Acronis

Report
II sem. 2024

Sintesi

Report Acronis sulle minacce digitali, secondo semestre 2024: L'incremento delle minacce basate sull'AI

Acronis Threat Research Unit

Autori:

Alexander Ivanyuk
Senior Director, Technology

Irina Artioli
Cyber Protection Evangelist, Acronis Threat Research Unit

Robert Neumann
Head of Acronis Threat Research Unit

Introduzione e riepilogo

Questo report semestrale di Acronis sulle minacce digitali offre un quadro globale di quanto rilevato dall'Acronis Threat Research Unit (TRU) e dai sensori Acronis nella seconda metà del 2024. I dati generali sul malware presentati nel report sono stati acquisiti tra luglio e dicembre del 2024 e riguardano le minacce che hanno preso di mira gli endpoint osservate in questo arco temporale.

Basato su oltre un milione di singoli endpoint distribuiti in tutto il mondo, il report include statistiche incentrate sulle minacce indirizzate ai sistemi operativi Windows, che hanno maggiore diffusione rispetto a quelle che colpiscono macOS e Linux.

- A dicembre del 2024, i paesi più colpiti dagli attacchi malware sono stati Emirati Arabi Uniti, Singapore e Italia.
- Nel quarto trimestre del 2024, Acronis ha bloccato più di 48 milioni di URL sugli endpoint, un aumento del 7% rispetto al terzo trimestre del 2024.
- Il 31,4% di tutte le e-mail ricevute nel secondo semestre del 2024 era spam e l'1,4% di queste conteneva malware o link di phishing.
- La percentuale più elevata di URL pericolosi bloccati sugli endpoint a dicembre del 2024 è stata registrata negli Emirati Arabi Uniti (16,2%), seguiti dal Brasile con il 13,2% e da Singapore con il 12%.
- Nel quarto trimestre del 2024 sono stati resi pubblici 1.712 casi di ransomware. RansomHub, Akira, Play e KillSec sono tra i gruppi che hanno maggiormente contribuito, con un totale di 580 vittime. A dicembre è stato molto attivo il gruppo di ransomware Cl0p, con 68 vittime.

Principali tendenze relative alla Cyber Security da luglio a dicembre 2024

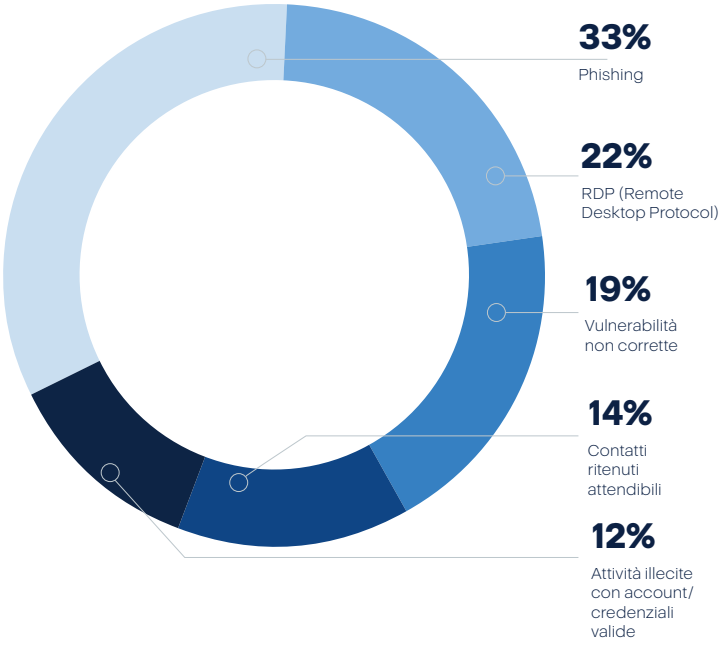
- Nel 2024 il ransomware ha preso di mira in misura crescente settori critici come quello dei trasporti, della sanità e manifatturiero; gli attaccanti hanno utilizzato tattiche personalizzate e strategie basate sull'AI per sfruttare le vulnerabilità e chiedere riscatti più elevati. Questa tendenza riflette l'evoluzione verso attacchi più complessi e su larga scala, che puntano ad aumentare le interruzioni operative e i proventi economici. Si conferma quindi il ruolo strategico degli MSP nella protezione delle organizzazioni, grazie alla loro offerta di misure di sicurezza e strategie di incident response avanzate.
- Le violazioni dei dati non accennano a diminuire e a gettare scompiglio nelle aziende di tutto il mondo.
- ChatGPT e sistemi simili di intelligenza artificiale generativa vengono sempre più utilizzati per creare contenuti dannosi, avviare gli attacchi e automatizzarli.
- Rispetto alla seconda metà del 2023, il numero di attacchi basati sulle e-mail rilevati nella seconda metà del 2024 è aumentato del 197%, mentre nello stesso arco di tempo è aumentato del 21% il numero di attacchi per organizzazione.

Principali minacce e tendenze della seconda metà del 2024

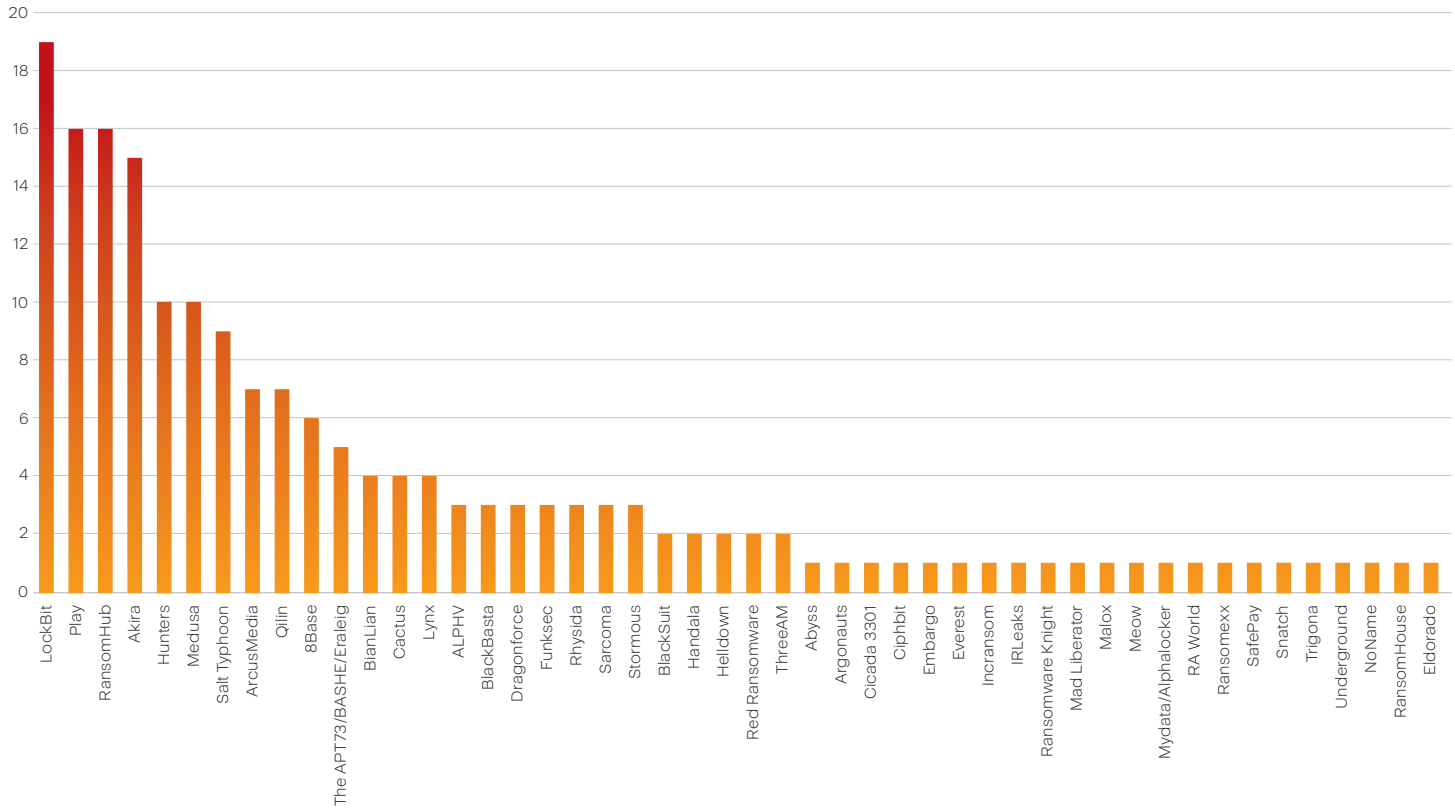
La verità sul ransomware nel 2024: un incremento del 5% e ransomware legati alle minacce APT che puntano agli MSP

Abbiamo continuato a monitorare gli attacchi sferrati ai managed service provider (MSP) ed esteso i dati da gennaio a dicembre 2024. Dall'analisi emerge che gli hacker hanno utilizzato prevalentemente campagne di phishing via e-mail, seguite dall'exploit delle vulnerabilità individuate nelle connessioni Remote Desktop Protocol (RDP) e negli strumenti di accesso remoto.

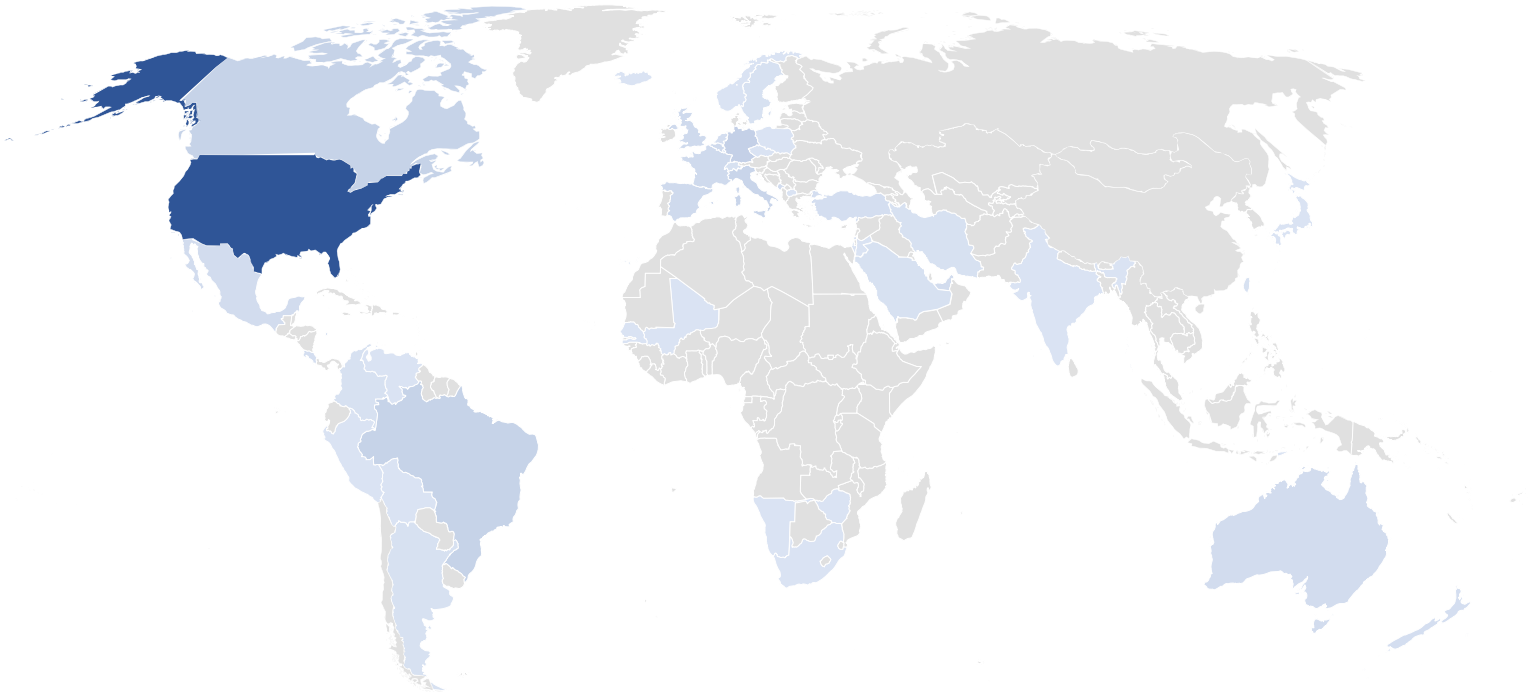
Vettore iniziale	Numero di vittime
Phishing	62
RDP (Remote Desktop Protocol)	40
Vulnerabilità non corrette	35
Contatti ritenuti attendibili	26
Attività illecite con account/credenziali valide	22



Gruppi di ransomware che prendono di mira gli MSP



Paesi più colpiti dagli attacchi agli MSP



Percentuale

1% 62%

Gli MSP diventano obiettivi sempre più appetibili per i criminali e sono colpiti dagli stessi tipi di vettori di attacco iniziali delle altre vittime. La nostra vasta analisi degli attacchi agli MSP durante il 2024 segnala ancora il phishing come metodo preferito, con 62 incidenti registrati, seguito dall'exploit di vulnerabilità non corrette, dall'utilizzo illecito del protocollo RDP e dagli attacchi da parte di contatti ritenuti attendibili. Compromissione delle credenziali e infiltrazione nella supply chain si confermano punti di accesso strategici. Pur non essendo nuovi, questi vettori continuano a essere efficaci contro gli MSP, il che evidenzia un'allarmante carenza nelle procedure di sicurezza basilari.

Tuttavia, la tendenza emergente e più preoccupante è la scelta degli MSP come destinazione per i gruppi di ransomware legati alle minacce persistenti avanzate (APT). Utilizzo di credenziali rubate, social engineering e attacchi alla supply chain sono alcune delle tattiche di spionaggio altamente sofisticate utilizzate da questi gruppi per introdursi nelle reti degli MSP e propagare il ransomware ai loro clienti. Incorporando il malware negli aggiornamenti software considerati attendibili o sfruttando le vulnerabilità delle soluzioni per l'accesso remoto, i gruppi di APT approfittano della fiducia implicita nelle relazioni tra MSP e clienti per ampliare il loro raggio d'azione.

Minacce digitali generate da AI: una nuova sfida

Nel contesto in continua evoluzione della Cyber Security, le minacce digitali generate tramite l'AI sono stati uno dei problemi più pressanti del 2024. L'AI rivoluziona vari settori e permette anche ai cybercriminali di sferrare attacchi sempre più sofisticati. Dallo sviluppo dei malware al social engineering, nelle mani dei criminali l'AI si rivela tanto uno strumento di innovazione quanto un'arma.

Osserviamo in modo più dettagliato le principali minacce legate all'AI emerse nel 2024.

1. Impiego dell'AI da parte dei cybercriminali

OpenAI lo conferma: gli autori delle minacce utilizzano ChatGPT e altri strumenti di AI generativa per creare malware, diffondere disinformazione e lanciare campagne di spear-phishing. In questa serie di casi recenti, i gruppi di hacker hanno sfruttato l'AI per potenziare i propri attacchi:

- TA547, noto anche come Scully Spider, ha utilizzato un loader PowerShell generato da AI per distribuire l'infostealer Rhadamanthys.
- Il gruppo cinese SweetSpecter ha preso di mira i dipendenti di OpenAI con e-mail di phishing contenenti allegati dannosi, dimostrando ancora una volta come l'utilizzo dell'AI permette ai criminali di mettere a punto attacchi più efficaci.

Gruppi come l'iraniano CyberAv3ngers e gli hacker sostenuti dalla Corea del Nord hanno utilizzato strumenti di AI simili a ChatGPT per sferrare potenti attacchi a infrastrutture critiche e appropriarsi di dati sensibili. Questi sviluppi riflettono le maggiori capacità disponibili anche ad attaccanti meno esperti, che ora sono in grado di eseguire operazioni complesse con l'aiuto dell'AI generativa.

2. AI generativa per creare malware

I modelli di AI generativa, compresi quelli non regolamentati come WormGPT, FraudGPT e DarkBERT, offrono ai cybercriminali modelli con cui creare con facilità malware e script di hacking personalizzati. Un esempio eclatante è quello del 25enne giapponese a cui sono bastate sei ore per scrivere un ransomware utilizzando ChatGPT.

Questi modelli di AI permettono agli hacker di aggirare le difese tradizionali generando nuovi vettori di attacco che sfuggono al rilevamento. Per far fronte a questa tendenza è necessario adottare una strategia di difesa solida e su più livelli.

3. Uso dell'AI da parte della Corea del Nord per le operazioni digitali

Con l'integrazione dell'AI, la Corea del Nord ha perfezionato le proprie attività informatiche. Sfruttando l'AI per creare falsi profili LinkedIn e video deepfake, gli hacker nordcoreani sono riusciti a infiltrarsi in aziende di tutto il mondo. Le false identità generate dall'AI hanno causato gravi violazioni, come il furto di criptovalute e di dati sensibili nell'ambito del settore della difesa.

4. Attacchi alla supply chain del software basati su AI

L'ampia diffusione di strumenti potenziati da AI ha reso la supply chain software un appetibile obiettivo per i criminali informatici. In un incidente avvenuto da poco, gli attaccanti hanno caricato pacchetti dannosi nel repository Python Package Index (PyPI), facendosi passare per modelli di AI molto diffusi come ChatGPT e Claude. Questi pacchetti, il cui download è stato eseguito migliaia di volte, contenevano un infostealer Java chiamato JarkaStealer. Dopo l'installazione, il malware ha sottratto dati sensibili, tra cui informazioni sul browser web e token di sessione.

5. Segnalazioni dell'FBI su meccanismi di frode basati su AI

L'FBI ha lanciato alcuni allarmi sull'impiego dell'AI per aumentare la portata e la complessità di alcuni meccanismi di frode. Dalle truffe romantiche alle false promozioni sugli investimenti, i contenuti generati dall'AI inducono più facilmente le vittime a cadere nei tranelli. Grazie a testi e immagini realistiche e a video deepfake, gli attaccanti possono mettere a punto truffe più convincenti che ottengono maggiore diffusione.

La doppia natura dell'AI: innovazione e uso improprio

La diffusione dell'AI tra i criminali informatici pone in luce la duplice natura di questa tecnologia. Se da un lato l'AI offre straordinarie opportunità di innovazione e di applicazione nei settori della sanità, delle finanze e della logistica, dall'altro il suo utilizzo improprio permette ai cybercriminali di creare attacchi più sofisticati, scalabili e automatizzati. È chiara quindi l'urgente necessità di strategie di Cyber Security complete che riescano a tenere il passo con la rapida evoluzione delle minacce.

In risposta all'aumento delle minacce digitali basate su AI, Acronis continua a migliorare le proprie soluzioni di sicurezza, garantendo alle aziende e ai singoli utenti misure di difesa innovative contro le nuove generazioni di attacchi. Le funzionalità di monitoraggio proattivo, rilevamento delle minacce basato su AI e risposta in tempo reale di Acronis Advanced Security + Extended Detection and Response (XDR) offrono alle organizzazioni gli strumenti per neutralizzare le minacce emergenti prima che provochino danni significativi.

Quattro consigli per mitigare le minacce basate su AI

1 **Adottare la sicurezza a più livelli**

Combina analisi comportamentale, rilevamento euristico e monitoraggio basato su AI per rilevare e bloccare le minacce generate da AI.

2 **Aggiornamento continuo contro le vulnerabilità individuate dall'AI**

Aggiorna regolarmente i software e i protocolli di sicurezza per garantire la protezione completa contro i tentativi di exploit delle vulnerabilità basati su AI.

3 **Formazione di personale e partner**

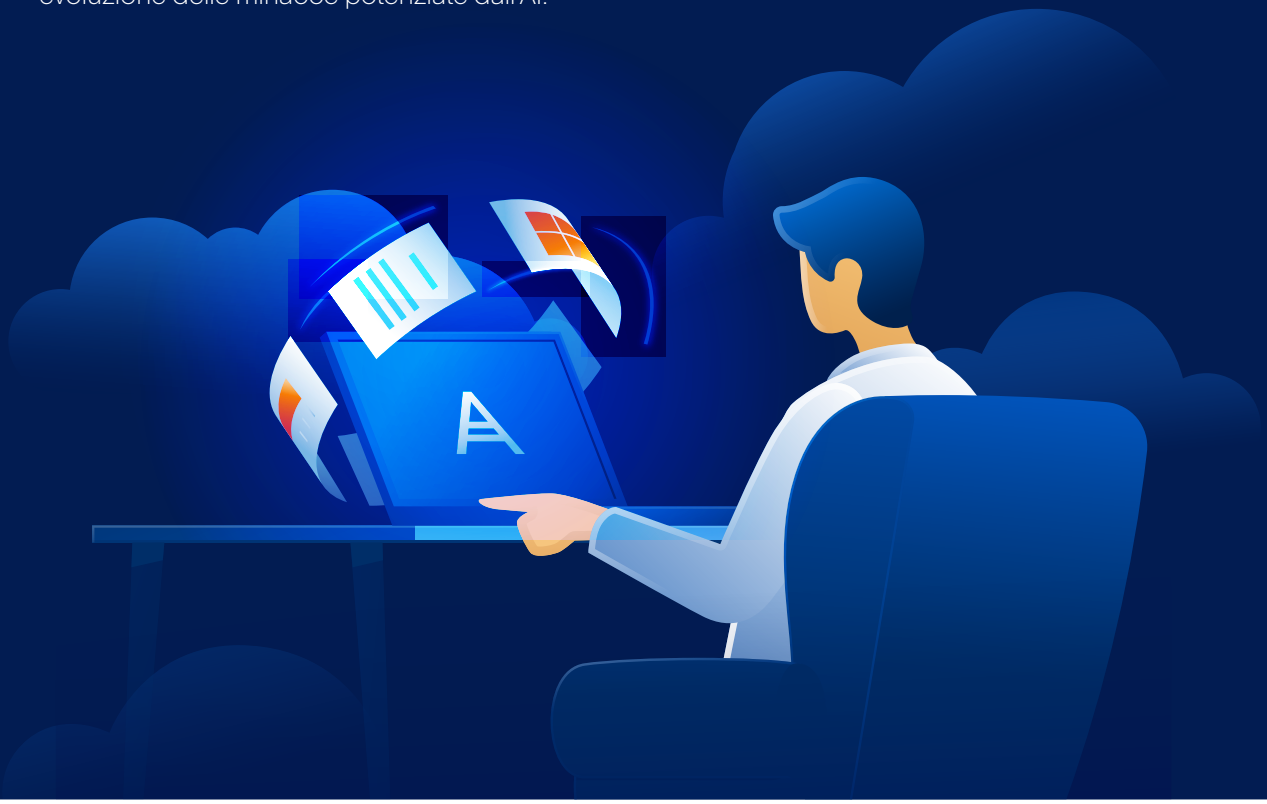
La consapevolezza è fondamentale. Garantisci una formazione regolare per riconoscere i tentativi di phishing, deepfake e altre tattiche di social engineering basate su AI.

4 **Utilizzo dell'AI per la difesa**

Così come la criminalità sfrutta l'AI per potenziare i propri attacchi, i fornitori di soluzioni di sicurezza devono avvalersi dell'AI per rilevare e neutralizzare le minacce in modo più rapido ed efficace.

Conclusioni

La maggiore diffusione delle minacce digitali assistite dall'AI registrata nel 2024 rappresenta un'evoluzione importante nel contesto della Cyber Security. Poiché l'AI offre strumenti per l'attacco e la difesa, per mantenersi un passo avanti è fondamentale che le organizzazioni adottino misure di sicurezza solide e basate su AI. Acronis sviluppa soluzioni di sicurezza avanzata pensate per affrontare queste sfide, che garantiscono la protezione completa necessaria a contrastare la minaccia crescente della criminalità potenziata dall'AI. Combinando monitoraggio proattivo, analisi comportamentale e meccanismi di difesa basati su AI, le aziende possono difendersi al meglio nel panorama in continua evoluzione delle minacce potenziate dall'AI.



Acronis

Acronis Threat Research Unit

Per saperne di più,
visita il sito acronis.com