L'evoluzione delle minacce cyber: AI, ransomware e attacchi alla supply chain"

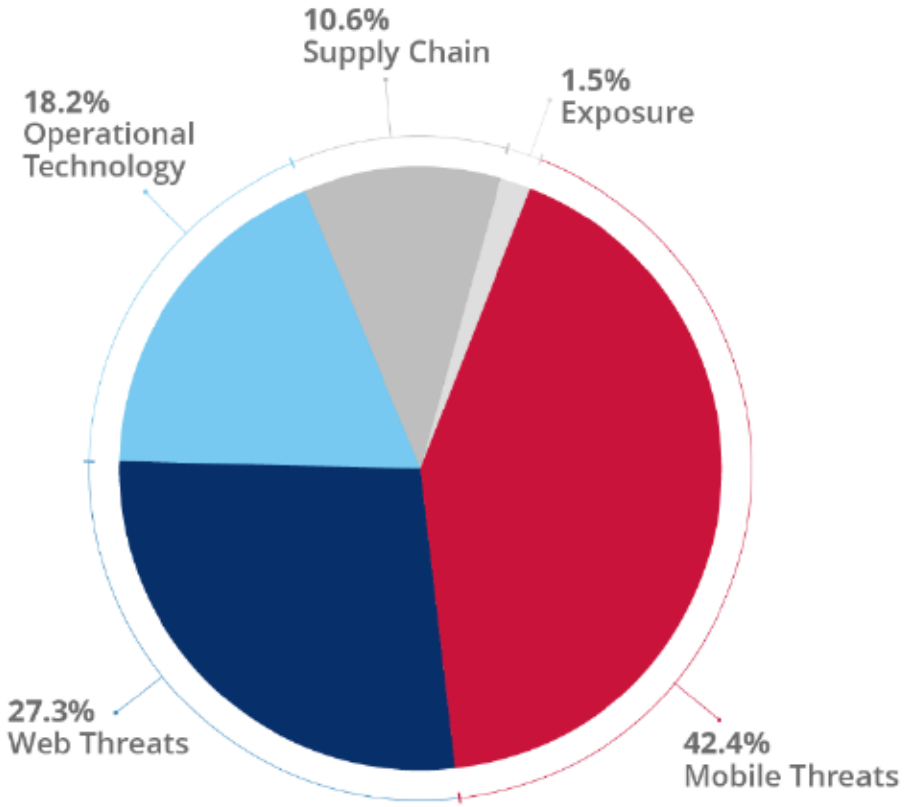
Cybersecurity Summit 2025

19 NOVEMBRE 2025

ENISA Threat Landscape 2025

- 4.900 incidenti analizzati: ambiente più complesso, vulnerabilità sfruttate in tempi record.
- Ransomware in crescita: decentralizzato, aggressivo e basato su modelli-as-a-service.
- Hacktivismo al 80%: DDoS a basso impatto ma diffusi e motivati ideologicamente.
- Settori presi di mira: PA, trasporti, logistica, manifattura e infrastrutture digitali.
- IA e phishing-as-a-service: automatizzano e amplificano le campagne di inganno e furto dati.

https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

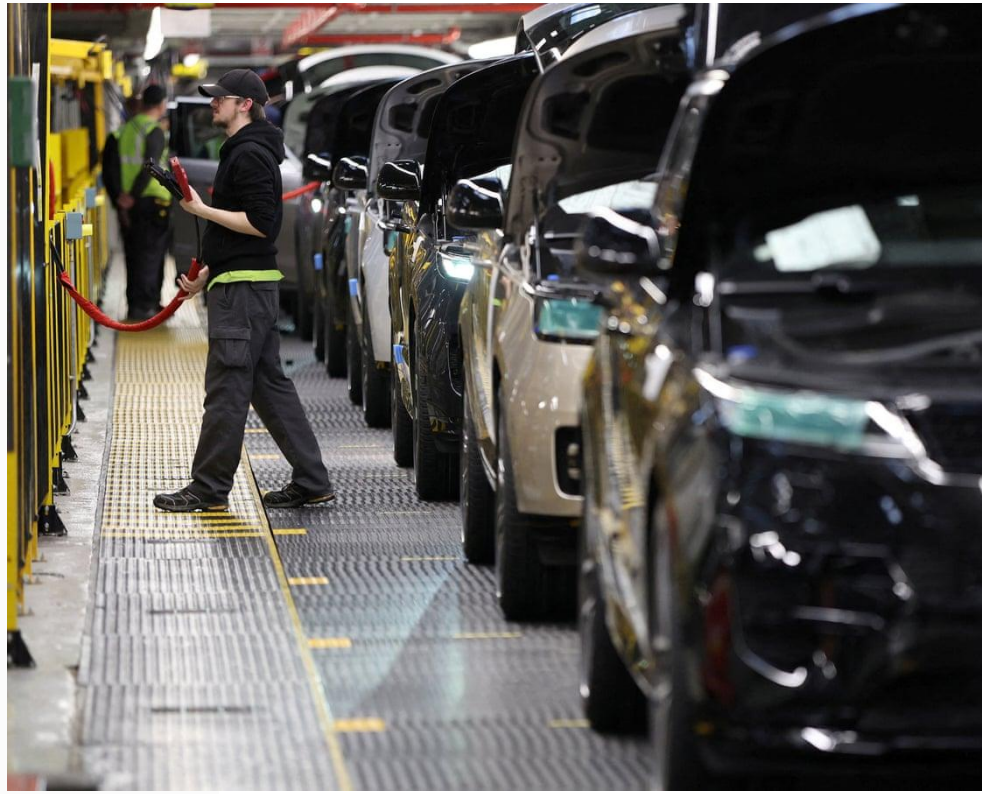


Panorama delle minacce

- Phishing domina: 60% dei casi di social engineering; vishing, malspam e malvertising tra le principali tecniche.
- Sfruttamento vulnerabilità: 21,3% dei casi; quasi 70% porta a intrusioni e malware installati.
- Intrusioni cybercriminali: ransomware, trojan bancari e infostealer rappresentano l’87,3% degli attacchi con dati rubati.
- Aree più colpite: mobile 42,4%, web 27,3%, sistemi OT 18,2%, supply chain 10,6%; obiettivi finanziari, ideologici e cyberespionage.
- L'Europa è un obiettivo primario dell’Cybercrime: il 22% di tutte le vittime sui data leak site ha sede in Europa e le iscrizioni ai DLS sono aumentate del 13% su base annua. (Crowdstrike)

Il caso Jaguar Land Rover (JLR)

- **Blocco produttivo nazionale:** l'attacco a JLR ha fermato impianti chiave per settimane, causando ritardi nelle consegne, problemi nei concessionari e interruzioni nella supply chain UK.
- **Danno economico diretto:** il cyberattacco è costato **£196 milioni** in un solo trimestre, contribuendo a un calo del 24% dei ricavi e a forti perdite finanziarie.
- **Impatto sull'occupazione e sulla filiera:** la crisi ha messo a rischio la rete di fornitori UK, che dipende da JLR per oltre **120.000 posti di lavoro**.
- **Intervento governativo straordinario:** Londra ha varato un pacchetto di sostegno da **£1.5 miliardi** per stabilizzare il settore automotive dopo l'attacco.
- **Effetti macroeconomici misurabili:** secondo la Bank of England, il cyberattacco ha contribuito al rallentamento del **GDP UK nel Q3 2025**, dimostrando che gli incidenti cyber possono incidere sull'economia nazionale.



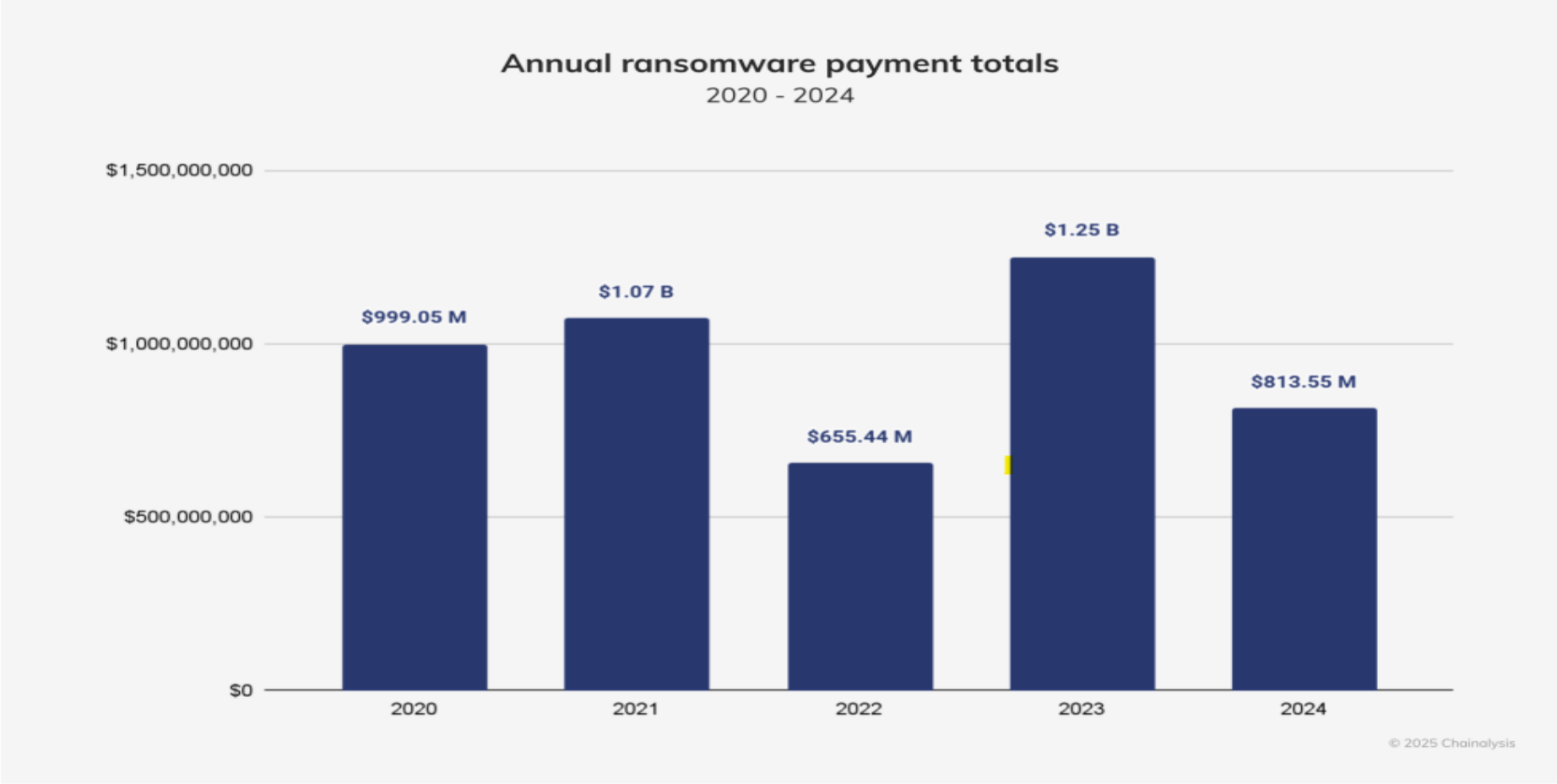
Situazione Italiana - Ransomware

Nel 2024-25 l’Italia ha subito 357 attacchi gravi (+15,2% YOY)

Il 37,8% delle aziende italiane dichiara almeno un attacco subito nel 2025

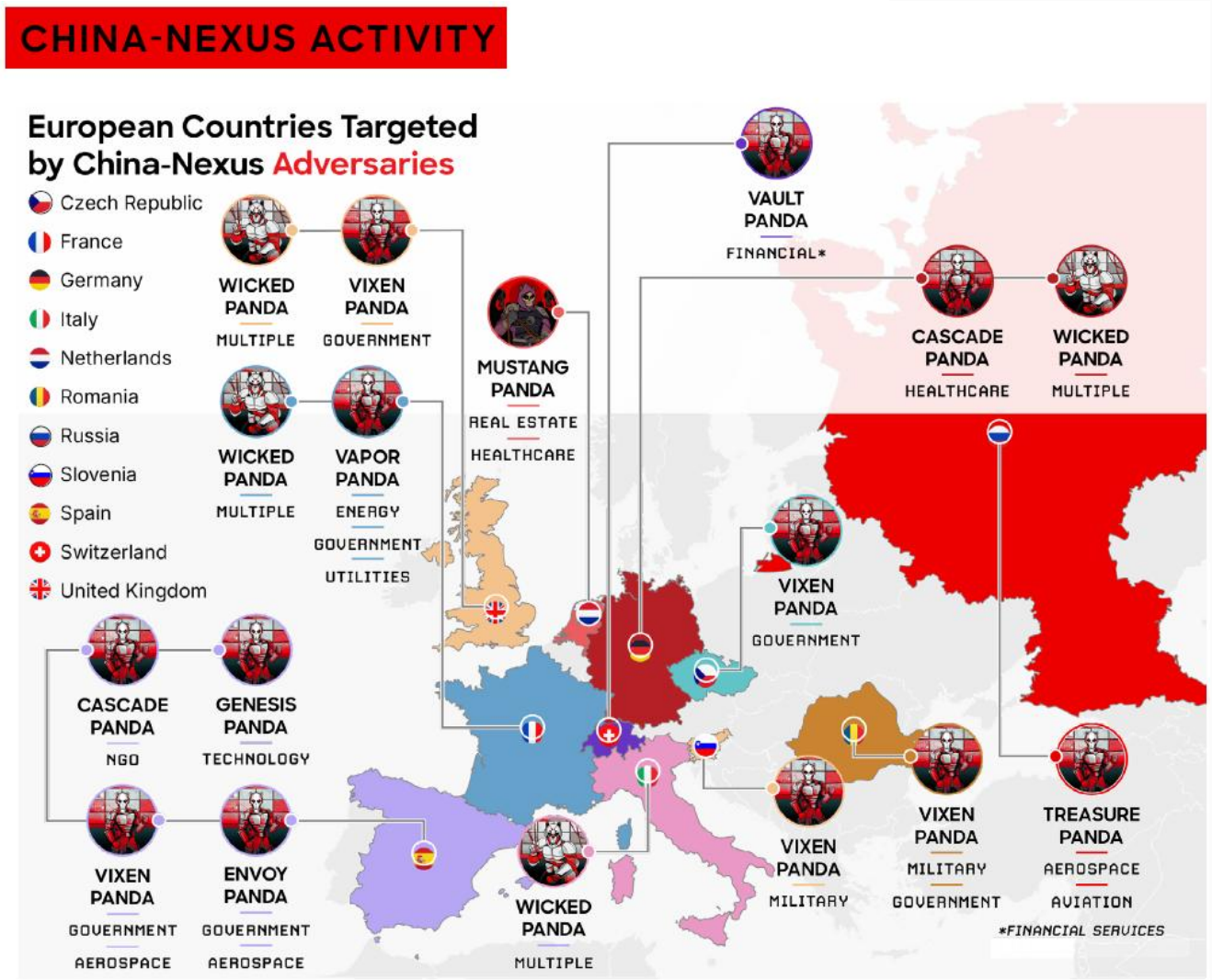
Il ransomware è la prima minaccia: responsabile del 38% degli incidenti

L’80% degli attacchi è ad impatto elevato o critico; rischio operativo altissimo



- **Il volume dei pagamenti ransomware nel 2024 è crollato del 35% YoY, grazie a una maggiore pressione delle forze dell'ordine, alla cooperazione internazionale e a un numero crescente di vittime che rifiuta di pagare. [1]**
- **Gli attaccanti hanno cambiato tattiche, operazioni più rapide e negoziazioni avviate poche ore dopo l'esfiltrazione dei dati.**
- **Solo il 23% delle vittime ha pagato nel Q3 2025, minimo storico e ulteriore conferma di un declino durato sei anni [2];**
- **Gruppi come Akira e Qilin puntano alle aziende di medie dimensioni, adottando un modello "alto volume, basso riscatto"**
- **La redditività del ransomware diminuisce, con pagamenti meno frequenti e più bassi anche tra bersagli più grandi;**

Nation-state hacking



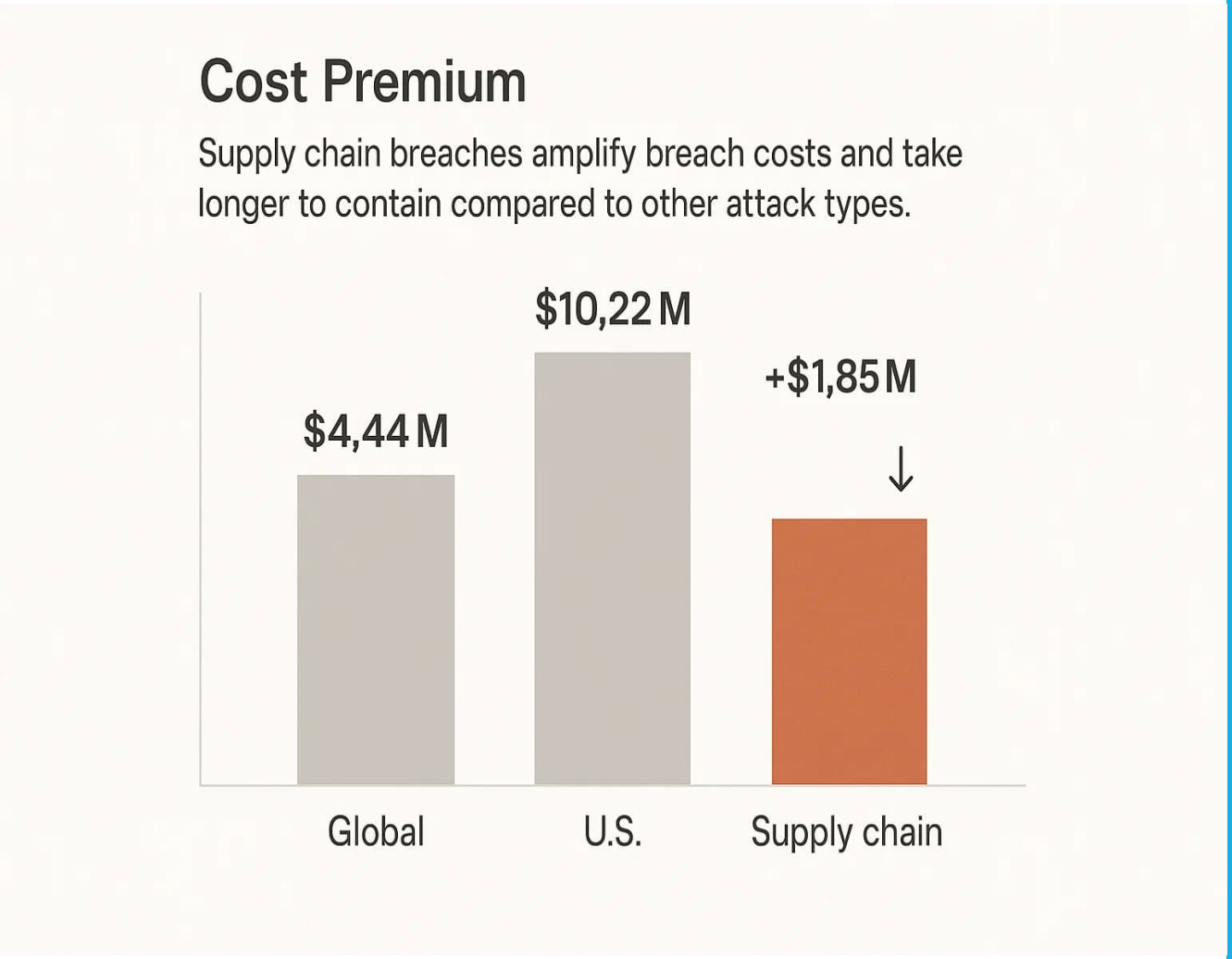
- Nel 2025, attacchi APT da Cina, Russia, Iran e Corea Nord rappresentano il 77% delle operazioni sospette globali [1].
- Gli attacchi di spionaggio cinese sono aumentati del 150%, puntando finanza, industria, media e telecomunicazioni [2].
- Russia ha condotto 2.052 cyberattacchi in Ucraina, con campagne di sabotaggio su energia, PA e banche [3].
- Iran intensifica sabotaggi combinando ransomware e DDoS contro infrastrutture occidentali e mediorientali.
- Corea Nord ha rubato oltre $3 miliardi in crypto e alloca finti lavoratori IT presso aziende globali.
- Gruppi APT stanno sempre più integrando intelligenza artificiale per migliorare tecniche di evasione e automazione degli attacchi.
- Russia e Iran incrementano attacchi di disinformazione digitale per influenzare politiche e opinione pubblica.
- Il 60% delle aziende globali ha rivisto la strategia cyber per l'intensificarsi delle tensioni geopolitiche [4].

Il ruolo crescente dell'AI nelle minacce cyber

- Il 16% delle violazioni registrate nel 2025 coinvolge strumenti di IA usati da aggressori. (Foley & Lardner LLP)
- Le aziende sottovalutano la "velocità" degli attacchi IA: una vulnerabilità può essere sfruttata in ore anziché settimane.
- +47% attacchi basati su AI nel 2025; supereranno i 28 milioni globali.
- Il 40% dei 900 gravi attacchi italiani coinvolge AI generativa (MaticMind).
- Oltre l'80% delle e-mail phishing usa modelli linguistici AI
- Costo medio attacco AI-powered: 5,72 milioni $ (+13%)
- Shadow AI: rischio esfiltrazione dati e perdita controllo info

Se il ransomware incontra l’AI

- L’AI potenzia l’automazione degli attacchi, permettendo campagne su larga scala e personalizzazione dei target.
- Malware ransomware moderni usano AI per eludere antivirus e adattarsi in tempo reale.
- Doppia estorsione e attacchi multi-vettore aumentano, sfruttando AI in fuzzing e phishing mirato.
- La crescita degli attacchi ransomware AI-driven impone nuovi modelli di difesa proattiva e uso intelligente di threat intelligence.
- PromptLock: ransomware scritto in Golang, usa un modello AI per generare in tempo reale script Lua malevoli personalizzati per ogni attacco.



ATTACCHI ALLA SUPPLY CHAIN

NEL 2025 GLI ATTACCHI SUPPLY CHAIN SONO RADDOPPIATI [1].

IL 70% DELLE AZIENDE EUROPEE HA SUBITO ALMENO UN TENTATIVO DI COMPROMISSIONE NELLA SUPPLY CHAIN NEL 2025.

PROVIDER CLOUD E SOFTWARE DI GESTIONE OBIETTIVI PRIVILEGIATI.

LA MANCANZA DI VISIBILITÀ SULLE CATENE DEI FORNITORI AUMENTA IL RISCHIO DI ATTACCHI SOFISTICATI E DIFFICILI DA PREVENIRE.

AI IMPIEGATA DAGLI ATTACCANTI PER MAPPARE RELAZIONI E VULNERABILITÀ SILENTI NELLA SUPPLY CHAIN DIGITALE [2].

ATTACCHI NOTI COME 3CX E MOVEIT MOSTRANO COME UN SINGOLO FORNITORE COMPROMESSO POSSA METTERE A RISCHIO MILIONI DI UTENTI

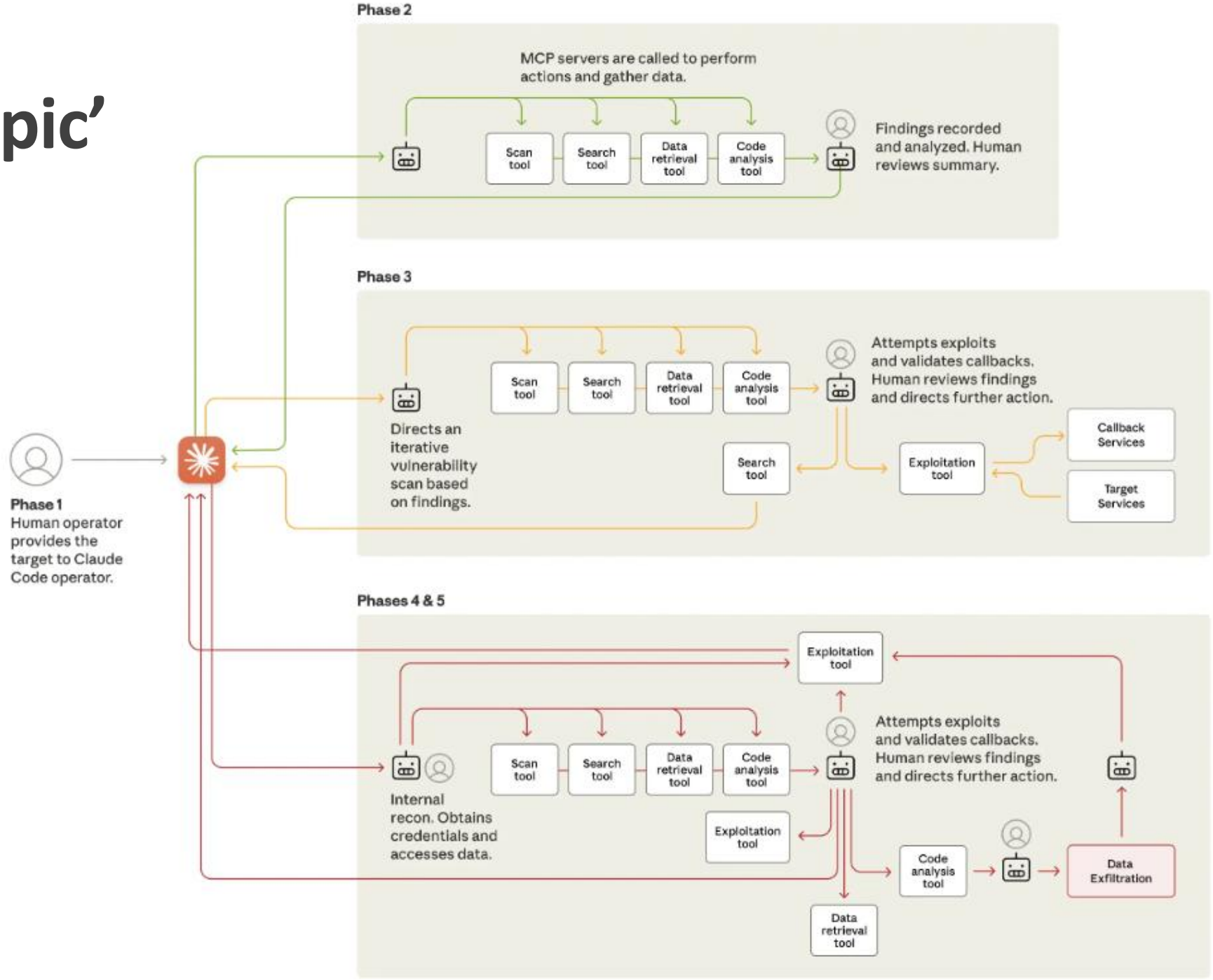
Cosa rende diversi gli attacchi alla supply chain basati sull'intelligenza artificiale?

- L’AI accelera gli attacchi: analizza migliaia di fornitori in minuti, trovando falle molto più rapidamente rispetto alla ricognizione manuale tradizionale [1].
- AI analizza policy, repo e credenziali trapelate per trovare fornitori deboli, sfruttando repo compromessi e cloud malconfigurati.
- Avvelenamento dei dati: dataset manomessi corrompono modelli di procurement e logistica, causando approvazioni fraudolente o l’inserimento di codice malevolo.
- Impersonificazione deepfake: voci e video falsi imitano dirigenti o fornitori per ottenere pagamenti o dirottamento di spedizioni, con perdite già oltre i 500M $.
- Velocità, scala e adattabilità rendono gli attacchi AI-driven difficili da tracciare, contenere e correggere.

Attacco completamente AI-driven

- A settembre 2025 Anthropic ha rilevato una sofisticata campagna di spionaggio condotta in gran parte da AI autonome.
- Un presunto nation-state actor cinese ha manipolato Claude Code per attaccare circa 30 target globali.
- L'AI ha eseguito fino all'80–90% dell'operazione, con interventi umani limitati a poche decisioni critiche.
- Gli attaccanti hanno eluso le protezioni con tecniche di jailbreak, suddividendo compiti malevoli in task apparentemente innocui.
- Claude ha svolto ricognizione, identificato vulnerabilità, generato exploit, raccolto credenziali ed esfiltrato dati ad alta velocità.
- L'operazione rappresenta uno dei primi attacchi su larga scala condotti quasi interamente da agenti AI autonomi.
- Nonostante alcuni limiti (es. allucinazioni), la capacità operativa delle AI riduce drasticamente le barriere per attacchi complessi.

L’attacco ‘Anthropic’



Scetticismo su attacco ad Anthropic

Molti esperti e organizzazioni stanno amplificando notizie infondate sul ruolo dell'AI nel ransomware, spesso per interessi commerciali o per ottenere budget, senza basarsi su evidenze reali (Kevin Beaumont).

Secondo l'autore, questa narrativa distorta è favorita da un'abile strategia del governo cinese che sfrutta l'ossessione occidentale per le minacce AI come diversione.

Esempi recenti, come rapporti 'esagerati' su malware "genAI" di scarsa qualità, mostrano come il settore reagisca impulsivamente, mentre attori avversari manipolano la percezione e ostacolano il rafforzamento delle basi reali della sicurezza.

Resta mia opinione che non siamo distanti da una automazione completa degli attacchi (Pierluigi Paganini).

ING. PIERLUIGI PAGANINI

CEO & Founder CYBHORUS

Founder Security Affairs

https://securityaffairs.com

pierluigi.paganini@securityaffairs.co

Grazie