RELIAQUEST®

Threat Landscape Report
Uncovering Critical Cyber Threats to Utilities

Date: November 1, 2023 – October 31, 2024

Top MITRE ATT&CK Techniques

81% of Utilities Alerts Involve Spearphishing

During the reporting period of November 2023 to October 2024, threat actors targeting the utilities sector relied on a disproportionately limited range of techniques, as revealed by GreyMatter data. Around **81%** of alerts from utilities customers involved **spearphishing**—whether internal (T1534), with links (T1566.002), or with attachments (T1566.001). This figure is significantly higher than the **23%** observed across all sectors during the same period, highlighting a unique vulnerability within the utilities sector.

This trend is likely explained by the unusual position of utilities employees, who often have access to both IT and operational technology (OT) environments. With their legacy infrastructure and critical need to avoid downtime, OT systems typically have weaker cybersecurity defenses. This means attackers can use spearphishing to more easily exploit these vulnerabilities. Once they've compromised a less secure OT system, they can then pivot to a more fortified IT environment, effectively bypassing its stronger security measures.

Armed with access to an organization's IT and OT systems, adversaries can exploit vulnerabilities on multiple fronts, potentially even gaining control over critical infrastructure. This access is a significant concern for utilities companies, as it presents various risk scenarios. In the short term, attackers could disrupt essential services like electricity and water supply, causing immediate societal and economic chaos. Alternatively, threat actors might choose to remain undetected within these systems, mapping out the architecture for potential future sabotage at strategically chosen times.

Sector Overview

The utilities sector saw a 42% surge in ransomware incidents over the past year. Ransomware groups such as "Play" are likely concentrating their attacks on this sector because of the need for utilities organizations to always be operational.

Characterized by a complex blend of IT and operational technology (OT) technologies, the utilities sector is also particularly susceptible to spearphishing attacks. Our data reveals that 81% of all true-positive alerts for our utilities customers are related to spearphishing, compared to just 23% across other sectors.

The sector's OT environments face specific risks due to existing vulnerabilities, as these systems often rely on legacy infrastructure that can be challenging to update. Utilities organizations should invest in automated responses, defense-in-depth strategies, and employee education to best protect against these risks. ReliaQuest customers who've adopted automated incident response have managed to contain threats in just two minutes, compared to 21 hours with manual responses.

Recommendations

While it seems simple, teaching employees to spot and report phishing emails really is a key defense against this threat, ensuring attacks can't progress any further.

Exploiting Third-Party Links: Internal Spearphishing in Utilities

Internal spearphishing came in at second place in our dataset, which likely reflects utilities organizations' close cooperation with a wide array of contractors and third parties. Employees in the sector frequently receive emails from numerous different senders, which may lead to reduced vigilance when interacting with unfamiliar messages, particularly those that appear to come from trusted sources. This makes it easier for phishing emails to slip through unnoticed. In addition, external parties or temporary contractors within utilities organizations may lack the security awareness of permanent employees. They might miss suspicious elements in apparently internal emails and be more likely to click on malicious links.

Organizations shouldn't underestimate the potential consequences of a phishing attack. When attackers gain access through successful phishing attempts, they can steal intellectual property (IP), jeopardizing a company's competitive advantage. Competitors or malicious entities could use this stolen IP to replicate proprietary technologies, undermining years of research and investment.

Recommendations

Internal spearphishing attacks can be hard to tackle and can't be easily mitigated with preventive measures. However, we advise utilities organizations to regularly analyze network traffic for any anomalies, such as unexpected data flows or processes that don't typically communicate over the network. We also recommend implementing advanced email security measures like GreyMatter Phishing Analyzer, which can analyze suspicious emails, take automated remedial actions, and promptly alert your security operations team about email-based malicious activities.

Utilities Sector Faces Unique DNS Challenges

While the **DNS application layer protocol** (T1071.004) didn't make the top five MITRE ATT&CK techniques for other sectors, it featured in almost **10%** of alerts in the utilities sector. This can be attributed to utilities companies frequently prioritizing the prevention of system downtime. For instance, US government regulations mandate reporting any disruptions exceeding 15 minutes and providing the necessary documentation.[1] Although these regulations emphasize safety, they can inadvertently result in unmonitored DNS traffic, as organizations singularly focus on maintaining uptime. In addition, the sector's extensive use of Internet of Things (IoT) devices, each generating DNS queries for communication, adds to the volume and complexity of DNS traffic. This increased traffic makes effective monitoring more challenging, allowing adversaries to establish secret command-and-control (C2) channels and maintain prolonged persistence in networks.

Once C2 channels are secured, this gives attackers the ability to severely disrupt operations, potentially causing failures in critical services like power distribution or water supply. These outages would likely require costly repairs, but could also increase operational expenses, impact revenue, and strain budgets. This tighter budget could force affected companies to reallocate resources, potentially leading to cuts in other areas. In severe cases, this financial pressure could result in staff layoffs in an attempt to balance budget with financial stability. The loss of skilled employees, especially in IT departments, can further exacerbate operational challenges and increase vulnerability to future cyber attacks.

Recommendations

To combat DNS-based C2 threats, implement DNS logging and analysis, which provides visibility into suspicious activities and allows for early detection and response. Deploy DNS security tools to automatically intercept and block malicious queries, preventing attackers from maintaining control over compromised systems. Ensure IoT devices are regularly updated and patched to close security gaps and reduce the risk of them being used as entry points for attacks.

MITRE ATT&CK ID	MITRE Technique	% of Incidents
T1566.002	Phishing: Spearphishing Link	31.5
T1534	Internal Spearphishing	27.9

T1566.001	Phishing: Spearphishing Attachment	21.5
T1008	Fallback Channels	9.6
T1071.004	Application Layer Protocol: DNS	9.4

In November 2024, we responded to a phishing attack on a utilities sector customer. A staff member received an email with a malicious link that led to a compromised website injected with "SocGholish" malware, designed to deliver additional payloads.

To remediate the incident, our teams deployed GreyMatter response playbooks to ban the malicious file hash, delete the email, and block the compromised website domain to prevent any further access. We also recommended blocking the sender's domain and conducting a full scan on the user's host to ensure complete remediation.

The key lesson learned from this is that proactive deployment of automation in cybersecurity processes can greatly improve an organization's resilience against attacks, ensuring much quicker responses and safeguarding critical infrastructure from extended vulnerabilities. If the customer had enabled GreyMatter Automated Response Playbooks, the remediation process could have been faster, as the suspicious file would have been quarantined immediately upon download.

GreyMatter Insights

Just 2 Minutes to Contain a Threat with AI and Automation

ReliaQuest GreyMatter collects security metrics across multiple sectors, including utilities, to uncover industry trends and challenges. The mean time to contain (MTTC) threats measures how quickly a security incident is contained after detection, providing key insights into the effectiveness of an organization's response.

Within ReliaQuest's customer base, the utilities sector ranks fourth in adopting automated response measures, with 73% of customers using GreyMatter's Automated Response Playbooks. This adoption rate is significantly higher than similar sectors that also integrate IT and OT systems, such as manufacturing, where just 44% of customers have implemented Automated Response Playbooks. Utilities organizations leveraging AI and automation with GreyMatter achieve an impressive average MTTC of just **two minutes**, far outpacing the **20 hours and 57 minutes** typically needed when relying on manual responses. The utilities sector's drive to cut incident response times through automation likely stems from the severe consequences of delayed threat containment and regulatory pressure to maintain consistent services. A delayed MTTC and slow remediation time could grant attackers a window of opportunity to deploy malicious software, like ransomware, to infiltrate systems and potentially interfere with, or even shut down, critical infrastructure. Such disruptions to critical services like power and water supply could affect thousands of customers and create cascading effects that impact businesses and emergency services. Problems with essential supplies could pose national security risks, endangering public safety and threatening economic stability.

In February 2024, we assisted a China-based renewable energy customer investigate an unauthorized access incident. After several brute-force attempts from a Dubai-based IP address, a suspicious user successfully gained network access.

Although the IP address was not flagged as malicious, we immediately verified the login with the customer and checked for unusual activity. The customer executed the GreyMatter response playbook Microsoft Entra ID, which reset the affected user's password, terminated any active sessions, and revoked cookies. The customer's initiative in running the response playbook likely secured the company's systems, effectively mitigating any potential risk from the unauthorized access while further investigation continued.

The key takeaway here is the benefit of having the appropriate response playbooks, as they empower organizations to quickly neutralize threats and secure their systems, further demonstrating the value of being proactive in securing corporate environments.

Findings from the Dark Web

Behind the Curtain: Threat Actors Eyeing OT Systems

Cybercriminals talk about various sectors on dark-web forums, especially Initial Access Brokers (IABs) who sell corporate access through compromised virtual private networks (VPNs) and Remote Desktop Protocol (RDP) tools. However, what's notable about the posts we observed about utilities sector companies is that threat actors have been discussing—and even publishing—access to OT systems. We even observed threat actors discussing Industrial Control Systems (ICSs).

For example, Figure 1 shows a threat actor on the Russian-language forum XSS who suggests specific Shodan search queries, known as "dorks," to locate Supervisory Control and Data Acquisition (SCADA) devices by country, with a focus on Unitronics devices and those on port 502. The actor also recommends creating an access control list of Classless Inter-Domain Routing (CIDR) ranges for Unitronics devices to scan for open port 20256.

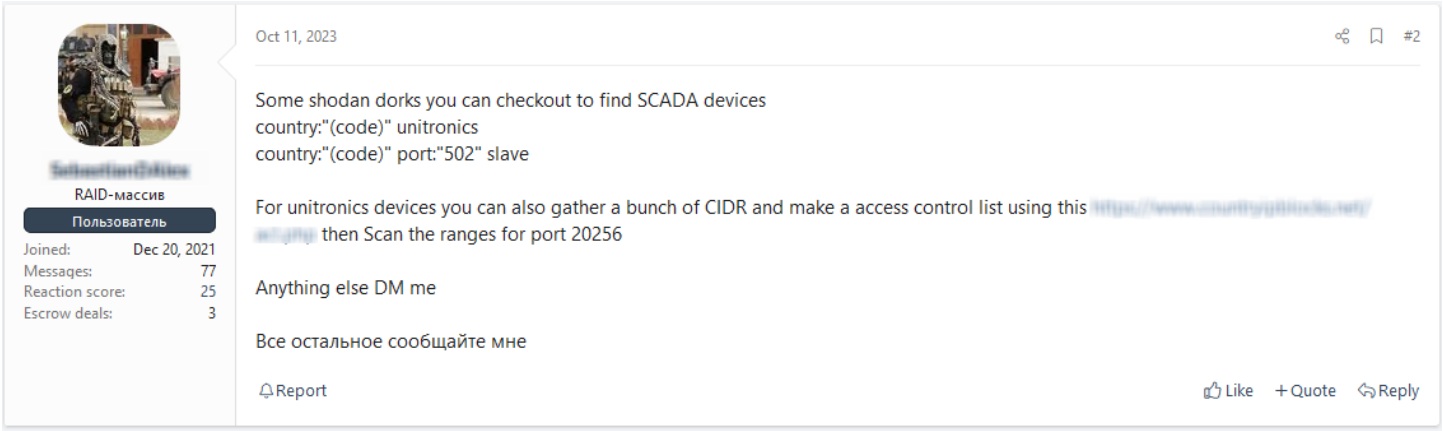

Figure 1: A threat actor shares a tutorial on how to search for internet-exposed SCADA devices

Meanwhile, some adversaries are capitalizing on the interest in OT platforms by selling access to IoT systems that manage these platforms. For example, as shown in Figure 2, a threat actor is offering 0-day access to an IoT system that controls OT devices using protocols like IEC-104, MODBUS, and MQTT. The threat actor enhances the appeal of this access by claiming that exploiting the vulnerability could enable buyers to "upload many file types that can be downloaded, with no pass/cookie, so can be used for malware/script hosting."

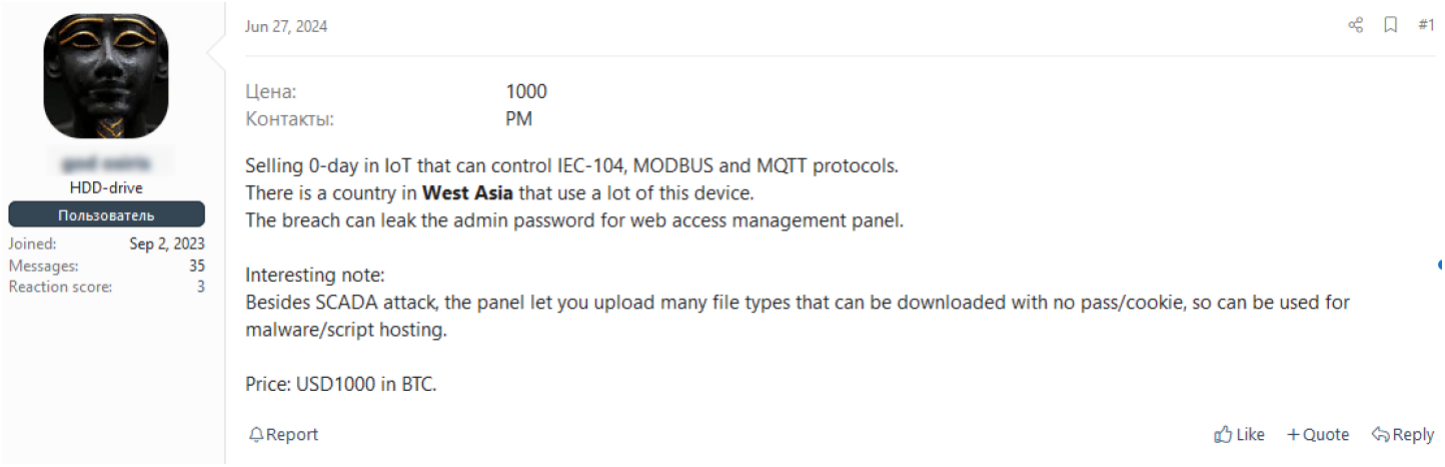

Figure 2: A threat actor sells alleged 0-day access to an IoT device that controls OT platforms

The possibility of threat actors gaining access to OT systems is likely a major concern for security teams in utilities organizations, so discussions on cybercriminal forums about searching for and targeting these systems, as well as selling access to them, is particularly disconcerting. These circumstances emphasize the critical need for utilities organizations to continuously monitor for signs that their corporate or industrial infrastructure may be compromised or at risk.

Recommendations

To prevent threat actors from discovering open ports through tools like Shodan, utilities companies are advised to adopt a comprehensive approach to network security. Start by conducting thorough network scans to identify and close unnecessary open ports, minimizing the attack surface. Implement robust firewall configurations to block unauthorized access and ensure that only essential services are exposed to the internet. Additionally, use intrusion detection and prevention systems (IDS/IPSs) to monitor for suspicious activity and consider deploying honeypots to detect and analyze unauthorized access attempts. Finally, enforce strict access controls for sensitive systems, ensuring that access is granted only to authorized personnel.

GreyMatter Digital Risk Protection Insights

Impersonating Domain Alerts Increase By 9%

During the reporting period, alerts from GreyMatter Digital Risk Protection (GreyMatter DRP) for impersonating domains in the utilities sector constituted 57% of all true-positive alerts, up from 48% in the same period last year.

While it's difficult to pinpoint any one reason for the recent increase, it's realistically possible that the rapid advancements in generative AI (GenAI) capabilities was a large contributing factor. Just as businesses are utilizing AI to enhance and scale their operations, cyber attackers are using it to amplify their tactics. AI enables attackers to automate the creation of highly convincing fake domains. Even if these malicious domains are taken down, AI tools can swiftly help attackers re-establish similar ones, perpetuating the threat. Additionally, cybercriminals are likely employing SEO poisoning techniques to ensure their malicious sites rank prominently in search results, thereby increasing the chances of targets engaging with these deceptive domains.

Impersonating domains pose a major threat to utilities companies due to their critical operations and trust-based relationships with stakeholders like customers and regulatory bodies. Attackers create fake domains that closely resemble legitimate ones, tricking employees, partners, or customers into revealing credentials. These credentials can then be used to access critical systems or sold on dark-web forums like Russian Market. Once attackers have these credentials, they can move laterally within the company's network, exploiting vulnerabilities to escalate privileges and control more systems and data. This lateral movement also allows attackers to map the network architecture and understand security measures, opening the door to more potent attacks in the future.

Recommendations

ReliaQuest customers can use GreyMatter DRP to swiftly detect and dismantle domain impersonation attempts. It efficiently identifies typosquatting and similar strategies, enabling security teams in the utilities sector to proactively identify fake domains. By doing so, it reduces credential exposure and protects data. Once a threat is identified, GreyMatter DRP alerts security teams to quickly initiate takedown requests with domain registrars or internet service providers (ISPs).

Open Ports: Cybercriminals' Popular Path into Utilities Networks

Although not as prevalent as impersonating domains in our dataset, the Open Port DRP alert is noteworthy. During the current reporting period, open ports constituted **9%** of all true-positive alerts among our customers, up from **7%** in the same period last year. Additionally, open ports ranked fourth in frequency for both periods, showing that this attack vector remains popular with threat actors.

Open ports are a favored attack vector for threat actors targeting the utilities sector due to several inherent challenges. The sheer complexity and vast scale of OT networks within these companies often hinder effective monitoring of all open ports and services, providing attackers with numerous entry points to exploit. Additionally, these environments often contain legacy systems not designed to handle traffic from typical scanning tools, making them susceptible to disruptions and less capable of defending against intrusions. Lastly, the use of diverse, proprietary, and industry-specific protocols complicates the standardization of security measures. As OT and IT systems become increasingly interdependent, exploiting a vulnerability in one area can have widespread repercussions, making these systems an attractive target for threat actors.

Open ports can serve as entry points for attackers to access sensitive systems, especially when legitimate tools are used to locate internet-exposed ports. We observed a threat actor using this tactic in February 2024. The “GhostSec” hacktivist group employed the Metasploit framework—a tool widely used by security researchers—to find open ports in Iranian utilities companies.[2] Metasploit's modular capabilities and specific OT system modules enabled GhostSec to target utilities companies with open ports in their OT environments, such as Modbus on Transmission Control Protocol (TCP) 502 or (Common Industrial Protocol) CIP on TCP 44818. Although the full extent of the damage caused by GhostSec's attack remains unclear, the crucial takeaway is significant: If hacktivist groups are exploiting open ports to target the utilities sector, it’s highly likely that other advanced cybercriminals such as ransomware groups or APT groups will also seek to exploit these vulnerabilities to infiltrate utilities networks.

Recommendations

We advise securing unnecessary open ports, employing firewalls, and continually monitoring network traffic as essential measures to protect systems against unauthorized access and attacks. By closing or securing open ports that aren’t essential for operations, you reduce the potential entry points for attackers, thereby minimizing your attack surface. Firewalls act as a barrier between internal networks and external threats, allowing only necessary and trusted traffic while alerting security teams to any suspicious activities. Continuous monitoring of network traffic enables real-time detection of anomalies, facilitating swift responses to potential threats.

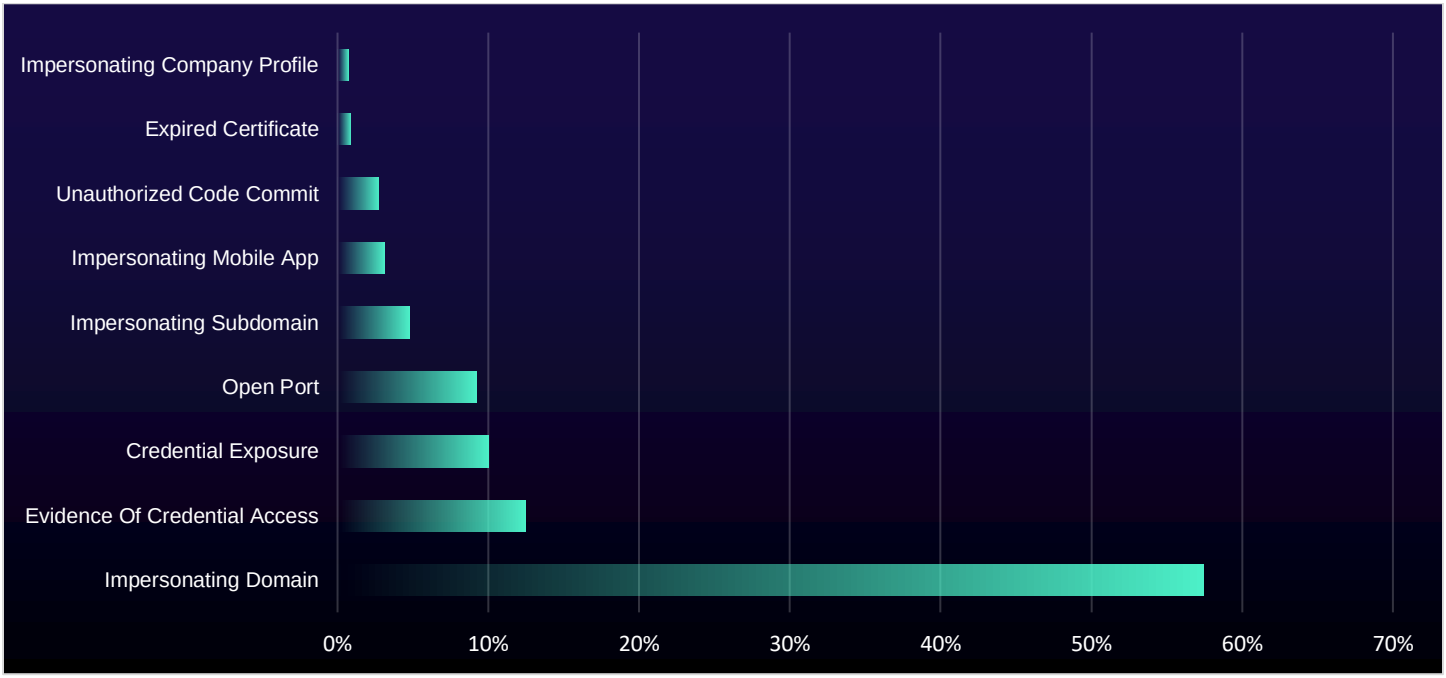

Figure 3: Percentage of GreyMatter DRP alerts for the utilities sector

Ransomware Activity Targeting Sector

Utilities Sector Hit by 42% Rise in Ransomware Data-Leak Listings

During the reporting period, 75 utilities sector organizations appeared on ransomware data-leak sites—a **42% increase** compared to the previous 12 months.

Utilities companies are consistently popular targets for ransomware groups, who use the threat of disrupting critical services to pressure these organizations into paying ransoms quickly to restore operations. Additionally, their management of sensitive data and infrastructure makes utilities companies high-value targets for financial gain and strategic leverage. The surge in attacks over the past year is likely connected to the continued growth of ransomware-as-a-service (RaaS) operations and the general increase in ransomware activity observed throughout 2024. The potential cost of operational losses and regulatory fines can exceed ransom demands, often incentivizing companies to pay attackers for quick service restoration. Research shows a disconnect between risk and budget in OT environments, where 66% of respondents identify "people" as the biggest risk, yet 52% of budgets are allocated to technology, with only 25% dedicated to workforce training, recruitment, and retention.[3]

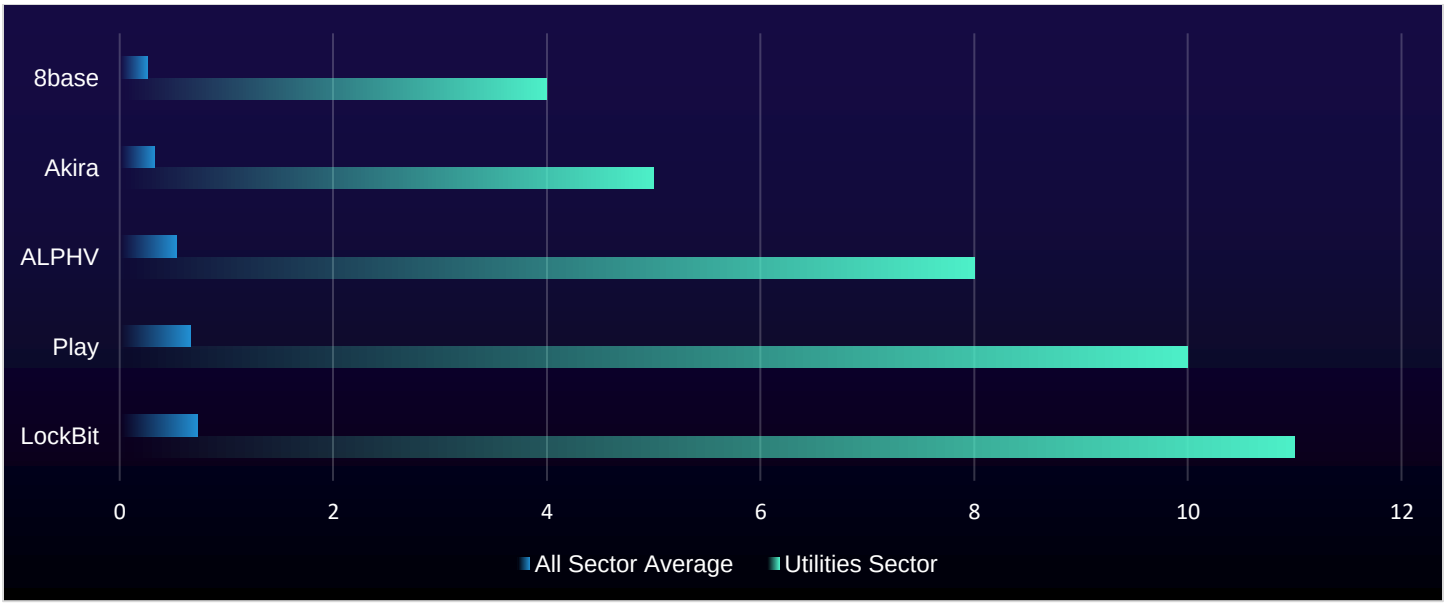

Figure 4: Utilities companies named per ransomware group compared to the all-sector average

The escalating ransomware attacks on utilities companies are a worrying trend for this industry sector. To supplement its reliance on OT systems, the sector is increasingly adopting Industrial Internet of Things (IIoT) technologies, which prioritize operability over cybersecurity. This leaves many critical systems with unaddressed vulnerabilities that ransomware operators could exploit if they ramp up their focus on this sector.

Additionally, smaller utilities companies often lack the budget to update or upgrade legacy systems, making them prime targets for ransomware. Researchers have suggested that a ransomware attack could lead to losses averaging 31% of operating income for small energy providers, compared to 13% for medium and 2% for large entities.[4]

Recommendations

To effectively defend utilities organizations against ransomware, establish a strong security foundation by proactively addressing vulnerabilities and implementing comprehensive security protocols and risk management strategies, which also support regulatory compliance. Develop a robust backup strategy to safeguard critical data and systems, ensuring resilience against attacks. Implement network segmentation to isolate OT networks from IT networks, preventing lateral threat movement and protecting OT systems from disruptions. Regularly train employees on risks like social engineering and phishing, as human error is often a factor in ransomware proliferation.

Second Only to LockBit, Play Intensifies Utilities Sector Attacks

In the 12 months leading up to our reporting period, the RaaS provider “Play” (aka PlayCrypt) listed three utilities sector victims on its data-leak site. From November 2023 to the end of October 2024, this number increased to ten. Despite still trailing behind first-place “LockBit” group in targeting utilities, the February 2024 law enforcement operations against LockBit have narrowed the gap to just one utilities victim. This increase is significant, as Play targeted only three utilities sector companies in the same period last year, marking a 233% rise in successful attacks.

Identifying the exact reasons for Play's increased targeting of utilities sector companies is challenging, but the ongoing shifts in the ransomware landscape likely plays a significant role. Analysis of Play's targeting patterns shows that while the group does not focus on specific sectors, it prefers large organizations, with known targets including medical, financial, manufacturing, real estate, and educational institutions. This preference for sizable organizations makes utilities companies attractive targets due to their typically large scale. Additionally, the upheaval in the ransomware environment means newer groups like Play may aim to target high-profile entities to garner maximum attention in both media and cybercriminal circles. This heightened visibility could help Play attract affiliates from declining groups like LockBit or disbanded groups like “ALPHV.”

Play uses sophisticated tools like Cobalt Strike for C2 activities and the “SystemBC” remote-access trojan (RAT) to gain and maintain access on compromised hosts. To evade detection, Play exploits Living off the Land binaries (LOLBins), using native Operating System (OS) processes instead of deploying traditional malware. This sophisticated approach,

along with its capability to develop custom exploitation tools and target new vulnerabilities, makes Play a formidable threat to utilities companies.

Recommendations

To mitigate the risk from Play, organizations should implement data loss prevention (DLP) software to block unauthorized access and prevent the encryption or leakage of sensitive documents, such as energy plant blueprints or technical schematics. We also recommend using Group Policy Objects (GPOs) to restrict remote-access tools commonly exploited by Play, such as RDP, SystemBC, and PSexec.

Key Threat: Volt Typhoon

"Volt Typhoon," first observed in 2023, is a China-linked advanced persistent threat (APT) group known for its sophisticated cyber attack techniques and ability to maintain persistent access and evade detection.

In early February 2024, multiple US intelligence agencies issued an advisory on the urgent cyber threat from China.[5] They specifically warned critical national infrastructure (CNI) organizations about state-sponsored adversaries, naming Volt Typhoon as a group poised to conduct disruptive or destructive cyberattacks against US CNI. The FBI also warned that Volt Typhoon had already infiltrated the IT environments of US communications, energy, transportation, and water companies.[6] They alleged that Volt Typhoon seeks to preposition itself "on IT networks to enable lateral movement to OT assets to disrupt functions."[7]

Volt Typhoon typically gains initial access via targeted spearphishing campaigns and exploiting vulnerabilities in old or unpatched networking appliances like routers. The group is known for its robust operational security, allowing it to remain undetected for extended periods, sometimes even over five years.[8] By using Living off the Land (LOTL) techniques, the group exploits a system's native tools and processes to evade detection, customizing its attack based on thorough research of the target organization. Volt Typhoon also frequently uses RDP with compromised administrator credentials to move laterally within infiltrated networks.[9]

Volt Typhoon poses a significant threat to utilities companies because of its ability to deeply embed itself within networks, making it nearly impossible to remove intruders without causing downtime. Once inside, these attackers often have a deep understanding of infiltrated networks, allowing them to remain undetected and maintain a persistent presence. In this context, it's realistically possible that even traditional downtime responses like reboots, isolations, and reimaging may be insufficient, as groups such as Volt Typhoon use sophisticated persistence methods across multiple endpoints.

Recommendations

To defend against Volt Typhoon, as a best practice, utilities sector organizations should prioritize implementing the following foundational measures.

- **Implement Detailed Logging and Automation**: Store logs securely in a centralized location and use automation tools to review them continuously, comparing activities against established baselines to detect anomalies.
- **Employ Security Hardening and Network Segmentation**: Use application allowlisting and monitor common LOLBins, while enhancing IT and OT network segmentation to isolate critical systems and reduce attack surfaces.
- **Ensure Robust Authentication and Authorization**: Implement strong controls across all network locations to secure interactions and prevent unauthorized access.

To further harden your defenses, ReliaQuest customers should implement rapid threat detection and containment strategies by activating the following GreyMatter detection rules.

Detection Rule	MITRE Technique	Summary
RQ – Execution from TSClient Mountpoint	T1021.001 – Remote Services: Remote Desktop Protocol	Volt Typhoon achieves lateral movement within compromised environments by accessing the domain controller through an RDP session using a compromised account with domain privileges. This rule detects execution from the RDP-shared mountpoint TSClient on a critical host, which may indicate an attempt at lateral movement.

RQ – IDS Web Shell	TA0003: T1505.003 – Web Shell TA0001: T1190 – Exploit Public-Facing Application TA0002: T1204.002 – Malicious File	Volt Typhoon exploits vulnerabilities in networking appliances like Fortinet, Ivanti, NETGEAR, Citrix, and Cisco, using web shells for persistence and data exfiltration. This rule detects when a web server sends or receives traffic identified by the IDS as web shell activity.
RQ – Administrator Enumeration	TA0007: T1087 – Account Discovery TA0007: T1069.002 – Domain Groups TA0007: T1087.002 – Domain Account	Volt Typhoon engages in thorough pre-compromise reconnaissance by conducting searches on target sites to gather host, identity, and network information, with a focus on network and IT administrator accounts. This rule looks to identify attackers engaging in reconnaissance on administrator groups.

For swift remediation, GreyMatter Automated Response Playbooks automatically contain threats upon detection, improving your MTTC and reducing the risk of a major breach. Alternatively, set GreyMatter response playbooks to "RQ Approved" for our analyst team to manage remediation, speeding up response times while retaining human discretion. Certain playbooks, such as Isolate Host, can be set to require phone approval to avoid business disruption.

- **Isolate Host:** Automatically isolates a specified host from the network, effectively countering RDP brute-force attacks by Volt Typhoon, blocking further exploitation or data exfiltration.
- **Terminate Active Sessions and Reset Passwords:** Revokes malicious sessions and forces password resets, cutting off access gained through spearphishing attacks by Volt Typhoon.
- **Disable User:** Disables accounts suspected to be compromised, revoking the adversary's access and preventing further advancement toward gaining sensitive information and deploying encryption.

Cyber Threat Forecast for Utilities Sector

Utilities to Confront Greater State-Sponsored Threats

Beijing Likely to Greenlight Increased Cyber Attacks on US Utilities

With the incoming Donald Trump administration's hawkish stance on China and proposals to impose high tariffs on Chinese goods, it's highly likely that Beijing will allow groups like Volt Typhoon to intensify their offensive operations against US utilities providers.[10]

U.S. intelligence assessments indicate that Volt Typhoon has been positioning itself within IT networks to enable lateral movement to OT assets, with the goal of disrupting CNI. Additionally, Trump's nominee for National Security Advisor, Mike Waltz, is recognized for his firm stance against China. Waltz, who currently serves on the House China Task Force and is a member of the Congressional Taiwan Caucus, has consistently pushed for speeding up the arming of Taiwan—a move likely to heighten tensions with Beijing. In this context, amid growing concerns over conflict in the Taiwan Strait, Volt Typhoon could be deployed to disrupt critical US infrastructure by targeting pipelines, water systems, transportation, and communications, thereby inciting panic and societal tensions to hinder US military mobilization efforts.

Iran-Linked Cyber Attacks Expected to Rise Amid Trump's Support for Israel

Similarly, we anticipate that the Trump administration's ongoing support for Israel will trigger an uptick in cyber attacks backed or linked to Iran, targeting both the US and Israel. This expected increase is in response to the president-elect's strong backing of Israel. This threat is especially concerning given that Israeli companies are heavily involved in manufacturing devices for utilities organizations.

Iranian-linked hacktivist groups, such as "CyberAv3ngers" (aka CyberAveng3rs and Cyber Avengers), have already successfully launched cyber attacks on multiple water and wastewater facilities in the US. These attacks specifically targeted Israeli-manufactured programmable logic controller (PLC) and Human-Machine Interface (HMI) used within these facilities.

Given these conditions, organizations in the utilities sector should remain vigilant about these persistent geopolitical tensions. This is especially crucial for those relying on Israeli-based suppliers, as cyber attacks on these suppliers could lead to significant supply-chain disruptions for utilities customers further downstream. The immediate effects might include

delays in product delivery, increased operational costs, and even a halt in production. As such, not only would the directly targeted companies be affected, but also the downstream customers dependent on their products or services. This scenario is especially concerning for organizations that use OT systems to operate critical infrastructure, such as water treatment plants, electricity, and other energy grids

Recommendations

Adversaries often exploit the path of least resistance, such as the flawed configuration of OT devices with unchanged default passwords. To prevent access via these vulnerabilities, collaborate with vendors and security experts or the ICS/OT cybersecurity community to identify devices with default passwords. Utilize host logs and network visibility to detect weak credentials, develop a remediation plan to replace default passwords or apply patches, and ensure future projects address default passwords during acceptance testing.

Water Companies at Risk as OT Hacktivism Continues to Evolve

In the short-term future, we expect hacktivism groups targeting OT to enhance their tactics and technical capabilities, as evidenced by a series of recent cyber incidents. Hacktivists are likely to change their tactics because their traditional methods, such as distributed denial of service (DDoS) attacks and website defacements, often go unnoticed and receive little media attention. In contrast, attacks on critical infrastructure draw significant media coverage, which helps them achieve their ideological goals. As geopolitical tensions continue in Europe and the Middle East, these high-profile attacks are expected to rise, providing hacktivists with a powerful tool to gain attention and exert influence. We anticipate that water companies will be at particularly high risk; the US Environmental Protection Agency has reported that at least 97 major US water systems have unpatched critical and high-severity vulnerabilities. Exploiting these vulnerabilities could impact almost 10% of the 1,062 water systems serving at least 50,000 people.[11]

The Iran-backed CyberAv3ngers, "Cyber Army of Russia Reborn," and Ukraine-backed "Blackjack" groups are all hacktivist organizations who have previously exploited existing weaknesses in OT systems to further their ideological goals. For instance, in late 2023, CyberAv3ngers exploited default OT system configurations at a Pennsylvania water facility, forcing the facility to switch to manual operations. Meanwhile, it's been reported that Cyber Army of Russia Reborn manipulated water tanks in Texas by exploiting Virtual Network Computing **(**VNC) technology vulnerabilities to adjust pressure setpoints.[12] And Blackjack developed custom malware, "Fuxnet," to disrupt sensor operations in Moscow municipalities OT monitoring network.[13]

Recommendations

The continued evolution of hacktivist tactics means that utilities companies must also adapt their defense strategies to counter the threat of hacktivist groups targeting OT systems. For instance, the CyberAv3ngers attack underscores the need for organizations to prioritize identifying and remediating default passwords and settings across all OT devices, collaborating with vendors and cybersecurity experts to mitigate these vulnerabilities. Similarly, Cyber Army of Russia Reborn's targeting of VNC technology vulnerabilities means that there is an increased need for enhanced security of remote-access technologies through strict access controls, regular updates, and network segmentation. Lastly, the development of custom malware like "Fuxnet" to disrupt OT monitoring networks highlights the importance of investing in advanced threat detection and response capabilities, deploying tailored OT intrusion detection and prevention systems, while also establishing a robust incident response plan.

Transition to Renewables Opens New Cyber Attack Opportunities

As utilities organizations worldwide shift towards renewable energy generation, the attack surface for cybercriminals is anticipated to expand.

Renewable energy sources, like offshore wind turbines and hydroelectric dams, are often in remote locations, requiring extensive cyber infrastructure to connect with onshore systems, thereby broadening the attack surface. In addition, there's an increasing integration of OT components into energy grids, including internet-connected distributed energy resources (DERs) that manage vast fleets of remote devices but often lack stringent cybersecurity measures.[14] In the solar power sector, photovoltaic (PV) diagnostic and monitoring systems—essential for measuring efficiency, detecting faults, and optimizing operations—are particularly vulnerable; researchers have identified over 130,000 PV systems accessible over the internet.[15]

While IT systems typically use password policies that lock users out after multiple failed attempts to enhance security, such measures are less feasible for OT systems like DERs.[16] Locking an OT system could cause significant operational disruptions, potentially halting energy production or distribution and threatening grid stability and community reliability.

Recommendations

Utilities sector customers are advised to implement a defense-in-depth cybersecurity approach that includes robust monitoring and incident response capabilities to detect and counteract potential attacks on OT systems. This includes incorporating robust network segmentation to isolate DER devices from critical infrastructure, reducing the risk of lateral movement in case of a breach. Deploy advanced IDS/IPS specifically designed for OT environments to monitor for unusual activity without disrupting operations. Regularly update and patch DER software to protect against known vulnerabilities and employ strong authentication methods that go beyond simple passwords, such as multifactor authentication (MFA) where practical. Additionally, conduct regular security audits and vulnerability assessments to identify and address potential weak points, and establish comprehensive incident response plans to ensure rapid containment and recovery from cyber incidents.

Conclusion

In examining the various threats facing the utilities sector, a common theme emerges: the convergence of IT and OT systems is expanding the attack surface, increasing organizational vulnerability to cyber threats. Adversaries are taking advantage of the interconnectedness and often weaker security measures of OT environments through tactics such as spearphishing, ransomware, and targeting open ports. Utilities companies should consider how investments in IT security can bolster their OT systems and support continuous modernization of their business.

Hacktivist groups, nation-state actors like Volt Typhoon, and cybercriminals are all exploiting these vulnerabilities to disrupt critical infrastructure. This underscores the urgent need for utilities companies to adopt comprehensive security strategies, including automated incident response to rapidly contain threats. Extending robust security protocols to third parties and contractors is also vital in preventing them from becoming weak links in their security operations. In addition, organizations mustn't overlook the importance of proper employee training to enhance vigilance against phishing attempts.

Lastly, utilities sector organizations can harden their overall security posture by implementing a comprehensive digital risk protection (DRP) strategy and tailored defensive solutions to proactively counter ransomware and credential abuse from dark-web sales, thereby mitigating risks before they escalate into serious threats.

---

[1] hxxps://www[.]avtecinc.com/industries/utilities/the-complete-guide-to-utility-cybersecurity
[2] hxxps://industrialcyber[.]co/news/otorio-reveals-ghostsec-hacktivist-group-now-targets-iranian-ics-in-support-of-hijab-protests/
[3] hxxps://www.sans.org/white-papers/sans-2024-state-ics-ot-cybersecurity/
[4] hxxps://www[.]utilitydive.com/news/ransomware-is-a-major-threat-to-smaller-utilities-manufacturers-and-health/647913/
[5] hxxps://www.cisa[.]gov/sites/default/files/2024-02/aa24-038a-jcsa-prc-state-sponsored-actors-compromise-us-critical-infrastructure_1.pdf
[6] hxxps://www.theguardian[.]com/world/2024/apr/19/fbi-china-hack-infrastructure
[7] hxxps://www.securityweek[.]com/cisa-chinas-volt-typhoon-hackers-planning-critical-infrastructure-disruption/
[8] hxxps://www.techtarget[.]com/searchsecurity/news/366569227/CISA-Volt-Typhoon-had-access-to-some-US-targets-for-5-years
[9] hxxps://www.cisa[.]gov/sites/default/files/2024-03/aa24 038a_csa_prc_state_sponsored_actors_compromise_us_critical_infrastructure_3.pdf
[10] hxxps://www.wired[.]com/story/trump-administration-cybersecurity-policy-reversals/
[11] hxxps://www.darkreading[.]com/vulnerabilities-threats/leaky-cybersecurity-holes-water-systems-risk
[12] hxxps://www.csoonline[.]com/article/3568804/russian-groups-hack-of-texas-water-system-underscores-critical-ot-cyber-threats.html
[13] hxxps://www.darkreading[.]com/ics-ot-security/dangerous-new-ics-malware-targets-orgs-in-russia-and-ukraine
[14] hxxps://www.energy[.]gov/ceser/articles/2024-cyber-baselines-raising-ceiling-energy-cybersecurity
[15] hxxps://cybersecuritynews[.]com/internet-exposed-solar-systems/
[16] hxxps://www.power-technology[.]com/features/the-energy-transition-means-increased-attack-surfaces-for-hackers/?cf-view