# **The Contemporary Cyber Threat Landscape: An In-Depth Analysis of the Energy Sector in July 2025**

## **1. Executive Summary: July 2025 in Review**

The threat landscape targeting the global energy sector experienced a notable acceleration in complexity and frequency in July 2025. This month was defined by a critical confluence of heightened geopolitical tensions and the continued technological convergence of information technology (IT) and operational technology (OT). Analysis of incidents reveals a dynamic environment where financially motivated ransomware groups have become more aggressive, while sophisticated nation-state actors are engaging in long-term espionage and strategic "prepositioning" for potential future disruption.

Key incidents in July highlighted the profound and often underestimated financial and operational risks associated with this evolving threat. Attacks on critical infrastructure, such as the Nova Scotia Power billing systems and the municipal IT network of St. Paul, Minnesota, demonstrated how digital compromises can lead to tangible, real-world consequences and widespread service outages. The month's most active threats were financially motivated ransomware groups, with new players like Qilin and INC Ransom leading in victim count. At the same time, critical vulnerabilities in widely used enterprise software became primary entry points for both criminal and state-sponsored campaigns. The evidence points to a strategic imperative for energy sector leadership to move beyond traditional, perimeter-focused security models. Defenses must now be built on a foundation of proactive, risk-aware, and highly segmented architectures that secure the entire enterprise, from the IT network down to the most critical OT environments.

## **2. The Evolving Threat Ecosystem: Actors and Motivations**

### **2.1. Geopolitical Drivers: The New Generation of Cyberwarfare**

Contemporary cyber threats to the energy sector are no longer isolated criminal acts but are often directly influenced by global geopolitical dynamics. Global energy security has returned to the forefront of international competition, and this friction is consistently reflected in cyberspace.1 Ongoing conflicts, such as the Russo-Ukraine war and instability in the Middle East, along with the "great power struggle" between the U.S. and China, are creating a permissive environment for cyber operations against critical infrastructure.2 The U.S. Department of Energy has warned that the energy infrastructure is facing "unprecedented threat levels".3

This environment has given rise to what some have termed a "new generation of warfare," where rival nations attempt to demonstrate their cyber-military capabilities by penetrating the critical infrastructure of their opponents and their allies.2 A significant portion of these activities are not immediately destructive but are driven by a long-term strategic objective. Up to a third of breaches in the energy industry are attributed to espionage.3 This involves threat actors, particularly those linked to China, Iran, North Korea, and Russia, engaging in campaigns to maintain persistent access and conduct network discovery, a process known as "prepositioning" for future disruptive actions.2 This sophisticated, patient approach means that a compromise may lie dormant for months or even years before an adversary chooses to activate their malicious payload. This long-term strategic imperative forces energy companies to consider a threat model that extends far beyond immediate financial gain.

The increasing professionalization of the cybercrime ecosystem has also introduced a critical layer of complexity to this geopolitical calculus. While a clear line has historically been drawn between financially motivated cybercriminals and politically motivated nation-state actors, the evidence suggests a blurring of these roles. Threat intelligence analysis indicates that the role of cybercriminal actors may be significant in enabling larger, state-sponsored campaigns by providing the necessary infrastructure and resources for offensive cyber operations.2 This means that a seemingly "simple" ransomware attack could, in fact, be a proxy operation or a cover for a more clandestine nation-state objective. This complex interplay makes definitive attribution an immense challenge and requires organizations to consider the full spectrum of motivations behind any given cyber incident, regardless of its initial appearance.

### **2.2. Threat Actor Taxonomy: A Blurring of Lines**

The threat ecosystem targeting the energy sector is diverse and highly segmented, comprising a range of actors with varying motivations and capabilities.

* **Financially Motivated Actors**: Ransomware-as-a-Service (RaaS) groups remain the most prominent and prolific threat. In July 2025, new data from Cyble indicated that Qilin led all ransomware activity for the third time in four months, claiming responsibility for 73 victims, or approximately 17% of the total reported attacks for the month.5 This group capitalized on the decline of a previous leader, RansomHub, to take the top spot. Other financially motivated groups identified as actively targeting the sector include RansomHub/DragonForce and HellCat.2 Their primary motivation is monetary, with ransomware attacks accounting for 44% of non-social engineering-based attacks.3
* **Nation-State APTs**: These are sophisticated, well-resourced actors with strategic objectives. The Lazarus Group, a North Korean-linked advanced persistent threat (APT) actor, is a prominent example. This group is unique in that it prioritizes both financial gain and political objectives, engaging in espionage, sabotage, and disruption.2 Another notable nation-state actor is Volt Typhoon, an APT attributed to China. Active since mid-2021, this group focuses on long-term espionage and network discovery, primarily in critical infrastructure, using "living-off-the-land" techniques to maintain access without being detected.4
* **Hacktivist Groups**: These actors are driven by ideological motivations rather than financial or state-sponsored goals. Groups like S16 and Noname057(16) are identified as actively targeting the energy sector.2 Some of these adversaries may be motivated by their opposition to climate change, seeing the energy industry as unethical, and they often seek to build credibility by publicizing alleged compromises of OT networks.2

## **3. Attack Campaign Retrospective: Key Incidents of July 2025**

July 2025 was marked by several high-profile cyber incidents that underscored the primary vectors of attack and the tangible impact on critical infrastructure and its supply chain.

### **3.1. Ransomware Dominance and New Players**

The month's data confirmed the sustained and increasing threat of ransomware. According to the Cyble 'Ransomware Landscape July 2025' update, the U.S. was the most attacked country with 223 victims, a number eight times greater than the second-place country, Canada.5 Qilin led all ransomware activity with 73 victims, followed by INC Ransom with 59.5 The INC Ransom group claimed responsibility for cyberattacks targeting a U.S.-based provider of advanced power transmission and distribution solutions, as well as a Canadian firm specializing in underwater infrastructure inspections and maintenance for industries like hydro, nuclear, oil, and gas.5 The frequency of attacks across various critical infrastructure sectors, including energy and utilities, demonstrates that no component of the energy value chain is immune to this threat.5

### **3.2. Significant Critical Infrastructure Compromises**

Several attacks in July had significant, real-world consequences, demonstrating the severity of the threat.

* **Nova Scotia Power**: This incident illustrates the long-term nature of many compromises. While the public impact and disclosure occurred in July 2025, the company confirmed that hackers had access to their systems from as early as March 19 to April 25.9 The attack did not cause a power outage but disrupted communication between customer power meters and internal billing systems, forcing the company to issue estimated bills.10 The breach also resulted in the theft of sensitive personal data, including names, dates of birth, social insurance numbers, and bank account details, affecting approximately 280,000 customers.9 This event highlights a crucial disconnect: the initial compromise and exfiltration of data can occur months before the public-facing consequences become apparent. This underscores the inadequacy of a purely reactive security posture and emphasizes the need for continuous monitoring and threat hunting to detect dormant adversaries before they can activate their malicious objectives.
* **St. Paul, Minnesota**: A "deliberate, coordinated, digital attack" on the city's municipal IT systems forced a complete shutdown of all services. The incident was severe enough to require the deployment of the National Guard's cyber protection unit to assist with recovery.12 This attack serves as a stark reminder of the physical impact of a digital compromise, as the city experienced widespread service outages.
* **SolarView Energy**: On July 30, 2025, this company suffered a zero-day DLL supply-chain attack through its SV-Manager auto-update feature. The injected malware enabled credential theft and compromised over 1 million records, causing estimated losses of $4 million and escalating risks for the company's partners.12

### **3.3. Supply-Chain and Software Ecosystem Compromises**

The energy sector's reliance on a complex web of third-party vendors and software makes the supply chain a critical attack vector. The Ingram Micro attack by the SafePay ransomware group is a prime example. The attack, which forced the global IT distributor to shut down core systems, was initiated by breaching a GlobalProtect VPN and resulted in the exfiltration of 3.5 TB of sensitive data.5 The attack caused significant disruption to the global tech supply chain, impacting distribution, licensing, and API infrastructure for days.12 This incident, along with the SolarView Energy breach, demonstrates that a single point of failure in a third-party vendor or software update process can have cascading effects on the entire ecosystem, including energy companies that rely on those products and services.

**Table 1: July 2025 Major Incident Timeline**

| Incident | Victim | Date of Attack | Attack Type | Initial Impact |
| --- | --- | --- | --- | --- |
| **Nova Scotia Power** | Canadian utility | March 19 - April 25, 2025 (Dwell Time) | Ransomware, Data Breach | Billing system disruption, data theft of 280,000 customers' PII. |
| **Ingram Micro** | IT solutions distributor | July 3, 2025 | Ransomware (SafePay) | 3.5 TB data exfiltration, shutdown of core systems, supply-chain disruption. |
| **St. Paul, MN** | Municipal government | July 2025 | Coordinated digital attack | City-wide IT systems shutdown, widespread service outages. |
| **SolarView Energy** | Energy company | July 30, 2025 | Supply-chain attack (Zero-day DLL) | Credential theft, compromise of 1M+ records, $4M loss. |

## **4. Technical Vulnerabilities and Observed TTPs**

Threat actors' success in July 2025 was largely predicated on the exploitation of known vulnerabilities and the use of sophisticated tactics, techniques, and procedures (TTPs) to gain and maintain access.

### **4.1. Exploitation of Public-Facing Applications**

A recurring theme in July was the targeting of public-facing applications and remote services as a primary initial access vector. A critical buffer overread vulnerability, dubbed "Citrix Bleed 2" (CVE-2025-5777), was actively exploited in the wild, leading to a sharp increase in exploitation attempts and an unprecedented 24-hour patch mandate from CISA for federal agencies.13 This flaw allowed unauthenticated remote attackers to retrieve sensitive data, including credentials and session tokens, from the server's memory.13

Other significant vulnerabilities exploited during the month included a SQL injection bug in FortiWeb (CVE-2025-25257) and critical zero-day vulnerabilities in on-premises Microsoft SharePoint (CVE-2025-53770/53771) used by Chinese-linked hackers to compromise U.S. federal agencies.12 The continued presence of these unpatched, high-severity flaws in enterprise software highlights a persistent security gap that adversaries are systematically leveraging to achieve their objectives.

### **4.2. TTPs Across the Attack Chain**

The TTPs observed in July 2025 demonstrate a playbook that is both opportunistic and highly sophisticated.

* **Initial Access**: Social engineering tactics, such as sustained phishing campaigns, are responsible for a significant 86% of cyberattacks against the energy industry.3 Beyond phishing, threat actors gain initial access by exploiting vulnerabilities in internet-facing applications (T1190) like the Citrix and FortiWeb flaws.14 They also use methods like drive-by compromise via malicious websites disguised as updates and exploiting vulnerable VPN platforms.15
* **Defense Evasion and Persistence**: Once inside a network, adversaries use legitimate remote access tools like AnyDesk and PsExec (T1219) to blend in with normal network activity and evade detection.17 They employ techniques to clear event logs (T1070.001) and use innocuous file names for malicious components, such as  
  Windows.exe, to avoid scrutiny.21
* **Lateral Movement and Credential Access**: To move deeper into the network, attackers dump credentials using tools like Mimikatz (T1003) and use stolen credentials to access other systems via Remote Desktop Protocol (RDP).16 These actions allow them to escalate privileges and access more sensitive parts of the network, which is a common step before deploying ransomware or exfiltrating data.

### **4.3. Command and Control (C2) Infrastructure**

A fundamental component of any successful cyberattack is the command and control (C2) infrastructure, which allows attackers to maintain persistent, covert communication with compromised devices.23 This channel is used to issue new instructions, download additional malware, and exfiltrate stolen data.23

The analysis of C2 in July revealed a significant shift in adversary behavior. Attackers are increasingly moving away from dedicated, easily blockable infrastructure and are instead "living off the cloud." Campaigns observed during the month utilized legitimate, widely used services to establish C2 communication, such as Cloudflare Tunnel and ngrok.14 North Korean actors, for example, have also been known to use the Telegram API for C2 communications, which further complicates detection.8 Because these services are often essential for legitimate business operations and may not be blocked by default, they provide attackers with a path of least resistance to maintain persistence and evade traditional perimeter defenses. This development necessitates a move from simple IP and domain blocklists to more advanced behavioral analytics that can detect the anomalous use of trusted services and protocols.

**Table 2: Summary of Key CVEs, IOCs, and TTPs (July 2025)**

| CVE/Vulnerability | Affected Product | MITRE ATT&CK Mappings | Example IOCs (July 2025) |
| --- | --- | --- | --- |
| **CVE-2025-5777** | Citrix NetScaler ADC/Gateway | T1190, T1185, T1133, T1003 | Observed C2: 88.99.215.73:4443 (TLS) |
| **CVE-2025-25257** | Fortinet FortiWeb | T1190, T1546.003, T1567.002 | Malicious Web-shell SHA-256: 66d4ee5... |
| **CVE-2025-53770/53771** | Microsoft SharePoint | T1190, T1059.001, T1562.001 | Persistent back-door access after patching. |
| **INC Ransom** | Power/Utilities Firms | T1486 (Data Encrypted for Impact) | Claimed attack on a U.S. power transmission provider. |
| **SafePay Group** | Ingram Micro | T1190, T1486, T1041 | VPN exploitation, data theft, leak site threats. |
| **Interlock Group** | Energy, Manufacturing | T1566.002, T1204.002, T1071.004 | Cloudflare Tunnel host: intops-jl4c1s.trycloudflare.com |

## **5. Quantified and Operational Impact**

The consequences of cyberattacks against the energy sector extend far beyond the immediate technical compromise. Analysis of recent data and incidents reveals a financial and operational impact that is both staggering and often underestimated.

### **5.1. Financial Fallout: Moving Beyond Direct Costs**

The financial exposure to OT cyber risk is projected to be immense. A recent Dragos-Marsh McLennan report, titled '2025 OT Security Financial Risk Report,' estimates that global OT cyber risk exposure could exceed **$300 billion** annually, with business interruption costs alone accounting for over **$172 billion**.25 This analysis, based on tens of thousands of simulations, indicates that indirect losses often account for as much as 70% of OT-related breaches and are a primary driver of risk.25

This disparity between direct and indirect costs is a critical element of risk management. For example, while a ransom demand may be in the millions, as was the case with the Colonial Pipeline incident 27, the true cost to the company and the economy is exponentially greater. The Colonial Pipeline attack, which targeted the company's IT billing system, forced a precautionary shutdown of the entire pipeline, causing widespread gasoline shortages and consumer panic across the Southeastern U.S..3 The cost was not the ransom payment itself but the business interruption, supply chain disruption, and resulting reputational damage.27 This illustrates a fundamental shift in risk: the financial impact is no longer limited to a ransom payment or the cost of data theft but is increasingly defined by the economic and social consequences of operational disruption.

The average cost of a data breach to a business in 2024 was over **$4.8 million**, a 10% increase from the previous year and the highest total ever recorded.25 Specific incidents from July 2025 provide a tangible scale for these costs. The supply-chain attack on SolarView Energy, for example, resulted in an estimated loss of

**$4 million** and compromised over 1 million records.12 These figures underscore the urgent need for executives to adopt a more comprehensive risk model that quantifies these indirect and systemic losses.

### **5.2. Operational Disruption and Cascading Effects**

The most significant consequence of cyberattacks on the energy sector is the translation of a digital compromise into a physical-world event. The convergence of IT and OT networks, driven by digitalization and the adoption of technologies like the Industrial Internet of Things (IIoT), has expanded the attack surface and created new vectors for disruption.2

* **Service Outages**: The Nova Scotia Power attack, while not causing a power outage, demonstrated that a cyber incident can still severely disrupt core services. The compromise of customer billing and communication systems impacted 280,000 customers and required manual intervention to restore functionality.9 Similarly, the "deliberate, coordinated, digital attack" on the city of St. Paul's IT network led to a complete shutdown of municipal services.12
* **Supply Chain Disruption**: The attacks on Ingram Micro and SolarView Energy show how a breach in one part of the supply chain can cripple a much larger ecosystem. These incidents disrupted core services and introduced risks to downstream partners, potentially slowing the deployment of critical technology needed for the ongoing energy transition.12
* **The Path of Least Resistance**: While OT-specific malware designed to cause physical damage is rare (with only nine publicly tracked cases), the incidents from July 2025 and historically, such as the Colonial Pipeline attack, reveal a strategic shift by adversaries. It is far easier and more common for a threat actor to compromise the less secure IT network via social engineering or unpatched vulnerabilities and then force a precautionary shutdown of the more critical OT systems.3 This highlights a crucial security vulnerability: attackers have found a low-effort, high-impact method to cause physical disruption by leveraging the interconnectedness of modern energy systems. Defenses must be architected to prevent an IT-level compromise from cascading into a critical operational shutdown.

**Table 3: Financial and Operational Impact Metrics**

| Metric | Value/Description | Source |
| --- | --- | --- |
| **Global OT Cyber Risk (Worst-Case)** | Exceeds $300 billion annually, with business interruption costs of over $172 billion. | 25 |
| **Average Cost of Data Breach (2024)** | Over $4.8 million, a 10% increase from the previous year. | 28 |
| **SolarView Energy Attack Loss** | Estimated $4 million in losses and over 1 million records stolen. | 12 |
| **Nova Scotia Power Impact** | Affected 280,000 customers with billing and data theft, with a dwell time of several months. | 9 |
| **Ransomware Attacks (July 2025)** | 423 total attacks reported, with the U.S. being the primary target (223 victims). | 5 |

## **6. Strategic Outlook and Defensive Recommendations**

The events of July 2025 reinforce that the cyber threat to the energy sector is not a theoretical risk but a persistent, evolving, and highly consequential challenge. To secure energy resilience and economic prosperity, a fundamental shift in cybersecurity strategy is required.

### **6.1. The IT/OT Nexus: Securing the Converged Enterprise**

The ongoing digitalization of the energy sector has blurred the lines between traditionally isolated IT and OT networks, creating both efficiencies and profound security vulnerabilities.2 To manage this risk, organizations must abandon the outdated siloed approach to security. The most effective controls for mitigating OT risk are not complex new technologies but a return to fundamentals, strategically applied. The Dragos-Marsh McLennan report found that incident response planning, defensible architecture, and ICS network visibility and monitoring are the top three controls most strongly correlated with risk reduction.25 Organizations should adopt and enforce a defensible architecture that includes robust network segmentation and microsegmentation to limit an adversary's ability to move laterally from the IT network into critical OT systems.30 The Department of Energy's Cybersecurity Capability Maturity Model (C2M2) provides a vetted framework for evaluating and improving an organization's cybersecurity posture for both IT and OT assets.32

### **6.2. The Role of Emerging Technologies**

Emerging technologies like artificial intelligence (AI) present a dual-use challenge and opportunity. While AI is being leveraged by attackers to create sophisticated phishing campaigns and impersonate officials for high-stakes social engineering attacks, it is also a game-changer for defense.12 AI-driven security systems can process vast amounts of data in real-time to detect anomalies, predict potential breaches, and automate responses, thereby significantly reducing the risk of attacks.28 A strategic defense should integrate AI as a critical component to improve operational performance and provide a proactive, adaptive layer of defense against a rapidly evolving threat landscape.28

### **6.3. Compliance and Regulatory Imperatives**

Governments and regulatory bodies are taking increasingly decisive action to protect critical infrastructure. The EU's NIS2 Directive and the UK's National Cyber Strategy impose stricter obligations on energy companies to enhance their security frameworks.28 Rather than viewing these as compliance burdens, forward-thinking organizations should treat regulation as a catalyst for innovation. These frameworks provide a clear roadmap for achieving a more transparent, secure, and resilient infrastructure, ultimately strengthening the organization's overall cybersecurity posture.29

### **6.4. Actionable Recommendations for Executive Leadership**

Based on the threat intelligence from July 2025, the following strategic and tactical recommendations are essential for energy sector organizations:

* **Prioritize Patching and Vulnerability Management**: Immediately remediate all vulnerabilities on CISA's Known Exploited Vulnerabilities (KEV) Catalog, particularly those affecting public-facing applications and VPNs, as these are primary initial access vectors for threat groups.14 A risk-based approach should be adopted to prioritize flaws that adversaries are actively exploiting.25
* **Enhance Supply Chain Vigilance**: The SolarView and Ingram Micro incidents underscore the critical risk posed by third-party vendors. Organizations should perform continuous audits and monitoring of all supply-chain software, with a specific focus on the security of auto-update mechanisms.12
* **Invest in Resilience, Not Just Defense**: Shift security investment from a purely defensive mindset to one that prioritizes resilience. The top three risk-reducing controls—incident response planning, defensible architecture, and ICS network visibility—should be at the top of the agenda.25 Develop and regularly test a comprehensive incident response plan that accounts for both IT and OT environments.31
* **Develop the Cyber Workforce**: Address the 42% shortfall in cybersecurity personnel by investing in awareness and training for all employees.33 This is crucial, as social engineering tactics, particularly phishing, remain the most common initial entry point into an organization.3
* **Implement Robust Controls**: Mandate phishing-resistant multi-factor authentication (MFA) for all services and enforce strong password policies.17 Implement continuous network monitoring with behavioral analytics to detect the use of legitimate C2 services like Cloudflare Tunnel, as this is a key indicator of post-compromise activity.14

#### Works cited

1. Energy security amid shifting geopolitics - YouTube, accessed August 14, 2025, <https://www.youtube.com/watch?v=PAQuIK1Itb0>
2. Resecurity warns of increased cyber threats to energy and nuclear ..., accessed August 14, 2025, <https://industrialcyber.co/utilities-energy-power-water-waste/resecurity-warns-of-increased-cyber-threats-to-energy-and-nuclear-facilities-from-hacktivists-and-nation-states/>
3. Cyber Security Threats in the Energy Sector | Verizon Business, accessed August 14, 2025, <https://www.verizon.com/business/resources/articles/s/cyber-security-threats-in-the-energy-sector/>
4. The Attribution Dividend: Protecting Critical Infrastructure from Cyber ..., accessed August 14, 2025, <https://www.swp-berlin.org/10.18449/2024C46/>
5. Cyble reveals US primary target with 223 ransomware victims amid rising attacks on critical infrastructure - Industrial Cyber, accessed August 14, 2025, <https://industrialcyber.co/critical-infrastructure/cyble-reveals-us-primary-target-with-223-ransomware-victims-amid-rising-attacks-on-critical-infrastructure/>
6. Qilin Leads Ransomware Groups Attacks for July 2025 - Cyble, accessed August 14, 2025, <https://cyble.com/blog/ransomware-groups-july-2025-attacks/>
7. industrialcyber.co, accessed August 14, 2025, <https://industrialcyber.co/utilities-energy-power-water-waste/resecurity-warns-of-increased-cyber-threats-to-energy-and-nuclear-facilities-from-hacktivists-and-nation-states/#:~:text=The%20most%20prominent%20threat%20actors,(16)%20(hacktivist).>
8. Dark Web Profile: Lazarus Group - SOCRadar® Cyber Intelligence Inc., accessed August 14, 2025, <https://socradar.io/apt-profile-who-is-lazarus-group/>
9. Nearly 300000 people were impacted by cyberattack on Nova Scotia Power - The Record, accessed August 14, 2025, <https://therecord.media/thousands-impacted-cyber-nova-scotia>
10. Weekly Cybersecurity Intelligence Report Cyber Threats & Breaches: July 02-09, 2025, accessed August 14, 2025, <https://firecompass.com/weekly-cybersecurity-intelligence-report-cyber-threats-breaches-july-02-09/>
11. Nova Scotia Power Confirms Ransomware Attack and Data Breach Impacting 280,000 Customers - Cyber Syrup, accessed August 14, 2025, <https://www.thecybersyrup.com/p/nova-scotia-power-confirms-ransomware-attack-and-data-breach-impacting-280-000-customers-5e13>
12. The 5 Biggest Cybersecurity Stories for July 2025 in the US - Nwaj ..., accessed August 14, 2025, <https://nwajtech.com/5-biggest-cybersecurity-stories-for-july-2025/>
13. FortiGuard Labs - Threat Intelligence Platform - Fortinet, accessed August 14, 2025, <https://www.fortinet.com/fortiguard/labs>
14. July 2025 Cyber Breaches: RCE, RAT, Supply Chain Attacks, accessed August 14, 2025, <https://firecompass.com/weekly-cybersecurity-intelligence-report-cyber-threats-breaches-july-09-16/>
15. July 2025 Cybersecurity News Recap - SWK Technologies, accessed August 14, 2025, <https://www.swktech.com/july-2025-cybersecurity-news-recap/>
16. Ghost (Cring) Ransomware Analysis, Simulation, and Mitigation - CISA Alert AA25-050A, accessed August 14, 2025, <https://www.picussecurity.com/resource/blog/ghost-ransomware-analysis-cisa-alert-aa25-050a>
17. Akira Ransomware Analysis, Simulation and Mitigation- CISA Alert AA24-109A, accessed August 14, 2025, <https://www.picussecurity.com/resource/blog/akira-ransomware-analysis-simulation-and-mitigation-cisa-alert-aa24-109a>
18. Interlock Ransomware Analysis, Simulation, and Mitigation - CISA Alert AA25-203A, accessed August 14, 2025, <https://www.picussecurity.com/resource/blog/cisa-alert-aa25-203a-interlock-ransomware-analysis>
19. Feds Issue Interlock Ransomware Warning as Healthcare Attacks Spike, accessed August 14, 2025, <https://www.hipaajournal.com/interlock-ransomware-alert-2025/>
20. #StopRansomware: Medusa Ransomware | CISA, accessed August 14, 2025, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-071a>
21. #StopRansomware: RansomHub Ransomware | CISA, accessed August 14, 2025, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a>
22. #StopRansomware: Ghost (Cring) Ransomware | CISA, accessed August 14, 2025, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-050a>
23. What is C2? Command and Control Infrastructure Explained - Varonis, accessed August 14, 2025, <https://www.varonis.com/blog/what-is-c2>
24. Understanding Command & Control (C2) Infrastructure | Blog - VulnCheck, accessed August 14, 2025, <https://vulncheck.com/blog/understanding-command-control-infrastructure>
25. OT cyber risk could exceed $300 billion, pushed by indirect losses ..., accessed August 14, 2025, <https://industrialcyber.co/risk-management/ot-cyber-risk-could-exceed-300-billion-pushed-by-indirect-losses-and-cascading-system-failures/>
26. Significant OT cyber incident costs could exceed $300B | SC Media, accessed August 14, 2025, <https://www.scworld.com/brief/significant-ot-cyber-incident-costs-could-exceed-300b>
27. Growing Ransomware Threats to the Energy Sector - CyberSaint, accessed August 14, 2025, <https://www.cybersaint.io/blog/growing-cyber-threats-to-the-energy-sector>
28. Growing cybersecurity threats in the energy sector and how businesses stay resilient, accessed August 14, 2025, <https://www.renewableuk.com/news-and-resources/guest-blog/growing-cyber-security-threats-in-the-energy-sector-and-how-businesses-stay-resilient/>
29. Q3 2025: 7 Embedded Software Trends Powering Smarter Energy Systems - Wirtek, accessed August 14, 2025, <https://www.wirtek.com/blog/q3-2025-7-embedded-software-trends-powering-smarter-energy-systems>
30. Was the 2025 Power Outage a Cyberattack? Full Analysis of Infrastructure Threats, accessed August 14, 2025, <https://www.webasha.com/blog/was-the-power-outage-a-cyberattack-full-analysis-of-infrastructure-threats>
31. RansomHub: Analyzing the TTPs of One of the Most Notorious Ransomware Variants of 2024 - Picus Security, accessed August 14, 2025, <https://www.picussecurity.com/resource/blog/ransomhub>
32. Cybersecurity Capability Maturity Model (C2M2) - Department of Energy, accessed August 14, 2025, <https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2>
33. Why the energy transition means more cyberattacks | Spectra by MHI, accessed August 14, 2025, <https://spectra.mhi.com/why-the-energy-transition-means-more-cyberattacks>
34. Joint Advisory: Medusa Ransomware Impacted 300 Critical Infrastructure Victims | Industrial Defender OT/ICS Cybersecurity Blog, accessed August 14, 2025, <https://www.industrialdefender.com/blog/medusa>