IBM Italy News Room

Studio IBM: cresce il peso dei cyber attacchi nel settore manifatturiero, anche per i maggiori rischi sulle supply chain

• In Italia, il 27% degli attacchi è costituito da ransomware, con il vettore di attacco più frequente rappresentato dallo sfruttamento delle vulnerabilità (56% dei casi analizzati). .

• Il 47% degli incidenti in Italia è stato rilevato nell'industria manifatturiera, che scalza il settore dei servizi finanziari e assicurativi dal primo posto

CAMBRIDGE, Massachusetts, 23 febbraio 2022 - IBM (NYSE: IBM) Security annuncia oggi il suo studio annuale X-Force Threat Intelligence Index da cui emerge come ransomware e sfruttamento delle vulnerabilità insieme abbiano "imprigionato" le imprese gravando ulteriormente sulle catene di approvvigionamento globali e con il manufatturiero come l'industria più colpita. Mentre il phishing è stata la causa più comune dei cyberattacchi nell'ultimo anno, IBM Security X-Force ha osservato un aumento del 33% negli attacchi causati dallo sfruttamento di vulnerabilità dei software non aggiornati: è questo il punto di ingresso preferito dai cybercriminali, causa del 44% degli attacchi ransomware nel 2021.

Lo studio descrive come nel 2021 gli autori di ransomware abbiano tentato di inserirsi nelle le supply chain globali puntando al settore manifatturiero, che è diventato il più attaccato del 2021 (23%), superando i settori dei servizi finanziari e assicurativi che sono stati al vertice per diversi anni. Portando avanti attacchi ransomware più che in qualunque altro settore d'industria, gli aggressori hanno scommesso sull'effetto a catena che l'interruzione delle attività di imprese manifatturiere avrebbe causato alle loro catene di approvvigionamento a valle, spingendole a pagare il riscatto. Un allarmante 47% degli attacchi al settore manifatturiero è stato causato da vulnerabilità che le organizzazioni vittime non avevano ancora corretto, o non potevano correggere, con *patch* di aggiornamento, evidenziando la necessità di gestire prontamente le vulnerabilità del software.

Il 2022 IBM Security X-Force Threat Intelligence Index traccia le nuove tendenze e i modelli di attacco che IBM Security ha osservato e analizzato dai propri dati - attingendo da miliardi di datapoint che spaziano dalla rete ai dispositivi di endpoint detection, dai casi di risposta agli incidenti, al tracciamento dei kit di phishing e altro - compresi i dati forniti da Intezer.

Alcuni dei punti salienti emersi nel report di quest'anno includono:

- **Le bande di ransomware sopravvivono agli sforzi di smantellamento da parte delle autorità.** Il ransomware rimane il principale metodo di attacco osservato nel 2021, con i gruppi ransomware che non mostrano alcun segno di arresto, nonostante il maggiore blocco del ransomware. Secondo il rapporto del 2022, la durata media della vita di un gruppo ransomware prima della chiusura o della creazione di una nuova famiglia di ransomware è di 17 mesi.

- **Le vulnerabilità mettono in luce il più grande "vizio" delle aziende.** X-Force rivela che per le aziende in Europa, Asia e Medio Oriente/Africa, le vulnerabilità non corrette da *patch* hanno causato circa il 50% degli attacchi nel 2021, evidenziando che le imprese sono ancora molto esposte alle vulnerabilità dovute alla rincorsa al *patching*.

- **Primi segnali di allarme della crisi cyber nel cloud.** I criminali informatici stanno gettando le basi per prendere di mira gli ambienti cloud: lo studio rivela un aumento del 146% di nuovo codice ransomware Linux e uno spostamento del target di attacco verso Docker, rendendo potenzialmente più facile per più attori di minacce fare leva sugli ambienti cloud per scopi malevoli.

"I criminali informatici di solito inseguono il denaro. Ora con i ransomware stanno puntando a ciò che amplifica i risultati," ha detto Charles Henderson, Head of IBM X-Force. "Le imprese dovrebbero capire che le vulnerabilità le mettono in una situazione di stallo - mentre gli attori di ransomware le usano a loro vantaggio. Questa non è una sfida binaria. La superficie di attacco sta diventando sempre più vasta e non è più sufficiente operare con il presupposto che ogni vulnerabilità nel proprio ambiente è stata corretta da patch: le imprese dovrebbero operare presupponendo di essere, prima o poi, vittime di attacco e migliorare di conseguenza la gestione delle vulnerabilità adottando una strategia Zero Trust."

I gruppi ransomware hanno “nove vite”

In risposta alla recente accelerazione delle azioni di contrasto al ransomware da parte delle forze dell'ordine, i gruppi ransomware potrebbero attivare dei piani di disaster recovery. L'analisi di X-Force rivela che la durata media della vita di un gruppo ransomware, prima di chiudere o cambiare brand, è di 17 mesi. Per esempio, REvil, responsabile del 37% di tutti gli attacchi ransomware nel 2021, ha resistito per quattro anni attraverso i rebrand, suggerendo la probabilità che riemerga di nuovo nonostante l’interruzione delle attività a seguito di un'operazione guidata da più governi avvenuta a metà del 2021.

Mentre i blocchi attuati dalle forze dell'ordine possono rallentare le attività degli attaccanti, questi sono attualmente anche appesantiti dalle spese necessarie per finanziare i loro rebranding o per ricostruire la loro infrastruttura. Poiché il loro campo d’azione è in cambiamento, è importante che le organizzazioni approfittino di questo momento per modernizzare le loro infrastrutture e mettere i propri dati in un ambiente che possa aiutare a salvaguardarli - sia che si tratti di on-premises o in cloud. Questo può aiutare le imprese a meglio gestire, controllare e proteggere i propri carichi di lavoro e, inoltre, a rendere più difficile l'accesso ai dati critici negli ambienti cloud ibridi, impedendo che gli attaccanti rendano la minaccia scalabile in caso di compromissione.

Le vulnerabilità determinano una crisi esistenziale (per alcuni)

Il rapporto X-Force evidenzia il numero record di vulnerabilità divulgate nel 2021, con le vulnerabilità nei Sistemi di Controllo Industriale che aumentano del 50% rispetto all'anno precedente. Sebbene negli ultimi dieci anni siano state divulgate oltre 146.000 vulnerabilità, la crescita maggiore è avvenuta solo in tempi recenti, caratterizzati dalla trasformazione digitale delle imprese, avvenuta in gran parte a seguito della pandemia. Questo ci suggerisce che la sfida nella gestione delle vulnerabilità deve ancora raggiungere il suo picco.

Allo stesso tempo, lo sfruttamento delle vulnerabilità come metodo di attacco sta diventando sempre più popolare. X-Force ha osservato un aumento del 33% rispetto all'anno precedente, con le due vulnerabilità più sfruttate nel 2021 che sono state trovate in applicazioni aziendali ampiamente utilizzate (Microsoft Exchange, Apache Log4J Library). La sfida delle imprese nel gestire le vulnerabilità potrebbe continuare ad aggravarsi con l'espansione delle infrastrutture digitali e l’aumento delle richieste di compliance rispetto a requisiti di audit e manutenzione, evidenziando l'importanza di operare partendo sempre dal presupposto di una possibile compromissione e applicare una strategia Zero Trust per proteggere le proprie architetture informatiche.

Gli attaccanti mirano agli spazi comuni nei cloud

Nel 2021, X-Force ha osservato che più aggressori stanno spostando i loro obiettivi verso le architetture containerizzate come Docker - di gran lunga il motore runtime di container dominante secondo RedHat. Gli aggressori riconoscono che i container rappresentano uno spazio comune alle organizzazioni e, quindi, stanno cercando i modi per massimizzare il loro ROI con malware che possano essere trasversali sulle piattaforme e utilizzati come punto di partenza per attaccare altri componenti delle infrastrutture delle loro vittime.

Il report 2022 invita a prestare attenzione anche ai continui investimenti nello sviluppo di malware Linux, precedentemente non osservati. Secondo i dati forniti da Intezer, si riscontra un aumento del 146% dei ransomware Linux basati su un nuovo codice. Dal momento che gli aggressori continuano a ricercare modi per scalare le operazioni attraverso gli ambienti cloud, le aziende devono cercare di avere una visibilità estesa sulla loro infrastruttura ibrida. Gli ambienti cloud ibridi che sono costruiti su interoperabilità e standard aperti

possono aiutare le organizzazioni a rilevare i punti ciechi e ad accelerare e automatizzare le risposte di sicurezza.

Il report di IBM X-Force si basa sui dati raccolti a livello mondiale nel 2021 per fornire informazioni specifiche sul panorama globale delle minacce informatiche e supportare i professionisti in cyber security sulle minacce più rilevanti per le loro organizzazioni. Il 2022 IBM Security X-Force Threat Intelligence Index è disponibile a questo link.

Ulteriori informazioni

- Webinar sui risultati del 2022 IBM Security X-Force Threat Intelligence Index, giovedì 3 marzo 2022 alle ore 17:00 CET. È possibile iscriversi da questo link.

- Blog post scritto dagli autori del report su IBM Security Intelligence blog.

IBM Security
IBM Security offre uno dei portafogli più evoluti e integrati di prodotti e servizi per la sicurezza aziendale. Il portafoglio, supportato dal team di ricerca di fama mondiale IBM Security X-Force, consente alle organizzazioni di gestire efficacemente il rischio e di difendersi dalle minacce emergenti. IBM gestisce una delle organizzazioni di ricerca, sviluppo e fornitura di soluzioni di sicurezza più vasta al mondo, monitora 150 miliardi di eventi di sicurezza al giorno in più di 130 paesi e ha ottenuto più di 10.000 brevetti di cyber security in tutto il mondo. Per ulteriori informazioni, www.ibm.com/security oppure @IBMSecurity su Twitter o visitare i blog di IBM Security Intelligence .

Claudia Ruffini - *IBM Communications Leader, Italia*
cla@it.ibm.com
Mobile: +39 335/6325093

Additional assets available online: Photos (

https://it.newsroom.ibm.com/XFTII2022