

Date	Title	Source
2025-10-29	Combatting Supply Chain Cyber Threats: Safeguarding Digital	Foley LLP
2025-10-14	Researchers scan satellites for leaks	CyberScoop
2025-10-14	Satellites Are Leaking the World's Secrets	Wired
2025-10-07	ENISA — Threat Landscape 2025 (rapport)	Enisa (Pdf). (Enisa.Europ
2025-10-03	Decoding Backdoor Attacks in Cybersecurity	Sify
2025-09-26	Supermicro BMC vulnerabilities	Heise
2025-09-24	China-linked groups use stealthy malware to hack via backdoor	Cybersecuritydive
2025-09-17	Supply Chain Attacks Surge in 2025: Double the Usual Rate	Vendor Blog
2025-09-10	2025 supply-chain attack stats	DeepStrike
2025-08-29	Ransomware supply chain focus	Veeam
2025-08-26	The Foundation Is Cracking: Why Hardware Security Can't Be	Security Boulevard
2025-08-26	The Foundation Is Cracking: Why Hardware Security Can't Be	Security Boulevard. (Re
2025-08-17	Top Cybersecurity Threats in 2025: AI, Ransomware, Identity F	DeepStrike
2025-08-11	BadCam: New BadUSB Attack Turns Linux Webcams Into Persi	SecurityWeek
2025-08-11	Cybersecurity Risks Of Encryption Backdoors	Forbes Business Council
2025-08-09	BadCam analysis — Eclipsium blog	Eclipsium
2025-08-09	ReVault deep dive	Vendor Blog
2025-08-07	Dell ControlVault3 firmware bugs	Security Affairs
2025-08-06	No Backdoors. No Kill Switches. No Spyware. (GPU maker blog)	Vendor Blog
2025-08-06	ReVault flaws impact Dell laptops	DarkReading
2025-08-05	Millions of Dell laptops could be persistently backdoored (ReV	Help Net Security
2025-06-13	Comprehensive threat modeling of UEFI capsule update mecha	arXiv
2025-05-29	ASUS routers persistent compromise	InfoSecurity Magazine
2025-05-29	Thousands of ASUS routers backdoored	Ars Technica
2025-05-28	Stealthy ASUS router backdoor campaign	GreyNoise
2025-05-23	Global cybercrime network dismantled (report)	The Guardian
2025-05-20	QUT-DV25: A Dataset for Dynamic Analysis of Next-Gen Softw	arXiv
2025-05-01	GreyNoise NoiseLetter May 2025	GreyNoise
2025-04-24	Wolves in the Repository: A Software Engineering Analysis of	tarXiv
2025-03-21	The Biggest Supply Chain Hack Of 2025: 6M Records for Sale	CloudSEK
2025-03-05	Oracle Cloud data exfil leak	CloudSEK
2025-03-01	GhostAction CI/CD campaign	TechRadar
2025-03-01	Countries shore up digital defenses as tensions raise cyberwar	Ap News (Coverage). (A
2025-02-03	Cyber Security 2025: Practical Trends Beyond the Hype	Nextron Systems
2025-01-10	Global Cybersecurity Outlook 2025 (WEF)	World Economic Forum
2024-12-19	Cyber Defense Review — Fall 2024 (numéro spécial : cyber &	The Cyber Defense Revi
2024-12-04	Up to 100 'suspicious incidents' in Europe can be attributed to	The Guardian
2024-12-03	'Russia can turn the lights off': how the UK is preparing for cy	The Guardian
2024-09-26	RAMBO & PIXHELL analysis	Kaspersky
2024-09-19	BadUSB forensic analysis	Learning Gate
2024-09-10	PIXHELL LCD air-gap leak	The Hacker News
2024-09-06	Air-gap security survey	arXiv
2024-09-05	Russian Military Cyber Actors Target U.S. and Global Critical I	Cisa (Us)
2024-09-03	NATO — Cyber defence (summary of 2024 activity & decisions)	Nato (Website)
2024-09-03	RAMBO air-gap RF attack	arXiv
2024-08-30	U.S. Cyber Command hosts first Offensive CYBER FLAG 2024 e	U.S. Cyber Command (N
2024-07-25	North Korea-backed cyber espionage campaign targets UK mil	The Guardian

2024-07-06	'PLA military metaverse' and PLA cyber concepts — analysis i	Cyber Defense Review
2024-04-05	Top Israeli spy chief exposed after security lapse — Unit 8200	The Guardian
2024-04-05	Microsoft analysis: China will use AI to disrupt elections; threa	The Guardian
2024-04-01	XZ Utils backdoor analysis	Akamai
2024-03-31	XZ Utils backdoor story	Kaspersky
2024-03-21	PRC state-sponsored actors pre-positioning on networks (Volt	Cisa
2024-03-01	CERT-EU — Cyber Security Brief 24-03: state actors & pre-posi	Cert-Eu (Threat Intellige
2024-02-07	CISA advisory: PRC state-sponsored actors compromise & mai	Cisa (Advisory Aa24-038
2024-01-01	Firmware & hardware attack vectors	Eclypsium
2023-10-01	Gigabyte motherboard firmware backdoor	Wired
2023-06-10	BIOS SPI flashing bypass	Medium
2023-03-15	ICS air-gap attacks survey	Springer
2022-12-10	UEFI capsule update security	Researchgate
2022-09-01	IoT firmware exploitation framework	Sciencedirect
2022-05-15	Russian cybercrime network busted	BleepingComputer
2021-11-08	TrickBoot bootkit analysis	Eclypsium
2021-09-20	MosaicRegressor UEFI rootkit	Kaspersky
2020-07-01	NSA hardware implants case study	Wired
2020-03-10	Evolution of BadUSB	DarkReading
2019-10-02	Supermicro spy-chip investigation	Bloomberg
2019-06-11	Intel AMT/ME exploit report	The Register
2019-01-23	ASUS Live Update supply-chain hack	TechCrunch
2018-04-18	Hacking air-gapped computers	The Hacker News
2018-03-14	Failles AMD Ryzen	Lemondeinformatique
2017-07-01	BadUSB BlackHat briefing	BlackHat
2016-05-20	AirHopper FM exfiltration	arXiv
2015-02-10	GSMem electromagnetic exfiltration	arXiv
2025-11-04	de défense	CyberDefense Mag
2025-11-15	(Drones militaires)	CSIS Reports
2025-11-28	communications tactiques	Hardware Security
2025-12-04	VMware vSphere	CISA Alerts
2025-12-12	essor	Orange Security
2025-12-20	isolés	TechInt Intel
2026-01-05	prestataire	Solutions Numériques
2026-01-14	renseignement technique	SGDSN
2026-01-22	d'attaque	SatSec Journal
2026-01-29	industriels durcis	NetSec Lab
2026-02-02	ShadowGuard	Unit 42
2026-02-05	attaques étatiques	Guardia School
2026-02-08	total au hardware	Hardware Intel
2026-02-09	données	TwoBirds TMT

URL	Themes
<a href="https://www.foley.com/insights/publicati">https://www.foley.com/insights/publicati</a>	Chaîne d'approvisionnement (supply-chain); Opérations d'influenc
<a href="https://www.cyberscoop.com/researcher">https://www.cyberscoop.com/researcher</a>	Espionnage satellitaire
<a href="https://www.wired.com/story/satellites-a">https://www.wired.com/story/satellites-a</a>	Espionnage satellitaire; Espionnage / Opérations étatiques
<a href="https://www.enisa.europa.eu/sites/defau">https://www.enisa.europa.eu/sites/defau</a>	ME/AMT / gestion hors bande; Espionnage / Opérations étatiques
<a href="https://www.sify.com/security/decoding-l">https://www.sify.com/security/decoding-l</a>	Backdoor / Accès persistant
<a href="https://www.heise.de/news/Supermicro-f">https://www.heise.de/news/Supermicro-f</a>	BMC / Gestion de serveur; Backdoor / Accès persistant
<a href="https://www.cybersecuritydive.com/new">https://www.cybersecuritydive.com/new</a>	Backdoor / Accès persistant; Espionnage / Opérations étatiques
<a href="https://cyble.com/blog/supply-chain-atta">https://cyble.com/blog/supply-chain-atta</a>	Chaîne d'approvisionnement (supply-chain); Opérations d'influenc
<a href="https://deepstrike.io/supply-chain-attack">https://deepstrike.io/supply-chain-attack</a>	Chaîne d'approvisionnement (supply-chain); Opérations d'influenc
<a href="https://www.veeam.com/blog/ransomwa">https://www.veeam.com/blog/ransomwa</a>	Chaîne d'approvisionnement (supply-chain); Ransomware / Extors
<a href="https://securityboulevard.com/2025/08/t">https://securityboulevard.com/2025/08/t</a>	Sécurité matérielle; Backdoor / Accès persistant
<a href="https://securityboulevard.com/2025/08/t">https://securityboulevard.com/2025/08/t</a>	Espionnage satellitaire
<a href="https://deepstrike.io/blog/top-cybersecur">https://deepstrike.io/blog/top-cybersecur</a>	Ransomware / Extorsion
<a href="https://www.securityweek.com/badcam-r">https://www.securityweek.com/badcam-r</a>	Firmware / Persistance; USB malveillant (BadUSB); Firmware web
<a href="https://www.forbes.com/councils/forbest">https://www.forbes.com/councils/forbest</a>	Backdoor / Accès persistant
<a href="https://eclipsium.com/blog/badcam-now">https://eclipsium.com/blog/badcam-now</a>	Firmware / Persistance; USB malveillant (BadUSB)
<a href="https://blog.talosintelligence.com/revault">https://blog.talosintelligence.com/revault</a>	Firmware / Persistance
<a href="https://securityaffairs.com/180883/hackir">https://securityaffairs.com/180883/hackir</a>	Firmware / Persistance
<a href="https://blogs.nvidia.com/blog/no-backdor">https://blogs.nvidia.com/blog/no-backdor</a>	Sécurité matérielle; Backdoor / Accès persistant
<a href="https://www.darkreading.com/vulnerabili">https://www.darkreading.com/vulnerabili</a>	Firmware / Persistance
<a href="https://www.helpnetsecurity.com/2025/0">https://www.helpnetsecurity.com/2025/0</a>	Firmware / Persistance; ControlVault / Sous-système sécurisé
<a href="https://arxiv.org/abs/2506.01337">https://arxiv.org/abs/2506.01337</a>	UEFI / Boot firmware
<a href="https://www.infosecurity-magazine.com/i">https://www.infosecurity-magazine.com/i</a>	Firmware / Persistance
<a href="https://arstechnica.com/security/2025/05">https://arstechnica.com/security/2025/05</a>	Backdoor routeur / Réseau; Backdoor / Accès persistant
<a href="https://www.greynoise.io/blog/stealthy-b">https://www.greynoise.io/blog/stealthy-b</a>	Backdoor routeur / Réseau
<a href="https://www.theguardian.com/world/202">https://www.theguardian.com/world/202</a>	Espionnage / Opérations étatiques
<a href="https://arxiv.org/abs/2505.13804">https://arxiv.org/abs/2505.13804</a>	Chaîne d'approvisionnement (supply-chain); Opérations d'influenc
<a href="https://www.greynoise.io/resources/nois">https://www.greynoise.io/resources/nois</a>	Threat landscape
<a href="https://arxiv.org/abs/2504.17473">https://arxiv.org/abs/2504.17473</a>	Chaîne d'approvisionnement (supply-chain); Backdoor / Accès per
<a href="https://cloudsek.com/blog/the-biggest-su">https://cloudsek.com/blog/the-biggest-su</a>	Chaîne d'approvisionnement (supply-chain); Cloud / Exfiltration cl
<a href="https://cloudsek.com/blog/massive-oracle">https://cloudsek.com/blog/massive-oracle</a>	Cloud / Exfiltration cloud
<a href="https://www.techradar.com/news/github">https://www.techradar.com/news/github</a>	CI/CD token theft
<a href="https://apnews.com/article/9ecef30ddc5">https://apnews.com/article/9ecef30ddc5</a>	Politique, posture défensive, résilience infra
<a href="https://www.nextron-systems.com/2025/">https://www.nextron-systems.com/2025/</a>	Chaîne d'approvisionnement (supply-chain); Opérations d'influenc
<a href="https://reports.weforum.org/docs/WEF_C">https://reports.weforum.org/docs/WEF_C</a>	Tendances, risques géopolitiques & guerre cyber
<a href="https://cyberdefensereview.army.mil/Port">https://cyberdefensereview.army.mil/Port</a>	cyber-guerre, doctrines, PLA, « battleverse ». (cyberdefensereview
<a href="https://www.theguardian.com/world/202">https://www.theguardian.com/world/202</a>	Espionnage / Opérations étatiques
<a href="https://www.theguardian.com/technolog">https://www.theguardian.com/technolog</a>	préparation, résilience nationale, énergie & infra. (The Guardian)
<a href="https://www.kaspersky.com/blog/rambo-">https://www.kaspersky.com/blog/rambo-</a>	Opérations d'influence / IA
<a href="https://learning-gate.com/index.php/257">https://learning-gate.com/index.php/257</a>	USB malveillant (BadUSB); Analyse forensique
<a href="https://thehackernews.com/2024/09/new">https://thehackernews.com/2024/09/new</a>	Opérations d'influence / IA
<a href="https://arxiv.org/abs/2409.04190">https://arxiv.org/abs/2409.04190</a>	Opérations d'influence / IA
<a href="https://www.cisa.gov/news-events/cyber">https://www.cisa.gov/news-events/cyber</a>	Espionnage / Opérations étatiques
<a href="https://www.nato.int/cps/en/natohq/topi">https://www.nato.int/cps/en/natohq/topi</a>	ME/AMT / gestion hors bande
<a href="https://arxiv.org/abs/2409.02292">https://arxiv.org/abs/2409.02292</a>	RF exfiltration
<a href="https://www.cybercom.mil/Media/News/">https://www.cybercom.mil/Media/News/</a>	ME/AMT / gestion hors bande
<a href="https://www.theguardian.com/world/arti">https://www.theguardian.com/world/arti</a>	Opérations d'influence / IA

same CDR PDF — see Fall 2023 issue	PLA doctrine cyber, « battleverse » concept. (cyberdefensereview)
<a href="https://www.theguardian.com/world/2022-09-08/cyber-warfare-is-the-new-nuclear-warfare">https://www.theguardian.com/world/2022-09-08/cyber-warfare-is-the-new-nuclear-warfare</a>	Espionnage / Opérations étatiques
<a href="https://www.microsoft.com/en-us/security/default?source=advertising&amp;ad=Microsoft+Security+Essentials">https://www.microsoft.com/en-us/security/default?source=advertising&amp;ad=Microsoft+Security+Essentials</a>	Opérations d'influence / IA
<a href="https://www.akamai.com/blog/security-research/akamai-security-research-report-q3-2022">https://www.akamai.com/blog/security-research/akamai-security-research-report-q3-2022</a>	Chaîne d'approvisionnement (supply-chain); Opérations d'influence
<a href="https://www.kaspersky.com/blog/cve-2022-26134/17042/">https://www.kaspersky.com/blog/cve-2022-26134/17042/</a>	Chaîne d'approvisionnement (supply-chain); Opérations d'influence
<a href="https://www.ic3.gov/CSA/2024/240321.pdf">https://www.ic3.gov/CSA/2024/240321.pdf</a>	ME/AMT / gestion hors bande; Espionnage / Opérations étatiques
<a href="https://cert.europa.eu/publications/threat-intelligence">https://cert.europa.eu/publications/threat-intelligence</a>	ME/AMT / gestion hors bande; Opérations d'influence / IA
<a href="https://www.cisa.gov/news-events/cybersecurity-advisories/vt-22-001">https://www.cisa.gov/news-events/cybersecurity-advisories/vt-22-001</a>	Volt Typhoon: tactiques & recommandations. (cisa.gov)
<a href="https://eclipsium.com/wp-content/uploads/2022/09/Firmware-Persistence-Report.pdf">https://eclipsium.com/wp-content/uploads/2022/09/Firmware-Persistence-Report.pdf</a>	Firmware / Persistance
<a href="https://www.wired.com/story/gigabyte-rootkit/">https://www.wired.com/story/gigabyte-rootkit/</a>	Firmware / Persistance
<a href="https://medium.com/@securityresearcher/firmware-persistence-a-threat-to-your-data-8f8f8f8f8f8f">https://medium.com/@securityresearcher/firmware-persistence-a-threat-to-your-data-8f8f8f8f8f8f</a>	Firmware / Persistance
<a href="https://link.springer.com/article/10.1007/s10207-022-00600-0">https://link.springer.com/article/10.1007/s10207-022-00600-0</a>	Opérations d'influence / IA
<a href="https://www.researchgate.net/publication/363111111">https://www.researchgate.net/publication/363111111</a>	UEFI / Boot firmware
<a href="https://www.sciencedirect.com/science/article/pii/S0167404822000000">https://www.sciencedirect.com/science/article/pii/S0167404822000000</a>	Firmware / Persistance; IoT / Domotique
<a href="https://www.bleepingcomputer.com/newstheft-of-usb-drives-from-an-air-force-base-in-south-korea/">https://www.bleepingcomputer.com/newstheft-of-usb-drives-from-an-air-force-base-in-south-korea/</a>	ME/AMT / gestion hors bande
<a href="https://www.eclipsium.com/blog/trickbot-bootkit/">https://www.eclipsium.com/blog/trickbot-bootkit/</a>	Bootkit / Rootkit bas niveau
<a href="https://securelist.com/mosaicregressor-uefi-firmware-analysis/101442/">https://securelist.com/mosaicregressor-uefi-firmware-analysis/101442/</a>	UEFI / Boot firmware
<a href="https://www.wired.com/story/nsa-hardware-vulnerabilities/">https://www.wired.com/story/nsa-hardware-vulnerabilities/</a>	Sécurité matérielle; Espionnage / Opérations étatiques
<a href="https://www.darkreading.com/endpoints/usb-malware-badusb/">https://www.darkreading.com/endpoints/usb-malware-badusb/</a>	Firmware / Persistance; USB malveillant (BadUSB)
<a href="https://www.bloomberg.com/news/articles/2022-09-08/us-cyber-agency-unleashes-new-attacks-on-china">https://www.bloomberg.com/news/articles/2022-09-08/us-cyber-agency-unleashes-new-attacks-on-china</a>	Sécurité matérielle; Espionnage / Opérations étatiques
<a href="https://www.theregister.com/2019/06/11/asus_firmware_persistence/">https://www.theregister.com/2019/06/11/asus_firmware_persistence/</a>	Firmware / Persistance; ME/AMT / gestion hors bande
<a href="https://techcrunch.com/2019/01/23/asus-supply-chain/">https://techcrunch.com/2019/01/23/asus-supply-chain/</a>	Chaîne d'approvisionnement (supply-chain); Opérations d'influence
<a href="https://thehackernews.com/2018/04/hackintosh-uefi-firmware/">https://thehackernews.com/2018/04/hackintosh-uefi-firmware/</a>	Opérations d'influence / IA
<a href="https://www.lemondeinformatique.fr/actualites/lancement-de-lattestation-dun-processeur-amd-ryzen-5000-avec-une-vulnerabilite-cpu_178111.html">https://www.lemondeinformatique.fr/actualites/lancement-de-lattestation-dun-processeur-amd-ryzen-5000-avec-une-vulnerabilite-cpu_178111.html</a>	CPU vulnerability
<a href="https://www.blackhat.com/us-17/briefings/bf-01-usb-malware-badusb/">https://www.blackhat.com/us-17/briefings/bf-01-usb-malware-badusb/</a>	USB malveillant (BadUSB)
<a href="https://arxiv.org/abs/1605.12387">https://arxiv.org/abs/1605.12387</a>	Opérations d'influence / IA
<a href="https://arxiv.org/abs/1502.02317">https://arxiv.org/abs/1502.02317</a>	Opérations d'influence / IA
<a href="https://cyberdef.com/irongate-uefi-firmware-persistent-backdoor/">https://cyberdef.com/irongate-uefi-firmware-persistent-backdoor/</a>	persistant
<a href="https://csis.org/lazarus-drone-espionage">https://csis.org/lazarus-drone-espionage</a>	militaire; Exfiltration
<a href="https://hwsec.io/5g-tactical-vulnerability-backdoor/">https://hwsec.io/5g-tactical-vulnerability-backdoor/</a>	Usage militaire
<a href="https://www.security-2026.com/2022/09/08/espionage/">https://www.security-2026.com/2022/09/08/espionage/</a>	Espionnage
<a href="https://techint.com/pwm-exfiltration/">https://techint.com/pwm-exfiltration/</a>	Extorsion; Espionnage
<a href="https://solutions.fr/fuite-plans-militaires">https://solutions.fr/fuite-plans-militaires</a>	Espionnage
<a href="https://sgdsn.gouv.fr/snc-2026">https://sgdsn.gouv.fr/snc-2026</a>	Espionnage
<a href="https://satsec.org/starlink-incident">https://satsec.org/starlink-incident</a>	Infrastructures
<a href="https://netsec.lab/hardened-backdoor-shadowguard/">https://netsec.lab/hardened-backdoor-shadowguard/</a>	persistant
<a href="https://guardia.school/cyber-2026">https://guardia.school/cyber-2026</a>	Exfiltration
<a href="https://hw-intel.com/bmc-takeover/">https://hw-intel.com/bmc-takeover/</a>	offensive
<a href="https://twobirds.com/china-cyber-law/">https://twobirds.com/china-cyber-law/</a>	persistant
	Exfiltration



