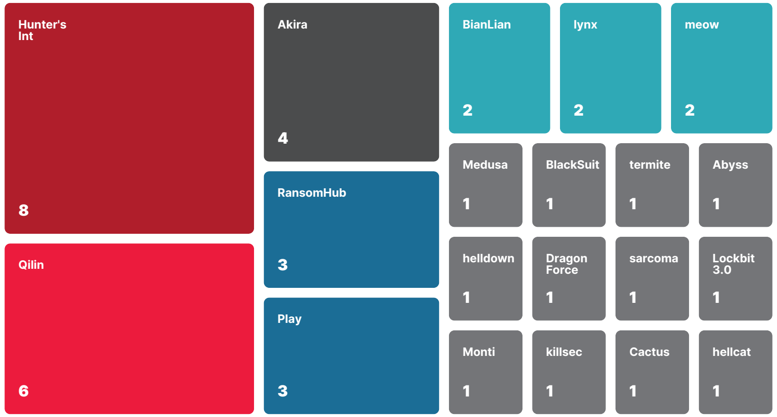


Figure 3. Ransomware groups targeting the energy and utilities sector and the number of attacks waged by each group in H2 2024

In our accompanying report, Energy and Utilities Deep Dive: Ransomware Threat Groups, we examine these threat groups in more detail.

The United States is the most often targeted country, accounting for 47% of the attacks followed by the European Union region (11%), Canada (8%), and United Kingdom (7%).

Top Countries Targeted

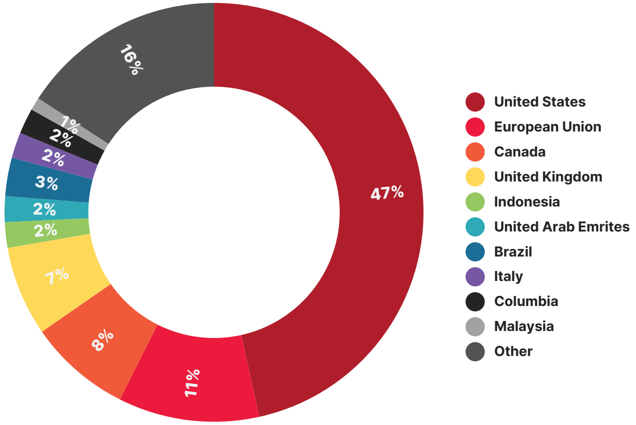


Figure 4. Countries and regions targeted by ransomware actors in the energy and utilities sector since H2 2022

Russian Hacking Group Claims Responsibility for Cyberattack on Indiana Wastewater Plant

April 2024, **StateScoop**

Mitigations to Reduce Risk

- **Implement Robust Network Segmentation:** Separate OT from IT networks to prevent lateral movement of attackers within systems. Limit access between critical systems and external networks, including the internet.

- **Invest in Threat Detection and Response Tools:** Deploy advanced intrusion detection systems (IDS) and intrusion prevention systems (IPS) tailored for OT environments. Leverage endpoint detection and response (EDR) solutions to monitor malicious activities across devices. Use security information and event management (SIEM) platforms for centralized visibility and real-time threat analysis.

- **Regularly Update and Patch Systems:** Ensure timely updates and patches for all software, firmware, and operating systems, especially legacy OT systems that are often overlooked. Establish a patch management schedule to systematically address vulnerabilities.

- **Conduct Regular Security Assessments:** Perform penetration testing to identify weaknesses in IT and OT networks. Undertake periodic risk assessments to evaluate and mitigate potential threats. Simulate phishing attacks to test employee awareness and response capabilities.

- **Enhance Employee Awareness and Training:** Provide regular cybersecurity training tailored to energy and utilities sector-specific threats. Educate employees on recognizing phishing attempts, social engineering tactics, and other common attack vectors. Create a culture of cybersecurity responsibility across all levels of the organization.

Ransomware Threat Groups

The Threat

We cover ransomware threat groups in more depth in our accompanying report. At a high level, here are some key points to consider:

While groups such as Conti, LockBit, Cl0p, and others dominate the headlines, our researchers wanted to shift the focus to lesser-known but active ransomware groups from the past year—specifically Play, 8Base, Hunters International, and Qilin—providing a comprehensive understanding of the evolving threat landscape.

Over the years, ransomware groups have shown resilience and adaptability, often dismantled by law enforcement only to reemerge under new identities. For example, the Conti group fractured in 2022 after internal leaks tied to differing views on the Russia-Ukraine war. Former members have since contributed to groups like BlackBasta, ALPHV/BlackCat, Royal, Akira, and Blacksuit. LockBit, one of the most prominent groups to rise in Conti's aftermath, continues to operate actively, regularly introducing new code and infrastructure despite takedown efforts.

Today's ransomware-as-a-service (RaaS) platforms are less concerned with targeting specific industries or regions and more focused on opportunistic, large-scale operations to extort payments in cryptocurrency. However, certain industries—such as healthcare, energy, and local government—remain more frequent victims due to their critical operations and higher likelihood of paying ransoms. Adding complexity is the role of affiliates and initial access brokers, whose motives may extend beyond financial gain, leveraging RaaS platforms to achieve broader objectives.

What Trustwave Is Seeing

A snapshot of each group's background is included below and intelligence on their operations, capabilities, victimology, and more can be found in our accompanying report.

Play

The Play ransomware group, also known as 'PlayCrypt', has been active since June 2022. They target a wide range of businesses and critical infrastructure across North America, South America, and Europe. By October 2023, the FBI estimated that around 300 entities had been impacted by this group.

8Base

8Base is a financially motivated RaaS affiliate program and data-extortion operation. Active since at least March 2022, they focus on stealing sensitive information for extortion purposes without deploying ransomware. They re-emerged under their current branding in early 2023 and became particularly active during the summer of 2023.

Hunters International

Hunters International is a financially motivated cybercriminal group operating under the RaaS model. They emerged in early October 2023, shortly after the Hive ransomware group was dismantled. They deny any direct affiliation with Hive, claiming to have independently acquired Hive's source code and infrastructure.

Qilin

Qilin is a ransomware group that has been active since early 2023. They are known for their sophisticated attack methods and their focus on high-value targets. The group has been linked to several high-profile attacks on critical infrastructure and large enterprises.

Mitigations to Reduce Risk

Noting the connection to the above section on ransomware trends, the recommended mitigations against these ransomware groups are the same as above.

- **Implement Robust Network Segmentation:** Separate OT from IT networks to prevent lateral movement of attackers within systems. Limit access between critical systems and external networks, including the internet.
- **Invest in Threat Detection and Response Tools:** Deploy advanced intrusion detection systems (IDS) and intrusion prevention systems (IPS) tailored for OT environments. Leverage endpoint detection and response (EDR) solutions to monitor malicious activities across devices. Use security information and event management (SIEM) platforms for centralized visibility and real-time threat analysis.
- **Regularly Update and Patch Systems:** Ensure timely updates and patches for all software, firmware, and operating systems, especially legacy OT systems that are often overlooked. Establish a patch management schedule to systematically address vulnerabilities.
- **Conduct Regular Security Assessments:** Perform penetration testing to identify weaknesses in IT and OT networks. Undertake periodic risk assessments to evaluate and mitigate potential threats. Simulate phishing attacks to test employee awareness and response capabilities.
- **Enhance Employee Awareness and Training:** Provide regular cybersecurity training tailored to energy and utilities sector-specific threats. Educate employees on recognizing phishing attempts, social engineering tactics, and other common attack vectors. Create a culture of cybersecurity responsibility across all levels of the organization.

Schneider Electric Reports Cyberattack, its Third Incident in 18 Months

November 2024, **CyberScoop**

IT/OT Convergence

The Threat

The convergence of IT and OT systems in the energy, utilities, and oil and gas sectors has created new opportunities for efficiency, automation, and innovation. By integrating these traditionally separate environments, organizations can optimize operations, improve decision-making through real-time data analytics, and enhance overall system performance. For example, predictive maintenance, remote monitoring, and automated control systems are now more accessible, leading to increased operational efficiency and reduced downtime.

However, this convergence has also introduced significant cybersecurity risks. IT systems, which typically handle business processes, data management, and communications, are often designed with flexibility, scalability, and remote access in mind. Meanwhile, OT systems, which control physical processes like power generation, distribution, and critical infrastructure, are generally more rigid and have been historically isolated from external networks to mitigate risks.

When these systems are integrated, they create new attack surfaces by connecting previously isolated, mission-critical OT systems to the broader IT ecosystem, including the Internet. This integration expands the potential for cyber threats, such as malware, ransomware, and data breaches, to compromise business operations and physical infrastructure.

Additionally, many OT systems are built on outdated software or legacy equipment that was not designed with modern cybersecurity standards in mind, or lack the ability to be patched, further increasing their vulnerability.

What Trustwave Is Seeing

Across Trustwave's energy and utilities clients, we observe a growing number of cybersecurity risks stemming from the increasing convergence of IT and OT systems. As these traditionally separate domains become more integrated, they introduce new vulnerabilities that cybercriminals can exploit.

Increased Attack Surface:

- **Connected Devices:** The proliferation of Internet of Things (IoT) devices in OT environments expands the attack surface, making it easier for attackers to gain access to critical systems.
- **Network Complexity:** Integrating IT and OT networks creates complex environments that are more difficult to secure and monitor.
- **Lack of Visibility:** Asset management and visibility remain major concerns in this sector. Organizations struggle to track where assets are located, what they have access to, and how they are interconnected, leaving critical gaps in security.

Vulnerabilities in OT Systems:

- **Legacy Systems:** Many OT systems are built on legacy technologies with outdated security protocols, making them vulnerable to exploitation.
- **Lack of Security Focus:** Traditionally, OT systems have prioritized reliability and safety over security, leaving them exposed to cyber threats.

Potential Consequences:

- **Physical Damage:** Successful cyberattacks on OT systems can lead to physical damage to infrastructure, equipment, or personnel.
- **Disruptions to Operations:** Attacks can cause disruptions to critical services, leading to power outages, supply shortages, or production halts.
- **Data Breaches:** Sensitive operational data, intellectual property, and customer information can be compromised.
- **Financial Loss:** Cyberattacks can result in significant financial losses due to damage, downtime, and potential legal liabilities.
- **Reputational Damage:** Security breaches can damage the reputation of companies and industries, leading to loss of customer trust and business opportunities.

Mitigations to Reduce Risk

- **Security Segmentation:** Isolating OT networks from IT networks can limit the potential impact of a breach.
- **Network Segmentation:** Dividing OT networks into smaller segments can reduce the attack surface and contain the spread of an attack.
- **Strong Access Controls:** Implementing robust access controls, such as multi-factor authentication (MFA) and role-based access, can prevent unauthorized access.
- **Regular Security Assessments:** Conducting regular vulnerability assessments and penetration testing can identify and address security weaknesses.
- **Employee Training:** Educating employees about cybersecurity best practices can help prevent human error, which is often a major factor in cyberattacks.
- **Incident Response Planning:** Developing a comprehensive incident response plan can help organizations respond effectively to cyberattacks and minimize their impact.

Volt Typhoon Hits Multiple Electric Utilities, Expands Cyber Activity

February 2024, **Dark Reading**

Evolving Regulatory Pressures

The Threat

As the energy, utilities, and oil and gas sectors continue to digitize and integrate new technologies, regulatory bodies have placed increasing emphasis on cybersecurity to protect critical infrastructure. While not a threat, as this section is labeled, the growing focus may significantly change the industry.

Given the critical nature of these sectors to national security, public safety, and economic stability, government agencies and industry groups are enacting and updating regulations to mitigate the growing cybersecurity risks. These regulatory frameworks aim to enforce compliance, enhance resilience, and create standardized security practices to safeguard against the rising tide of cyber threats.

Key Electricity Distributor in Romania Warns of 'Cyber Attack in Progress'

December 2024, **The Record**

What Trustwave Is Seeing

While not an exhaustive list, the national and regional regulations below are putting cybersecurity protocols at the forefront of the sector, with an increased focus on OT security, mandatory incident reporting, third-party risk management, and insurance requirements.

- **US: NERC CIP** (North American Electric Reliability Corporation - Critical Infrastructure Protection): NERC CIP is a set of cybersecurity standards designed to secure the North American bulk power system. These standards cover a range of cybersecurity topics, including access control, incident response, and recovery, among others. NERC CIP 013-1, for example, was specifically updated to address supply chain risks, making it clear that third-party cybersecurity risks are a growing concern in the energy sector. The latest version, CIP-013-1, requires companies to implement security controls to protect against supply chain vulnerabilities that could affect critical infrastructure.

- **US: Cybersecurity Maturity Model Certification** (CMMC): For contractors working with the US Department of Defense (DoD), the CMMC was introduced to evaluate the cybersecurity maturity of defense contractors in industries critical to national security, including energy and utilities. It sets requirements for cybersecurity controls at five levels of maturity, with compliance required to do business with the DoD.

- **EU and UK: NIS Directive** (Network and Information Security Directive): The EU's NIS Directive requires energy providers to implement robust cybersecurity measures and report significant incidents to national authorities. The directive has been a driving force in mandating critical infrastructure sectors (including energy and utilities) to improve their preparedness for cyberattacks. The directive applies to operators of essential services (OES) and digital service providers (DSPs,) and includes measures for risk assessment, incident management, and network resilience. The UK also implemented its own NIS regulations.

- **UK: The Digital Economy Act:** The UK government passed the Digital Economy Act to address evolving cybersecurity challenges, particularly regarding the increasing interconnectedness of IT and OT systems. This act mandates greater reporting of cybersecurity incidents and enforces higher standards of data protection for operators in sectors such as energy.
- **Australia: Critical Infrastructure Act** (SOCI): SOCI is a central piece of legislation aimed at securing critical infrastructure across several sectors, including energy, utilities, and oil & gas. The 2018 amendments introduced mandatory cybersecurity reporting for critical infrastructure providers, requiring them to notify the Australian government of cybersecurity incidents and to implement risk management plans. The government has also introduced penalties for non-compliance. This has placed a significant emphasis on ensuring that entities in critical sectors like energy and utilities maintain robust security frameworks to prevent cyberattacks.
- **The Oil and Gas Industry Security Regulations** (OGISR): The OGISR sets out specific rules for cybersecurity measures in the oil and gas industry, especially around offshore drilling, and exploration. These regulations focus on securing operational technology (OT) environments and mitigating risks posed by cyberattacks targeting critical systems like drilling rigs and production platforms.

Mitigations to Reduce Risk

To navigate this complex regulatory environment, energy companies must adopt a proactive approach to cybersecurity, including:

- **Risk Assessments:** Conducting regular risk assessments to identify and prioritize vulnerabilities.
- **Strong Cybersecurity Programs:** Implementing robust cybersecurity programs that address all aspects of the organization, including IT and OT systems.
- **Employee Training and Awareness:** Educating employees on cybersecurity best practices to reduce human error.
- **Incident Response Planning:** Developing and testing incident response plans to minimize the impact of cyberattacks.
- **Collaboration with Regulators:** Engaging with regulators to understand their expectations and seek guidance.

Threat Actor Techniques by Attack Stage

Data breaches and compromises come in many forms, but they often follow a similar pattern. Attackers gain access, escalate privileges, establish a foothold, steal, or destroy data, and then vanish. Trustwave SpiderLabs analyzed data from across our clients to understand the path that threat actors take within the energy and utilities industry and the techniques they deploy at each stage.

Initial Access Techniques

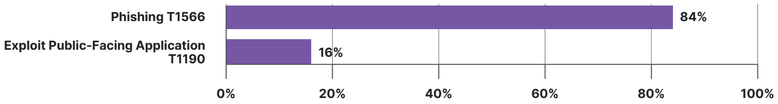


Figure 5: Initial access techniques used by attackers of energy and utilities providers

A majority of initial access techniques used by threat actors to gain entry to energy and utilities entities were phishing (84%). Following that, threat actors exploited public-facing applications (16%), such as F5 BIG-IP attacks relying mostly on Apache Log4J (CVE-2021-44228).

Execution Techniques

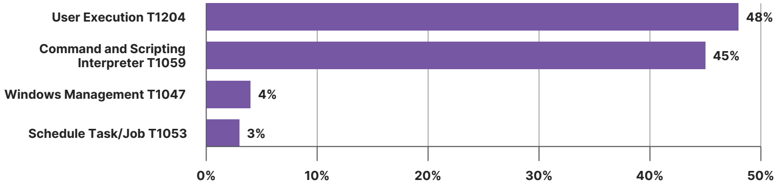


Figure 6: Execution techniques used by attackers of energy and utilities providers

In energy and utilities security incidents, execution techniques predominantly involved user execution of malicious files (48%). Adversaries often rely upon social engineering to convince users into executing malicious files and links. In a few cases, malicious Docker images were also noted. Attackers also used command and scripting interpreter techniques (45%), relying mostly on malicious uses of PowerShell and Unix Shell commands to execute or/and download payloads. Scheduled task creation (3%) involving malicious Microsoft Word documents and service execution using RemCom tools was also observed.

Credential Access Techniques

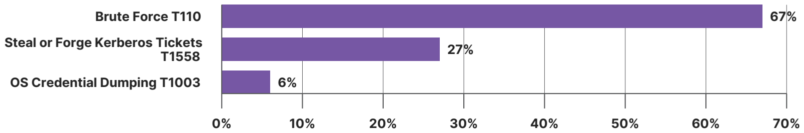


Figure 7: Credential access techniques used by attackers of energy and utilities

Credential access techniques observed in attacks against energy and utilities providers relied mostly on generic brute-force attacks against web-facing applications (67%), followed by Kerberoasting attempts (27%) and OS credential dumping attempts from LSASS memory using Mimikatz (6%). Forced authentication attempts - NTLM Relay Attacks on Active Directory Certificate Services (AD CS) using PetitPotam were also observed. In one of the incidents analyzed, attackers were able to access unsecured application credentials stored in registry.

Lateral Movement Techniques

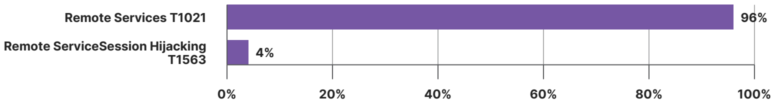


Figure 8: Lateral movement techniques used by attackers of energy and utilitiess

To move laterally within energy and utilities organizations, attackers predominantly relied on remote services (96%), mostly SMB/Windows Admin Shares, and also Remote Desktop Protocol (RDP). Remote service session hijacking attempts were also related to RDP. Use of alternate authentication material, or pass the ticket, was also observed.

Persistence Techniques

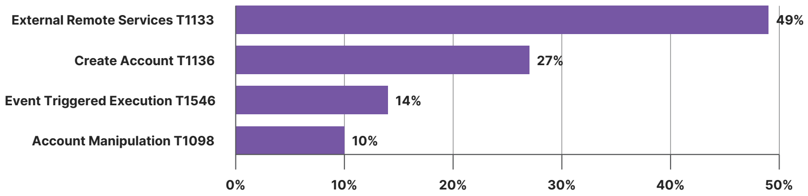


Figure 9: Persistence techniques used by attackers of energy and utilities providers

Lastly, the persistence techniques observed in the security incidents utilized mostly RDP (49%), local account creation (27%), account manipulation (10%), and event-triggered execution (14%); attackers attempted to hijack sticky keys binary (sethc.exe) and leverage Netsh helper DLL. Login Autostart Execution using registry Run Key and Startup Folder were also observed.

Costa Rica State Energy Company Calls in US Experts to Help with Ransomware Attack

December 2024, **The Record**

Conclusion & Key Takeaways

The energy and utilities sector faces a unique set of cybersecurity challenges, largely due to its critical role in powering national economies and global infrastructure. As the lines between OT and IT continue to blur, the sector finds itself increasingly vulnerable to sophisticated cyberattacks. The growing prevalence of ransomware, combined with aging infrastructure, and reliance on outdated systems, adds further complexity to the landscape. In addition, the sector's high geopolitical importance makes it a prime target for nation-state actors.

To navigate these challenges, energy and utility companies must prioritize cybersecurity at every level, ensuring that their operations are not only secure but also resilient to emerging threats.

Key Takeaways

- **Ransomware Threats:** Attacks targeting energy and utility providers have surged, making it clear that a robust cybersecurity strategy is essential to combating this persistent threat and minimizing its impact.
- **IT/OT Convergence:** While integrating IT and OT systems has unlocked greater efficiencies, it has also exposed critical infrastructure to new risks. A unified cybersecurity approach across both domains is now more important than ever.
- **Regulatory Compliance:** With stringent and evolving cybersecurity regulations in place, staying compliant is not just about avoiding penalties—it's also about reducing vulnerabilities and safeguarding the integrity of critical infrastructure.
- **Aging Infrastructure:** The sector's reliance on outdated technologies creates significant security gaps. To stay ahead of modern threats, companies must invest in upgrading systems and enhance collaboration between IT and OT teams.
- **Geopolitical Significance:** The energy sector's strategic importance makes it a prime target for state-sponsored cyberattacks. Providers must be ready to defend against highly sophisticated threats that are as much about national security as they are about financial gain.

By addressing these key areas, energy and utility providers can better prepare for the evolving cyber threat landscape. Strengthening defenses, investing in new technologies, and maintaining a proactive security strategy will help ensure the continued reliability and safety of operations, even in the face of growing risks.

Trustwave®