Introduzione e sommario

Acronis è stata la prima azienda a implementare la Cyber Protection integrata e completa per proteggere tutti i dati, le applicazioni e i sistemi. Questo tipo di protezione informatica richiede costanti attività di ricerca e monitoraggio delle minacce, nonché l'adozione dei cinque vettori della protezione: salvaguardia, accessibilità, privacy, autenticità e sicurezza (noti anche con l'acronimo SAPAS). Nell'ambito di questa strategia, Acronis gestisce quattro centri CPOC (Cyber Protection Operation Center) in diverse zone del mondo per monitorare e svolgere indagini sulle minacce digitali 24 ore su 24, 7 giorni su 7.

Abbiamo inoltre rinnovato i nostri prodotti di punta: Acronis Cyber Protect Cloud, una soluzione cloud aggiunta alla piattaforma Acronis Cyber Cloud, e Acronis Cyber Protect 15, una soluzione on-premise. Già prima di rilasciare questi prodotti Acronis era uno dei leader nel mercato della protezione dei dati grazie alla sua tecnologia anti-ransomware innovativa Acronis Active Protection, che nel corso del tempo si è evoluta consolidando l'esclusiva competenza di Acronis nel bloccare le minacce sferrate contro i dati. È tuttavia importante notare che le tecnologie di rilevamento basate su intelligenza artificiale e analisi comportamentale, sviluppate da Acronis a partire dal 2016, sono state successivamente perfezionate al fine di contrastare tutte le forme di malware e altre potenziali minacce.

Questo report si occupa del panorama delle minacce rilevato dai nostri sensori e analisti nella prima metà del 2022.

I dati generali sul malware presentati nel report sono stati raccolti da gennaio a giugno di quest'anno e riflettono le minacce rivolte agli endpoint che abbiamo rilevato durante tale periodo.

Il report illustra un quadro globale ed è basato su oltre 700.000 endpoint singoli distribuiti in tutto il mondo. La maggior parte delle statistiche prese in esame riguarda le minacce ai sistemi operativi Windows, che sono molto più diffuse rispetto a quelle ai sistemi macOS e Linux. Osserveremo gli sviluppi della situazione e nel prossimo report potremmo includere anche i dati sulle minacce a macOS e Linux.

I sei numeri principali del primo semestre 2022: ↘

- I paesi più colpiti dal malware nel secondo trimestre 2022 sono Stati Uniti, Germania e Brasile.
- Nel secondo trimestre 2022, Acronis ha bloccato 21 milioni di URL sugli endpoint, con un aumento del 10% rispetto al primo trimestre.
- Il 26,5% di tutte le e-mail ricevute è spam e l'1% di queste contiene malware o link di phishing.
- Ogni esemplare di malware circola in media per 2,3 giorni prima di scomparire. L'81% degli esemplari è stato osservato una sola volta.
- In soli due anni, il gruppo specializzato nel ransomware Conti ha guadagnato 2,7 miliardi di dollari in criptovalute; le statistiche indicano che a gennaio 2022 sono state registrate oltre 1.000 vittime, con un volume di riscatti di oltre 150 milioni di dollari.
- Si calcola che i danni del ransomware a livello mondiale supereranno i 30 miliardi di dollari entro il 2023.

Alcuni dei trend relativi alla Cyber Security osservati nella prima metà del 2022 sono i seguenti: ↘

- Il ransomware continua a essere la minaccia numero uno per le grandi e medie imprese, anche per settori critici come quelli governativo e sanitario.
- Le credenziali esfiltrate o rubate hanno causato quasi la metà delle violazioni segnalate nel primo semestre 2022. Il furto di credenziali continua a essere una delle forze trainanti delle violazioni, che permette agli hacker di organizzare agevolmente campagne di phishing e ransomware.
- Le piattaforme di social media Twitter e Facebook, nonché DHL e Microsoft, sono stati tra i brand più sfruttati per il phishing a livello mondiale nella prima metà del 2022.
- Gli attacchi sferrati agli MSP sono in aumento, e ciò solleva problematiche di responsabilità. Oltre l'80% degli MSP ha registrato un aumento degli attacchi contro i propri clienti negli ultimi 12 mesi.
- In 475 su 12.985 hanno segnalato vulnerabilità attivamente sfruttate nella prima metà del 2022.
- I sistemi operativi Linux sono sempre più nel mirino dei cybercriminali, specialmente di quelli che prendono di mira istanze e contenitori cloud.

Che cosa troverete in questo report:

- I principali trend della sicurezza e delle minacce che abbiamo osservato nella prima metà del 2022
- Perché registriamo un numero crescente di minacce indirizzate alle criptovalute
- Perché aumentano le minacce agli MSP e ai sistemi operativi alternativi
- Statistiche generali sul malware e principali famiglie esaminate
- Statistiche sul ransomware con un'analisi approfondita delle minacce più pericolose
- Quali vulnerabilità contribuiscono al successo degli attacchi
- I nostri suggerimenti in fatto di sicurezza