# Weekly Cybersecurity Intelligence Briefing: September 8-15, 2025

## I. Executive Summary: The Week in Review

The cybersecurity landscape over the past seven days was defined by a critical and dangerous convergence of sophisticated nation-state campaigns and evolving cybercriminal tactics. The primary trends reveal a strategic shift by adversaries to achieve deeper, more disruptive access to critical infrastructure. The era of simple data theft is giving way to a new phase of pre-positioned cyber exploitation, supply chain weaponization, and direct attacks on operational technology (OT). This briefing provides a strategic overview of the week's most significant developments, distilling complex events into key takeaways for executive and board-level leadership.

The dominant themes of the week include the strategic pre-positioning by foreign adversaries, which suggests their intent is not merely espionage but the ability to execute future disruptive or destructive actions. The proliferation of supply chain attacks, from the open-source software ecosystem to core industrial and business applications, demonstrates that an organization's security perimeter is no longer a static defense. Instead, the security posture must now extend to include its entire digital ecosystem, from code dependencies to third-party vendors. This week also highlighted a persistent vulnerability in defenses, as nation-state actors continue to exploit decades-old flaws and poor cyber hygiene to gain access to critical systems, underscoring a fundamental gap between the perceived and actual security state of many networks.

Key incidents that exemplify these trends include the "Great NPM Heist" 1, a devastating JavaScript supply chain attack that affected over two billion weekly downloads. This incident exposes the profound fragility of the open-source software that underpins a vast portion of the modern digital economy. In the manufacturing sector, the prolonged breach at Jaguar Land Rover 2 and the active exploitation of a core industrial software platform, Dassault Systèmes DELMIA Apriso 3, signal a direct and coordinated threat to global industrial operations. Simultaneously, the announced "retirement" of the prominent cybercriminal alliance "Scattered LAPSUS$ hunters 4.0" 4 is a significant development, but one that warrants extreme caution. A group of this caliber, having just claimed a major breach, is likely engaging in a tactical pause or rebranding effort rather than a true dissolution. The overall strategic implication is that organizations must now operate with a heightened level of vigilance, assuming that the most dangerous threats are those that are the least visible. Immediate strategic recommendations for C-level leadership include a dedicated focus on holistic supply chain risk management, prioritizing the remediation of known exploited vulnerabilities, and a fundamental re-evaluation of foundational network security controls.

## II. Strategic Threat Analysis: The Geopolitical & Criminal Battleground

The threats observed this week reveal a sophisticated and multi-layered battleground where nation-states and criminal organizations operate with distinct but often intersecting goals. The intelligence suggests a move toward more impactful, pre-meditated campaigns.

### The Evolving Nation-State Threat Matrix

According to the latest Homeland Threat Assessment (HTA) from the Department of Homeland Security, the most pressing foreign threats to critical infrastructure in the United States remain the People's Republic of China (PRC), Russia, and Iran.5 This assessment is not a generic warning; it is a specific, intelligence-backed evaluation of their motives and tactics.

The PRC's strategy is one of strategic pre-positioning, aiming to gain and maintain a foothold on US critical infrastructure networks. This is not solely for espionage or data theft, but to enable disruptive or destructive attacks in a future conflict scenario. The HTA highlights the use of "living off the land" techniques by PRC-linked groups such as Volt Typhoon 5, which use legitimate network administration tools to evade detection. This tactic makes attribution and defense incredibly difficult. The recent activity of Chinese-linked groups, including Linen Typhoon, Violet Typhoon, and Storm 2603 1, weaponizing a SharePoint Server vulnerability to target high-value government entities—including the U.S. Department of Homeland Security, the National Institutes of Health, and the National Nuclear Security Administration—demonstrates a clear and methodical focus on gaining access to the nation's most sensitive networks. The strategic implication is a profound shift from a theoretical risk to a present and active threat to national security and economic stability.

The Russian Federation employs a multi-vector approach. An FBI public service announcement details how cyber actors attributed to the Russian Federal Security Service (FSB) Center 16 are exploiting legacy, end-of-life networking devices using a seven-year-old vulnerability, CVE-2018-0171.6 This is a critical finding, as it shows that state-sponsored actors are not exclusively focused on zero-days but are successfully leveraging poor cyber hygiene to broadly target US and global entities across critical infrastructure sectors. The exploitation of an outdated vulnerability to collect configuration files and enable unauthorized access to thousands of devices illustrates a deep strategic paradox: the most sophisticated threats often exploit the most fundamental vulnerabilities. The Russian approach is further complicated by the use of criminal hacktivists sympathetic to their cause, who carry out disruptive, highly visible attacks, such as those against municipal water distribution systems.5 This dual-pronged strategy—where one group conducts quiet reconnaissance while another performs loud, disruptive attacks—is more resilient and dangerous than a single, high-tech campaign.

### Ransomware & Cybercrime: A Period of Change & Deception

The criminal landscape is marked by a mix of new entrants and established players. The emergence of new ransomware groups like Yurei 7 and EXTEN 8 highlights the low barrier to entry for financially motivated criminals. Yurei, in its first week of operation, targeted a food manufacturing company in Sri Lanka 7, using a publicly available open-source ransomware codebase to rapidly escalate its operations. These groups primarily employ a "double-extortion" model, not only encrypting files but also exfiltrating sensitive data and threatening to publish it if the ransom is not paid.7 This demonstrates that even actors who are not highly sophisticated can pose a significant and damaging threat.

At the same time, established threats persist. The Akira ransomware group is once again actively exploiting a vulnerability in SonicWall firewalls with SSLVPN enabled.9 This resurgence is a testament to the persistence and adaptability of these criminal operations; they do not simply disappear but often return to old, successful tactics after a brief period of inactivity.

Perhaps the most significant development in the cybercrime sphere is the announced shutdown of the "Scattered LAPSUS$ hunters 4.0" alliance on their Telegram channel.4 This group, which includes prominent criminal entities like Scattered Spider, LAPSUS$, and ShinyHunters, claimed responsibility for the Jaguar Land Rover breach shortly before the announcement. However, analysts remain skeptical, as the source material explicitly warns that "silence from a threat group does not equal safety".4 The apparent "going dark" could be a tactical maneuver to evade law enforcement scrutiny, a rebranding effort, or a strategic shift to a more clandestine, private operation. The JLR incident serves as a public demonstration of their capabilities before they move underground. The strategic implication is that organizations cannot afford to let their guard down. The underlying threat, including stolen data and the expertise of these actors, has not vanished; it has merely become less visible.

| Threat Actor/Group | Attribution | Key Incident(s) this Week | Observed TTPs | Primary Target Sectors |
| --- | --- | --- | --- | --- |
| **Linen Typhoon, Violet Typhoon, Storm 2603** | People's Republic of China (PRC) Nation-State | Espionage against U.S. government entities, including DHS, NIH, and National Nuclear Security.1 | Weaponizing SharePoint Server vulnerabilities, pre-positioning on networks, "living off the land" techniques.1 | Government Facilities, Critical Infrastructure, Federal Agencies |
| **Russian FSB Center 16** | Russian Federation Nation-State | Exploitation of legacy networking devices, collecting configuration files from thousands of US entities.6 | Exploitation of end-of-life devices and old vulnerabilities (CVE-2018-0171), use of legacy protocols (SMI, SNMPv1/v2), deploying custom malware like "SYNful Knock".6 | Critical Infrastructure, specifically Communications, Energy, Water |
| **UNC6040, UNC6395** | Financially Motivated Cybercrime | Data theft and extortion campaigns targeting Salesforce platforms via a breached third-party application (Salesloft Drift).4 | Vishing, compromised OAuth tokens, exploiting supplier GitHub accounts, use of modified Salesforce Data Loader, custom Python scripts.4 | Financial Services, Technology, Enterprise Software Users |
| **Yurei Ransomware** | Cybercrime | Emerged on September 5, first victim a Sri Lankan food manufacturer, quickly grew to three victims from India and Nigeria.7 | Double-extortion model (encrypt and exfiltrate), use of open-source codebase (Prince-Ransomware), targets Windows-based systems.7 | Manufacturing, diverse industries using Windows infrastructure |
| **Akira Ransomware** | Cybercrime | Resurgence in attacks exploiting a previously disclosed vulnerability in SonicWall firewalls.9 | Exploiting vulnerabilities in network security appliances (SonicWall firewalls) with SSLVPN enabled, ransomware deployment.9 | Diverse industries, especially those using vulnerable SonicWall devices |
| **Scattered LAPSUS$ hunters 4.0** | Financially Motivated Cybercrime | Claimed responsibility for the Jaguar Land Rover breach.2 Announced "shutdown" of operations on September 12.4 | Social engineering, account takeovers, targeting high-profile organizations, data theft, and extortion.4 | Automotive, Manufacturing, Technology |

## III. Supply Chain Under Siege: A Critical Risk Briefing

The week's intelligence reveals that the supply chain is no longer an ancillary risk; it is a primary and highly effective attack vector for both financially motivated and state-sponsored adversaries. The incidents of the past seven days highlight the interconnected nature of supply chain risk, from open-source code to industrial software, and demonstrate that a strong internal security posture is no longer sufficient.

### The Software Supply Chain: The "Great NPM Heist"

The "Great NPM Heist" was a devastating JavaScript supply chain attack that occurred on September 8, 2025.1 It was not a breach of a single company but a large-scale attack on the software ecosystem itself. The attack vector was a phishing-enabled account takeover of a single, trusted open-source developer, Josh Junon.1 This single compromise allowed attackers to inject malicious code into 18 core JavaScript utilities that are downloaded over two billion times per week.1

The malicious code was highly sophisticated, specifically designed to target cryptocurrency wallets and transactions in browser environments.1 It used a two-pronged approach: passive address replacement, which silently swapped legitimate cryptocurrency addresses with attacker-controlled ones, and active transaction hijacking, which intercepted transaction requests from browser extensions before they were signed. The code was heavily obfuscated to evade automated security scanners and was designed to fail in server-side environments, a clever tactic that delayed discovery. The attack was ultimately discovered not by a security tool, but when build pipelines began to fail with a

ReferenceError.1 This revelation underscores the fragility of the open-source software ecosystem and the inadequacy of current security measures against sophisticated, multi-stage attacks. This incident forces every organization to confront the unmanageable risk of its own software dependencies. Every business and government agency is now a consumer of an open-source supply chain that can be weaponized with a single, successful phishing email, a fact that fundamentally alters the landscape of cyber risk.

### The IT & OT Supply Chain: Attacks on the Backbone

Beyond open-source code, attacks on the IT and OT supply chains present a direct and immediate threat. An FBI flash alert warned of two cybercriminal groups, UNC6040 and UNC6395, targeting Salesforce platforms in data theft and extortion attacks.4 The initial access for these attacks was gained through the breach of the GitHub account for a third-party application, Salesloft Drift.4 This incident mirrors the NPM heist in principle, but with a business-to-business (B2B) twist. The compromise of a single supplier's development environment led to a widespread data theft campaign against their customers, highlighting the expanding attack surface and the urgent need for rigorous vendor security management.

Further, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) added CVE-2025-5086 to its Known Exploited Vulnerabilities (KEV) Catalog this week.10 This critical flaw exists in Dassault Systèmes DELMIA Apriso, a Manufacturing Operations Management (MOM) software used by numerous industrial organizations. The vulnerability allows for remote code execution and has a CVSS score of 9.0.3 The fact that this flaw is being actively exploited, with attacks originating from an IP address in Mexico and deploying a decade-old trojan known as

Zapchast 3, is of extreme importance. This is a direct, quantifiable threat to the manufacturing sector's operational technology. The strategic implication is that adversaries are using proven, re-tooled malware and newly discovered exploits to target the IT/OT nexus. The operational imperative is no longer just to secure the corporate network; it is to secure the entire production lifecycle, from design to delivery.

## IV. Vulnerability Intelligence: Key Exploits & Mitigation

The past week brought forth a range of critical vulnerabilities, many of which are already being exploited or have a high likelihood of future weaponization. Timely remediation of these flaws is the single most effective way to reduce an organization's exposure to cyberattacks.

### CISA's Known Exploited Vulnerabilities (KEV) Catalog

CISA's KEV catalog serves as the single most important resource for prioritizing patching efforts. Over the past week, CISA added four new vulnerabilities to the catalog, signaling that they are being actively exploited in the wild.10 The most notable additions include the Linux Kernel Time-of-Check Time-of-Use vulnerability (

CVE-2025-38352) and the Dassault Systèmes DELMIA Apriso remote code execution flaw (CVE-2025-5086). The latter is particularly critical due to its direct link to the manufacturing and industrial control sectors.3 CISA strongly urges all organizations, not just federal agencies, to prioritize the remediation of these vulnerabilities as part of their vulnerability management practice.

### Microsoft Patch Tuesday Analysis

Microsoft's September Patch Tuesday addressed 81 vulnerabilities.12 While none were known to be actively exploited at the time of the release, several pose a significant risk and are considered prime candidates for future weaponization. Two stand out due to their potential for widespread impact:

* **Windows SMB Elevation of Privilege (CVE-2025-55234):** An authentication Elevation of Privilege (EoP) flaw in the Windows Server Message Block (SMB) protocol.12 Microsoft has assigned a CVSS Base score of 8.8 and believes this vulnerability is "more likely than most to be exploited within the next 30 days".12 The ability to elevate privileges over a network via a commonly used protocol makes this a top-level concern for lateral movement and network compromise.
* **Windows Hyper-V Remote Code Execution (CVE-2025-55224):** A critical remote code execution (RCE) vulnerability in the Hyper-V virtualization platform.13 An attacker who successfully exploits this flaw could gain control of a Hyper-V host and, by extension, all virtual machines running on it. An attacker who can exploit this vulnerability can achieve lateral movement, pivot from a single compromised machine to an entire virtualized environment, and seize control of critical services, making this a top-level concern for any organization running data centers or cloud infrastructure.

### Zero-Day Exploits in the Wild

Beyond the scheduled patches, several zero-day vulnerabilities were actively exploited. A zero-click vulnerability (CVE-2025-55177) in WhatsApp, used in conjunction with a separate Apple OS-level flaw (CVE-2025-43300), was exploited in targeted spyware campaigns.14 This demonstrates that personal devices remain a significant weak link for high-value targets. A critical remote code execution vulnerability in Citrix NetScaler ADC and Gateway products (

CVE-2025-7775) has also been exploited as a zero-day since early May.14 This flaw allows attackers to deploy web shells and establish persistent access, making it a critical entry point for sophisticated threat groups.15

| CVE ID | Affected Product(s) | Vulnerability Type | CVSS Score | Status | Strategic Importance |
| --- | --- | --- | --- | --- | --- |
| **CVE-2025-5086** | Dassault Systèmes DELMIA Apriso | Deserialization of Untrusted Data / RCE | 9.0 | Actively Exploited (KEV Catalog) 3 | Direct and active threat to the manufacturing and OT sectors, allowing attackers to disrupt industrial processes.3 |
| **CVE-2025-55234** | Windows SMB Protocol | Elevation of Privilege (EoP) | 8.8 | Publicly Known, High Exploit Likelihood | Allows authenticated attackers to gain administrator privileges, enabling lateral movement and network takeover.12 |
| **CVE-2025-55224** | Windows Hyper-V | Remote Code Execution (RCE) | N/A (Critical) | Patched 13 | A core virtualization flaw that could allow an authenticated attacker to compromise an entire virtualized environment and all its guests.13 |
| **CVE-2025-7775** | Citrix NetScaler ADC & Gateway | Remote Code Execution (RCE) | N/A (Critical) | Actively Exploited (Zero-Day) 14 | Used by attackers as an initial foothold to establish persistent access and deploy web shells, a common tactic for APTs targeting critical infrastructure.15 |
| **CVE-2025-55177** | WhatsApp iOS and Mac | Zero-click RCE | N/A | Actively Exploited (Zero-Day) 14 | Part of a sophisticated spyware campaign, it demonstrates the vulnerability of personal devices, which are often a weak link for high-value targets.14 |
| **CVE-2018-0171** | Cisco Smart Install | RCE | N/A | Actively Exploited 6 | An old, seven-year-old vulnerability actively exploited by Russian FSB actors to compromise and collect configuration files from critical infrastructure networks.6 |
| **CVE-2025-38352** | Linux Kernel | Time-of-Check Time-of-Use | N/A | Actively Exploited (KEV Catalog) 11 | A highly critical vulnerability that could allow an attacker to gain a foothold on Linux-based systems.11 |
| **CVE-2025-53690** | Sitecore Multiple Products | Deserialization of Untrusted Data | N/A | Actively Exploited (KEV Catalog) 11 | An actively exploited flaw in a content management system that could lead to full system compromise.11 |

## V. Sector-Specific Impact & Case Studies

This section ties the broader trends and vulnerabilities to specific critical infrastructure sectors, providing a direct mapping of the intelligence to operational realities.

### Manufacturing & Critical Manufacturing

The manufacturing sector was a primary target this week, facing threats from both highly organized cybercriminals and state-sponsored actors. The breach at **Jaguar Land Rover (JLR)** is the most significant public case.2 The cyberattack resulted in a prolonged production halt at its UK and global factories. The cascading effects extended to suppliers and retailers, who were left operating without the computer systems and databases necessary for sourcing parts or registering vehicles. The prolonged physical and financial disruption serves as a stark case study in the real-world consequences of a cyberattack on a large industrial player. The claimed responsibility by the Scattered Spider/LAPSUS$ alliance 2 demonstrates the growing appetite of major criminal groups for high-impact industrial sabotage.

Complementing this, the active exploitation of the **Dassault Systèmes DELMIA Apriso** vulnerability (CVE-2025-5086) poses a direct, systemic threat to the sector's operational technology.3 As this software manages core production processes, an attacker who exploits this flaw could gain a foothold to disrupt, manipulate, or halt production across an entire network.

### Energy & Water

The DHS HTA for 2025 confirms that both Russia and the PRC are actively targeting the Energy and Water sectors for pre-positioning and disruptive attacks.5 The FBI's recent warning about the Russian FSB's campaign exploiting legacy protocols and end-of-life devices 6 is a direct and actionable threat to the Supervisory Control and Data Acquisition (SCADA) and other industrial control systems that manage power grids and water treatment facilities. The fact that a nation-state is successfully exploiting a seven-year-old vulnerability to collect configuration files from thousands of devices demonstrates a persistent and critical gap in the cyber defenses of these sectors. The European Commission's call for a stronger EU energy security framework 16 is a direct policy response to these escalating geopolitical and cyber threats.

### Financial Services

The financial services sector, including fintech and cryptocurrency, was directly affected by the **"Great NPM Heist."** The attack's ultimate goal was not just to compromise software, but to steal cryptocurrency by hijacking wallet transactions and replacing addresses.1 This incident, which impacted packages used by a vast swathe of the digital economy, proves that an organization's perimeter is now inextricably linked to the security of the entire open-source ecosystem. Furthermore, the data breach at

**TransUnion**, a major consumer credit reporting agency, resulted in the exposure of sensitive personal information for over 4.4 million individuals.14 This includes full names, billing addresses, phone numbers, and unredacted Social Security Numbers, highlighting the persistent threat of large-scale data theft in the financial services sector.

### Government Facilities

Government networks remain a primary target for both espionage and disruptive attacks. The **State of Nevada** experienced a cyberattack that resulted in widespread disruption of government services, websites, and phone systems.14 This is a real-world example of how a successful attack can impact public administration and the delivery of essential services. Chinese-linked groups like Linen Typhoon are actively targeting government agencies such as the U.S. Department of Homeland Security and the National Institutes of Health.1 This persistent targeting demonstrates that government systems are a primary objective for intelligence gathering and strategic pre-positioning.

| Critical Infrastructure Sector | Relevant Threat(s) | Specific Incident(s) from this Week | Strategic Implication |
| --- | --- | --- | --- |
| **Manufacturing** | Nation-State & Organized Cybercrime, Supply Chain Vulnerabilities | **Jaguar Land Rover (JLR)** production halt due to cyberattack.2 Active exploitation of | **Dassault Systèmes DELMIA Apriso** vulnerability (CVE-2025-5086).3 | Digital attacks are now causing direct, prolonged physical and financial disruption to industrial operations. The IT/OT nexus is a key attack surface. |
| **Energy & Water** | Nation-State, Poor Cyber Hygiene | Russian FSB's exploitation of legacy networking devices.6 DHS HTA confirms targeted pre-positioning by PRC, Russia, Iran.5 EU launches review of energy security framework.16 | Adversaries are not just targeting new zero-days; they are exploiting basic, decades-old security gaps to gain persistent access to critical utility control systems. |
| **Financial Services** | Cybercrime, Software Supply Chain | The **"Great NPM Heist"** and its targeting of cryptocurrency wallets.1 | **TransUnion** data breach exposing sensitive financial and personal data.14 | The financial sector's reliance on open-source code and third-party vendors creates a vast and vulnerable attack surface, moving the security perimeter far beyond traditional network boundaries. |
| **Government Facilities** | Nation-State, Disruptive Attacks | **State of Nevada** services disrupted by a cyberattack.14 Chinese-linked groups targeting the U.S. Department of Homeland Security and National Institutes of Health.1 | Government systems are a primary objective for both intelligence gathering (espionage) and highly visible, disruptive attacks designed to impact public confidence and administration. |

## VI. Strategic Recommendations & Outlook

The intelligence from the past week synthesizes into clear, actionable guidance for executive leadership. The dominant message is that the threat landscape is defined by a dangerous paradox: sophisticated adversaries are finding success by exploiting fundamental flaws in an organization's defense.

First, an immediate return to **foundational cyber hygiene** is an imperative. The FBI's warning about the exploitation of a seven-year-old vulnerability by Russian state-sponsored actors 6 serves as a powerful reminder that complex, expensive security tools are irrelevant if basic controls are ignored. The first priority for any organization must be to identify and replace all end-of-life devices and to prioritize the timely patching of all known exploited vulnerabilities, especially those listed in the CISA KEV catalog.10

Second, organizations must fundamentally **re-evaluate their supply chain risk management**. The "Great NPM Heist" 1 and the Salesloft/Drift incident 4 prove that a company's perimeter extends far beyond its own network. It now includes every third-party vendor, every cloud service provider, and every open-source library used in its software. Organizations must move toward a holistic view of supply chain risk, from the enterprise software they purchase to the code libraries those vendors use. The adoption of a Software Bill of Materials (SBOM) is no longer a technical recommendation but a strategic necessity, as recognized by guides from CISA and its international partners.17

Third, security teams must enhance their **threat intelligence and response capabilities**. The apparent shutdown of a major criminal group 4 and the re-tooling of old malware for new attacks 3 demonstrate that a superficial understanding of threats is insufficient. Security teams must look beyond public-facing announcements and analyze the underlying tactics and motivations. This requires an in-depth threat intelligence function that can identify tactical shifts and anticipate future attacks.

The future outlook, as highlighted in the DHS Homeland Threat Assessment 5, is a continued rise in physical and disruptive attacks on critical infrastructure. This week's events—from the JLR production halt to the active exploitation of industrial control systems—show that this is not a distant threat. The future of cyber conflict will increasingly be defined by attacks that transition from the digital realm into the physical world, impacting public safety, economic stability, and national security. The time to prepare for this future is not tomorrow, but now.

#### Works cited

1. The Cybersecurity Battleground: September 2025's Most Critical ..., accessed September 15, 2025, <https://breached.company/the-cybersecurity-battleground-september-2025s-most-critical-threats/>
2. Jaguar Land Rover says cyber-attack has affected 'some data ..., accessed September 15, 2025, <https://www.theguardian.com/business/2025/sep/10/jaguar-land-rover-says-cyber-attack-has-affected-some-data>
3. Critical CVE-2025-5086 in DELMIA Apriso Actively Exploited, CISA Issues Warning, accessed September 15, 2025, <https://thehackernews.com/2025/09/critical-cve-2025-5086-in-delmia-apriso.html>
4. FBI Warns of UNC6040 and UNC6395 Targeting Salesforce Platforms in Data Theft Attacks, accessed September 15, 2025, <https://thehackernews.com/2025/09/fbi-warns-of-unc6040-and-unc6395.html>
5. Homeland Threat Assessment 2025 - Homeland Security, accessed September 15, 2025, <https://www.dhs.gov/sites/default/files/2024-10/24_0930_ia_24-320-ia-publication-2025-hta-final-30sep24-508.pdf>
6. Russian Government Cyber Actors Targeting Networking Devices, Critical Infrastructure, accessed September 15, 2025, <https://www.ic3.gov/PSA/2025/PSA250820>
7. Yurei the New Ransomware Group on the Scene - Check Point ..., accessed September 15, 2025, <https://research.checkpoint.com/2025/yurei-the-ghost-of-open-source-ransomware/>
8. Weekly Intelligence Report – 12 September 2025 - CYFIRMA, accessed September 15, 2025, <https://www.cyfirma.com/news/weekly-intelligence-report-12-september-2025/>
9. SonicWall SSLVPN Exploitation 'Ongoing' By Ransomware Group: Researchers - CRN, accessed September 15, 2025, <https://www.crn.com/news/security/2025/sonicwall-sslvpn-exploitation-ongoing-by-ransomware-group-researchers>
10. CISA Adds One Known Exploited Vulnerability to Catalog | CISA, accessed September 15, 2025, <https://www.cisa.gov/news-events/alerts/2025/09/11/cisa-adds-one-known-exploited-vulnerability-catalog>
11. CISA Adds Three Known Exploited Vulnerabilities to Catalog, accessed September 15, 2025, <https://www.cisa.gov/news-events/alerts/2025/09/04/cisa-adds-three-known-exploited-vulnerabilities-catalog>
12. September Patch Tuesday handles 81 CVEs – Sophos News, accessed September 15, 2025, <https://news.sophos.com/en-us/2025/09/10/september-patch-tuesday-handles-81-cves/>
13. Microsoft and Adobe Patch Tuesday, September 2025 Security Update Review | Qualys, accessed September 15, 2025, <https://blog.qualys.com/vulnerabilities-threat-research/2025/09/09/microsoft-patch-tuesday-september-2025-security-update-review>
14. 1st September – Threat Intelligence Report - Check Point Research, accessed September 15, 2025, <https://research.checkpoint.com/2025/1st-september-threat-intelligence-report/>
15. The Operational Technology Threat Landscape: Insights from IBM X-Force, accessed September 15, 2025, <https://www.ibm.com/think/x-force/the-operational-technology-threat-landscape-insights-from-x-force>
16. Commission takes first step to strengthen the EU's energy security framework, accessed September 15, 2025, <https://energy.ec.europa.eu/news/commission-takes-first-step-strengthen-eus-energy-security-framework-2025-09-15_en>
17. CISA: Home Page, accessed September 15, 2025, <https://www.cisa.gov/>