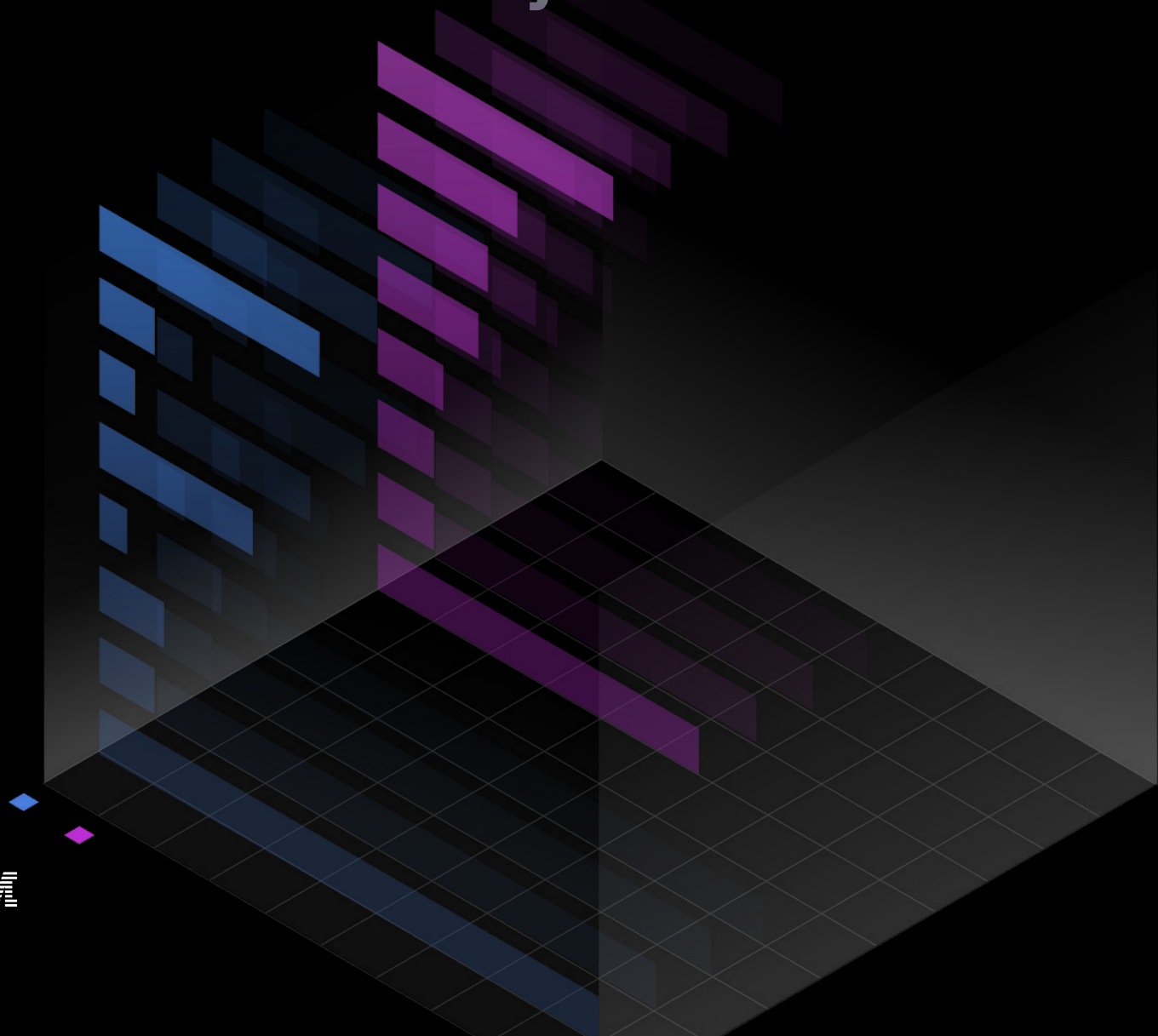
IBM Security

X-Force Threat Intelligence Index 2021

Executive summary



IBM

Introduzione

L'anno 2020 è stato senza dubbio uno dei più significativi e di trasformazione degli ultimi tempi: la pandemia globale e la crisi economica hanno impattato la vita di milioni di persone, determinando anche fermenti sociali e politici. Le aziende ne hanno risentito profondamente e molte di esse hanno compiuto un importante passaggio alla forza lavoro distribuita.

Nell'universo informatico, le circostanze straordinarie del 2020 hanno offerto ai cybercriminali l'opportunità di sfruttare le vulnerabilità delle reti di comunicazione e di prendere di mira supply chain e infrastrutture critiche. L'anno si è concluso com'è iniziato: con la scoperta di una minaccia dalle conseguenze globali, che ha preteso una risposta rapida. Un attacco verso organizzazioni della pubblica amministrazione e aziende del settore privato (in gran parte attribuito ad attori nation state che hanno sfruttato una backdoor di un software per il monitoraggio della rete) ha dimostrato che è necessario anticipare il rischio di terze parti e che, tuttavia, non è possibile prevederlo.

Per aiutare le organizzazioni a far fronte alle sfide odierne, IBM Security X-Force valuta gli scenari delle minacce informatiche e permette alle aziende di conoscere a fondo la loro evoluzione, i rischi associati e gli strumenti per prioritizzare misure di cybersecurity. Oltre a offrire una premium threat intelligence, analizziamo l'ampia mole di dati raccolti e produciamo X-Force Threat Intelligence Index, un approfondimento annuale sullo scenario delle minacce e delle loro evoluzioni.

Fra i trend da noi monitorati, il ransomware ha continuato a crescere fino a diventare il tipo di minaccia più frequente, rappresentando il 23% degli eventi di sicurezza ai quali X-Force ha risposto nel 2020. Gli attaccanti ransomware hanno intensificato la pressione per estorcere il pagamento combinando la crittografia dei dati alle minacce di rilasciare i dati su siti pubblici. Secondo le stime di X-Force, grazie al successo di questi schemi di attacco, nel 2020 un singolo gruppo di cybercriminali ransomware ha potuto incassare profitti per oltre 123 milioni di dollari.[1]

Sempre nel 2020, le aziende manifatturiere hanno dovuto far fronte a un aumento di attacchi ransomware e di altri attacchi. Il settore dell'industria manifatturiera nel suo complesso è stato il secondo settore più preso di mira dopo il settore finanziario-assicurativo; nel 2019 era l'ottavo. X-Force ha individuato attaccanti sofisticati che impiegavano campagne mirate di spear phishing per attaccare aziende manifatturiere e organizzazioni non governative coinvolte nella supply chain dei vaccini contro il COVID-19.

1. Tutti gli importi citati in questo rapporto sono espressi in dollari statunitensi.

Gli attaccanti hanno anche innovato il loro malware e in particolare quello rivolto a Linux, il codice open source che supporta infrastrutture cloud e storage dei dati business-critical. Nel 2020 delle analisi a cura di Intezer hanno individuato 56 nuove famiglie di malware Linux, evidenziando così un livello di innovazione ben più alto di quello presente in altri tipi di minaccia.

C'è motivo di sperare che il 2021 abbia le premesse per essere un anno migliore. I trend sono notoriamente difficili da prevedere, l'unica costante della quale possiamo essere certi è il cambiamento. Di fronte alle mutevoli sfide della cybersecurity, la resilienza richiede un'intelligence utilizzabile e una visione strategica per il futuro di una sicurezza più aperta e più connessa.

“Uniti si vince”: con questo spirito IBM Security ha il piacere di presentare X-Force Threat Intelligence Index 2021. I risultati indicati questo rapporto possono aiutare i team di sicurezza, gli specialisti del rischio, i decision maker, i ricercatori, i media a capire lo scenario delle minacce nell'ultimo anno per prepararsi alle sfide future.

Executive summary

IBM Security X-Force ha lavorato su miliardi di dati raccolti nell'arco di tutto il 2020 dai clienti IBM e da fonti pubbliche, analizzando tipi e vettori di attacco, ed effettuando confronti globali e di settore. Riportiamo di seguito alcuni dei principali risultati presentati nel Report X-Force Threat Intelligence Index.

23%

Percentuale di attacchi ransomware

Nel 2020 il ransomware è stato il metodo di attacco più diffuso; ha rappresentato il 23% di tutti gli incidenti ai quali IBM Security X-Force ha risposto e offerto rimedio.

123+ milioni di $

Stima dei profitti di un ransomware noto

X-Force stima prudentemente che nell'arco del 2020 gli attori del ransomware Sodinokibi (detto anche REvil) abbiano realizzato profitti per almeno 123 milioni di $ e rubato circa 21,6 terabyte di dati.

25%

Percentuale di attacchi nel primo trimestre 2020 dovuti alla principale vulnerabilità

Gli attaccanti hanno sfruttato una falla di Citrix e hanno approfittato di questa vulnerabilità nel 25% di tutti gli attacchi nei primi tre mesi dell'anno e nell'8% di tutti gli attacchi nel 2020.

35%

Percentuale di individuazione e sfruttamento di vulnerabilità nei principali vettori di infezione

L'individuazione e lo sfruttamento di vulnerabilità è balzata al primo posto nella classifica dei vettori di infezione nel 2020 superando il phishing, primo vettore nel 2019.

2

Posizione dell'industria manifatturiera nella classifica dei principali settori attaccati

L'industria manifatturiera è stata la seconda industria più attaccata nel 2020, superata solo dai servizi finanziari; nel 2019 era all'ottavo posto.

5 ore

Durata dei video di addestramento agli attacchi individuati sul server di un gruppo cybercriminale

Gli errori di attaccanti per conto dello stato iraniano hanno permesso ai ricercatori di X-Force di scoprire circa 5 ore di video su un server mal configurato e di estrarre conoscenze sulle loro tecniche.

100+

Dirigenti oggetto di campagne mirate di phishing

A metà del 2020, X-Force ha svelato una campagna globale di phishing che ha raggiunto più di 100 alti dirigenti con ruoli di gestione e procurement, in una task force che acquisisce dispositivi di protezione individuale (DPI) per la battaglia contro il COVID-19.

49%

Crescita percentuale delle vulnerabilità correlate ai sistemi di controllo industriale, 2019-2020

Le vulnerabilità correlate ai sistemi di controllo industriale (ICS) individuate nel 2020 sono aumentate del 49% su base annua rispetto al 2019.

56

Numero delle nuove famiglie di malware Linux

Il numero delle nuove famiglie di malware Linux scoperte nel 2020 è stato di 56, il livello più alto mai raggiunto. Il dato rappresenta un aumento del 40% su base annua dal 2019-2020.

31%

Percentuale degli attacchi in Europa

L'Europa è stata la regione più attaccata nel 2020 - anno in cui ha registrato il 31% degli attacchi osservati da X-Force -, seguita da Nord America (27%) e Asia (25%).

Guardare al futuro

Nel 2021, un'eterogeneità di minacce vecchie e nuove richiederà ai team di sicurezza di rivolgere l'attenzione a molti rischi contemporaneamente. In base all'analisi di X-Force, di seguito sono elencati alcuni punti principali per le priorità del nuovo anno.

— **Nel 2021 la superficie di rischio continuerà a crescere.** Migliaia di nuove vulnerabilità potrebbero impattare applicazioni e dispositivi vecchi e nuovi.

— **Gli attacchi ransomware a doppia estorsione si protrarranno verosimilmente lungo tutto il 2021.** Gli attaccanti che diffondono pubblicamente dati sui siti volti a danneggiare le aziende colpite, faranno ulteriori pressioni in modo che le infezioni ransomware abbiano costi altissimi.

— **Gli attaccanti continueranno ad individuare diversi vettori di attacco.** Continueranno ad essere presi di mira sistemi Linux, sistemi Operational Technology (OT), dispositivi IoT e ambienti cloud. Via via che gli attacchi a questi sistemi e dispositivi diventano più avanzati, gli attaccanti possono reindirizzare velocemente le loro attività, soprattutto dopo incidenti di alto profilo.

— **Ogni settore ha la propria quota di rischio.** Il cambiamento da un anno all'altro nella focalizzazione degli attacchi verso uno specifico settore evidenzia il rischio per tutti i settori industriali, oltre alla necessità di progressi significativi e di maturità dei programmi di cybersecurity a tutto campo.

Indicazioni per la resilienza

Dai risultati di IBM Security X-Force evidenziati in questo report, emerge che la threat intelligence e solide capacità di risposta sono misure efficaci per mitigare le minacce in evoluzione, indipendentemente dal settore o dal paese in cui si opera.

Consigli di X-Force per migliorare la preparazione nel far fronte alle minacce informatiche del 2021:

Anticipare le minacce. Utilizzare la threat intelligence per comprendere meglio le motivazioni e le tattiche degli attaccanti, potendo così assegnare priorità alle risorse di sicurezza.

Per rispondere al ransomware la preparazione è indispensabile. Pianificare di subire un attacco ransomware - considerando di affrontare anche le tecniche miste di ransomware e di estorsione per il furto di dati - ed eseguire regolarmente il piano può essere determinante per la risposta dell'azienda nel momento critico.

Verificare la gestione delle patch nell'azienda. Poiché l'anno scorso l'individuazione e lo sfruttamento di vulnerabilità sono stati il vettore di infezione più comune, occorre rafforzare l'infrastruttura e potenziare i rilevamenti interni in modo da individuare e fermare con rapidità ed efficacia i tentativi di sfruttamento automatizzato della vulnerabilità.

Proteggersi dalle minacce interne. Utilizzare soluzioni di data loss prevention (DLP), formazione e monitoraggio per evitare che figure interne all'azienda ne violino inavvertitamente o dolosamente i sistemi.

Creare e addestrare un team di risposta agli incidenti interno all'organizzazione. Se questo non fosse possibile, utilizzare un'efficace funzione di risposta agli incidenti per rispondere tempestivamente agli incidenti ad alto impatto.

Eseguire lo stress test del piano di risposta agli incidenti dell'azienda. Gli esercizi di simulazione o le attività in cyber range possono fornire al team un'esperienza critica per migliorare i tempi di reazione, ridurre i tempi di inattività e, in ultima analisi, ridurre i costi nell'eventualità di una violazione.

Implementare l'autenticazione a più fattori (MFA). Aggiungere layer di protezione agli account continua a essere una delle priorità più efficaci per la sicurezza delle aziende.

Eseguire, testare, conservare i backup offline. Garantire la presenza di backup e la loro efficacia attraverso test nel mondo reale fa una differenza fondamentale per la sicurezza dell'azienda, soprattutto in considerazione della ripresa delle attività ransomware mostrata dai dati 2020.

Cos'è IBM Security X-Force

IBM Security X-Force offre capacità di insight, rilevamento e risposta, per migliorare la postura di sicurezza dei clienti.

IBM Security X-Force Threat Intelligence unisce esperienza dei SOC IBM, ricerca, indagini sulla risposta agli incidenti, dati commerciali e open sources per aiutare i clienti a comprendere le minacce emergenti e prendere rapidamente decisioni informate in materia di sicurezza.

Inoltre, il team altamente specializzato di X-Force Incident Response offre rimedi strategici che aiutano le aziende a ottenere un migliore controllo su incidenti e violazioni della sicurezza.

X-Force unito alle esperienze in cyber range di IBM Security Command Center prepara gli utenti alla realtà delle minacce di oggi.

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 forniamo agli utenti abbonati un vasto insieme di analisi attuali e all'avanguardia sulla nostra piattaforma Premier Threat Intelligence.

Fare il prossimo passo

Scoprire come orchestrare la propria risposta agli incidenti con IBM Security >

Cos'è IBM Security

IBM Security lavora insieme ai propri clienti per proteggere il business 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 principi 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 moderno e 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 saperne di più, visitare www.ibm.com/security, seguire @IBMSecurity su Twitter o leggere il blog IBM Security Intelligence.

Contributori

Autrice principale:
Camille Singleton

Contributi di:
Allison Wikoff
Ari Eitan (Intezer)
Charles DeBeck
Charlotte Hammond
Chenta Lee
Chris Sperry
Christopher Kiefer
Claire Zaboeva
David McMillen
David Moulton
Dirk Hartz
Georgia Prassinos
Ian Gallagher (Intezer)
John Zorabedian
Joshua Chung
Kelly Kane
Lauren Jensen
Limor Kessem
Mark Usher
Martin Steigemann
Matthew DeFir
Megan Radogna
Melissa Frydrych
Michelle Alvarez
Mitch Mayne
Nick Rossman
Patty Cahill-Ingraham
Randall Rossi
Richard Emerson
Salina Wuttke
Scott Craig
Scott Moore

IBM Corporation
New Orchard Road
Armonk, NY 10504

Prodotto negli Stati Uniti d'America
Febbraio 2021

IBM **Security**