IBM **Security**

X-Force Threat Intelligence Index 2022: Executive Summary

IBM

Indice

Executive summary

Il mondo continua a confrontarsi con una pandemia persistente, il passaggio al lavoro da casa e quindi al successivo ritorno in ufficio, oltre ai cambiamenti geopolitici generano una costante sensazione di sfiducia. Tutto ciò genera caos, ed è nel caos che prospera la criminalità informatica. Nel 2021, IBM Security® X-Force® ha rilevato come gli autori di minacce abbiano sfruttato opportunisticamente questo panorama mutevole per adottare tattiche e tecniche di penetrazione nelle organizzazioni di tutto il mondo.

IBM Security X-Force Threat Intelligence Index mappa le nuove tendenze e i modelli di attacco che sono stati osservati e analizzati con i nostri dati, attinti da miliardi di punti, dai dispositivi di rilevamento di rete ed endpoint, dagli sforzi di risposta agli incidenti (incident response, IR), dal monitoraggio dei nomi di dominio e da altro ancora. Questo report rappresenta il culmine di questa ricerca che è stata basata sui dati raccolti da gennaio a dicembre 2021.

Forniamo quindi questi risultati come risorsa ai clienti IBM, ai ricercatori nel settore della sicurezza, ai responsabili delle policy, ai media e in generale all'ampia comunità di professionisti della sicurezza e responsabili aziendali.

Dato il panorama instabile e la continua evoluzione dei tipi di minacce e dei vettori di minacce, per stare al passo con gli aggressori e rafforzare le tue risorse critiche, avrai bisogno di informazioni dettagliate sulla threat intelligence.

Report Highlight

Principali tipi di attacco: Nel 2021 quello ransomware è risultato nuovamente il tipo di attacco principale, nonostante la percentuale di attacchi ransomware corretti da X-Force sia diminuita di quasi il 9% anno su anno. REvil: è un tipo di ransomware, che X-Force definisce anche Sodinokibi. È stato il ceppo di ransomware più comune che X-Force ha osservato per il secondo anno, costituendo il 37% tra tutti ransomware, seguito dal Ryuk al 13%. L'attività delle forze dell'ordine è stata probabilmente la forza principale per respingere gli attacchi di ransomware e botnet IoT nel 2021, ma ciò non ne preclude una potenziale ripresa nel 2022.

Vulnerabilità della supply chain: La sicurezza della supply chain è tornata al centro dell'attenzione del governo, e dei responsabili politici, grazie al il decreto legislativo dell'amministrazione Biden sulla sicurezza informatica e con le indicazioni del Dipartimento per la sicurezza interna degli Stati Uniti, di CISA e NIST che hanno raddoppiato le indicazioni sull'approccio “zero trust”. Queste linee guida mettono in risalto le vulnerabilità e le relazioni di fiducia. Lo sfruttamento delle vulnerabilità è stato il principale vettore iniziale di attacco nel settore manifatturiero, un settore alle prese con gli effetti delle pressioni e dei ritardi della supply chain.

Brand maggiormente vittime di phishing: X-Force ha monitorato da vicino nell'intero arco del 2021 il modo in cui i criminali informatici hanno utilizzato i kit per il phishing e la nostra ricerca ha rivelato che Microsoft, Apple e Google sono stati i primi tre brand che i criminali hanno tentato di imitare. Questi mega brand sono stati bersagliati ripetutamente dal phishing, poiché gli aggressori evidentemente cercavano di trarre vantaggio dalla loro popolarità e dalla fiducia che molti consumatori ripongono in essi.

Gruppi di minacce attivi: ITG17 (MuddyWater), protagonista di minacce di sospetta origine governativa iraniana, il gruppo di criminali informatici ITG23 (Trickbot) e Hive0109 (LemonDuck) sono alcuni tra i gruppi di minacce rilevati dagli analisti dell'intelligence di X-Force più attivi nel 2021. I gruppi di minacce in tutto il mondo hanno esercitato la propria maestria e si sono infiltrati in più organizzazioni. Il malware utilizzato è stato integrato con maggiori tecniche di superamento delle strutture difensive, in alcuni casi ospitato tramite piattaforme di archiviazione e messaggistica basate su cloud per superare i controlli di sicurezza. Queste piattaforme sono state violate per celare il comando e il controllo delle comunicazioni nel contesto del traffico di rete legittimo. I protagonisti delle minacce hanno inoltre continuato a sviluppare versioni di malware su Linux, per accedere più facilmente agli ambienti cloud.

Statistiche chiave

21%

Quota di attacchi ransomware

Nello scorso anno gli attacchi ransomware sono stati quelli principalmente rilevati da X-Force, scendendo al 21% degli attacchi dal 23% dell'anno precedente. I protagonisti di attacchi ransomware REvil (alias Sodinokibi) sono stati responsabili del 37% di tutti gli attacchi ransomware.

17 mesi

Tempo medio prima del rebranding o dello scioglimento di un gruppo di aggressori ransomware

I gruppi di aggressori che utilizzano ransomware, studiati da X-Force, hanno avuto una durata media di 17 mesi prima del rebranding o dello scioglimento. REvil, uno dei gruppi di aggressori di maggior successo, ha chiuso nell'ottobre 2021 dopo 31 mesi (due anni e mezzo).

41%

Percentuale di attacchi che sfruttano il phishing per l'accesso iniziale

Le operazioni di phishing si sono dimostrate la via principale di violazione nel 2021, il 41% degli incidenti risolti da X-Force ha infatti utilizzato questa tecnica per ottenere l'accesso iniziale.

33%

Aumento del numero di incidenti causati dallo sfruttamento delle vulnerabilità dal 2020 al 2021

Quattro delle prime cinque vulnerabilità sfruttate nel 2021 sono state nuove vulnerabilità, inclusa la vulnerabilità Log4j CVE-2021-44228, che è stata classificata al secondo posto, nonostante sia stata divulgata solo a dicembre.

Triplicazione

Dell'acquisizione di clic da campagne di phishing mirate che prevedono anche chiamate telefoniche

La percentuale di clic di una campagna di phishing mirata media è stata del 17,8%, ma le campagne di phishing mirate che hanno previsto una telefonata (vishing o phishing vocale) sono state tre volte più efficaci, ottenendo un clic dal 53,2% delle vittime.

146%

Aumento di ransomware Linux con nuovo codice

Secondo Intezer, la percentuale di ransomware Linux con codice (nuovo) univoco è aumentata anno su anno del 146%, indicando un aumento del livello di innovazione del ransomware Linux.

N. 1

Posizione del settore Manifatturiero nella classifica degli attacchi

Quello manifatturiero ha sostituito quello dei servizi finanziari come il settore più attaccato nel 2021, rappresentando il 23,2% degli attacchi risolti da X-Force l'anno scorso. Il ransomware è stato il tipo di attacco principale, rappresentando il 23% degli attacchi alle aziende manifatturiere.

61%

La quota di violazioni nel settore manifatturiero tra le organizzazioni connesse all'OT

Lo scorso anno, il sessantuno per percento degli incidenti nelle organizzazioni connesse all'OT si sono verificati nel settore manifatturiero. In aggiunta, il 36% degli attacchi alle organizzazioni connesse all'OT erano ransomware.

2.204%

Aumento della ricognizione nell'OT

Tra gennaio e settembre 2021, gli aggressori hanno aumentato del 2.204% la propria ricerca di dispositivi Modbus OT di controllo di supervisione e acquisizione dei dati accessibile via Internet.

74%

Quota di attacchi IoT originati da Mozi botnet

Nel 2021 il 74% degli attacchi contro i dispositivi IoT sono partiti da Mozi botnet.

26%

Quota di attacchi globali che hanno preso di mira l'Asia

Il 26 percento di tutti gli attacchi ha avuto come obiettivo l'Asia. L'Asia è stata l'area geografia più colpita del 2021.

Le minacce che abbiamo menzionato in questo report possono destare preoccupazione, poiché si evidenzia la grave e crescente minaccia dei ransomware, le rinnovate minacce di BEC e phishing e le diverse violazioni zero-day che gli hacker hanno sfruttato nell'ultimo anno. Tuttavia, la nostra intenzione è che queste informazioni aiutino le organizzazioni a comprendere meglio l'attuale panorama delle minacce e aiutino a creare fiducia nelle azioni da intraprendere per combatterle.

Alcuni principi di security che X-Force ha trovato utili nella lotta alle odierne minacce informatiche includono un approccio zero trust, l'automazione della risposta agli incidenti e l'estensione della capacità di rilevamento e risposta.

Zero trust aiuta a diminuire il rischio derivante dagli attacchi

Zero trust è un cambio di paradigma, un nuovo modo di affrontare i problemi di sicurezza, che presuppone che si sia già verificata una violazione e che mira a rendere più difficile per un utente malintenzionato lo spostamento all'interno di una rete. Il fulcro della sua azione è l'individuazione dell'ubicazione dei dati critici e di chi vi ha accesso, oltre alla creazione di una rete di solide misure di verifica tali da garantire che solo le persone autorizzate accedano a tali dati nel modo giusto.

I ricercatori di X-Force confermano che i principi di un approccio zero trust, inclusi l'implementazione della MFA (Multi-Factor Authentication) e del principio del privilegio minimo, possono ridurre la vulnerabilità delle organizzazioni ai principali tipi di attacco identificati in questo report, in particolare ransomware e BEC.

L'applicazione del principio del privilegio minimo ai controller di dominio e agli account degli amministratori di dominio in particolare aumenta le barriere per i creatori di attacchi ransomware, poiché molti di questi cercano di distribuire ransomware su una rete da un controller di dominio compromesso. Inoltre, l'implementazione della MFA aumenta la difficoltà per i criminali informatici che cercano di impossessarsi degli account di posta elettronica, richiedendogli un'ulteriore autenticazione oltre alle credenziali rubate.

Scopri come creare un approccio zero trust →

L'automazione della sicurezza migliora le risposte agli incidenti

Il team di X-Force affronta centinaia di incidenti ogni anno, in molteplici aree geografiche, assistendo gli analisti interni della risposta agli incidenti e affrontando una vasta gamma di tipologie di attacco. La velocità è essenziale, sia nell'identificare ed eliminare i protagonisti delle minacce prima che possano distribuire ransomware su una rete, sia per risolvere i problemi in modo rapido ed efficiente per dedicare larghezza di banda al successivo incidente. In questo ambiente frenetico, l'automazione della sicurezza è fondamentale: delegare alle macchine le attività che potrebbero richiedere ore di lavoro di un un analista o un team e identificare i meccanismi per migliorare i flussi di lavoro.

A metà del 2021, IBM ha donato alla Open Cybersecurity Alliance uno strumento di automazione per il rilevamento delle minacce volto ad assistere gli analisti dei centri operativi di sicurezza (SOC) per gestire velocemente le indagini forensi e gli incidenti informatici. Inoltre, il team X-Force IR utilizza IBM Security QRadar SOAR per migliorare le proprie capacità di risposta agli incidenti.

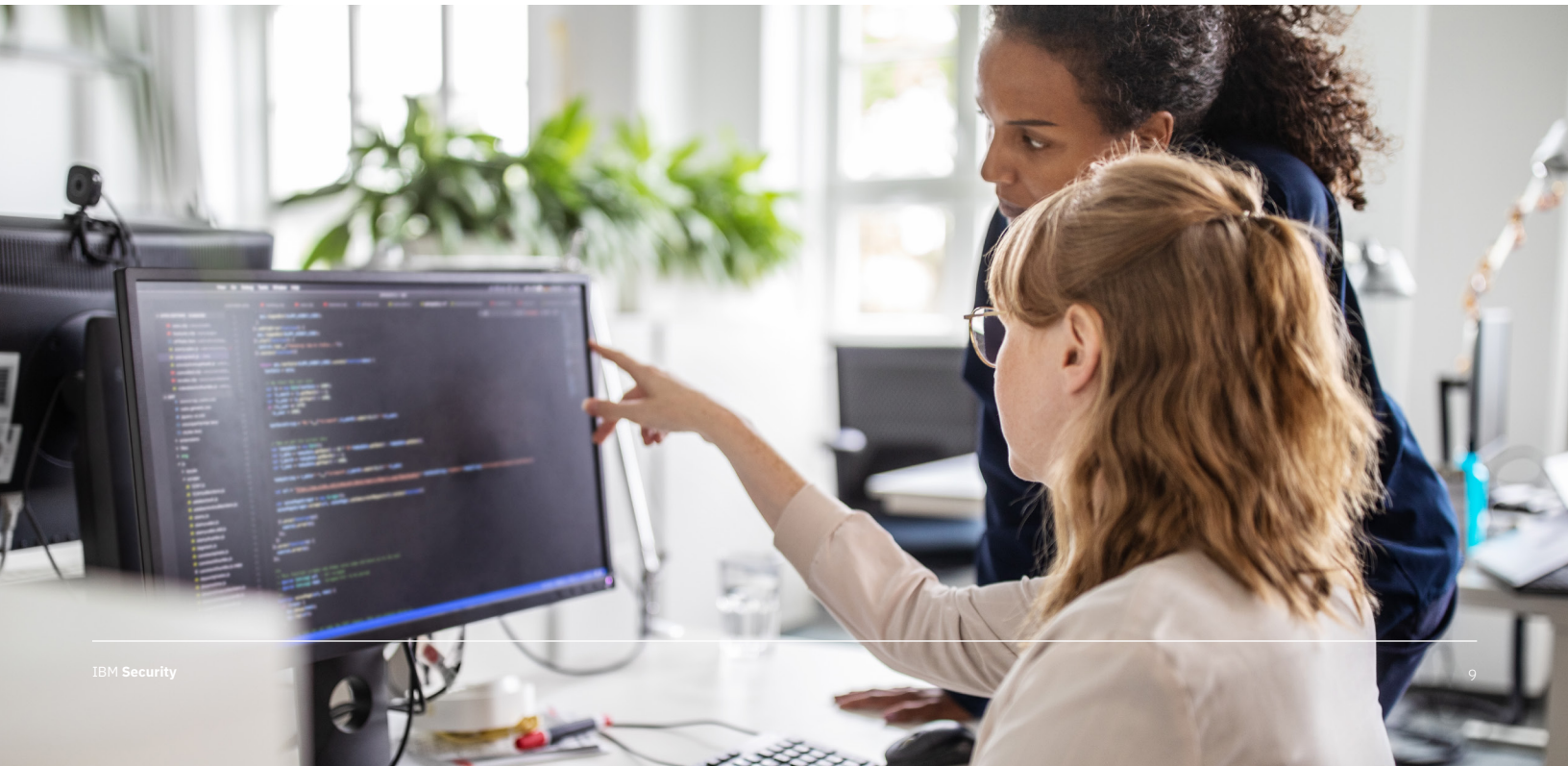
Scopri di più sui servizi di risposta agli incidenti di IBM →

L'estensione del rilevamento e della risposta fornisce un vantaggio significativo

Le tecnologie di rilevamento e risposta, in particolare quando diverse soluzioni vengono combinate in un'unica soluzione estesa (XDR), offrono alle organizzazioni un vantaggio significativo nell'identificazione e nell'eliminazione degli aggressori da una rete prima che siano in grado di raggiungere la fase finale del loro attacco, come la distribuzione di ransomware o il furto di dati.

In diversi casi, quando il team X-Force IR ha implementato una soluzione di rilevamento e risposta degli endpoint (EDR) o XDR sulla rete di un cliente, l'IR ha immediatamente acquisito ulteriori informazioni che hanno aiutato a identificare le attività degli aggressori e ad affrontarle rapidamente. Le tecnologie XDR aiutano a promuovere l'incremento degli accessi ai server e altri tipi di attacco rilevati da X-Force, il che indica che un aggressore viene identificato e fermato prima che l'operazione possa raggiungere la conclusione desiderata.

Scopri di più su IBM Security QRadar XDR →



Suggerimenti

I seguenti suggerimenti includono azioni specifiche che le organizzazioni possono intraprendere per proteggere meglio le proprie reti dalle minacce presentate in questo report.

Sviluppa un piano di risposta per i ransomware. Ogni settore e ogni area geografica è a rischio di un attacco ransomware e il modo in cui il tuo team risponde nel momento critico può fare la differenza nella quantità di tempo e denaro persi per una risposta.

— Prevedi, nel tuo piano di risposta, azioni di contenimento immediate, ciò di cui le parti interessate e le forze dell'ordine dovrebbero essere informate, come la tua organizzazione memorizzerà e ripristinerà in modo sicuro i backup e un luogo alternativo da cui sia possibile eseguire le funzioni aziendali critiche durante la fase di ripristino.

— Includi nel tuo piano uno scenario di furto e perdita di dati in conseguenza di un attacco ransomware: questa è una strategia oggi molto utilizzata e rilevata in una percentuale molto elevata di attacchi ransomware risolti da X-Force.

— Usa le esercitazioni sui ransomware per valutare anche la possibilità che la tua organizzazione paghi un riscatto e quali fattori potrebbero alterare le tue conclusioni.

— Assicurati che il tuo piano di risposta ai ransomware includa un'emergenza specifica per un incidente sul cloud, poiché potrebbe richiedere strumenti e competenze diversi.

— Evita il danneggiamento dei dati in conseguenza di attacchi di malware o ransomware con soluzioni di storage flash che aiutino a prevenire la perdita di dati, promuovere la continuità operativa e ridurre i costi dell'infrastruttura.

— LA Definitive Guide to Ransomware di X-Force fornisce ulteriori suggerimenti dettagliati su come rispondere a un attacco ransomware. Il team di risposta agli incidenti di X-Force può anche condurre una valutazione del livello di adeguatezza della protezione da ransomware della tua organizzazione per aiutare a definire e testare un piano di risposta agli incidenti ransomware. Allo stesso modo, l'X-Force Command Center prepara le organizzazioni a un attacco ransomware, tenendo conto sia della risposta commerciare che tecnica richiesta.

Implementa l'autenticazione a più fattori (MFA) su ciascun punto di accesso remoto di una rete. X-Force ha rilevato rispetto al passato che un maggior numero di organizzazioni hanno implementano la MAF con maggiore successo. Ciò sta letteralmente alterando il panorama delle minacce, costringendo i protagonisti delle minacce a trovare nuovi modi per compromettere le reti, piuttosto che sfruttare il furto delle credenziali, e diminuendo l'efficacia delle campagne di acquisizione via e-mail.

— La MFA può ridurre il rischio di diversi tipi di attacco, inclusi ransomware, furto di dati, BEC e accesso al server.

— Inoltre, le tecnologie di gestione dell'identità e dell'accesso semplificano ogni anno l'implementazione della MAF, sia per i team di implementazione che per gli utenti finali.

Adotta una strategia stratificata per combattere il phishing. Sfortunatamente, oggi non esiste uno strumento o una soluzione in grado di prevenire tutti gli attacchi di phishing e i protagonisti delle minacce continuano a perfezionare il social engineering e le tecniche di rilevamento anti-malware per aggirare i controlli definiti. Pertanto, consigliamo di implementare diversi livelli di soluzioni che hanno maggiori possibilità di rilevare e-mail di phishing.

— In primo luogo, un'effettiva consapevolezza e formazione degli utenti è fondamentale e deve includere esempi del mondo reale.

— In secondo luogo, utilizzare una soluzione di sicurezza del software di email per affidare a una macchina il compito di identificare e filtrare i messaggi potenzialmente dannosi.

— In terzo luogo, implementare diverse difese che possano aiutare a rilevare rapidamente malware o movimenti laterali nel caso in cui un'e-mail di phishing dovesse passare, tra cui il rilevamento di malware basato sul comportamento, il rilevamento e la risposta degli endpoint (EDR- endpoint detection and response), le soluzioni di rilevamento e prevenzione delle intrusioni (IDPS -intrusion detection and prevention solutions) e un sistema di sicurezza delle informazioni e della gestione degli eventi (SIEM - security information and event management).

Perfeziona e sviluppa il tuo sistema di gestione delle vulnerabilità. La gestione delle vulnerabilità è un'arte: dall'identificazione delle vulnerabilità più probabili per l'architettura di rete della tua organizzazione, alla definizione della loro gestione senza interrompere nulla nel processo.

— Avere un team dedicato alla gestione delle vulnerabilità e assicurarsi che questo team disponga di risorse adeguate e del supporto necessario può fare la differenza nel garantire che la tua rete sia protetta dal potenziale sfruttamento delle vulnerabilità.

— Ti consigliamo di dare la priorità a tutte le vulnerabilità menzionate in questa valutazione e che sono applicabili alla tua organizzazione.

— X-Force Exchange di IBM include anche un repository delle vulnerabilità, con associati i livelli di criticità, per aiutarti a identificare le vulnerabilità più problematiche e X-Force Red può fornire servizi di scansione e gestione specifici delle vulnerabilità.

Scopri di più nel report completo →

Cos'è IBM Security X-Force

IBM Security X-Force è un gruppo di responder, hacker, ricercatori e analisti dedicati alle minacce. Il nostro portfolio comprende prodotti e servizi di attacco e difesa, basati su una vista a 360 gradi sulle minacce. Con X-Force come partner per la sicurezza, la probabilità e l'impatto di una violazione dei dati sono ridotti al minimo.

IBM Security X-Force Threat Intelligence mette insieme la telemetria delle operazioni di sicurezza, la ricerca, le indagini sulla risposta agli incidenti, i dati commerciali e gli open source di IBM per aiutare i clienti a comprendere le minacce emergenti e prendere rapidamente decisioni consapevoli sulla sicurezza.

Inoltre, il team X-Force Incident Response fornisce servizi di rilevamento, risposta, riparazione e addestramento per aiutarti a ridurre al minimo l'impatto di una violazione dei dati.

X-Force in combinazione con l'esperienza IBM Security Command Center addestra il tuo team, dagli analisti fino ai dirigenti, ad essere pronto per la realtà delle minacce odierne. X-Force Red, il team di hacker di IBM Security, fornisce servizi di sicurezza e simula attacchi, inclusi test di penetrazione, gestione delle vulnerabilità e simulazione di eventi avversi.

Durante tutto l'anno i ricercatori di IBM X-Force forniscono anche ricerche e analisi continue sotto forma di blog, white paper, webinar e podcast, presentando nuove conoscenze relative ad attori delle minacce avanzate, nuovi malware e nuovi metodi di attacco. Inoltre, tramite le nostre soluzioni X-Force Threat Intelligence, forniamo agli utenti abbonati una vasta gamma di analisi aggiornate e all'avanguardia.

Prenota una consulenza con uno dei nostri esperti di X-Force →

Cos'è IBM Security

IBM Security collabora con i propri clienti per proteggere le aziende con un portfolio avanzato e integrato di prodotti e servizi per la sicurezza enterprise, integrati con AI e un moderno approccio alla strategia di security che si avvale di approccio zero trust, contribuendo al successo di fronte all'incertezza. Allineiamo la strategia di security al business; integriamo soluzioni disegnate per proteggere utenti, risorse e dati digitali; implementiamo la tecnologia per gestire le difese contro le minacce crescenti. Aiutiamo a gestire e governare il rischio a supporto degli ambienti cloud ibridi di oggi.

Il nostro nuovo approccio aperto, la piattaforma IBM Cloud Pak for Security , è basato su RedHat Open Shift e supporta gli odierni ambienti ibridi multicloud con un ampio ecosistema di partner. Con Cloud Pak for Security, soluzione software containerizzata enterprise-ready, l'utente può gestire la sicurezza dei dati e delle applicazioni integrando rapidamente gli strumenti specifici già presenti, per generare insights più approfonditi sulle minacce negli ambienti cloud ibridi e lasciando i dati dove si trovano, per una facile orchestrazione e automazione della risposta.

Per ulteriori informazioni, visita la pagina www.ibm.com/security o il blog IBM Security Intelligence.

Collaboratori

Camille Singleton
Charles DeBeck
Joshua Chung
Dave McMillen
Scott Craig
Scott Moore
Charlotte Hammond
John Dwyer
Melissa Frydrych
Ole Villadsen
Richard Emerson
Guy-Vincent Jourdan
Vio Onut
Stephanie Carruthers
Adam Laurie
Michelle Alvarez
Salina Wuttke
Georgia Prassinos
John Zorabedian
Mitch Mayne
Limor Kessem
Ian Gallagher
Ari Eitan

IBM Italia S.p.A.
Circonvallazione Idroscalo
20090 Segrate (Milano) Italia

Prodotto negli Stati Uniti d'America nel febbraio 2022