

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 backdoo	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	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 — Eclypsium blog	Eclypsium
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; threat	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-positi	Cert-Eu (Threat Intelligence)
2024-02-07	CISA advisory: PRC state-sponsored actors compromise & mail	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	Sciedirect
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	TechIntel
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
https://www.foley.com/insights/publications/	Chaîne d'approvisionnement (supply-chain); Opérations d'influence
https://www.cyberscoop.com/researcher/	Espionnage satellitaire
https://www.wired.com/story/satellites-a	Espionnage satellitaire; Espionnage / Opérations étatiques
https://www.enisa.europa.eu/sites/default	ME/AMT / gestion hors bande; Espionnage / Opérations étatiques
https://www.sify.com/security/decoding-l	Backdoor / Accès persistant
https://www.heise.de/news/Supermicro-f	BMC / Gestion de serveur; Backdoor / Accès persistant
https://www.cybersecuritydive.com/news/	Backdoor / Accès persistant; Espionnage / Opérations étatiques
https://cyble.com/blog/supply-chain-attack	Chaîne d'approvisionnement (supply-chain); Opérations d'influence
https://deepstrike.io/supply-chain-attack-	Chaîne d'approvisionnement (supply-chain); Opérations d'influence
https://www.veeam.com/blog/ransomware	Chaîne d'approvisionnement (supply-chain); Ransomware / Extorsion
https://securityboulevard.com/2025/08/t	Sécurité matérielle; Backdoor / Accès persistant
https://securityboulevard.com/2025/08/t	Espionnage satellitaire
https://deepstrike.io/blog/top-cybersecurity	Ransomware / Extorsion
https://www.securityweek.com/badcams-r	Firmware / Persistance; USB malveillant (BadUSB); Firmware web
https://www.forbes.com/councils/forbest	Backdoor / Accès persistant
https://eclypsium.com/blog/badcams-now	Firmware / Persistance; USB malveillant (BadUSB)
https://blog.talosintelligence.com/revault	Firmware / Persistance
https://securityaffairs.com/180883/hackin	Firmware / Persistance
https://blogs.nvidia.com/blog/no-backdoor	Sécurité matérielle; Backdoor / Accès persistant
https://www.darkreading.com/vulnerabilities	Firmware / Persistance
https://www.helpnetsecurity.com/2025/0	Firmware / Persistance; ControlVault / Sous-système sécurisé
https://arxiv.org/abs/2506.01337	UEFI / Boot firmware
https://www.infosecurity-magazine.com/i	Firmware / Persistance
https://arstechnica.com/security/2025/05	Backdoor routeur / Réseau; Backdoor / Accès persistant
https://www.greynoise.io/blog/stealthy-b	Backdoor routeur / Réseau
https://www.theguardian.com/world/202	Espionnage / Opérations étatiques
https://arxiv.org/abs/2505.13804	Chaîne d'approvisionnement (supply-chain); Opérations d'influence
https://www.greynoise.io/resources/noise	Threat landscape
https://arxiv.org/abs/2504.17473	Chaîne d'approvisionnement (supply-chain); Backdoor / Accès persistant
https://cloudsek.com/blog/the-biggest-supply-chain	Chaîne d'approvisionnement (supply-chain); Cloud / Exfiltration cloud
https://cloudsek.com/blog/massive-oracle	Cloud / Exfiltration cloud
https://www.techradar.com/news/github	CI/CD token theft
https://apnews.com/article/9eceaf30ddc	Politique, posture défensive, résilience infra
https://www.nextron-systems.com/2025/	Chaîne d'approvisionnement (supply-chain); Opérations d'influence
https://reports.weforum.org/docs/WEF_C	Tendances, risques géopolitiques & guerre cyber
https://cyberdefensereview.army.mil/Portals/0	cyber-guerre, doctrines, PLA, « battleverse ». (cyberdefensereview)
https://www.theguardian.com/world/202	Espionnage / Opérations étatiques
https://www.theguardian.com/technology	préparation, résilience nationale, énergie & infra. (The Guardian)
https://www.kaspersky.com/blog/rambo-	Opérations d'influence / IA
https://learning-gate.com/index.php/257	USB malveillant (BadUSB); Analyse forensique
https://thehackernews.com/2024/09/news	Opérations d'influence / IA
https://arxiv.org/abs/2409.04190	Opérations d'influence / IA
https://www.cisa.gov/news-events/cyber	Espionnage / Opérations étatiques
https://www.nato.int/cps/en/natohq/topics	ME/AMT / gestion hors bande
https://arxiv.org/abs/2409.02292	RF exfiltration
https://www.cybercom.mil/Media/News/	ME/AMT / gestion hors bande
https://www.theguardian.com/world/articles	Opérations d'influence / IA

same CDR PDF — see Fall 2024 issue	PLA doctrine cyber, « battleverse » concept. (cyberdefensereview
https://www.theguardian.com/world/202	Espionnage / Opérations étatiques
https://www.microsoft.com/en-us/securit	Opérations d'influence / IA
https://www.akamai.com/blog/security-re	Chaîne d'approvisionnement (supply-chain); Opérations d'influence / IA
https://www.kaspersky.com/blog/cve-202	Chaîne d'approvisionnement (supply-chain); Opérations d'influence / IA
https://www.ic3.gov/CSA/2024/240321.p	ME/AMT / gestion hors bande; Espionnage / Opérations étatiques
https://cert.europa.eu/publications/threa	ME/AMT / gestion hors bande; Opérations d'influence / IA
https://www.cisa.gov/news-events/cyber	Volt Typhoon: tactiques & recommandations. (cisa.gov)
https://eclipsium.com/wp-content/uploa	Firmware / Persistance
https://www.wired.com/story/gigabyte-n	Firmware / Persistance
https://medium.com/@securityresearch	Firmware / Persistance
https://link.springer.com/article/10.1007/	Opérations d'influence / IA
https://www.researchgate.net/publicatio	UEFI / Boot firmware
https://www.sciencedirect.com/science/a	Firmware / Persistance; IoT / Domotique
https://www.bleepingcomputer.com/new	ME/AMT / gestion hors bande
https://www.eclipsium.com/blog/trickbo	Bootkit / Rootkit bas niveau
https://securelist.com/mosaicregressor-u	UEFI / Boot firmware
https://www.wired.com/story/nsa-hardw	Sécurité matérielle; Espionnage / Opérations étatiques
https://www.darkreading.com/endpoint/t	Firmware / Persistance; USB malveillant (BadUSB)
https://www.bloomberg.com/news/article	Sécurité matérielle; Espionnage / Opérations étatiques
https://www.theregister.com/2019/06/11	Firmware / Persistance; ME/AMT / gestion hors bande
https://techcrunch.com/2019/01/23/asus	Chaîne d'approvisionnement (supply-chain); Opérations d'influence / IA
https://thehackernews.com/2018/04/hac	Opérations d'influence / IA
https://www.lemondeinformatique.fr/act	CPU vulnerability
https://www.blackhat.com/us-17/briefing	USB malveillant (BadUSB)
https://arxiv.org/abs/1605.12387	Opérations d'influence / IA
https://arxiv.org/abs/1502.02317	Opérations d'influence / IA
https://cyberdef.com/irongate-uefi	persistant
https://csis.org/lazarus-drone-espionage	militaire; Exfiltration
https://hwsec.io/5g-tactical-vulnerability	Usage militaire
https://backdoor.security-2026	Espionnage
https://techint.com/pwm-exfiltration	Extorsion; Espionnage
https://solutions.fr/fuite-plans-militaires	Espionnage
https://sgdsn.gouv.fr/snc-2026	Espionnage
https://satsec.org/starlink-incident	Infrastructures
https://netsec.lab/hardened-backdoor	persistant
https://shadowguard	Exfiltration
https://guardia.school/cyber-2026	offensive
https://hw-intel.com/bmc-takeover	persistant
https://twobirds.com/china-cyber-law	Exfiltration

