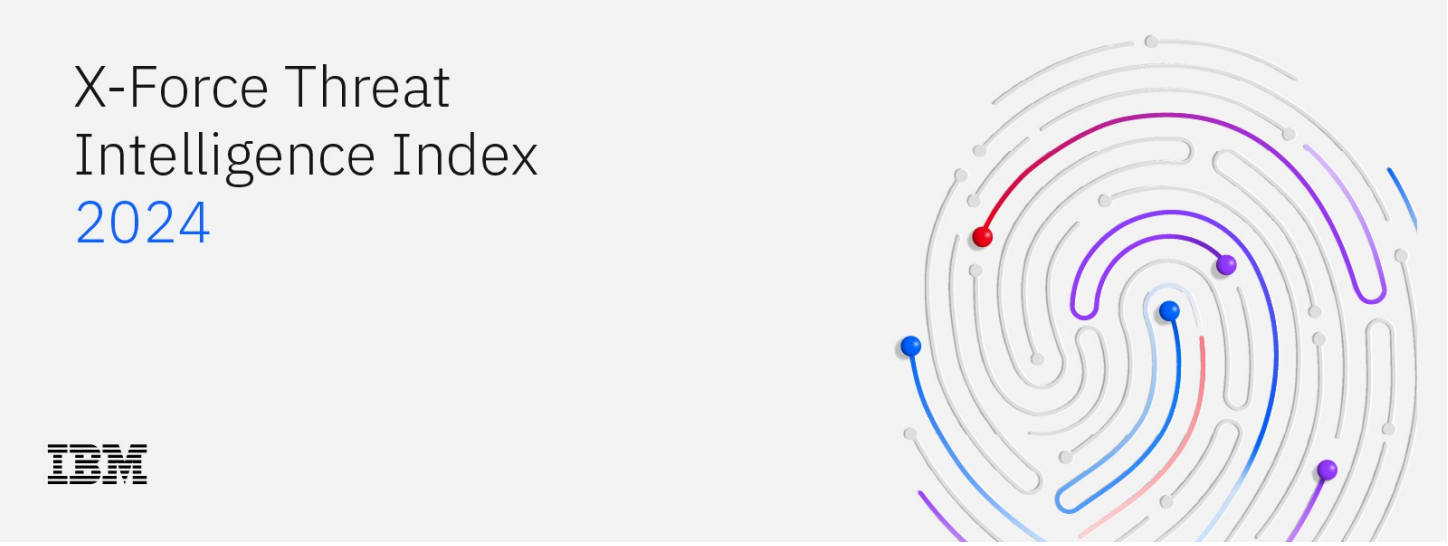
IBM Italy News Room

Report IBM: in Europa l'identità digitale è sotto attacco e per le aziende si allungano i tempi di ripristino dalle violazioni subite

L'Europa è stata la regione più bersagliata nel 2023 con il 32% degli incidenti globali, passando dal secondo posto del 2022 al primo



Italia, 21 febbraio 2024 - IBM oggi ha pubblicato il report X-Force Threat Intelligence Index 2024 che evidenzia l'emergere di una crisi globale in materia di identità digitale dovuta al fatto che è raddoppiato lo sfruttamento delle identità digitali degli utenti da parte dei criminali informatici con l'obiettivo di danneggiare le imprese di tutto il mondo. Secondo IBM X-Force, la divisione dei servizi di sicurezza di IBM Consulting, nel 2023, i criminali informatici hanno individuato l'opportunità di accedere alle reti aziendali, utilizzando account validi, anziché effettuare una compromissione.

L'X-Force Threat Intelligence Index si basa su insight e osservazioni che derivano dal monitoraggio di oltre 150 miliardi di eventi legati alla cybersecurity che si verificano ogni giorno, in più di 130 paesi. Inoltre, i dati sono stati raccolti e analizzati da più fonti all'interno di IBM, inclusi IBM X-Force Threat Intelligence, Incident Response, X-Force Red, IBM Managed Security Services e i dati forniti da Red Hat Insights e Intezer, che hanno contribuito al report per il 2024.

Alcuni aspetti rilevanti osservati nel Report 2024 che ha analizzato il 2023:

- Quasi un attacco su tre osservato a livello mondiale ha preso di mira l'Europa (32%), un numero mai raggiunto prima d'ora in una singola area analizzata.

- Sempre nel 2023, i paesi più colpiti sono stati il Regno Unito (27%), la Germania (15%), la Danimarca (14%), il Portogallo (11%), l'Italia (8%) e la Francia (8%).

- In tutta Europa, X-Force ha osservato un aumento del 66% degli attacchi causati dall'uso di account validi rispetto all'anno precedente.

- I principali punti deboli registrati sono le identità digitali e le e-mail, entrambi sfruttati nel 30% delle violazioni di account validi e phishing.

- I malware si sono rivelati l'azione malevola più diffusa, con il 44% degli incidenti, e l'Europa è l'area ad aver subito il maggior numero di attacchi ransomware a livello globale (26%).

- I tre fattori che hanno impattato maggiormente le organizzazioni europee sono stati la raccolta di credenziali (28%), l'estorsione (24%) e la fuga di dati (16%).

- Tra i settori più colpiti, vi è quello manifatturiero, che è passato dal secondo posto del 2022 al primo nel 2023, con il 28% degli incidenti.

- Al secondo posto si colloca il settore dei servizi professionali rivolti a imprese e consumatori con il 25% degli attacchi, seguito dai servizi finanziari e assicurativi e dal settore energetico che hanno registrato rispettivamente il 16% e il 14% di attacchi.

- Nel complesso, l'Europa ha subito la percentuale più elevata di incidenti nel settore dell'energia (43%) e in quello finanziario e assicurativo (37%).

Alcune importanti evidenze rilevate nell'Unione Europea:

- Quasi il 70% degli attacchi contro le organizzazioni europee a cui X-Force ha risposto si trova negli **Stati membri dell'UE**.

- Quasi il 74% degli attacchi osservati ha riguardato infrastrutture critiche.

- Il malware è stato la principale tipologia di attacchi osservata, pari al 40%. A ciò è seguito l'uso di strumenti legittimi (26%) e l'accesso ai server (15%). Il ransomware è stato il principale tipo di malware osservato in quasi il 26% degli attacchi malware.

"Sebbene l'attenzione riservata agli attacchi ingegnerizzati dall'AI sia maggiore rispetto ai problemi di sicurezza più noti e basilari, sono questi ultimi ad essere ancora oggi i più diffusi", ha affermato **Charles Henderson**,

Global Managing Partner, IBM Consulting e Head of IBM X-Force. *"Le identità compromesse vengono utilizzate ripetutamente contro le aziende, un problema che è destinato ad acuirsi poiché gli aggressori utilizzeranno l'AI per ottimizzare le loro tattiche."*

Una crisi legata alle identità a livello globale destinata a peggiorare

Lo sfruttamento di account validi è diventato la via più facile per i criminali informatici, con miliardi di credenziali compromesse accessibili sul Dark Web. Nel 2023 X-Force ha visto gli aggressori investire sempre di più in tattiche volte a ottenere le identità degli utenti, con un aumento del 266% dei furti di dati, progettati per rubare informazioni riconducibili all'identità personale, come e-mail, credenziali di social media e app di messaggistica, dati bancari o di portafogli di criptovalute e altro ancora.

Questo "ingresso facile" per gli aggressori è più complesso da rilevare e comporta una risposta costosa da parte delle aziende. Secondo X-Force, gli incidenti più gravi causati da criminali informatici che utilizzano account validi richiedono ai responsabili della sicurezza misure di risposta più complesse del 200% rispetto all'incidente medio, oltre alla necessità di distinguere tra attività di utenti legittimi e malintenzionati sulla rete. Il Cost of a Data Breach Report 2023 di IBM ha infatti rilevato che le violazioni causate da credenziali rubate o compromesse hanno richiesto circa 11 mesi per essere rilevate e recuperate: il ciclo di vita della risposta più lungo rispetto a qualsiasi altro vettore di infezione.

Questo ampio raggio d'azione nell'attività online degli utenti è stato evidente nello smantellamento, da parte dell'FBI e delle forze dell'ordine europee nell'aprile 2023, di un forum globale di criminalità informatica che ha raccolto i dati di accesso di oltre 80 milioni di account utente. Le minacce basate sull'identità continueranno a crescere man mano che i cybercriminali sfrutteranno l'intelligenza artificiale generativa per ottimizzare i loro attacchi. Già nel 2023, X-Force ha osservato oltre 800.000 post su AI e GPT nei forum del Dark Web, ribadendo che queste innovazioni hanno attirato l'attenzione e l'interesse dei criminali informatici.

Di seguito i principali dati emersi dal report a livello globale:

Gli attacchi alle infrastrutture critiche rivelano i "passi falsi" del settore. In quasi l'85% degli attacchi

ai settori critici, la compromissione si sarebbe potuta limitare grazie all'applicazione di patch, all'autenticazione a più fattori oppure al principio del privilegio minimo. Ciò significa che quella che storicamente è stata descritta come "sicurezza di base" potrebbe essere più difficile da realizzare di quanto si pensi.

- In tutto il mondo, quasi il 70% degli attacchi a cui X-Force ha risposto era rivolto ad organizzazioni di infrastrutture critiche, evidenziando che i criminali informatici stanno scommettendo sulla necessità di uptime di questi obiettivi di alto valore per portare avanti i loro progetti.

- Quasi l'85% degli attacchi a cui X-Force ha risposto in questo settore è stato causato dallo sfruttamento di applicazioni pubbliche, da e-mail di phishing e dall'utilizzo di account validi. Quest'ultimo rappresenta un rischio maggiore per il settore, con DHS CISA che afferma che la maggior parte degli attacchi riusciti contro le agenzie governative, le organizzazioni di infrastrutture critiche e gli enti governativi a livello statale nel 2022 ha implicato l'uso di account validi. Ciò evidenzia la necessità per queste organizzazioni di eseguire frequentemente stress test dei loro ambienti per rilevare potenziali esposizioni e sviluppare piani di incident response.

Gruppi di ransomware passano ad un modello di business semplificato. Gli attacchi ransomware alle aziende hanno riscontrato un calo quasi del 12% lo scorso anno, poiché le organizzazioni più grandi hanno scelto di non pagare e decriptare, a favore della ricostruzione dell'infrastruttura. Con questa crescente resistenza, che probabilmente ha un impatto sulle aspettative degli aggressori di ottenere un guadagno dall'estorsione basata sulla codifica, si è osservato che gruppi, in precedenza specializzati nel ransomware, si sono focalizzati sul furto di informazioni.

AI generativa: la prossima grande frontiera da proteggere. L'analisi di X-Force prevede che quando una singola tecnologia di AI generativa si avvicinerà al 50% della quota di mercato o quando il mercato si consoliderà a tre o meno tecnologie, potrebbe scattare il momento della maturità dell'AI come superficie di attacco, portando ulteriori investimenti in nuovi strumenti da parte dei criminali informatici.

- Perché i criminali informatici possano raggiungere un ROI derivante dai loro attacchi, le tecnologie che prendono di mira devono essere diffuse nella maggior parte delle organizzazioni di tutto il mondo. Proprio come i fattori tecnologici che in passato hanno favorito le attività dei criminali informatici, come osservato con i ransomware e la diffusione del mercato di Windows Server, le truffe BEC e la diffusione di Microsoft 365 o il cryptojacking e il consolidamento del mercato Infrastructure-as-a-Service, questo modello si estenderà molto probabilmente all'AI.

- Sebbene l'AI generativa sia attualmente in una fase antecedente al mercato di massa, è fondamentale che le aziende proteggano i loro modelli di intelligenza artificiale prima che i criminali informatici vadano a rimodulare le loro attività. Le aziende devono acquisire consapevolezza che l'infrastruttura sottostante esistente rappresenta una via di accesso ai loro modelli di AI, che non richiede tattiche innovative da parte dei cybercriminali per essere presa come bersaglio, evidenziando la necessità di un approccio olistico alla sicurezza nell'era dell'AI generativa, come sottolineato nell'IBM Framework for Securing Generative AI.

Che fine ha fatto il phishing? Pur rimanendo uno dei principali vettori di infezione, gli attacchi di phishing hanno registrato una diminuzione del 44% del volume rispetto al 2022. L'analisi di X-Force indica che l'AI può ottimizzare gli attacchi, riducendo i tempi di quasi due giorni; pertanto, il vettore di infezione rimarrà una scelta preferita dai criminali informatici.

Tutti sono vulnerabili – RedHat Insights ha rilevato che il 92% dei clienti ha almeno una CVE (Common Vulnerabilities and Exposures) con exploit noti, non affrontati, nel loro ambiente al momento della scansione, e l'80% delle prime dieci vulnerabilità rilevate tra i sistemi nel 2023 ha ricevuto un punteggio di gravità di base CVSS 'Alto' o 'Critico'.

Il "kerberoasting" ripaga – X-Force ha osservato un aumento del 100% negli attacchi di tipo "kerberoasting", in cui i criminali informatici tentano di impersonare gli utenti per aumentare i privilegi abusando dei ticket di Microsoft Active Directory.

Configurazioni errate – Le attività di *penetration testing* di X-Force Red indicano che le configurazioni errate della sicurezza rappresentano il 30% delle esposizioni totali identificate, osservando oltre 140 modi in cui gli autori di attacchi possono sfruttarle.

Sulla base di questa ricerca, IBM X-Force ha elaborato alcune raccomandazioni per le aziende:

- **Ridurre il raggio d'azione** – le organizzazioni dovrebbero prendere in considerazione l'integrazione di soluzioni per ridurre i danni che un incidente materia di sicurezza dei dati potrebbe potenzialmente causare, riducendo il raggio d'azione dello stesso, ovvero l'impatto potenziale dell'evento in seguito alla compromissione di particolari utenti, dispositivi o dati. Ciò potrebbe includere l'integrazione di un framework di privilegi minimi, la segmentazione della rete e un "identity fabric" che estenda le moderne funzionalità di sicurezza, rilevamento e risposta nel contesto in cui spesso sono presenti applicazioni e sistemi obsoleti.

- **Eseguire stress-test degli ambienti e preparare un piano** – ingaggiare dei servizi di hacking per eseguire stress test dell'ambiente e identificare le falle esistenti che i criminali informatici potrebbero sfruttare per accedere alla rete ed eseguire attacchi. Inoltre, per ridurre i tempi di risposta, rimedio e recupero da un attacco, è fondamentale disporre di piani di *incident response* personalizzati per l'ambiente

specifico. Questi piani dovrebbero essere regolarmente aggiornati e includere una risposta inter-organizzativa, incorporare gli stakeholder al di fuori dell'IT e testare le linee di comunicazione tra i team tecnici e la leadership aziendale.

- **Adottare l'AI in modo sicuro** – le organizzazioni dovrebbero concentrarsi sui seguenti principi per mettere in sicurezza l'adozione dell'AI: preservare i dati di addestramento sottostanti all'AI, proteggere i modelli, il loro utilizzo e la loro logica. È fondamentale salvaguardare anche l'infrastruttura più ampia che interagisce con i modelli di intelligenza artificiale. IBM ha recentemente introdotto un Framework for Securing Generative AI completo per aiutare le aziende a stabilire le priorità in termini di difesa in funzione dei rischi e del loro potenziale impatto.

Ulteriori risorse

- Scaricare una copia del **2024 X-Force Threat Intelligence Index**.
- Iscriversi al webinar **2024 IBM X-Force Threat Intelligence** giovedì 21 marzo alle 09:00 ET.
- Contattare il team **IBM X-Force** per approfondimenti.

IBM

IBM è un'azienda leader a livello mondiale nel settore del cloud ibrido, dell'AI e dei servizi alle imprese e opera con le imprese di oltre 175 Paesi aiutandole a capitalizzare sugli insight dei loro dati, a semplificare i processi aziendali, a ridurre i costi e a ottenere un vantaggio competitivo nei loro settori d'industria. Quasi 4.000 enti governativi e aziende in aree infrastrutturali critiche come quelle dei servizi finanziari, delle telecomunicazioni e sanità si basano sulla piattaforma cloud ibrida di IBM e su Red Hat OpenShift per realizzare la loro trasformazione digitale in modo rapido, efficiente e sicuro. Le innovazioni di IBM nell'ambito dell'AI, del quantum computing, delle soluzioni cloud specifiche per settore d'industria e nei servizi sono offerte con opzioni open e flessibili. Tutto questo è supportato dal ben noto impegno di IBM per la trasparenza, la responsabilità, l'inclusività e il servizio. Per maggiori informazioni, visitate il sito www.ibm.com.

LinkedIn: IBM

Contatti
Morgana Stell - *External Relations Leader, IBM Italia*
email:morgana.stell@it.ibm.com
mobile:335 7693528

---

https://it.newsroom.ibm.com/xforceindex2024