IBM Security Report: nel 2020 raddoppiati gli attacchi ai settori strategici nella lotta al COVID-19

Durante la pandemia, i ransomware hanno portato milioni di dollari alle organizzazioni cybercriminali, i malware opensource sono aumentati del 40% e le piattaforme di collaborazione online sono state tra gli obiettivi più colpiti

CAMBRIDGE, Mass., 24 febbraio 2021 - IBM (NYSE: IBM) Security ha pubblicato l'X-Force Threat Intelligence Index 2021 che quest'anno mette in evidenza come gli attacchi informatici siano stati in grado di evolversi e adattarsi sfruttando le difficoltà socioeconomiche, aziendali e politiche causate dalla pandemia. IBM Security X-Force ha infatti rilevato come i cybercriminali abbiano indirizzato i propri attacchi alle organizzazioni strategiche nella lotta contro il COVID-19, quali ospedali, aziende farmaceutiche, produttori di apparecchiature medicali e operatori energetici.

Secondo il nuovo report, gli attacchi informatici al settore sanitario, manifatturiero ed energetico sono raddoppiati rispetto all'anno precedente. I cybercriminali hanno preso di mira le organizzazioni che non potevano permettersi di interrompere le proprie attività critiche, come i soccorsi e le catene di approvvigionamento e dell'energia legate al COVID-19.

L'industria manifatturiera e quella energetica sono state le principali vittime dei cyberattacchi nel 2020, seconde solo al settore finanziario e assicurativo, un primato dovuto anche all'aumento di quasi il 50% delle vulnerabilità nei sistemi di controllo industriale (ICS) da cui entrambe dipendono fortemente.

"La pandemia ha ridefinito le infrastrutture critiche e i cybercriminali hanno saputo sfruttare da subito questa consapevolezza. Molte organizzazioni si sono trovate inaspettatamente in prima linea nella risposta al COVID-19, per supportare la ricerca, sostenere le catene di approvvigionamento di vaccini e alimenti o produrre dispositivi di protezione personale", ha affermato Nick Rossmann, Global Threat Intelligence Lead, IBM Security X-Force. *"Il profilo della vittima ideale per gli aggressori è mutato con l'evolversi degli eventi: un aspetto che evidenzia, ancora una volta, la grande adattabilità, intraprendenza e perseveranza degli avversari informatici".*

L'X-Force Threat Intelligence Index si basa su approfondimenti e analisi derivanti dal monitoraggio di oltre 150 miliardi di eventi di security al giorno in più di 130 Paesi. I dati vengono raccolti e analizzati da più fonti all'interno di IBM, tra cui IBM Security X-Force Threat Intelligence and Incident Response, X-Force Red, IBM Managed Security Services. Al Report 2021 hanno contribuito anche Quad9 e Intezer.

X-Force Threat Intelligence Index 2021 – Highlights

- **In aumento i malware su Linux** - L’aumento del 40% delle famiglie di malware legate a Linux nell'ultimo anno, secondo Intezer, e del 500% dei malware scritti in Go nei primi sei mesi del 2020, dimostrano come i cybercriminali stiano accelerando la migrazione dei malware verso Linux, per essere in grado di attaccare più facilmente piattaforme diverse, inclusi gli ambienti cloud.
- **La pandemia delinea i brand più soggetti a spoofing -** In un anno caratterizzato da distanziamento sociale e lavoro a distanza, i brand che offrono strumenti collaborativi come Google, Dropbox e Microsoft o aziende come Amazon e PayPal sono stati tra i primi 10 marchi più soggetti ad attacchi di spoofing nel 2020, un tipo di attacco che consiste nel falsificare l’”identità” applicativa. Rientrano in questa classifica anche YouTube e Facebook, le piattaforme più utilizzate nel 2020 come fonte di informazione. Ha fatto il suo ingresso nella lista, posizionandosi al settimo posto, il brand Adidas particolarmente ricercato per le nuove linee di sneaker Yeezy e Superstar.
- **I gruppi ransomware hanno sviluppato un modello di business redditizio** : il ransomware è stato la causa di quasi un attacco su quattro a cui X-Force ha risposto nel 2020. Alcuni di questi si sono evoluti in modo aggressivo per attuare tattiche di doppia estorsione. Secondo le stime di X-Force, utilizzando questo modello, Sodinokibi, il gruppo di ransomware più monitorato nel 2020, avrebbe guadagnato oltre 123 milioni di dollari nell'ultimo anno, riuscendo ad estorcere il pagamento a circa due terzi delle vittime dei propri attacchi.

La crescita dei malware open-source minaccia gli ambienti cloud

Durante la pandemia, molte aziende hanno accelerato l'adozione del cloud. Un recente sondaggio di Gartner ha rilevato che quasi il 70% delle organizzazioni che oggi utilizzano servizi cloud prevedono di incrementare gli investimenti su questo paradigma, come conseguenza della trasformazione digitale causata dal COVID-19[1]. Gli ambienti cloud possono quindi diventare un bersaglio per i cybercriminali.

Inoltre, con la maggior diffusione del malware open source, secondo IBM i cybercriminali stanno cercando nuovi modi per incrementare i margini di profitto - possibilmente riducendo i costi - con attacchi più efficaci e redditizi. Il rapporto evidenzia che gruppi cyber criminali come APT28, APT29 e Carbanak si stanno spostando verso l’open-source, indicando un’accelerazione verso un maggior numero di attacchi al cloud nell’anno che sta arrivando.

Il rapporto rivela anche che i cybercriminali sfruttano la scalabilità della potenza di calcolo dagli ambienti cloud, con conseguenti pesanti addebiti alle organizzazioni vittime: Intezer ha osservato come oltre il 13% di codice nel malware di cryptomining di Linux sia totalmente nuovo.

Con il cloud nel mirino degli attaccanti, X-Force raccomanda un approccio zero-trust alla strategia di sicurezza. Le organizzazioni devono inoltre proteggere i dati più sensibili adottando il confidential computing come componente centrale dell’infrastruttura di sicurezza. Criptando i dati in uso, è possibile ridurre il rischio di attacco da parte di cybercriminali, anche nel caso in cui questi ultimi siano già in grado di accedere agli ambienti più sensibili.

Criminali informatici che si fingono brand noti

Il rapporto di IBM X-Force evidenzia che nel 2020 i cybercriminali si sono spesso camuffati dietro i nomi di brand fidati. Adidas, uno dei marchi più noti al mondo, è stato il brand maggiormente preso di mira, data l'alta richiesta da parte dei consumatori. Gli attacchi organizzati consistevano nell'indirizzare l'utente alla ricerca dell'ultima sneaker verso siti Web dannosi, progettati per assomigliare quanto più possibile agli originali. In questo modo, i criminali informatici hanno potuto mettere in atto frodi sui pagamenti online, rubare i dati finanziari / bancari degli utenti, raccogliere le credenziali o infettare i dispositivi delle vittime con malware.

Il rapporto indica che la maggior parte dello spoofing Adidas è associato alla domanda per le linee di sneaker Yeezy e Superstar. La linea Yeezy da sola ha generato entrate pari a 1,3 miliardi di dollari nel 2019 ed è stata una delle sneaker più vendute di Adidas. È dunque probabile che l'attenzione intorno alla nuova linea di Adidas abbia spinto i cybercriminali a sfruttare la domanda per trarre grossi profitti.

Il ransomware è l'attacco più diffuso del 2020

Secondo il report, nel 2020 il numero di attacchi ransomware è cresciuto rispetto al 2019: quasi il 60% di quelli analizzati da X-Force è caratterizzato da una strategia di doppia estorsione in base alla quale i dati sono crittografati e rubati e le vittime minacciate della loro diffusione qualora non avvenga il pagamento del riscatto. Il 36% dei data breach tracciati da X-Force nel 2020 era stato originato da attacchi ransomware, suggerendo che data breach e attacchi ransomware comincino a coincidere.

Il gruppo di ransomware più attivo segnalato nel 2020 è stato Sodinokibi (noto anche come REvil), che rappresenta il 22% di tutti i ransomware osservati da X-Force. IBM stima che Sodinokibi abbia esfiltrato circa 21,6 terabyte di dati, e che quasi due terzi delle vittime abbiano pagato il riscatto richiesto, mentre circa il 43% ha perso i propri dati. Il risultato è che i responsabili di Sodinokibi hanno guadagnato oltre 123 milioni di dollari nell'ultimo anno.

Come Sodinokibi, anche le altre tipologie di ransomware che più hanno avuto successo nel 2020 hanno fatto leva sul furto e sul leak di dati, sulla creazione di cartelli ransomware-as-a-service e sull'outsourcing di elementi chiave delle proprie operazioni a criminali informatici specializzati. In risposta a questi attacchi ransomware più aggressivi, X-Force consiglia di limitare l'accesso ai dati sensibili e proteggere gli account attraverso un sistema di gestione degli accessi privilegiati (PAM) e la verifica dell'identità degli accessi (IAM).

Il report pone l'accento anche su altre evidenze:

- **Le vulnerabilità superano il phishing come vettore di infezione più comune** : l'individuazione e lo sfruttamento di vulnerabilità ha rappresentato il metodo più efficace per effettuare delle violazioni (35%), superando, per la prima volta da anni, il phishing (31%).
- **L'Europa è il continente maggiormente attaccato nel 2020** : il 31% degli attacchi a cui X-Force ha

risposto nel 2020 era indirizzato a Paesi Europei, ai vertici della classifica mondiale per violazioni subite, tra cui, al primo posto, gli attacchi ransomware. Con origine nella maggior parte dei casi all'interno della stessa Europa, sono stati quasi il doppio di quelli perpetrati in Nord America e in Asia.

Il report illustra i dati raccolti da IBM nel 2020 e fornisce informazioni approfondite sul panorama globale delle minacce, informando i professionisti della sicurezza sulle minacce più rilevanti per le loro organizzazioni.

X-Force Threat Intelligence Index 2021 è disponibile al seguente link: https://www.ibm.biz/threatindex2021

IBM Security

IBM Security offre uno dei portfolio più completi e integrati di prodotti e servizi per la protezione aziendale. Il portfolio, supportato dal team di ricerca di fama mondiale IBM X-Force, consente alle organizzazioni di gestire con efficacia il rischio e difendersi dalle minacce emergenti. IBM dirige una delle organizzazioni di ricerca, sviluppo e delivery di soluzione di sicurezza più grandi al mondo, monitora 150 miliardi di eventi di security al giorno in più di 130 Paesi e ha ottenuto oltre 10.000 brevetti di sicurezza. Per maggiori informazioni, visita il sito www.ibm.com/security, segui @IBMSecurity su Twitter o visita il blog di IBM Security Intelligence.

---

[1] Gartner, comunicato stampa, *Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 18% in 2021*, 17 Novembre 2020

For further information: Claudia Ruffini IBM Media Relations 335 6325093 cl@it.ibm.com