CYBERSECURITY EXECUTIVE BRIEF: JULY 2025

Cybersecurity Insights for Decision-Makers | 2-Minute Executive Summary | Full Analysis: ~10 Pages

---

EXECUTIVE SUMMARY: NATION-STATE AND AI THREATS RESHAPE DEFENSES

July 2025 signals a seismic shift in cybersecurity, with nation-state hackers and AI-driven malware outpacing traditional defenses. Chinese Salt Typhoon breached nine U.S. telecoms, including Verizon and AT&T, harvesting metadata from over one million users via lawful intercept systems [1-4]. Russia's APT28 unleashed LAMEHUG, the first LLM-powered malware, using Hugging Face APIs for adaptive attacks [25]. A SharePoint zero-day (CVE-2025-53770) hit 400+ organizations, including nuclear security [5-8]. Healthcare faced 444 ransomware attacks, with DaVita losing 900,000 records [12-14]. Leaders must pivot to resilience to stay ahead of relentless threats.

Critical Actions Required

- 🔴 **IMMEDIATE:** Rotate all SharePoint ASP.NET MachineKeys—400+ organizations hit via CVE-2025-53770 [5-8].
- 🔴 **THIS WEEK:** Implement out-of-band verification for all privileged access changes—helpdesk social engineering is the primary attack vector [9-11].
- 🟡 **THIS MONTH:** Develop and thoroughly test redundant telecommunications using diverse providers; plan for scenarios where all channels are down for 72 hours or multiple days due to Salt Typhoon's infrastructure control [1-4].
- 🟢 **MONITOR:** Deploy behavioral analytics to counter AI-driven malware—signature detection struggles against adaptive threats [25].

Key Metrics and Trends

Metric	This Month	Change	Impact
Major Breaches	176M people	+45%	$142M crypto stolen [51-52]
Days to Exploit	4 days	-60%	Patch windows shrinking [32]
Ransoms Paid	$1.8M avg	+28%	Healthcare remains a top target [12-14]
Top Sector Hit	Healthcare	444 incidents	17-day recovery [12-14]

Board Takeaways

- **Infrastructure at Risk:** With Salt Typhoon extracting metadata from 1M users across nine U.S. telecoms, build redundancy for critical communications now [1-4].
- **AI-Driven Threats:** Malware adapts faster than traditional defenses; prioritize behavioral analytics [25].
- **Third-Party Vulnerabilities:** Helpdesks are a primary attack vector; verify all access changes out-of-band [9-11, 26-28].
- **Resilience First:** Plan for 17-day disruptions; insurance may exclude nation-state attacks [41].

Act now to build resilience or risk becoming August's breach statistic. Full analysis below.

STRATEGIC CYBERSECURITY DEEP DIVE: JULY 2025

Actionable Insights for Leaders

1. Overview: Decoding July's Cyber Threat Surge

July 2025 exposed a new battleground in cybersecurity, with advanced actors exploiting trusted systems and AI innovations. Salt Typhoon's telecom breach—labeled the worst in U.S. history by the FBI—compromised nine carriers, exposing metadata from one million users [1-4]. APT28's AI-driven LAMEHUG malware evaded defenses via real-time adaptation [25]. A SharePoint zero-day hit 400+ organizations, including nuclear infrastructure [5-8]. Healthcare remains a top target, with historic data showing most victims paying, but no publicly confirmed healthcare ransom payments in July 2025 [12-14, 51-52]. Resilience is now non-negotiable in this contested digital landscape. Nation-state actors (Salt Typhoon, APT28) and criminal groups (ShinyHunters) share tactics, from lawful intercept exploitation to third-party vishing [1-4, 25-28].

2. Critical Incidents

2.1 Top Five Incidents

1. Salt Typhoon's Telecommunications Control [1-4]

Chinese Ministry of State Security's Salt Typhoon maintained persistent access to nine U.S. telecoms (Verizon, AT&T, T-Mobile, others) for over a year, extracting metadata of more than a million Americans. They exploited CALEA lawful intercept systems, turning infrastructure against us [2-3].

- **Business Impact:** Communications are at risk of foreign intelligence monitoring.
- **Technical Details:** Exploits in Cisco IOS XE (CVE-2025-20281, CVE-2025-20282) [33], Demodex Windows rootkit, CALEA system compromise.
- **Responses and Outcomes:** Treasury sanctioned Sichuan Juxinhe Network [4]. FBI issued $10M bounties [4]. National Guard uncovered 12-month breach [1]. Telecoms remain vulnerable to metadata extraction, requiring alternative communication strategies.
- **Recommended Actions:** Implement end-to-end encryption. Test 72-hour telecom outage scenarios. Verify sensitive communications out-of-band.

2. SharePoint Zero-Day Breaches Nuclear Security [5-8]

Storm-2603, Linen Typhoon, and Violet Typhoon exploited CVE-2025-53770 (CVSS 9.8) for unauthenticated RCE on SharePoint 2016/2019/Subscription Edition. Over 4,600 attacks hit 400+ organizations, including the National Nuclear Security Administration (July 18) [6-7].

- **Business Impact:** Stolen MachineKeys enable persistent access. Patches alone are insufficient.

- **Technical Details:** MachineKey theft via pipe-delimited HTTP responses. 32% of vulnerabilities weaponized within 24 hours [32].
- **Responses and Outcomes:** Microsoft patched July 19 and 21 [8]. Despite patches, some organizations reported continued unauthorized access, highlighting the need for forensic analysis [7].
- **Recommended Actions:** Rotate all MachineKeys immediately. Enable AMSI. Conduct forensic analysis back to May 2025.

3. Allianz Life's Social Engineering Breach [9-11, 26-28]

ShinyHunters and Scattered Spider breached Salesforce CRM via third-party helpdesk vishing, stealing 1.4M SSNs, addresses, and birth dates. Attackers impersonated employees to reset MFA, leveraging a hybrid ransomware-extortion model [26-28].

- **Business Impact:** Third-party access is a critical vulnerability. Identity theft is likely.
- **Technical Details:** No vulnerabilities—pure social engineering. Similar attacks hit Qantas, LVMH [10].
- **Responses and Outcomes:** Allianz offered 24-month identity protection [9]. Others adopted callback verification [11]. Similar attacks on Qantas and LVMH indicate systemic third-party risks across industries [10, 23].
- **Recommended Actions:** Implement out-of-band verification for all privileged changes. Remove third-party production access where possible.

4. Healthcare's Ransomware Crisis [12-14, 40]

Interlock ransomware hit 444 healthcare organizations, with DaVita losing over 900,000 records [13]. Kettering Health was down three weeks [14]. Novel "ClickFix" technique tricks users into pasting malicious PowerShell [12].

- **Business Impact:** The average of downtime following ransomware incidents in healthcare is 17-days. More than enough to threaten patient care. [40].
- **Technical Details:** Drive-by downloads from legitimate sites. Base64-encoded PowerShell targets VMware ESXi [12].
- **Responses and Outcomes:** Texas Tech Health Sciences lost over 900,000 records [14]. Average ransom: $1.8M [12]. Some hospitals implemented offline backups, reducing recovery times by 20% where applied [40].
- **Recommended Actions:** Block PowerShell from browsers. Maintain 30-day offline backups. Contract incident response now.

5. Russia's LLM-Powered Malware [25]

APT28's LAMEHUG (attributed with medium confidence) malware uses Qwen2.5-Coder-32B via Hugging Face APIs to generate unique payloads per host, targeting Ukrainian government systems [25].

- **Business Impact:** Adaptive malware challenges traditional defenses, requiring new detection strategies.
- **Technical Details:** Cloud-hosted LLM generates Base64-encoded commands, hiding C2 in legitimate API traffic (api-inference.huggingface.co).
- **Responses and Outcomes:** Ukraine deployed behavioral detection [25]. Vendors rushed AI defenses. Early adopters of behavioral analytics reported 30% faster detection of adaptive threats [25].
- **Recommended Actions:** Deploy behavioral analytics. Monitor API traffic to AI services. Assume static defenses are ineffective.

2.2 Other Significant Incidents

- **Cloud Misconfigurations:** Sweden's Risika exposed 100M records via Elasticsearch [15]. McDonald's McHire leaked 64M applicant records with password "123456" [16]. UK Co-op lost 6.5M loyalty members' data via third-party [17, 23-24].
- **Supply Chain Attacks:** North Korea's 67 npm packages (17,000 downloads) [29-31]. Ingram Micro lost 3.5TB, disrupting global ordering [20-22].
- **Telecommunications:** Orange France faced service disruptions for corporate customers and customers services, potentially linked to Salt Typhoon [18-19].
- **Russian ISP Espionage:** Secret Blizzard/Turla conducted ISP-level MITM attacks on foreign embassies in Moscow via SORM infrastructure [36].
- **Smart Buildings:** 13 vulnerabilities in Honeywell's Tridium Niagara Framework exposed over 1M smart buildings to HVAC and physical security compromise [37-38].
- **Critical Infrastructure:** CISA reported train braking system vulnerabilities, increasing risks to transportation networks [39].

3. Key Threat Actors

- **China (Salt Typhoon, Storm-2603, Linen Typhoon):** Targets telecoms, government, nuclear infrastructure for persistent access. New: Weaponizing lawful intercept systems [1-4].
- **Russia (APT28, Secret Blizzard):** Disrupts Ukraine, tests AI warfare. New: LLM-powered malware [25], ISP-level MITM attacks [36].

- **North Korea (Contagious Interview):** Targets crypto and IP via fake technical interviews. New: 67 malicious npm packages [29-31].
- **Criminal Groups (Scattered Spider + ShinyHunters):** Hybrid ransomware-extortion targeting SaaS, healthcare. New: Operational merger [26-28].

4. New Attack Methods

- **AI-Powered Malware:** Generates unique payloads, adapts to defenses, uses legitimate AI infrastructure for C2 [25].
- **Helpdesk Social Engineering:** Primary enterprise attack vector, bypassing technical controls via vishing [9-11, 26-28].
- **ClickFix Exploitation:** Tricks users into pasting malicious PowerShell, framed as browser troubleshooting [12].
- **Zero-Day Weaponization:** 32% of vulnerabilities exploited within 24 hours, shrinking patch windows [32].

5. Sector Impact Analysis

- **Healthcare (38% of incidents):** 444 reported attacks, average 17-day recovery. DaVita: 915,952 records exposed (early 2025). Most affected organizations in recent years have paid ransoms, though July 2025 saw no publicly confirmed healthcare ransom payments.
- **Financial Services (12%):** Allianz Life: 1.4M PII including Tax IDs [9]. Helpdesk social engineering universal [26-28]. Out-of-band verification rare.
- **Technology (9%):** Ingram Micro: 3.5TB stolen [20-22]. npm supply chain attacks [29-31]. Locked registries with scanning effective.
- **Telecommunications (6%):** Salt Typhoon hit 9 carriers [1-4]. No successful defenses—assume compromise.
- **Critical Infrastructure:** Niagara Framework vulnerabilities expose smart buildings [37-38]. Train braking system flaws reported [39].

Cross-Industry Threats and Vulnerabilities

- SharePoint zero-days [5-8], third-party access exploitation [26-28], cloud misconfigurations [15-17], AI service APIs as attack infrastructure [25], Citrix vulnerabilities [34].

6. Regulatory Update

Regulatory Implications by Sector

- **Healthcare:** HHS considering mandatory ransom reporting [40].
- **Financial:** SEC probing disclosure delays [41].
- **Telecom:** FCC reviewing infrastructure security under CALEA Section 105 [42].

Regulatory Timeline

- **Effective Now:** Under CISA Binding Operational Directive 22-01, federal agencies must remediate KEV-listed vulnerabilities within **15 days for internet-facing** and **25 days for other listed** flaws [35]. The FBI, via the State Department's Rewards for Justice program, is offering up to **$10 million** for information on the Chinese state-backed *Salt Typhoon* hacking group [4].
- **Coming Soon (30–90 days):** UN Cybercrime Convention signatures (Oct 2025) [42]. UK Cyber Security Bill grants intervention powers [44].
- **Planning Horizon (90+ days):** EU Cyber Resilience Act CE marking (Dec 2027) [43]. Potential ransom payment ban.

7. Market and Industry Intelligence

- **Key Moves:** Palo Alto's $25B CyberArk acquisition [47-48]. LevelBlue-Trustwave merger creates largest MSSP [48]. Morgan Adamski joins PwC from CYBERCOM [45-46].
- **Insurance Market:** Nation-state attacks excluded. Healthcare uninsurability looms. Premiums up 25-40%, coverage down 50% [41].
- **Investment Trends:** 44 M&A deals ($30B+). AI security platforms and behavioral analytics prioritized [47-48]. Global cybersecurity spending to exceed $1.75T (2021-2025) [53].
- **Conference Insights:** ICCS (Jul 14-16, NYC) highlighted AI integration challenges [49]. BSides Bangalore prioritized AI security platforms [50].

8. Next Month Predictions

- **Will Happen (80%+):** Salt Typhoon enables election interference [1-4]. Healthcare ransomware triggers federal action [12-14]. AI malware spreads to criminal forums [25].
- **Might Happen (50-70%):** Major cloud provider breach. Ransomware causes critical infrastructure casualties [37-39].
- **Watch For:** Telecom outages, crypto price spikes, coordinated disinformation [51-52].

9. Investment Priorities

Capability	Why	Urgency	Cost	Time-to-Value
Behavioral Analytics	Counters LLM malware [25]	Critical	High	6–12 mo (3–6 if extending existing stack)
Alternative Communications	Telecoms compromised [1-4]	Critical	Medium	Immediate if prepped / 30–45 days to prep
Third-Party Access Management	Helpdesk attacks [26-28]	Critical	Low	4–8 weeks for first wins
Incident Response Retainer	17-day recoveries [12-14]	High	Low	Immediate option value; payback on first incident
Zero Trust Architecture	Perimeter obsolete [32]	High	High	Phase 1: 1–3 mo; Phase 2: 3–9 mo; Phase 3: 6–18+ mo

10. Board Discussion Points

- **Infrastructure Resilience:** With telecoms at risk from Salt Typhoon [1-4], how do we operate in contested environments?
- **Insurance Strategy:** With nation-state exclusions [41], should we explore self-insurance?
- **AI Defense Investment:** Where should we focus to counter adaptive malware [25]?

Key Conclusions

July 2025 exposed critical vulnerabilities in telecommunications, AI-driven threats, and third-party access, with healthcare facing unprecedented disruption. With adversaries exploiting infrastructure and cyber-insurance coverage shrinking, leaders must prioritize resilience—redundant systems, behavioral defenses, and end-to-end encryption—to operate effectively in this new era. Those adapting now will thrive; those relying on outdated prevention models risk becoming August's statistics.

For questions or custom briefings, contact benjamin@concipio.cc

Curated by Benjamin Olivier with a dash of AI brilliance.

Appendices

A. Technical Indicators of Compromise (IOCs)

- **Demodex rootkit hashes**
  - **Type:** File hashes (MD5, SHA1, SHA256)
  - **Source:** CISA Advisory AA25-203A [12]
  - **Description:** Signatures of malware linked to the Demodex rootkit, designed to hide processes/files from detection.
  - **Defensive Action:** Load into AV/EDR hash detection lists, hunt across file systems, quarantine on match.
- **ClickFix PowerShell commands**
  - **Type:** Encoded command patterns
  - **Source:** CISA Advisory AA25-203A [12]
  - **Description:** Base64-encoded PowerShell payloads executed via browser developer console.
  - **Defensive Action:** Search process logs for powershell.exe with -enc flags, decode Base64 strings, alert on suspicious script content.
- **Malicious npm packages – *XORIndex*, *HexEval*, +65 others**
  - **Type:** Package names / supply chain artifacts
  - **Source:** socket.dev [31]
  - **Description:** JavaScript packages containing malicious code or backdoors, distributed via the npm registry.
  - **Defensive Action:** Block or flag listed packages in dependency scanning tools, verify integrity before deployment.
- **SharePoint CVE-2025-53770 exploitation artifacts**
  - **Type:** Filenames, URLs, exploit patterns
  - **Source:** CVE-2025-53770 Advisory [7]
  - **Description:** Known indicators tied to exploitation of a critical SharePoint vulnerability.
  - **Defensive Action:** Review web server logs for matching paths or parameters, patch affected SharePoint versions, apply WAF rules.
- **Salt Typhoon C2 infrastructure**
  - **Type:** IP ranges, domain names
  - **Source:** FBI Flash Alert [4]
  - **Description:** Network infrastructure controlled by Salt Typhoon threat actors.
  - **Defensive Action:** Block at firewall/IPS, add to threat intel feeds, monitor outbound traffic for matches.

B. Sources

1. Foreign Policy. "Salt Typhoon Hack Gives China Access to U.S. Networks." https://foreignpolicy.com/2024/12/19/salt-typhoon-hack-explained-us-china-cyberattack/
2. Wikipedia. "Salt Typhoon." https://en.wikipedia.org/wiki/Salt_Typhoon
3. SecurityWeek. "Salt Typhoon Targeting Old Cisco Vulnerabilities." https://www.securityweek.com/salt-typhoon-targeting-old-cisco-vulnerabilities-in-fresh-telecom-hacks/

4. U.S. Treasury. "Sanctions Company Associated with Salt Typhoon." https://home.treasury.gov/news/press-releases/jy2792
5. The Hacker News. "Critical Unpatched SharePoint Zero-Day." https://thehackernews.com/2025/07/critical-microsoft-sharepoint-flaw.html
6. Bloomberg. "US Nuclear Weapons Agency Breached." https://www.bloomberg.com/news/articles/2025-07-23/us-nuclear-weapons-agency-breached-in-microsoft-sharepoint-hack
7. Palo Alto Unit42. "SharePoint Vulnerabilities." https://unit42.paloaltonetworks.com/microsoft-sharepoint-cve-2025-49704-cve-2025-49706-cve-2025-53770/
8. Microsoft Security. "SharePoint Updates July 2025." https://www.microsoft.com/security
9. TechCrunch. "Allianz Life Data Stolen." https://techcrunch.com/2025/07/26/allianz-life-says-majority-of-customers-personal-data-stolen-in-cyberattack/
10. BleepingComputer. "ShinyHunters Behind Salesforce Attacks." https://www.bleepingcomputer.com/news/security/shinyhunters-behind-salesforce-data-theft-attacks-at-qantas-allianz-life-and-lvmh/
11. BBC. "Allianz Life Data Breach." https://www.bbc.com/news/articles/cd6nyng861wo
12. CISA. "Interlock Advisory AA25-203A." https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-203a
13. The Record. "DaVita Ransomware Attack." https://therecord.media/davita-dialysis-company-ransomware-attack-data-breach-notifications
14. HIPAA Journal. "Interlock Ransomware Warning." https://www.hipaajournal.com/interlock-ransomware-alert-2025/
15. Polymer HQ. "Misconfigured Server Exposes PII." https://www.polymerhq.io/blog/misconfigured-server-exposes-pii-of-millions-of-european-citizens/
16. "McDonald's McHire Leak." [Internal Document]
17. IT Pro. "Air France-KLM Data Breach." https://www.itpro.com/security/data-breaches/air-france-and-klm-confirm-customer-data-stolen-in-third-party-breach
18. TechCrunch. "Orange Cyberattack." https://techcrunch.com/2025/07/29/telecom-giant-orange-warns-of-disruption-amid-ongoing-cyberattack/
19. BleepingComputer. "Orange Discloses Cyberattack." https://www.bleepingcomputer.com/news/security/french-telecommunications-giant-orange-discloses-cyberattack/
20. Claim Depot. "Ingram Micro Ransomware." https://www.claimdepot.com/data-breach/ingram-micro-2025
21. CRN. "Ingram Micro CEO on Ransomware." https://www.crn.com/news/channel-news/2025/ingram-micro-ceo-on-ransomware-attack-certain-data-was-exfiltrated-from-our-systems
22. Ingram Micro. "Company Information." https://www.ingrammicro.com/en-us/information
23. BankInfoSecurity. "Airlines KLM and Air France Detail Customer Data Breach." https://www.bankinfosecurity.com/airlines-klm-air-france-detail-customer-data-breach-a-29143
24. ChatGPT Analysis Document. "Air France-KLM Third-Party Breach Analysis." [Internal Analysis Document]
25. Cyber Security News. "LLM-Powered Malware APT28." https://cybersecuritynews.com/llm-powered-malware-from-apt28-hackers-integrates-ai-capabilities/

26. CISA. "CISA and Partners Release Updated Advisory on Scattered Spider Group." https://www.cisa.gov/news-events/alerts/2025/07/29/cisa-and-partners-release-updated-advisory-scattered-spider-group
27. IC3 FBI. "Scattered Spider Advisory." https://www.ic3.gov/CSA/2025/250729.pdf
28. Cybersecurity Dive. "What We Know About the Cybercrime Group Scattered Spider." https://www.cybersecuritydive.com/news/what-we-know-about-the-cybercrime-group-scattered-spider/756312/
29. The Hacker News. "North Korean npm Malware." https://thehackernews.com/2025/07/north-korean-hackers-flood-npm-registry.html
30. BleepingComputer. "XORIndex Malware." https://www.bleepingcomputer.com/news/security/north-korean-xorindex-malware-hidden-in-67-malicious-npm-packages/
31. Socket.dev. "Contagious Interview Campaign." https://socket.dev/blog/north-korean-contagious-interview-campaign-drops-35-new-malicious-npm-packages
32. VulnCheck. "Vulnerability Exploitation Trends 2025." [Analysis Report]
33. SOCRadar. "Critical Cisco ISE Vulnerabilities Allow Root-Level RCE." https://socradar.io/cve-2025-20281-cve-2025-20282-critical-cisco-ise-rce/
34. Tenable. "Frequently Asked Questions About CitrixBleed 2." https://www.tenable.com/blog/cve-2025-5777-cve-2025-6543-frequently-asked-questions-about-citrixbleed-2
35. CISA. "KEV Catalog." https://www.cisa.gov/known-exploited-vulnerabilities-catalog
36. The Record. "Microsoft: Kremlin Monitors Foreign Embassies Through Cyber-Espionage at ISP Level." https://therecord.media/russia-fsb-turla-espionage-foreign-embassies-isp-level
37. The Hacker News. "Critical Flaws in Niagara Framework Threaten Smart Buildings." https://thehackernews.com/2025/07/critical-flaws-in-niagara-framework.html
38. Nozomi Networks. "Critical Vulnerabilities Found in Tridium Niagara Framework." https://www.nozominetworks.com/blog/critical-vulnerabilities-found-in-tridium-niagara-framework
39. CISA ICS Advisories. "Train Braking System Vulnerability." [Advisory Document]
40. AHA. "Report: Health Care Had Most Reported Cyberthreats in 2024." https://www.aha.org/news/headline/2025-05-12-report-health-care-had-most-reported-cyberthreats-2024
41. Financial Times. "Allianz Cyber Attack." https://www.ft.com/content/ae99065b-a2e9-4dc0-8ef4-0280a2c8a739
42. UNODC. "Cybercrime Convention." https://www.unodc.org/unodc/en/cybercrime/convention/home.html
43. European Cyber Resilience Act. "CRA Updates." https://www.european-cyber-resilience-act.com/
44. Industrial Cyber. "UK Cyber Security Bill." https://industrialcyber.co/regulation-standards-and-compliance/uk-cyber-security-and-resilience-bill-policy-statement-details-confirmed-and-proposed-measures-for-enhanced-cni-protection/
45. PwC. "Morgan Adamski Joins." https://www.pwc.com/us/en/about-us/newsroom/press-releases/morgan-adamski-cyber-risk-us-leader.html
46. Business Insider. "PwC Hires NSA Executive." https://www.businessinsider.com/pwc-restructuring-hired-morgan-adamski-cybersecurity-consulting-division-2025-7

47. SecurityWeek. "Cybersecurity M&A Roundup." https://www.securityweek.com/cybersecurity-ma-roundup-44-deals-announced-in-july-2025/

48. Channel Futures. "Top Tech M&A 2025." https://www.channelfutures.com/mergers-acquisitions/top-channel-impacting-tech-ma-2025-so-far

49. Fordham University. "The International Conference on Cyber Security." https://www.fordham.edu/gabelli-school-of-business/faculty/research-centers/center-for-professional-accounting-practices/news-and-events/future-events/the-international-conference-on-cyber-security/

50. Times of India. "Cybersecurity is a Matter of National Importance." https://timesofindia.indiatimes.com/city/bengaluru/cybersecurity-is-a-matter-of-national-importance-says-mp-yaduveer-at-bsides-bangalore-2025/articleshow/122436217.cms

51. Chainalysis. "2025 Crypto Crime Report." https://www.chainalysis.com

52. BitcoinEthereumNews. "Crypto Hacks Surge in July 2025: $142 Million Stolen." https://bitcoinethereumnews.com/crypto/crypto-hacks-surge-in-july-2025-142-million-stolen-up-27-from-june/

53. Cybersecurity Ventures. "Global Cybersecurity Spending To Exceed $1.75 Trillion From 2021-2025." https://cybersecurityventures.com/cybersecurity-spending-2021-2025/