IBM Italy News Room

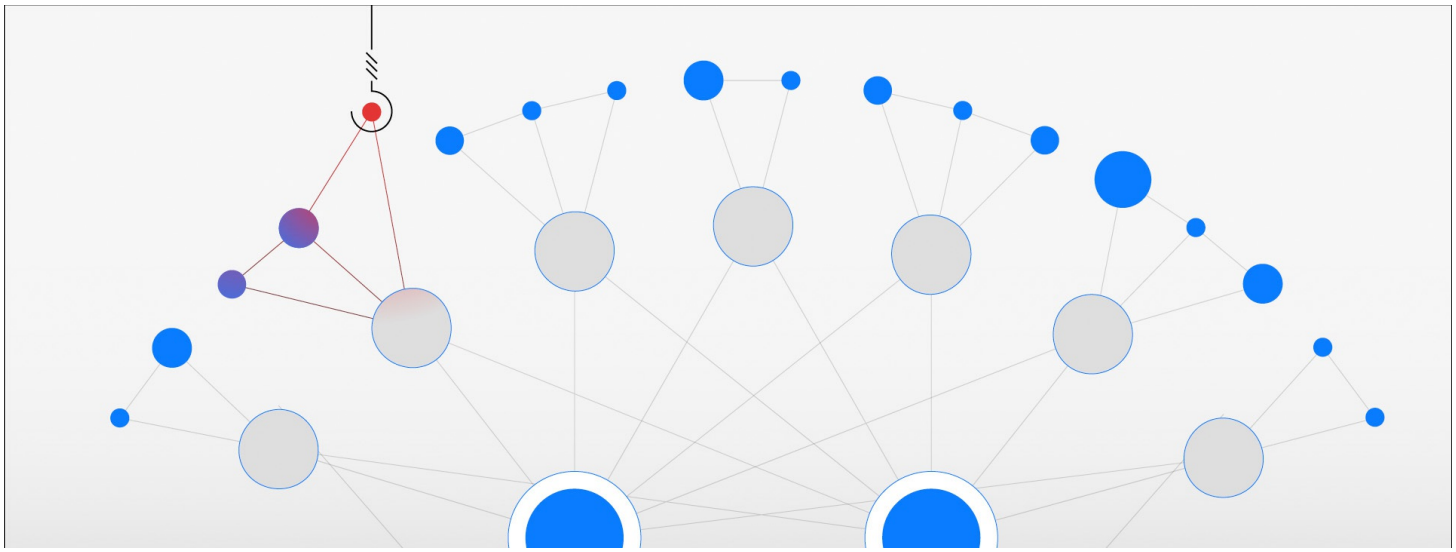
IBM Security X-Force: nel 2022 gli attacchi ransomware persistono nonostante sia migliorato il loro rilevamento

Nel 2022 in Italia, gli attacchi più comuni alle aziende hanno sfruttato backdoor, ransomware, accesso ai server e malware bot. Nei due terzi dei casi, i cybercriminali hanno usato applicazioni che si affacciano sul web.

L'Italia rappresenta l'8% degli attacchi subiti in Europa verso il 43% del Regno Unito.

Nel mondo, il settore manifatturiero si conferma quello più attaccato con circa il 25% dei casi in crescita rispetto al 2021, seguito sempre dal settore finanziario e assicurativo anche se in decrescita al 19%.

I tentativi di "thread hijacking" delle email sono in aumento; il tempo medio delle richieste di riscatto passa da mesi a giorni.



ARMONK, NY - 22 febbraio 2023 - IBM Security ha diffuso oggi il suo report annuale **X-Force Threat Intelligence Index**, da cui risulta che sebbene la quota di incidenti legati al ransomware sia diminuita solo leggermente (4 punti percentuali) nel 2022 rispetto all'anno precedente, i difensori hanno avuto comunque più successo nel rilevare e prevenire i ransomware. Nonostante questo, gli aggressori continuano a evolversi, infatti il report mostra che il tempo medio per completare un attacco ransomware è sceso da 2 mesi a meno di 4 giorni.

Secondo quanto emerso dal report, l'azione principale degli aggressori nel 2022 è stato l'utilizzo di backdoor, che consentono l'accesso remoto ai sistemi. Nel 67% dei casi d'uso di backdoor per attacchi di tipo ransomware, i tecnici IT sono stati in grado di rilevare la backdoor prima che il ransomware venisse distribuito. L'aumento contenuto nell'uso di backdoor può essere in parte attribuito al loro elevato valore di mercato. Infatti, X-Force ha osservato che i cybercriminali vendono l'accesso alle backdoor esistenti per 10.000 dollari,

rispetto ad esempio ai dati delle carte di credito rubate, che oggi possono essere venduti per meno di 10 dollari.

“L’aumento degli investimenti verso le soluzioni per il rilevamento e la risposta agli incidenti di sicurezza ha permesso ai difensori di bloccare i cybercriminali nelle prime fasi dell’attacco”, ha dichiarato Charles Henderson, Head of IBM Security X-Force. “Ma è solo una questione di tempo prima che il problema backdoor di oggi diventi la crisi ransomware di domani. Gli aggressori trovano sempre nuovi modi per non essere rilevati. Una buona difesa non è più sufficiente. Per non dover più sottostare all’infinita rincorsa degli aggressori, le aziende devono adottare una strategia di sicurezza proattiva e basata sulle minacce.”

Il report IBM Security X-Force Threat Intelligence Index tiene traccia delle tendenze e dei modelli di attacco nuovi ed esistenti, attingendo a miliardi di dati provenienti da dispositivi di rete ed *endpoint*, da attività di *incident response* e da altre fonti.

Di seguito alcuni dei principali risultati dello studio 2023:

- **Estorsione: rimane il metodo preferito dai cybercriminali**. L’estorsione si conferma anche nel 2022 il principale obiettivo dei cybercriminali, ottenuta attraverso attacchi ransomware o la compromissione delle e-mail aziendali. L’Europa è stata la più bersagliata da questo tipo di attacchi, con il 44% delle estorsioni osservate, in quanto i cybercriminali hanno cercato di sfruttare le tensioni geopolitiche.

- **I criminali informatici sfruttano le conversazioni via e-mail**. Il thread hijacking ha registrato un aumento significativo nel 2022, infatti i criminali sfruttano account e-mail compromessi, per entrare nelle conversazioni come partecipanti autorizzati. Il tasso di tentativi mensili di questa tipologia è aumentato del 100% rispetto al 2021.

- **Gli exploit esistenti continuano a funzionare.** La percentuale di “*exploit”* noti rispetto alle vulnerabilità è diminuita del 10% dal 2018 al 2022, a causa del fatto che il numero di vulnerabilità ha raggiunto un altro record nel 2022. I risultati indicano che gli *exploit legacy* hanno permesso a vecchie infezioni da malware, come WannaCry e Conficker, di continuare a esistere e a diffondersi.

Pressione estorsiva applicata (in modo non uniforme)

I criminali informatici spesso prendono di mira i settori, le aziende e le regioni più vulnerabili con schemi predefiniti di estorsione, applicando una forte pressione psicologica per costringere le vittime a pagare. L'industria manifatturiera ha subito il maggior numero di estorsioni nel 2022, ed è stata l’industria più attaccata per il secondo anno consecutivo. Le aziende manifatturiere sono un target particolarmente attraente per gli estorsori, data la tolleranza estremamente bassa per i danni causati dall’inattività.

Oltre al ransomware, i criminali sono sempre alla ricerca di nuovi modi per estorcere denaro alle vittime. Una

delle ultime tattiche in voga consiste nel rendere i dati rubati più accessibili anche alle vittime secondarie, coinvolgendo clienti e i partner commerciali, e aumentando così la pressione sull'organizzazione presa di mira dall'attacco. I cybercriminali continueranno a sperimentare con le notifiche alle vittime per aumentare i costi potenziali e l'impatto psicologico degli attacchi informatici, rendendo fondamentale che le aziende dispongano di un piano di risposta agli incidenti personalizzato, che tenga conto anche dell'impatto che gli attacchi hanno sugli stakeholder e l'intero ecosistema dell'organizzazione.

Thread Hijacking in ascesa

Nel 2022 l'attività di *thread hijacking* delle e-mail è aumentata, con il raddoppio dei tentativi di attacco mensili da parte dei cybercriminali rispetto ai dati del 2021. Nel corso dell'anno, X-Force ha scoperto che gli aggressori hanno utilizzato questa strategia per distribuire Emotet, Qakbot e IcedID, software dannosi che spesso provocano infezioni da ransomware.

Con il phishing come principale causa di attacchi informatici nello scorso anno, e il forte aumento del thread hijacking, è chiaro che gli aggressori sfruttano la fiducia che i dipendenti hanno nelle e-mail, per questo motivo è fondamentale che le aziende sensibilizzino i dipendenti sul thread hijacking per ridurre il rischio di esserne vittime.

L'importanza di perfezionare e maturare i programmi di gestione della vulnerabilità

Dal 2018 il rapporto tra *exploit* conosciuti e vulnerabilità si è ridotto di 10 punti percentuali. I criminali informatici hanno già accesso a oltre 78.000 *exploit* noti, rendendo più facile sfruttare le vulnerabilità più vecchie e non corrette. Anche dopo 5 anni, le vulnerabilità che portano alle infezioni da WannaCry rimangono una minaccia significativa — X-Force riporta un aumento dell'800% del traffico di ransomware WannaCry nei dati di telemetria dall'aprile 2022. L'uso continuato di *exploit* più vecchi evidenzia la necessità per le organizzazioni di perfezionare e maturare i programmi di gestione delle vulnerabilità, compresa una migliore comprensione della superficie di attacco e la definizione delle priorità delle *patch* in base al rischio.

Ulteriori risultati del report del 2023:

- **I phisher "rinunciano" ai dati delle carte di credito.** Il numero di criminali informatici che prendono di mira le informazioni delle carte di credito nei kit di phishing è diminuito del 52% in un anno, indicando che gli aggressori stanno dando priorità alle informazioni di identificazione personale come nomi, email e indirizzi di casa, che possono essere venduti a un prezzo più alto sul *dark web* o utilizzati per condurre ulteriori operazioni.

- **Il Nord America ha subito il peso degli attacchi in ambito energetico.** Il settore energetico si è confermato al quarto posto tra i settori più colpiti nell'ultimo anno, nel contesto di un commercio energetico mondiale già tumultuoso. Le organizzazioni del settore energetico del Nord America hanno rappresentato il 46%

di tutti gli attacchi al settore osservati nell'ultimo anno, con un aumento del 25% rispetto ai livelli del 2021.

- **Asia in cima all'elenco degli obiettivi.** Rappresentando quasi un terzo di tutti gli attacchi a cui X-Force ha risposto nel 2022, l'Asia ha visto più attacchi informatici di qualsiasi altra regione. Il settore manifatturiero ha rappresentato quasi la metà di tutti i casi osservati in Asia lo scorso anno.

Il report contiene dati raccolti da IBM a livello globale nel 2022 per fornire informazioni dettagliate sul panorama delle minacce globali e rendere noto alla comunità di sicurezza le minacce più rilevanti per le loro organizzazioni.

È possibile scaricare una copia del report completo IBM Security X-Force Threat Intelligence del 2023 qui.

Ulteriori fonti

- Ulteriori informazioni sui risultati principali del report sono contenute in questo blog IBM Security Intelligence.

- Iscriviti al webinar 2023 IBM Security X-Force Threat Intelligence Index di giovedì 2 marzo 2022, alle 11:00. ET qui

Informazioni su IBM Security

IBM Security aiuta a proteggere le aziende e le amministrazioni mondiali con un portafoglio integrato di prodotti e servizi di sicurezza, che includono funzionalità dinamiche di automazione e AI. Tali soluzioni, supportate dalla ricerca IBM Security X-Force®, consentono alle organizzazioni di prevedere le minacce, proteggere i dati e rispondere con velocità e precisione agli attacchi, senza compromettere gli ambienti digitali. Con i propri esperti di sicurezza in tutto il mondo, IBM è richiesta da migliaia di organizzazioni come partner per valutare, implementare e gestire le trasformazioni delle strategie di sicurezza informatica. IBM gestisce una delle organizzazioni di ricerca, sviluppo e delivery di servizi di cybersecurity più grandi al mondo, monitora oltre 150 miliardi di eventi di sicurezza al giorno in oltre 130 paesi ed ha ottenuto più di 10.000 brevetti relativi alla sicurezza informatica in tutto il mondo.

Per maggiori informazioni:
Paola Piacentini, *IBM external Relations Leader*

email: paola_piacentini@it.ibm.com.
tel. + 39 335 1270646

---

https://it.newsroom.ibm.com/IBMSecurityX-Force