Acronis

Report sulle minacce digitali del secondo semestre 2023

Incessante aumento degli attacchi informatici: PMI e MSP nel mirino

Introduzione e riepilogo

Il report illustra un quadro globale basandosi su oltre un milione di endpoint singoli distribuiti in tutto il mondo e si concentra su 15 paesi chiave. 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.

Autori:

Alexander Ivanyuk
Senior Director, Technology

Candid Wuest
VP of Product Management

Irina Artioli
Cyber Protection Evangelist

Conclusioni principali

- Nell'ultimo trimestre del 2023, i paesi più colpiti dagli attacchi malware sono Singapore, Spagna e Brasile.
- Nello stesso periodo, Acronis ha bloccato quasi 28 milioni di URL sugli endpoint, un calo del 36% rispetto al quarto trimestre del 2022.
- Il 33,4% di tutte le e-mail ricevute è spam e l'1,5% di queste contiene malware o link di phishing.
- Ogni esemplare di malware circola in media per 2,1 giorni prima di scomparire.
- Nel quarto trimestre del 2023 sono stati resi pubblici 1.353 casi di ransomware. LockBit, Play e ALPHV sono tra i gruppi che hanno maggiormente contribuito. A dicembre è stato molto attivo il gruppo di ransomware Toufan, con 91 vittime.

Alcuni trend relativi alla Cyber Security osservati tra luglio e dicembre 2023

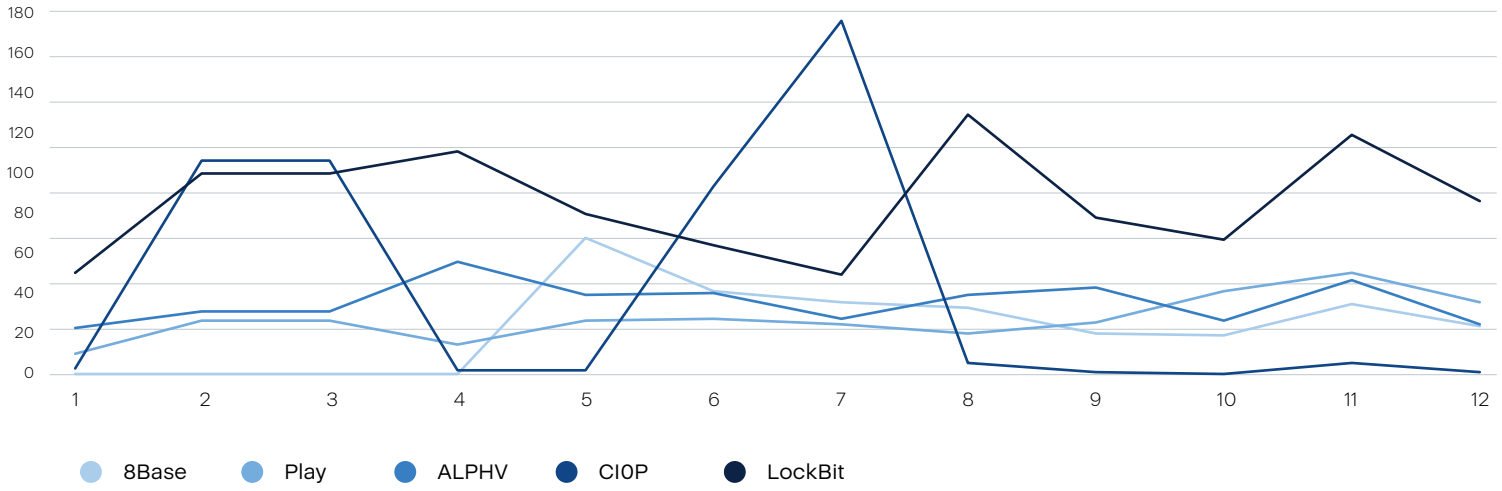
- Il ransomware continua a essere la minaccia numero uno per le grandi e medie imprese, anche per settori critici come quelli governativo e sanitario, tra gli altri. Di recente, gli autori di ransomware hanno sfruttato a proprio vantaggio le unità vulnerabili per infiltrarsi nei sistemi e disabilitare gli strumenti di sicurezza.
- I furti di dati sono la seconda minaccia più diffusa, causa di numerose violazioni dei dati insieme all'ormai convenzionale utilizzo delle credenziali rubate.
- ChatGPT e sistemi simili di Intelligenza Artificiale generativa vengono già utilizzati per creare contenuti dannosi, avviare gli attacchi e automatizzarli.
- Il numero di attacchi via e-mail rilevati nel 2023 è aumentato del 222% rispetto alla seconda metà del 2022.

1. Le varianti di ransomware continuano a diminuire, ma le aziende perdono ancora dati e denaro

Dall'analisi dei dati del 2023 emerge che i seguenti gruppi di ransomware risultano essere stati i più attivi in termini di numero totale di vittime:

LockBit (1.000) | **CI0P (487)** | **BlackCat/ALPHV (415)** | **Play (322)** | **8Base (269)**

I primi 5 gruppi specializzati in ransomware per mese e numero di vittime



I gruppi LockBit e BlackCat/ALPHV già nel 2022 avevano un ruolo di primo piano tra i gruppi specializzati in ransomware. Tenendo il passo per tutto il 2023, hanno colpito numerose vittime di alto profilo. Nel dicembre 2023, il Dipartimento di Giustizia degli Stati Uniti ha rivelato che l'FBI, in collaborazione con forze dell'ordine internazionali, è riuscito ad accedere ai server del gruppo ALPHV, prendendo il controllo delle attività e acquisendo le chiavi di decrittografia. L'operazione ha consentito di evitare il versamento di circa 68 milioni di dollari in riscatti, aiutando 500 vittime a recuperare gratuitamente i propri file. Secondo l'FBI, il gruppo ALPHV ha violato oltre 1.000 entità, ha chiesto oltre 500 milioni di dollari di riscatto e ne ha ricevuti più di 300 milioni.

2. Gli attacchi agli MSP non accennano a diminuire

Non è facile identificare gli attacchi sferrati specificamente contro gli MSP o gli MSSP, perché molti di questi eventi non vengono resi pubblici o sono segnalati come attacchi generici contro il cliente finale. Uno dei pochi esempi noti è la recente violazione ad alta visibilità che ha interessato gli account e-mail nel cloud Microsoft di diverse agenzie governative degli Stati Uniti. Secondo quanto riferito, sono state sottratte 60.000 e-mail appartenenti a 10 account del Dipartimento di Stato degli Stati Uniti. A settembre, Microsoft ha comunicato l'identificazione di altre vulnerabilità che hanno permesso a Storm-0558, un gruppo di hacker collegato alla Cina, di manomettere gli account e-mail nel cloud di alcuni funzionari statunitensi.

Secondo Microsoft, a seguito di un crash del sistema Windows avvenuto nel 2021, una falla ha consentito l'acquisizione e la memorizzazione impropria di una chiave di autenticazione di Azure Active Directory e un'altra ne ha impedito il rilevamento. Molti MSP e MSSP fanno largo uso di Azure e dei servizi che offre. Questi Service Provider sono potenziali vittime di simili attacchi, perché potrebbero non essere in grado di rilevare l'accesso illegale alle e-mail dei loro clienti a causa della limitata visibilità che hanno sui sistemi.

3. Le e-mail pericolose e di phishing restano il principale vettore di infezione

Rispetto alla seconda metà del 2022, il numero complessivo degli attacchi basati sulle e-mail rilevati nel 2023 è aumentato del 222%, mentre nello stesso arco di tempo è aumentato del 54% il numero di attacchi per organizzazione. Queste statistiche evidenziano l'intensificarsi delle minacce, con l'e-mail che resta il principale vettore di attacco, e l'urgenza per le organizzazioni di rafforzare le misure di difesa contro queste attività dannose.

Non sorprende che il 91,1% delle organizzazioni abbia subito un attacco con phishing potenziato dall'AI.

Nel 2023, ogni e-mail analizzata conteneva in media 2,7 tra file e URL, ciascuno dei quali poteva rappresentare una potenziale minaccia. Come previsto, nel 2023 si è registrato un aumento del 15% del numero di file e URL per ogni e-mail analizzata. Ciò significa che le organizzazioni devono aumentare la vigilanza, perché il numero medio è salito a circa tre file e URL per ogni e-mail scansionata.

4. La minaccia dell'AI: i cyber criminali si avvalgono di strumenti avanzati basati sull'AI per attaccare le aziende

La promessa dell'AI è un futuro di efficienza e innovazioni rivoluzionarie; se però da un lato la tecnologia si è evoluta per potenziare le capacità umane, dall'altro sono aumentate anche le potenzialità di abuso. Negli ultimi anni è emerso anche un aspetto più oscuro dell'AI, i cui potenti strumenti vengono utilizzati dai criminali per generare attacchi sempre più sofisticati. La diffusione al grande pubblico di ChatGPT, lo scorso anno, ha intensificato questa minaccia.

I criminali informatici utilizzano in modo illecito i servizi di AI generativa come ChatGPT, e hanno anche sviluppato strumenti AI pericolosi come WormGPT e FraudGPT, commercializzati tramite forum web illeciti dopo aver attinto a grandi modelli linguistici (LLM) esclusivi, sviluppati appositamente con finalità illegali. Spesso questi strumenti vengono offerti su sottoscrizione. Simili ai più diffusi LLM, non hanno limitazioni né filtri e vengono addestrati su dati selezionati in modo da consentire gli attacchi; di ciò non abbiamo al momento conferme, ma è altamente probabile.

Paese	Percentuale di rilevamento a novembre	Percentuale di rilevamento a dicembre	Percentuale di rilevamento normalizzata a dicembre
Australia	1,8%	1,4%	15,2%
Brasile	10,2%	8,6%	22,3%
Canada	5,5%	4,7%	9,2%
Francia	3,6%	4,3%	21,0%
Germania	8,4%	8,0%	21,6%
Italia	5,6%	6,1%	23,4%
Giappone	2,8%	2,5%	16,6%
Paesi Bassi	1,2%	1,5%	27,6%
Singapore	5,3%	6,1%	55,6%
Sudafrica	1,2%	1,2%	18,0%
Spagna	2,8%	3,1%	41,3%
Svizzera	3,6%	3,6%	20,2%
Emirati Arabi Uniti	0,8%	1,0%	28,6%
Regno Unito	4,5%	4,5%	17,3%
Stati Uniti	17,8%	16,2%	18,2%

WormGPT è un modulo di AI basato sul modello linguistico GPTJ sviluppato nel 2021 e già utilizzato in attacchi di compromissione delle e-mail aziendali (BEC) e di altro tipo. È stato fonte di ispirazione per strumenti simili, in particolare FraudGPT, utilizzato per creare contenuti dannosi, come e-mail di phishing e strumenti di cracking, o per attività fraudolente con le credenziali delle carte di credito. DarkBART, ChaosGPT e DarkBERT sono altri pericolosi strumenti basati su AI. Sviluppato dalla sudcoreana S2W Security e addestrato con i dati del dark web, DarkBERT è stato in origine progettato per contrastare la criminalità informatica ma, come ChatGPT, viene ora sfruttato con finalità illecite.

Per un'analisi approfondita delle tendenze e delle statistiche sulle minacce digitali del secondo semestre 2023, leggi il report completo.

Primi 10 paesi: rilevamenti di malware normalizzati

Posizione	Paese	Percentuale di clienti con rilevamenti di malware - Dicembre 2023
1	Namibia	74,5%
2	Bahrain	59,6%
3	Serbia	58,3%
4	Egitto	56,3%
5	Singapore	55,6%
6	Sri Lanka	54,8%
7	Israele	47,7%
8	Finlandia	43,6%
9	Corea del Sud	42,4%
10	Repubblica di Moldavia	41,8%

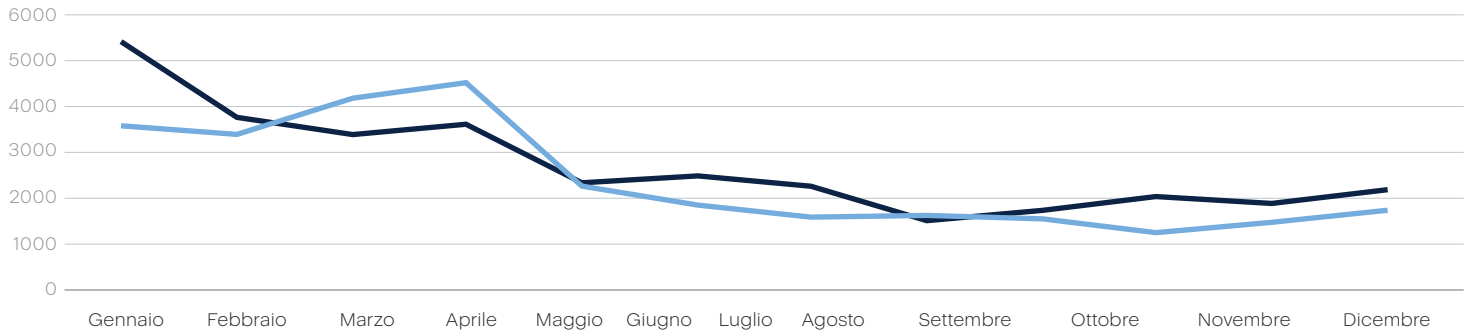
Primi 10 paesi: rilevamenti di ransomware globali per trimestre, normalizzati

Posizione	Paese	Percentuale di rilevamenti di ransomware globali - 3° trim. 2023	Percentuale di rilevamenti di ransomware globali - Ottobre 2023	Percentuale di rilevamenti di ransomware globali - Novembre 2023
1	Corea del Sud	45,2%	10,4%	13,3%
2	Cina	26,6%	7,8%	9,6%
3	Filippine	18,9%	6,8%	7,3%
4	Giappone	13,9%	3,1%	4,2%
5	Taiwan	10,7%	3,4%	3,3%
6	Germania	9,3%	2,4%	2,9%
7	Romania	7,7%	1,9%	2,8%
8	Repubblica Ceca	6,8%	1,9%	1,8%
9	Turchia	4,9%	1,9%	1,9%
10	Polonia	5,3%	1,8%	1,5%

Attività di ransomware nei paesi chiave

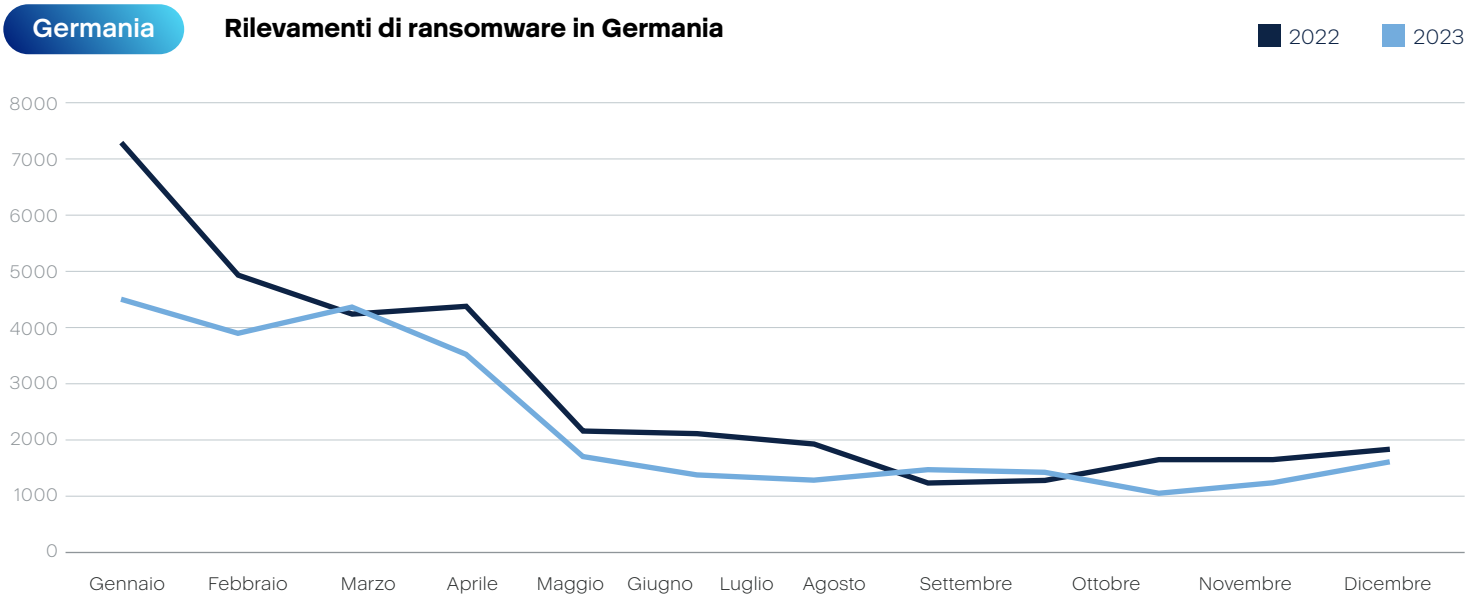
Stati Uniti

Rilevamenti di ransomware negli Stati Uniti



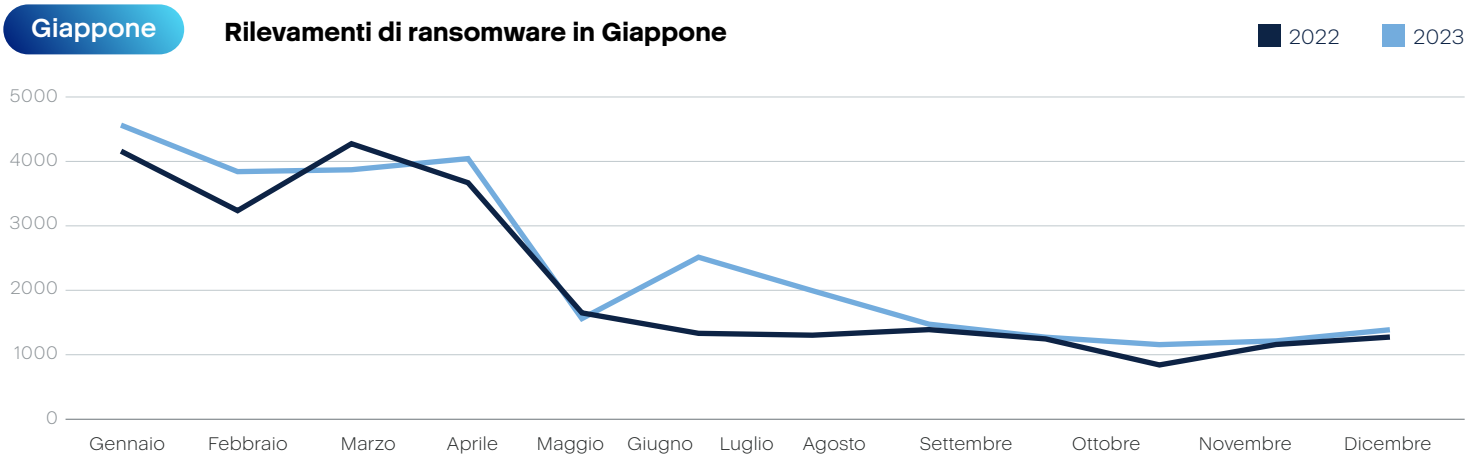
Germania

Rilevamenti di ransomware in Germania



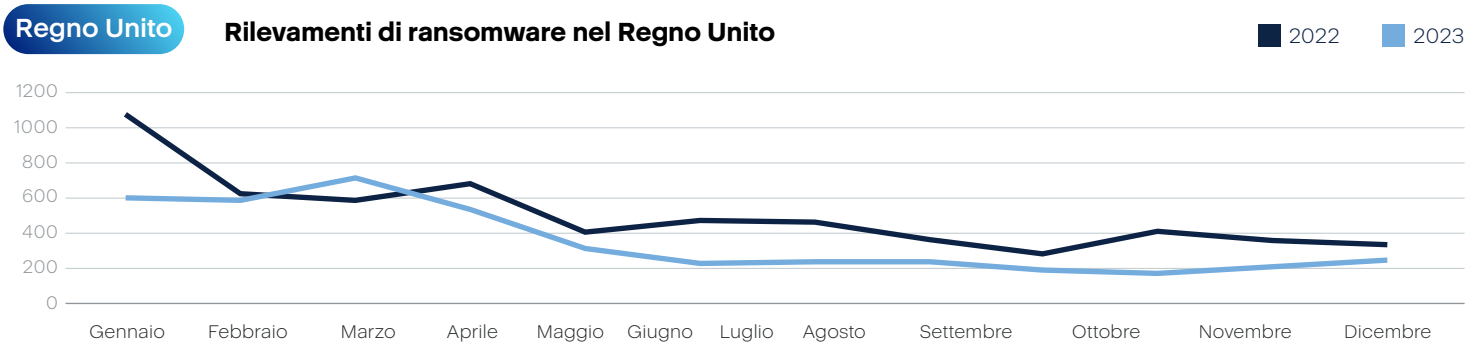
Giappone

Rilevamenti di ransomware in Giappone



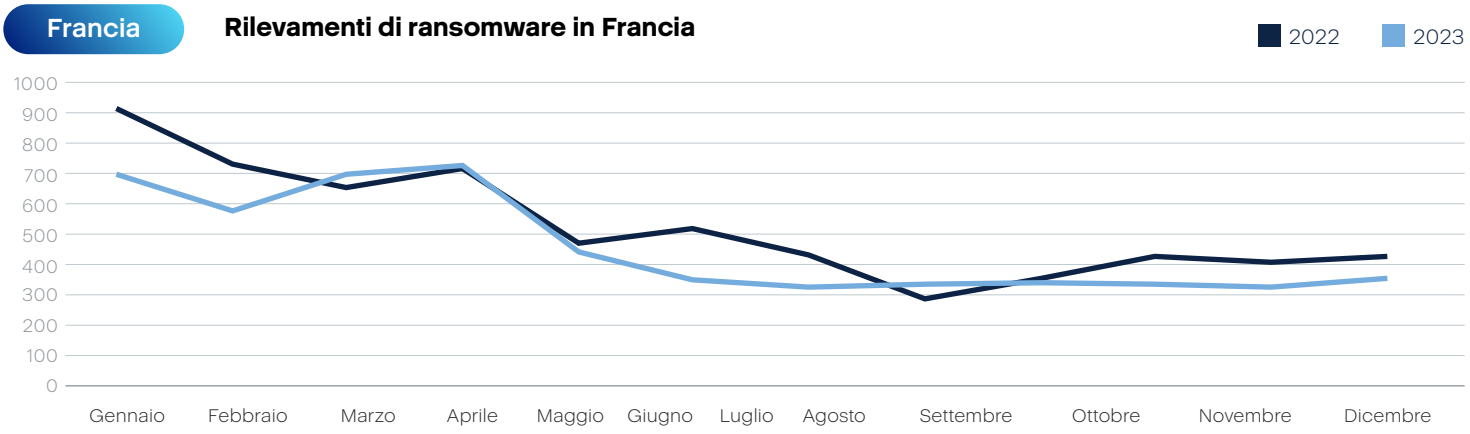
Regno Unito

Rilevamenti di ransomware nel Regno Unito



Francia

Rilevamenti di ransomware in Francia



Siti web pericolosi

Paesi chiave con URL bloccati - Dicembre 2023

Posizione	Paese	Percentuale di URL bloccati a dicembre 2023
1	Giappone	21,2%
2	Emirati Arabi Uniti	18,7%
3	Stati Uniti	18,2%
4	Brasile	17,6%
5	Singapore	17,3%
6	Francia	17,2%
7	Germania	16,4%
8	Paesi Bassi	15,0%
9	Sudafrica	14,7%
10	Spagna	13,4%
11	Australia	13,1%
12	Italia	12,9%
13	Regno Unito	11,3%
14	Svizzera	10,2%
15	Canada	5,1%

Acronis

Per saperne di più, visita acronis.com