# OTCE\_SOTI\_MANU\_2025\_8\_July

## **Executive Summary**

The manufacturing sector remains a top target for a diverse range of threat actors, from state-sponsored Advanced Persistent Threats (APTs) to financially motivated ransomware gangs, during July 2025. The period was marked by a significant increase in attacks on critical infrastructure and industrial control systems (ICS) and a troubling convergence of state-sponsored and cybercriminal tactics.

A key development is the blurring of lines between state-sponsored and financially motivated actors, with groups leveraging similar tools and techniques for different ends, such as espionage versus extortion.1 The Ingram Micro ransomware attack serves as a definitive case study of how a single compromise in the IT supply chain can cause cascading operational and financial disruption across the broader manufacturing ecosystem.3 The month also saw the active exploitation of critical zero-day vulnerabilities in widely used software like WinRAR and Microsoft SharePoint, demonstrating a shift in attacker focus toward subverting trusted perimeter and communication tools.5 Geopolitical tensions, particularly surrounding the U.S.-China-Taiwan semiconductor supply chain, are directly manifesting in targeted cyberattacks for intellectual property theft and long-term disruption.7 The true cost of attacks is increasingly dominated by indirect losses, such as operational downtime and supply chain fallout, which can account for up to 70% of total financial damage and often lead to precautionary shutdowns of operational technology (OT) systems.9

This analysis indicates that organizations must move beyond traditional perimeter defenses and implement a holistic, risk-based security posture that addresses supply chain dependencies, protects converged IT/OT networks, and prepares for sophisticated, AI-enhanced social engineering campaigns.

## **1. Threat Landscape: Manufacturing Sector Overview (July 2025)**

The manufacturing sector continues to face the highest volume of cyberattacks globally, accounting for 26% of all recorded email threats in Q2 2025. The semiconductor industry, a key segment of manufacturing, has seen a sixfold surge in attacks since 2022, a trend driven by both espionage and supply-chain compromises.7 This persistent targeting is rooted in several inherent vulnerabilities unique to the industry. Manufacturers operate under high-pressure conditions where any downtime immediately halts production, leading to severe financial losses.11 This operational pressure is a strategic lever for adversaries, who can use the threat of business interruption to demand quick ransom payments.11 Furthermore, many manufacturing facilities rely on legacy ICS and SCADA platforms that lack modern security controls, creating a vast and vulnerable attack surface.11

Geographically, the threat is not evenly distributed. The United States remains the most attacked country by a significant margin, with 223 ransomware victims in July alone, a number eight times greater than second-place Canada.13 North America has been identified as a primary hotspot and "ground zero for OT cyberattacks" due to the region's appeal to threat actors and the rapid pace of industrial digitalization.9 Europe is the second most targeted region, with Italy, the United Kingdom, Germany, France, and Spain experiencing a high number of victims. The rapid expansion of the attack surface, fueled by industrial digitalization and the proliferation of connected IoT devices, has made once-isolated OT systems increasingly internet-facing and remotely accessible. This trend has placed critical infrastructure squarely in the crosshairs of a diverse range of adversaries.9

## **2. Threat Actor Profiles and Campaign Analysis**

### **2.1 Financially Motivated Actors: Ransomware and Extortion Gangs**

Ransomware remains the dominant threat to the manufacturing sector, with attacks jumping by 46% from Q4 2024 to Q1 2025.16 July 2025 continued this trend, with manufacturing being the third most targeted industry by ransomware, suffering 39 attacks during the month.13 This threat is driven by a number of prominent groups and Ransomware-as-a-Service (RaaS) operations.

* **Cl0p:** This group was the most prolific in Q1 2025, accounting for approximately 22% of global ransomware activity. The group's significant surge was driven by the exploitation of Cleo Managed File Transfer vulnerabilities, which heavily impacted manufacturing supply chains.2
* **SafePay/Akira:** The SafePay group was responsible for the high-profile Ingram Micro attack in July, which caused a global outage and severely disrupted operations.3 However, one source attributes this same attack to the Akira ransomware gang, which is also known for double extortion and targeting manufacturing.2 The discrepancy in attribution underscores the evolving and often obfuscated nature of modern cybercrime, where groups may operate under different names or share tools and affiliates.
* **InterLock:** This group claimed responsibility for the March 2025 attack on National Presto Industries, a company that supplies a military contractor.11 The group alleged it stole millions of files and encrypted systems, which points to a strategic choice of target that blurs the lines between purely financial motivation and state-sponsored espionage.
* **Sarcoma:** A RaaS group that used double extortion and supply chain attacks to disrupt operations at Unimicron, a global leader in printed circuit board production, in late January 2025.11

A particularly concerning trend in 2025 is the fusion of cybercrime and state-sponsored attacks.1 Groups like Qilin have been linked to "nation-state convergence," suggesting they are not solely driven by financial gain but may be used as a tool of statecraft.2 This hybrid approach complicates attribution, allowing state actors to leverage the financial motives of criminal groups to achieve strategic objectives while maintaining plausible deniability.

### **2.2 State-Sponsored and Espionage Actors: APTs**

Nation-state actors are well-resourced and highly trained groups that are shifting their focus from simple data theft to long-term disruption strategies that can cripple production during geopolitical flashpoints.1 Their primary goals are espionage, data theft, and network disruption, often with a focus on critical infrastructure and defense contractors.12

* **APT41:** This China-backed APT group launched a targeted campaign in July 2025, infiltrating multiple Taiwanese semiconductor companies through a compromised software update. The group's objective was to steal proprietary chip designs and process data, a clear example of economic espionage linked directly to geopolitical competition over the semiconductor industry.7
* **Volt Typhoon:** A Chinese state-sponsored group that has demonstrated the capability to access critical infrastructure systems in Guam and the continental United States using stealthy "living-off-the-land" techniques.21 The group's focus on power grids and water controls indicates a strategic objective of pre-positioning for potential disruption during a future conflict.21
* **UNC5221:** This state-affiliated actor highlights the vulnerability of remote access systems. The group exploited a vulnerability in ICS VPN appliances (CVE-2025-22457) to pivot into OT networks, demonstrating that VPNs are a critical entry point for nation-state espionage.7
* **RomCom Group:** This group used a zero-day vulnerability in WinRAR (CVE-2025-8088) as part of a spearphishing campaign observed in July. The campaign specifically targeted financial, manufacturing, defense, and logistics companies in Europe and Canada.5

The data suggests a sophisticated interplay between trade policy, economic pressure, and cyber espionage. A government may use tariffs to incentivize domestic production, while state-backed actors simultaneously conduct cyberattacks to steal the very intellectual property the tariffs are designed to protect.7 This strategic feedback loop represents a new, complex threat model where cyber espionage is used as an asymmetric response to economic policies, undermining their effectiveness and turning any company with strategic intellectual property into a target.7

## **3. Attack Campaigns: A July 2025 Timeline**

The following case studies provide a detailed view of the most significant cyber incidents impacting the manufacturing and related sectors in July 2025.

### **Case Study: The Ingram Micro SafePay Ransomware Attack (July 3-4, 2025)**

The Ingram Micro attack, a defining incident of the month, began over the July 4th holiday weekend, a period often exploited by threat actors to maximize damage before discovery.3 The SafePay ransomware gang reportedly gained initial access through a misconfigured or unpatched VPN gateway using stolen credentials, a common tactic for this group.4 This attack vector has become a high-value target for adversaries, challenging the long-held assumption that perimeter and access tools are the primary line of defense.26

Once inside, the SafePay group encrypted critical systems, including Ingram Micro's Xvantage distribution platform and Impulse license provisioning system, which are used for order fulfillment and partner services globally.3 The attackers also reportedly exfiltrated sensitive data before encrypting the systems, suggesting a double extortion strategy.4 The attack forced the company to shut down its internal systems, causing a global outage and a ripple effect of "cascading delays" for vendors, resellers, and enterprise procurement teams.4 Ingram Micro's response included company-wide password and MFA resets, phased system recovery, and enhanced monitoring.3

### **Case Study: RomCom Group's WinRAR Zero-Day Campaign (July 18-21, 2025)**

On July 18, 2025, security researchers discovered a previously unknown zero-day vulnerability in WinRAR, now identified as CVE-2025-8088, which the RomCom group was actively exploiting.5 This path traversal vulnerability used alternate data streams (ADS) to hide malicious files within a seemingly benign RAR archive.5 The campaign, which lasted from July 18-21, used spearphishing emails with job application lures to target manufacturing, defense, and financial companies in Europe and Canada.5

When a victim opened the crafted archive, the malicious files were silently deployed to the system.5 The payloads varied, including a Mythic agent, a SnipBot variant, and a RustyClaw downloader, which often used anti-analysis conditions to evade detection.5 To achieve persistence, the attackers used a malicious LNK file to add the payload to the Windows startup directory, ensuring execution upon user login.5 WinRAR released a patched version on July 30, 2025, to address the vulnerability.5

The following table provides a summary of other significant publicly disclosed cyberattacks and related activities in July 2025.

| Date | Affected Entity | Threat Actor (Claimed) | Attack Vector | Impact Summary |
| --- | --- | --- | --- | --- |
| July 2-10 | Ingram Micro | SafePay/Akira | Stolen VPN credentials | Global outage, disrupted distribution and licensing platforms, delayed orders and shipments. |
| July 18-21 | Multiple Manufacturing, Defense, and Financial firms in Europe and Canada | RomCom Group | WinRAR zero-day (CVE-2025-8088) | Spearphishing campaign delivering various backdoors via a path traversal vulnerability. |
| July 20 | U.S. National Guard | Chinese state-backed hackers | Unknown | Breach to steal network configurations, potentially exposing sensitive infrastructure details. |
| July 20 | Dell | World Leaks | Unknown | Breach of a test lab platform resulting in unauthorized access to limited customer information. |
| Throughout July | Various | Qilin, Cl0p, RansomHub | Various, including MFT exploits and RaaS model | Qilin ransomware claims over 70 victims in July; RansomHub is associated with an attacking IP address in the Ingram Micro attack.3 |

## **4. Technical Vulnerability and TTP Analysis**

### **4.1 Zero-Day and Critical Vulnerabilities**

A significant trend in July 2025 was the active exploitation of zero-day vulnerabilities in widely used software and perimeter devices. This demonstrates a shift in adversary focus toward subverting trusted applications and network security tools.

* **WinRAR Path Traversal (CVE-2025-8088):** Discovered in July, this vulnerability allowed attackers to execute a malicious file by hiding it within a RAR archive using alternate data streams. The exploit enabled the silent deployment of payloads, including the Mythic agent and RustyClaw downloader, in targeted spearphishing campaigns.5
* **Microsoft SharePoint RCE (CVE-2025-53770):** A new Remote Code Execution (RCE) vulnerability chain, dubbed "ToolShell," was actively exploited in the wild, starting on July 18, 2025, to compromise on-premise SharePoint servers globally.6 This highlights a critical vulnerability in a widely deployed enterprise application and the ongoing threat to on-premise systems.
* **Perimeter Device Vulnerabilities:** A critical SQL injection vulnerability (CVE-2025-25257) with a CVSS score of 9.6 was patched in Fortinet's FortiWeb firewall, allowing unauthenticated remote command execution.26 This incident, alongside the UNC5221 campaign that exploited an ICS VPN appliance vulnerability (CVE-2025-22457), demonstrates a systemic problem where perimeter defenses themselves are becoming the new breach vector.7

### **4.2 Key Tactics, Techniques, and Procedures (TTPs)**

Threat actors targeting the manufacturing sector are using a combination of persistent and emerging TTPs to achieve their objectives.

* **Initial Access & Execution:** Attackers are using AI-enhanced, hyper-personalized phishing campaigns, which are becoming more difficult to detect.1 The "ClickFix" social engineering technique experienced a 517% surge, as it bypasses traditional security controls by relying on user execution rather than exploit delivery.3 Attacks like the one on Ingram Micro also show that gaining access through compromised perimeter devices, such as VPNs and firewalls, is a preferred method for initial access.4
* **Defense Evasion & Persistence:** Ransomware groups like RansomHub are leveraging advanced tools such as EDRKillshifter to evade Endpoint Detection and Response (EDR) systems.2 Furthermore, many manufacturing facilities still rely on outdated ICS and SCADA platforms, which lack modern security controls and provide a persistent, attractive target for a wide range of threat actors.11 The use of custom and heavily obfuscated phishing kits also makes it difficult for security teams to reverse-engineer or detect malicious campaigns.10
* **Exfiltration and Command-and-Control (C2):** Attackers often use a variety of methods to exfiltrate stolen data, from legitimate file shares and database read volumes to anomalous DNS requests.29 The C2 infrastructure is a key component of these attacks, as seen with the dismantling of four C2 servers and nine domains used by the BlackSuit ransomware group for deploying payloads and extorting victims.28

The following table summarizes the most critical vulnerabilities and exploits observed in July 2025.

| CVE ID | Affected Product | Vulnerability Type | CVSS Score (if available) | Active Exploitation | Associated Threat Actors/Campaigns |
| --- | --- | --- | --- | --- | --- |
| CVE-2025-8088 | WinRAR | Path Traversal via ADSes | Not available | Yes, as of July 18, 2025 | RomCom Group, targeting manufacturing, defense, and financial sectors. |
| CVE-2025-53770 | Microsoft SharePoint | Remote Code Execution | Not available | Yes, as of July 18, 2025 | "ToolShell" exploit chain, compromising on-premise SharePoint servers. |
| CVE-2025-25257 | Fortinet FortiWeb firewall | SQL Injection | 9.6 | Not available | N/A, vulnerability disclosure in July 2025. |
| CVE-2025-22457 | ICS VPN appliances | Unknown | Not available | Yes | UNC5221, a state-affiliated actor. |

## **5. Geopolitical Context and Strategic Espionage**

The cyber domain has become a primary theater for international conflict, with mounting geopolitical competition leading to an increase in the scope and sophistication of cyberattacks.1 Geopolitical events can be a direct precursor to targeted cyber campaigns.

The semiconductor industry provides a clear example of this dynamic. Taiwan's dominance in dedicated contract chipmaking, with a 64% global market share, makes it a critical geopolitical linchpin.8 A conflict or blockade in the region could result in a catastrophic global economic loss of $10 trillion, far exceeding other recent conflicts.8

The U.S. has implemented trade policies, such as the proposed 100% tariff on semiconductor imports, to force a strategic shift of chip production to American soil and reduce dependency.24 This economic pressure has led to a direct response in the cyber domain. In July 2025, the China-backed APT41 group infiltrated multiple Taiwanese semiconductor companies to steal proprietary chip designs and process data.7 This is not a coincidence; it is a sophisticated, strategic feedback loop where cyber espionage is used as an asymmetric response to economic policies, aimed at obtaining the technology that the tariffs are designed to protect. For the manufacturing sector, this means that companies with strategically valuable intellectual property are at risk of being targeted by state-sponsored actors, regardless of their direct ties to government or defense contracts.11

## **6. Impact and Financial Assessment**

### **6.1 Financial Impact: The Cost of a Breach**

The financial impact of cyberattacks on the manufacturing sector is escalating at an alarming rate. According to a new Dragos-Marsh McLennan report, global losses from cyberattacks on the sector are rising by 125% each year, a faster rate than in any other industry.11 The report warns that global OT cyber risk exposure could exceed $300 billion, with a worst-case scenario projecting a global financial risk of $329.5 billion.9

A crucial finding from this analysis is that indirect losses often dominate the total cost of a breach, accounting for up to 70% of the financial impact.9 These costs extend far beyond the immediate ransom payment or data theft and include business interruption, supply chain fallout, recovery costs, and reputational damage.9 This indicates that organizations that focus solely on preventing a ransom payment are strategically underestimating their total financial exposure.

### **6.2 Operational and Supply Chain Disruption**

The convergence of IT and OT networks means that a compromise in one can lead to a shutdown of the other. The report has documented multiple incidents where a cyber incident led directly to operational disruption. Attacks on Nucor Corporation, Masimo, and National Presto Industries all resulted in the suspension of production or temporary shutdowns to contain the breach, demonstrating the tangible link between a cyber incident and physical operational disruption.11

The Ingram Micro attack serves as a prime example of a cascading supply chain failure. The outage of its IT systems caused widespread disruption to its downstream customers, delaying order processing, shipments, and licensing for partners.4 This highlights the systemic risk inherent in an interconnected, digitally dependent ecosystem and demonstrates that the real financial risk is not the ransom itself, but the systemic and cascading operational damage that can cripple entire supply chains.

## **7. Strategic Recommendations for Mitigation**

Based on the analysis of the threat landscape in July 2025, the following strategic recommendations are provided to enhance the manufacturing sector's cyber resilience:

* **Implement a Zero Trust Architecture:** The failure of traditional perimeter defenses, such as VPNs and firewalls, necessitates a shift to a Zero Trust model that assumes no user or device can be trusted by default. This approach helps to contain lateral movement and limit the impact of an initial compromise.26
* **Harden Remote Access Infrastructure:** The Ingram Micro attack and the UNC5221 campaign highlight VPNs as a critical entry point for threat actors. Organizations must enforce strong multi-factor authentication (MFA), regularly patch all VPN appliances, and actively monitor for unusual login attempts and traffic.4
* **Prioritize Risk-Based Vulnerability Management:** A risk-based approach to vulnerability management is critical. Security teams should prioritize patching flaws that are known to be actively exploited in the wild, such as the WinRAR and SharePoint zero-days observed in July, rather than patching indiscriminately.5
* **Enhance Supply Chain Cyber Resilience:** Given the prevalence of supply chain attacks, manufacturers must increase due diligence on third-party vendors and develop clear incident response plans that include communication protocols for downstream partners. This will help mitigate the cascading effects of a single breach.4
* **Address the Human Element:** The rise of AI-enhanced social engineering and tactics like "ClickFix" requires a more sophisticated approach to employee training. Organizations must move beyond generic advisories and focus on helping employees recognize advanced, hyper-personalized attacks.1
* **Improve IT/OT Network Segmentation and Visibility:** To prevent an IT network compromise from causing a costly shutdown of OT systems, organizations must implement robust network segmentation. This limits the blast radius of an attack and ensures operational continuity in the event of an incident.9
* **Report and Collaborate:** Organizations should urgently report potential malicious activity to authorities like CISA and the FBI. Collaboration with government and law enforcement is essential for developing a broader defense against sophisticated nation-state actors.19

#### Works cited

1. Nation-State Cyberwarfare Escalates in 2025: APT Groups Target Critical Infrastructure, accessed August 14, 2025, <https://synconova.com/2025/06/12/nation-state-cyberwarfare-2025-apt-groups-critical-infrastructure/>
2. Dragos Industrial Ransomware Analysis: Q1 2025, accessed August 14, 2025, <https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q1-2025/>
3. Weekly Report: New Hacking Techniques and Critical CVEs July 2-10, 2025 - FireCompass, accessed August 14, 2025, <https://firecompass.com/weekly-report-new-hacking-techniques-and-critical-cves-july-2-10/>
4. IT provider Ingram Micro hit by SafePay ransomware - Field Effect, accessed August 14, 2025, <https://fieldeffect.com/blog/it-provider-ingram-micro-hit-by-safepay-ransomware>
5. Update WinRAR tools now: RomCom and others exploiting zero-day ..., accessed August 14, 2025, <https://www.welivesecurity.com/en/eset-research/update-winrar-tools-now-romcom-and-others-exploiting-zero-day-vulnerability/>
6. Eye Security Uncovers Actively Exploited Zero-Day in Microsoft ..., accessed August 14, 2025, <https://www.eye.security/blog/eye-security-uncovers-actively-exploited-zero-day-in-microsoft-sharepoint-cve-2025-53770>
7. Six-Fold Surge in Cyberattacks and $1B in Ransomware Losses Are ..., accessed August 14, 2025, <https://www.ien.com/artificial-intelligence/news/22947866/sixfold-surge-in-cyberattacks-and-1b-in-ransomware-losses-are-reshaping-the-global-semiconductor-industry>
8. The World's Growing Reliance on Taiwan's Semiconductor Industry - Vision of Humanity, accessed August 14, 2025, <https://www.visionofhumanity.org/the-worlds-dependency-on-taiwans-semiconductor-industry-is-increasing/>
9. 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/>
10. Manufacturing sector remains top target for cyber criminals, new report warns, accessed August 14, 2025, <https://www.themanufacturer.com/articles/manufacturing-sector-remains-top-target-for-cybercriminals-new-report-warns/>
11. Major Cyber Attacks Targeting Manufacturing Industry in 2025 ..., accessed August 14, 2025, <https://socradar.io/major-cyber-attacks-manufacturing-industry-in-2025/>
12. Top 7 Cyber Attacks Threatening Manufacturing Companies - BitLyft, accessed August 14, 2025, <https://www.bitlyft.com/resources/cyber-attacks-threatening-manufacturing-companies>
13. 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/>
14. New Google Cloud–Mandiant report warns of escalating cyber threats to manufacturing, energy OT systems, accessed August 14, 2025, <https://industrialcyber.co/reports/new-google-cloud-mandiant-report-warns-of-escalating-cyber-threats-to-manufacturing-energy-ot-systems/>
15. Top Cyber Threats in Manufacturing | MxD, accessed August 14, 2025, <https://www.mxdusa.org/2025/02/13/top-cyber-threats-in-manufacturing/>
16. Ransomware Attacks Targeting Industrial Operators Surge 46% in One Quarter, Honeywell Report Finds, accessed August 14, 2025, <https://www.honeywell.com/us/en/press/2025/06/ransomware-attacks-targeting-industrial-operators-surge-46-percent-in-one-quarter-honeywell-report-finds>
17. Ingram Micro Ransomware Attack: Strengthening Supply Chain Risk Assessment, accessed August 14, 2025, <https://firecompass.com/ingram-micro-ransomware-attack-strengthening-supply-chain-risk-assessment/>
18. July 2025: Biggest Cyber Attacks, Ransomware Attacks and Data ..., accessed August 14, 2025, <https://www.cm-alliance.com/cybersecurity-blog/july-2025-biggest-cyber-attacks-ransomware-attacks-and-data-breaches>
19. Nation-State Threats | Cybersecurity and Infrastructure Security Agency CISA, accessed August 14, 2025, <https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors>
20. Cyber threats to financial stability in a complex geopolitical landscape, accessed August 14, 2025, <https://www.ecb.europa.eu/press/financial-stability-publications/fsr/focus/2025/html/ecb.fsrbox202505_01~5b8c62e6c6.en.html>
21. US military readiness in the Pacific requires strengthening Guam's power grid - Atlantic Council, accessed August 14, 2025, <https://www.atlanticcouncil.org/blogs/energysource/us-military-readiness-in-the-pacific-requires-strengthening-guams-power-grid/>
22. Closing the Gaps in the Strengthening Cyber Resilience Act | ITIF, accessed August 14, 2025, <https://itif.org/publications/2025/08/11/closing-the-gaps-in-the-strengthening-cyber-resilience-act/>
23. Homeland Threat Assessment 2025, accessed August 14, 2025, <https://www.dhs.gov/sites/default/files/2024-10/24_0930_ia_24-320-ia-publication-2025-hta-final-30sep24-508.pdf>
24. Trump's 100% tariff likely to shift more Taiwan's semiconductor industry to US, accessed August 14, 2025, <https://m.economictimes.com/tech/technology/trumps-100-tariff-likely-to-shift-more-taiwans-semiconductor-industry-to-us/articleshow/123187116.cms>
25. Taiwan's Semiconductor Industry Outlook Amid the U.S. 100% Tariff Surge in 2025, accessed August 14, 2025, <https://datatrack.trendforce.com/blog/content/43433/taiwans-semiconductor-industry-outlook-amid-the-u-s-100-tariff-surge-in-2025>
26. Cyber Attack News – Risk Roundup – Top Stories for July 2025 - Xage Security, accessed August 14, 2025, <https://xage.com/blog/cyber-attack-news-risk-roundup-top-stories-for-july-2025/>
27. Ransomware attack on major IT reseller leaves MSPs dangling - The Stack, accessed August 14, 2025, <https://www.thestack.technology/ransomware-attack-on-major-it-reseller-leaves-msps-dangling/>
28. Law Enforcement Seizes BlackSuit Ransomware Servers Targeting ..., accessed August 14, 2025, <https://gbhackers.com/law-enforcement-seizes-blacksuit-ransomware/>
29. Indicators of Compromise (IOCs) - Fortinet, accessed August 14, 2025, <https://www.fortinet.com/resources/cyberglossary/indicators-of-compromise>
30. What Is Data Exfiltration? Meaning & Prevention | Proofpoint US, accessed August 14, 2025, <https://www.proofpoint.com/us/threat-reference/data-exfiltration>
31. Geopolitical Risk Dashboard | BlackRock Investment Institute, accessed August 14, 2025, <https://www.blackrock.com/corporate/insights/blackrock-investment-institute/interactive-charts/geopolitical-risk-dashboard>
32. Cybercrime To Cost The World $10.5 Trillion Annually By 2025, accessed August 14, 2025, <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>