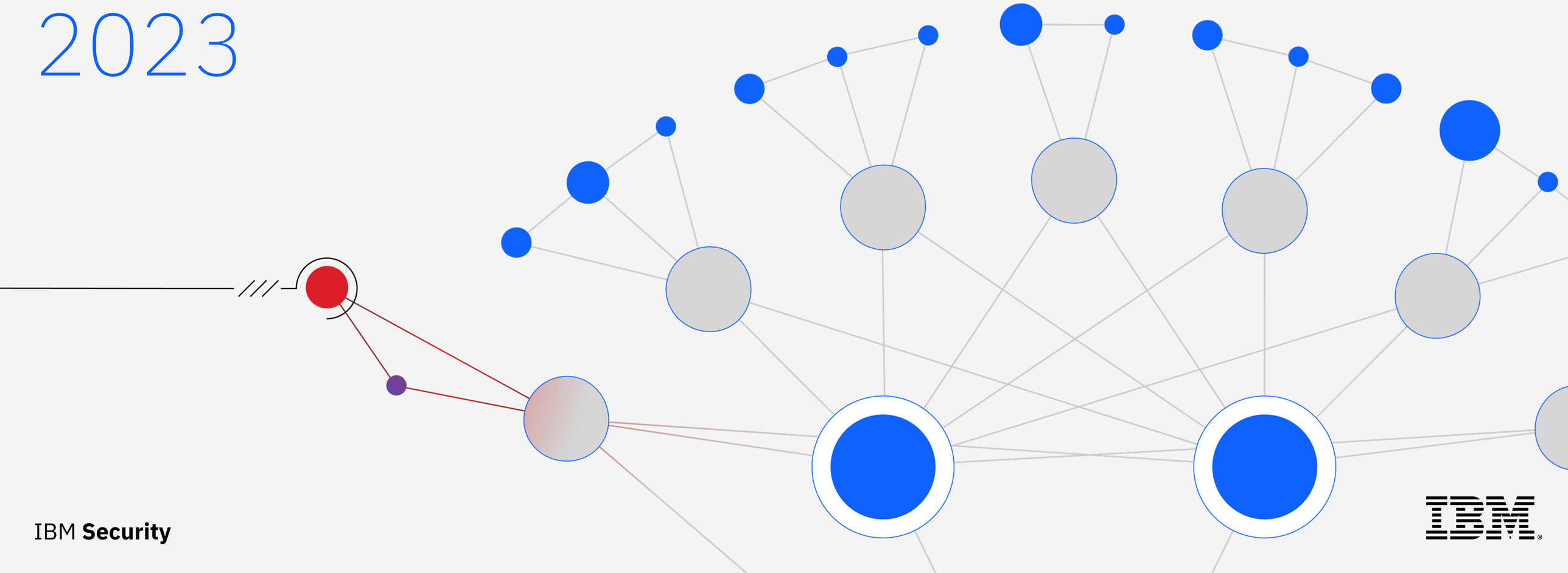
X-Force Threat Intelligence Index 2023

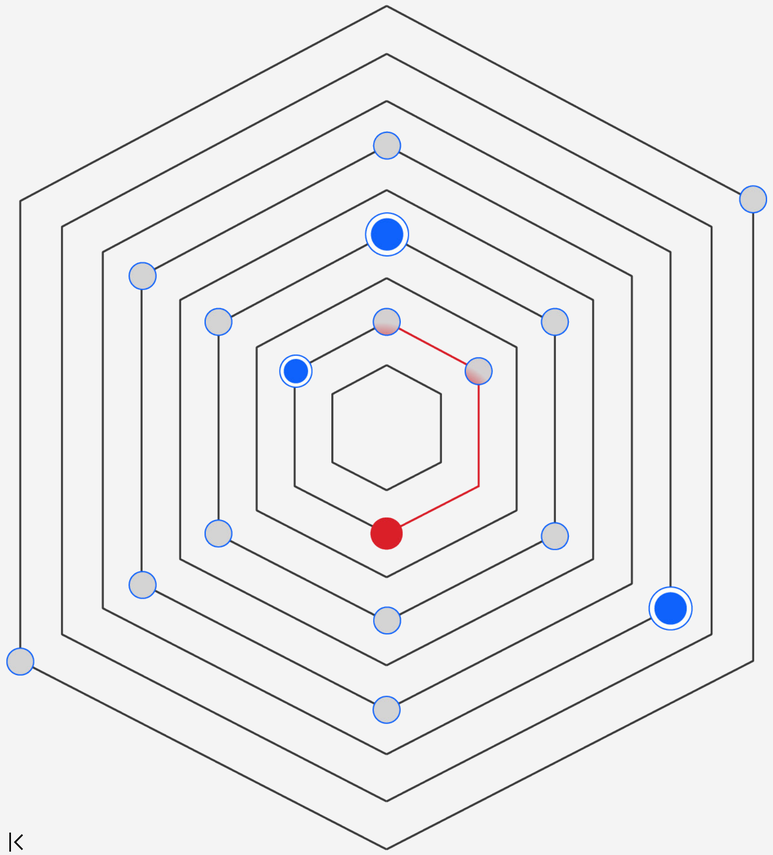


IBM **Security**

Sommario

01

Il documento in sintesi



Il 2022 è stato un altro anno difficile per la sicurezza informatica. Non sono mancati gli eventi che hanno contribuito a complicare le cose, primi tra tutti le persistenti conseguenze della pandemia e lo scoppio del conflitto militare in Ucraina. Le interruzioni hanno reso il 2022 un anno di sconvolgimenti e costi in termini economici, geopolitici e umani, determinando le condizioni caotiche ideali per il prosperare dei criminali informatici.

E così è stato.

IBM Security® X-Force® ha riscontrato l'opportunismo degli autori di minacce, i quali traggono vantaggio dalle situazioni di disordine sfruttandole a proprio vantaggio per infiltrarsi nei sistemi di governi e organizzazioni di tutto il mondo.

IBM Security X-Force Threat Intelligence Index 2023 traccia tendenze e pattern di attacco, nuovi e consolidati, includendo miliardi di datapoint provenienti da dispositivi di rete e endpoint, misure di risposta agli incidenti (IR), database relativi a vulnerabilità ed exploit e altro ancora. Il presente report consiste in una raccolta completa dei nostri dati di ricerca da gennaio a dicembre 2022.

Forniamo questi risultati come risorsa per clienti IBM, ricercatori di sicurezza informatica, policy maker, media e, più in generale, per la comunità dei professionisti e leader del settore sicurezza. L'instabile panorama odierno, con le sue minacce sempre più malevoli e sofisticate, richiede uno sforzo collaborativo per proteggere attività e cittadini. Oggi più che mai, per stare al passo con gli aggressori e fortificare le risorse critiche ci si deve armare di intelligence sulle minacce (threat intelligence) e insight sulla sicurezza.

In questo modo anche tu potrai prosperare.

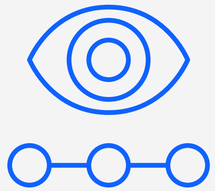
In che modo è cambiata la nostra analisi dei dati per il 2022

Nel 2022, abbiamo modificato il metodo d'esame di parte dei nostri dati. Tali modifiche ci consentono di offrire analisi ricche di insight più approfonditi e allinearci meglio ai framework standard del settore. Di conseguenza, ciò consente di prendere decisioni di sicurezza più informate e proteggere meglio la propria organizzazione dalle minacce.

Le modifiche al nostro metodo d'analisi del 2022 hanno incluso:

- **Vettori di accesso iniziale:** l'adozione del framework MITRE ATT&CK per tracciare i vettori di accesso iniziale ci permette di allineare meglio i risultati di ricerca al settore della sicurezza informatica più in generale e di identificare importanti tendenze a livello tecnico.
- **Compromissioni zero day ed exploit:** le informazioni estrapolate dal nostro corposo database delle vulnerabilità, che include quasi 30 anni di dati, ci aiuta a contestualizzare l'analisi e identificare l'effettiva minaccia determinata dalle vulnerabilità. Tale processo contestualizza anche la graduale diminuzione di exploit ingannevoli e zero days efficaci.
- **Metodi degli autori di minacce e loro impatto:** separare i passi compiuti dagli autori di minacce durante un attacco dall'impatto effettivo di un incidente ci ha consentito di individuare le fasi critiche di un incidente. A sua volta, tale processo ha rivelato le aree che chi reagisce a un attacco dovrebbe essere preparato a gestire in seguito a un incidente.

Punti salienti del report



Principali azioni rilevate per raggiungere gli obiettivi: per quasi un quarto di tutti gli incidenti verificatisi nel 2022, la distribuzione di backdoor ha rappresentato il 21% delle principali azioni per raggiungere l'obiettivo. In particolare, un picco di inizio anno di Emotet, un malware polivalente ha contribuito in modo significativo all'aumento delle attività backdoor osservate negli anni. Nonostante questo picco di attività backdoor, i ransomware, che hanno occupato il primo posto sin almeno dal 2020, hanno rappresentato un'ampia percentuale degli incidenti, con il 17% dei casi, facendo di tale malware una delle minacce più durature.

L'attacco più diffuso ad impattare sulle aziende è stata l'estorsione: l'estorsione è stata il più evidente impatto degli autori di minacce nel 27% dei casi. Nel 30% degli incidenti di estorsione, le vittime appartenevano al settore manifatturiero, confermando la tendenza dei criminali informatici a sfruttare un settore in difficoltà.

Il principale vettore di accesso iniziale è stato il phishing: il phishing rimane il principale vettore di accesso iniziale, individuato nel 41% degli incidenti, seguito dallo sfruttamento di applicazioni rivolte al pubblico, nel 26% dei casi. Le infezioni dovute a macro malware sono cadute in disuso, probabilmente per la decisione di Microsoft di bloccare di default le macro. Nel 2022, l'uso di file malevoli ISO e LNK è cresciuto fino a diventare la tattica principale per distribuire malware attraverso gli spam.

Aumento di hacktivism e malware distruttivi: il conflitto russo in Ucraina ha dato spazio a ciò che molti, nella comunità della cybersecurity, attendevano essere una vetrina su come l'informatica potesse determinare un modo moderno di fare la guerra. Sebbene al momento di questa pubblicazione le peggiori previsioni relative al cyberspazio non si siano concretizzate, si è registrata una notevole ripresa di hacktivism e malware distruttivi. Inoltre, X-Force ha osservato mutamenti senza precedenti nel mondo della sicurezza informatica, dove si registra una maggiore cooperazione tra gruppi di criminali informatici e gruppi di Trickbot che prendono di mira le organizzazioni ucraine.

03

Statistiche chiave

27%

Percentuale di attacchi con estorsione

Gli autori di minacce hanno tentato di estorcere denaro alle vittime in oltre un quarto degli incidenti a cui X-Force ha risposto nel 2022. Nell'ultimo decennio, le loro tattiche si sono evolute, una tendenza che dovrebbe continuare dato che gli autori di minacce cercano guadagni in maniera sempre più aggressiva.

21%

Percentuale di incidenti che hanno visto la distribuzione di backdoor

L'anno scorso, la distribuzione di backdoor è stata la principale azione mirata a raggiungere gli obiettivi, verificatasi oltre una volta su cinque incidenti segnalati in tutto il mondo. L'efficace intervento dei sistemi di difesa ha probabilmente impedito agli autori di minacce di raggiungere ulteriori obiettivi con il possibile utilizzo di ransomware.

17%

Percentuale di attacchi ransomware

Anche in quello che per alcune delle bande di ransomware più prolifiche è stato un anno caotico, i ransomware hanno rappresentato la seconda azione per raggiungere l'obiettivo più diffusa, immediatamente dopo le distribuzioni backdoor, continuando a interrompere le attività aziendali. La percentuale di incidenti ransomware è scesa dal 21% del 2021 al 17% del 2022.

41%

Percentuale di incidenti che coinvolgono il phishing per l'accesso iniziale
Nel 2022, le operazioni di phishing hanno continuato ad essere il percorso di compromissione più adottato, con il 41% degli incidenti corretti da X-Force che avevano utilizzato tale tecnica per ottenere accesso iniziale.

100%

Aumento del numero di tentativi mensili di thread hijacking
Nel 2022, sono stati registrati il doppio dei tentativi mensili di thread hijacking rispetto ai dati del 2021. E-mail spam portatrici di Emotet, Qakbot e IcedID hanno fatto largo impiego di thread hijacking.

52%

Calo nelle segnalazioni di phishing kit per l'acquisizione dei dati di carte di credito
La quasi totalità dei phishing kit analizzati attraverso i dati ha tentato di raccogliere nomi, 98% dei casi, indirizzi e-mail, 73%, indirizzi domestici, 66%, e password, 58%. Le informazioni relative alle carte di credito, che ancora nel 2021 sono state prese di mira nel 61% dei casi, hanno perso il favore degli autori di minacce: i dati dimostrano che nel 2022 sono state cercate soltanto nel 29% dei phishing kit, con un calo del 52%.

62%

Percentuale di attacchi che utilizzano allegati di spear phishing
Gli aggressori hanno prediletto gli allegati ingannevoli, distribuiti da loro o in combinazione con link o spear phishing tramite servizio.

26%

Percentuale di vulnerabilità con exploit noti nel 2022
Il 26% delle vulnerabilità del 2022 presentavano exploit noti. Secondo i dati tracciati da X-Force sin dai primi anni '90, negli ultimi anni tale percentuale sta calando, dimostrando i vantaggi di un processo di gestione patch ben mantenuto.

31%

Percentuale degli attacchi globali che hanno preso di mira la regione Asia-Pacifico
La regione Asia-Pacifico ha conservato il primo posto tra le regioni più attaccate nel 2022, contando il 31% degli incidenti complessivi. Si tratta di una statistica che rappresenta un aumento di cinque punti percentuali rispetto al totale degli attacchi a cui X-Force ha risposto nella regione nel 2021.

04

Principali vettori di accesso iniziale

Nel 2022, X-Force è passato dal tracciamento dei vettori di accesso iniziale come categorie generiche, per es. phishing e credenziali rubate, a quello delle tecniche di accesso iniziale elencate nel framework MITRE ATT&CK Matrix for Enterprise. Questo cambiamento consente a X-Force di tracciare importanti tendenze più dettagliatamente a livello tecnico. Inoltre, fornisce dati più facilmente utilizzabili e confrontabili tra loro e si allinea con gli sforzi di standardizzazione del settore in generale.

Principali vettori di accesso iniziale nel 2022

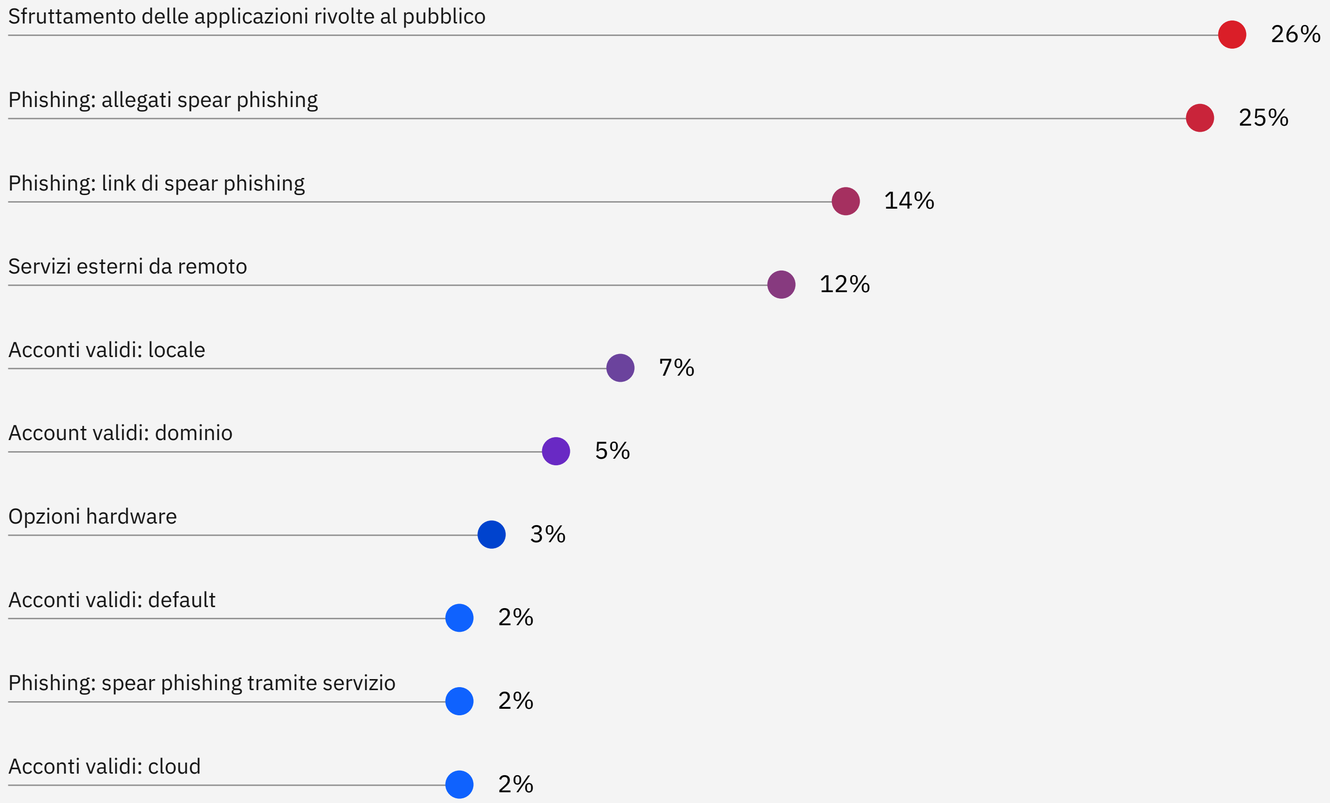


Figura 1: Principali vettori di accesso iniziale osservati da X-Force nel 2022. Fonte: X-Force

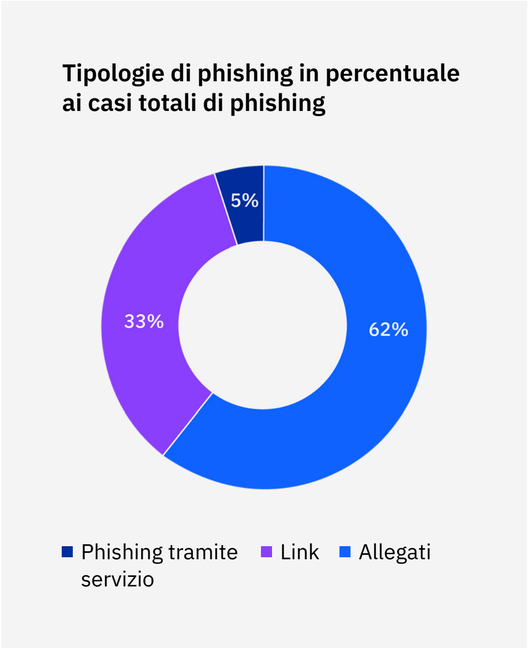


Figura 2: Sottotecniche di phishing in percentuale al totale dei casi di phishing osservati da X-Force nel 2022. Fonte: X-Force

Phishing

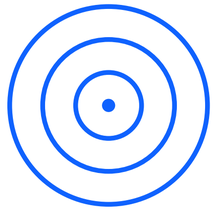
Il phishing (T1566), attraverso allegati, link o servizio, rimane il principale vettore di infezione, costituendo il 41% degli incidenti risolti complessivamente da X-Force nel 2022. Si tratta di una percentuale rimasta ai valori del 2021, dopo essere aumentata del 33% nel 2020. Osservando gli incidenti di phishing nel complesso, gli allegati di spear phishing (T1566.001) sono stati utilizzati nel 62% dei casi, i link di spear phishing (T1566.002) nel 33% e lo spear phishing come servizio (T1566.003) nel 5%. In alcuni casi, X-Force ha rilevato da parte degli aggressori anche un uso contemporaneo di phishing tramite allegati, link e come servizio.

I dati IBM X-Force Red del 2022 evidenziano ulteriormente il valore che phishing e credenziali mal gestite hanno per gli autori di minacce. Nel 2022, test di penetrazione non autorizzata dei clienti di X-Force Red hanno rivelato un'autenticazione o una gestione impropria delle credenziali in circa il 54% dei casi. Il team di X-Force Red Adversary Simulation ha condotto regolari azioni di spear phishing con codici QR che miravano ai token di autenticazione a più fattori (MFA). Molte organizzazioni non avevano visibilità di applicazioni ed endpoint esposti attraverso la gestione di accesso e identità e portali single sign-on (SSO), come Okta.

Al secondo posto, lo sfruttamento delle applicazioni rivolte al pubblico (T1190), definito come la capacità di sfruttare un punto debole di un computer connesso a Internet o di un programma, è risultato nel 26% degli incidenti a cui X-Force ha dovuto rispondere. Questo dato è correlato a quello che i precedenti rapporti di Threat Intelligence Index chiamavano "sfruttamento della vulnerabilità" e segna un calo rispetto al 34% del 2021.

In terza posizione, l'abuso di account validi (T1078) è stato individuato nel 16% degli incidenti rilevati. Si tratta di casi in cui i malintenzionati hanno ottenuto e abusato delle credenziali di account esistenti come mezzo per ottenere l'accesso. Tali incidenti hanno incluso account cloud (T1078.004) e account di default (T1078.001), ognuno nel 2% dei casi, account di dominio (T1078.002), 5%, e account locali (T1078.003) nel 7% dei casi.

Il tentativo di raccogliere informazioni relative a carte di credito è sceso dal 61% dei casi nel 2021, al 29% dei phishing kit nel 2022.



I phishing kit durano più a lungo e mirano ai PII piuttosto che ai dati delle carte di credito

IBM Security ha analizzato migliaia di phishing kit in tutto il mondo per due anni di seguito, scoprendo che le distribuzioni di kit sono operative più a lungo e raggiungono più utenti. Il dato indica che il ciclo di vita dei phishing kit osservati è più che raddoppiato negli anni, mentre il valore mediano della distribuzione nell'insieme dei dati è rimasto relativamente basso: 3,7 giorni.

In generale, la distribuzione più breve è durata alcuni minuti e la più lunga, scoperta nel 2022, oltre tre anni. La nostra analisi ha rilevato quanto segue:

- L'anno scorso, un terzo dei kit distribuiti è durato circa 2,3 giorni, oltre il doppio di quanto sono durati l'anno precedente quando la stessa proporzione non è durata più di un giorno.
- La metà circa di tutti i kit segnalati ha colpito 93 utenti, mentre nel 2021 ciascuna distribuzione non superava la media di 75 vittime potenziali.
- Il numero massimo di vittime causate da un attacco di phishing segnalato è stato di poco superiore a 4.000, anche se si è trattato di un'eccezione.
- Il 98% dei phishing kit analizzati cercava di raccogliere i nomi degli utenti. Il 73% collezionava indirizzi e-mail, il 66% indirizzi di casa e il 58% cercava di carpire le password.
- Il tentativo di raccogliere informazioni relative a carte di credito è sceso dal 61% dei casi nel 2021, al 29% dei phishing kit nel 2022.
- Il numero ridotto di phishing kit alla ricerca di dati relativi a carte di credito indica che i truffatori preferiscono dare priorità alla raccolta di informazioni di identificazione personale (PII), che consentono loro opzioni più ampie e nefaste. Le PII possono essere raccolte e vendute sul dark web, o su altri forum, oppure utilizzate per condurre ulteriori operazioni contro le vittime.

Principali marchi vittime di spoofing

Si è osservato che tra i marchi vittime di spoofing ci sono soprattutto grandi nomi del settore tecnologico. X-Force ritiene che questo cambio di direzione rispetto al 2021 sia dovuto alla migliorata capacità di individuare i marchi da attaccare, piuttosto che agire esclusivamente contro obiettivi che i kit devono aggredire di default. Molti phishing kit sono polivalenti e il brand vittima di spoofing può essere modificato alterando un semplice parametro. Per esempio, un kit può essere predisposto per effettuare lo spoofing contro Gmail, ma l'aggiornamento di una sola linea lo può trasformare in un attacco di spoofing contro Microsoft.

Le credenziali rubate a tali servizi sono preziose. Ottenere accesso agli account che le vittime utilizzano per gestire interi tratti della loro presenza online può consentire l'accesso ad altri account. La particolare attenzione degli aggressori a questo tipo di accesso iniziale è evidenziata nel Cloud Threat Landscape Report del 2022. Rispetto a quanto osservato nel 2021, il report ha rilevato un aumento di oltre tre volte (200%) del numero di account cloud messi in vendita sul dark web.

Principali marchi vittime di spoofing negli anni

	2022	2021
1	Microsoft	Microsoft
2	Google	Apple
3	Yahoo	Google
4	Facebook	BMO Harris Bank
5	Outlook	Chase
6	Apple	Amazon
7	Adobe	Dropbox
8	AOL	DHL
9	PayPal	CNN
10	Office365	Hotmail

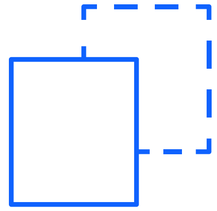
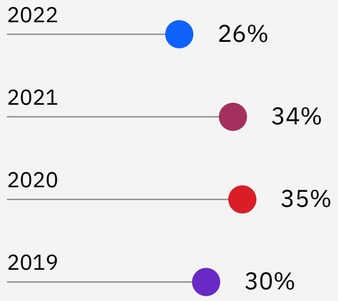


Figura 3: Questa classifica riporta i principali marchi vittime di spoofing nel 2021 e nel 2022, dimostrando che gli autori di minacce sono sempre più concentrati sui grandi marchi di prodotti tecnologici.
Fonte: Dati IBM su phishing kit

Percentuale di incidenti provocati dallo sfruttamento di vulnerabilità negli ultimi quattro anni



Vulnerabilità

Lo sfruttamento della vulnerabilità, acquisito per il 2022 come sfruttamento delle applicazioni rivolte al pubblico (T1190), si è classificato al secondo posto tra i principali vettori di infezione ed è stato uno dei metodi di compromissione dei sistemi preferiti dagli aggressori sin dal 2019. Le vulnerabilità sono state sfruttate nel 26% degli attacchi a cui X-Force ha dovuto rimediare nel 2022, rispetto al 34% del 2021, al 35% del 2020 e al 30% del 2019.

Non tutte le vulnerabilità sfruttate dagli autori di minacce hanno comportato un incidente informatico. Nel 2022, il numero di incidenti determinati dallo sfruttamento di vulnerabilità è diminuito del 19% rispetto al 2021, dopo essere aumentato del 34% rispetto al 2020. X-Force ritiene che questa oscillazione sia motivata dalla diffusione della vulnerabilità Log4J alla fine del 2021.

Lo sfruttamento dell'accesso rappresenta un'importante area di ricerca a cui il team di X-Force Red Adversary Simulation Services si è dedicato nella continua simulazione di minacce avanzate. Il team si è concentrato ancora di più sulla ricerca di vulnerabilità per lo sfruttamento di sistemi operativi (OS) e applicazioni per aumentare gli accessi ed eseguire l'escalation dei privilegi. Tale attenzione è stata in gran parte dovuta alle passate esercitazioni con clienti di lunga data, che hanno rafforzato i tradizionali percorsi di attacco di Active Directory, e alla necessità di stanare nuovi percorsi di attacco.

Sebbene le vulnerabilità siano un diffuso vettore di accesso iniziale, e ogni anno il settore reagisca a molte delle principali vulnerabilità, queste non sono tutte uguali. Per chi deve prendere delle decisioni, è importante avere piena visione del panorama delle vulnerabilità e assicurarsi di avere i mezzi per comprendere la reale minaccia che una data vulnerabilità rappresenta per le loro reti.

Quasi 30 anni fa, X-Force ha iniziato a realizzare un corposo database delle vulnerabilità, anticipando l'avvento del sistema Common Vulnerabilities and Exposures (CVE). Oggi si tratta di uno dei database più completi nel settore della sicurezza informatica. Sebbene le vulnerabilità rappresentino un grave rischio per la sicurezza, esistono molte più vulnerabilità segnalate che exploit ingannevoli noti. Inoltre, nonostante l'attenzione pubblica verso i zero day, l'attuale numero di zero day è sovrastato dal numero totale di vulnerabilità note.

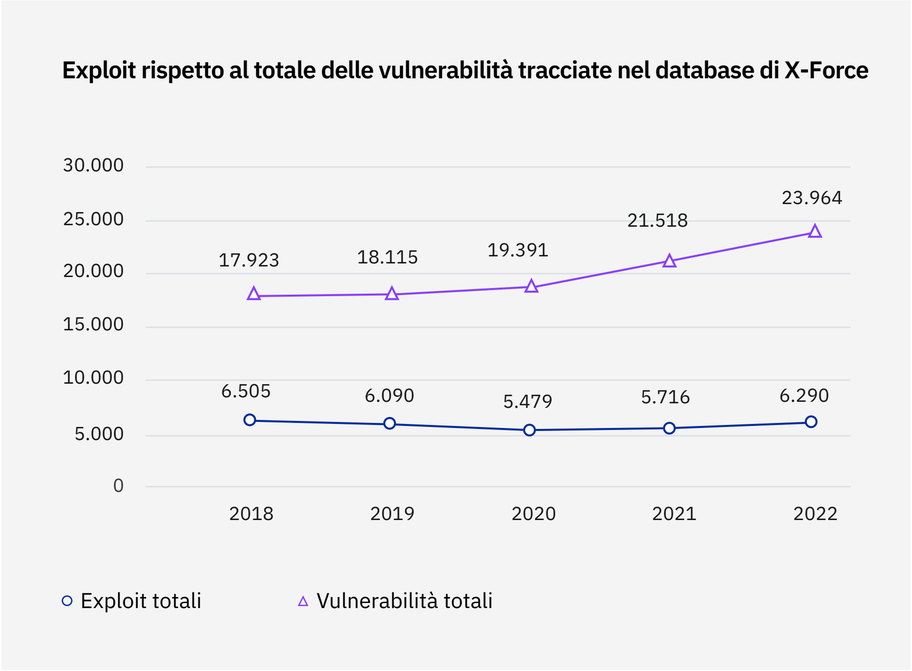


Figura 4: Grafico relativo al database delle vulnerabilità di X-Force su vulnerabilità e exploit negli ultimi cinque anni. Fonte: X-Force

Ogni anno il numero di vulnerabilità scoperte segna un nuovo record. Nel 2022, il numero complessivo di vulnerabilità tracciate è stato di 23.964, rispetto alle 21.518 del 2021. La tendenza all'aumento annuale delle vulnerabilità dura da un decennio.
A beneficio di chi deve difendersi, l'analisi del nostro database delle vulnerabilità ha dimostrato che negli ultimi anni la percentuale di exploit noti e praticabili è calata rispetto alle vulnerabilità segnalate: 36% nel 2018, 34% nel 2019, 28% nel 2020, 27% nel 2021 e 26% nel 2022.

Questi numeri possono mutare con l'esposizione a zero day ed exploit sviluppati per vulnerabilità già datate, a volte anni dopo che sono state identificate. Dietro questo calo si nascondono diverse possibili spiegazioni. In primo luogo, la creazione di programmi di bug bounty ufficiali ha incentivato l'individuazione proattiva delle vulnerabilità all'interno delle applicazioni. Inoltre, esiste un certo numero di vulnerabilità ampiamente diffuse e consolidate che gli aggressori già utilizzano come mezzo di sfruttamento dei sistemi, riducendo il bisogno di sviluppare nuovi exploit. Probabilmente, il calo è dovuto a una combinazione di più fattori, ma non indica che lo sfruttamento delle vulnerabilità non sia più una minaccia.

Mentre la percentuale di exploit rispetto alle vulnerabilità diminuisce, negli ultimi cinque anni è aumentata la pericolosità degli exploit tracciati da X-Force. Nel 2018, il 58% delle vulnerabilità aveva un punteggio CVSS (Common Vulnerability Scoring System) medio di

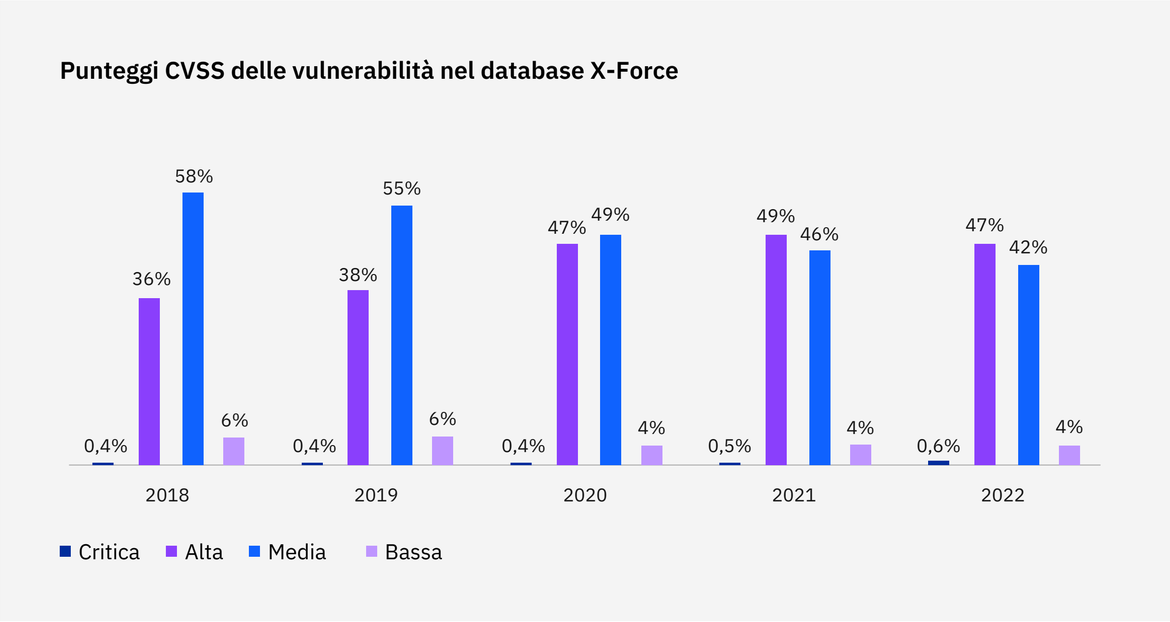


Figura 5: Database delle vulnerabilità di X-Force sulla pericolosità delle vulnerabilità tracciate nel nostro sistema. Fonte: X-Force

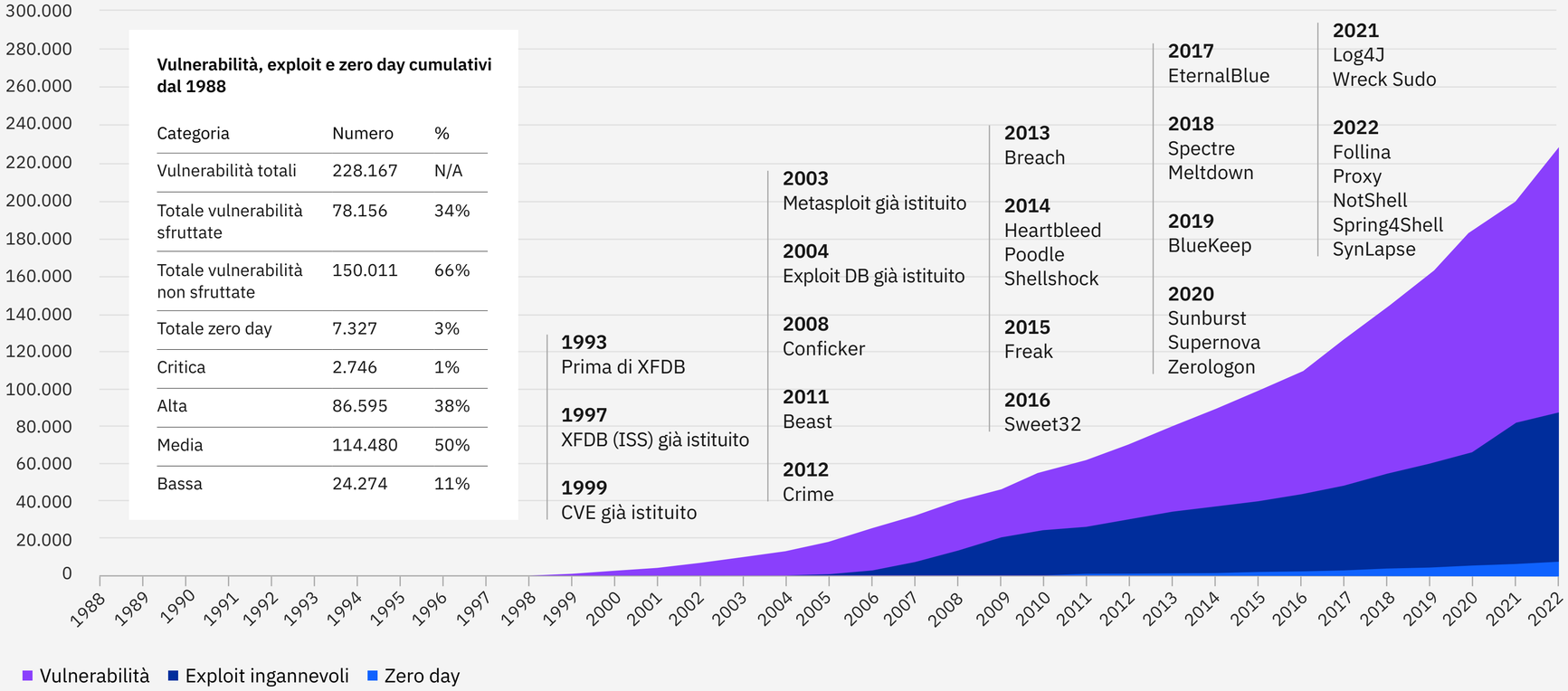
4,0-6,9 su 10, rispetto al 36% con punteggio di 7,0-9,9. La differenza tra questi due parametri è stata invertita nel 2021 e le vulnerabilità ad elevata pericolosità ora contano cinque punti percentuali in più rispetto a quelle con punteggio medio.

E ancora, di tutte le vulnerabilità tracciate da X-Force a partire dal 1988, il 38% risulta di pericolosità elevata, di cui soltanto l'1% arriva al punteggio critico di 10. Metà delle vulnerabilità tracciate risulta mediamente pericolosa con il restante 11% che si piazza in basso, con un punteggio di 3,9 o inferiore. Di per sé, questi punteggi non sono in relazione con la pericolosità reale di un CVE, in quanto non tengono conto di come si realizza lo sfruttamento o se effettivamente se ne registra uno. Tuttavia, i punteggi aiutano chi si deve difendere a confrontare le vulnerabilità e assegnare le priorità di intervento. Nella pagina che segue, il grafico in Figura 6 consente di mettere in prospettiva la vera natura del problema di vulnerabilità che il settore della sicurezza informatica deve affrontare.

Vulnerabilità delle tecnologie operative (OT)

Le vulnerabilità dei sistemi di controllo industriale (ICS) rilevate nel 2022 sono diminuite per la prima volta in due anni: 457 nel 2022 rispetto a 715 nel 2021 e 472 nel 2020. Ciò si potrebbe spiegare con i cicli di vita degli ICS e come vengono gestiti e applicati i patch. Gli aggressori sanno che per via dell' esigenza di tempi di indisponibilità ridotti, di cicli di vita delle apparecchiature di lunga durata e di software datati e meno supportati, molti componenti ICS e reti OT sono ancora a rischio di vulnerabilità risalenti al passato. Le infrastrutture sono mantenute molti anni più a lungo rispetto alle normali workstation d'ufficio, il che estende la durata delle vulnerabilità specifiche degli ICS oltre quelle che possono sfruttare le IT.

Il problema della vulnerabilità



Vulnerabilità, exploit e zero day cumulativi dal 1988

Categoria	Numero	%
Vulnerabilità totali	228.167	N/A
Totale vulnerabilità sfruttate	78.156	34%
Totale vulnerabilità non sfruttate	150.011	66%
Totale zero day	7.327	3%
Critica	2.746	1%
Alta	86.595	38%
Media	114.480	50%
Bassa	24.274	11%

Figura 6: Grafico relativo alla crescita di vulnerabilità, exploit e zero day dal 1988. È inclusa una timeline dei maggiori eventi riguardanti le vulnerabilità a partire dal 1993. XFDB sta per X-Force Database ed Exploit DB sta per Exploit Database. Fonte: X-Force

Principali azioni per raggiungere gli obiettivi

In precedenza, X-Force Threat Intelligence Index ha esaminato la categoria dei principali attacchi in generale. Per il 2022, X-Force ha suddiviso questa classificazione in due distinte categorie: le azioni specifiche che gli autori di minacce hanno intrapreso sulle reti delle vittime, o azioni avversarie per raggiungere l'obiettivo, e l'effetto, o l'impatto, sulla vittima previsto o realizzato di tale azione.

Secondo i dati di risposta agli incidenti di X-Force, la distribuzione di backdoor è stata l'azione per raggiungere l'obiettivo più diffusa, riscontrata nel 21% di tutti gli incidenti segnalati. Seguono ransomware con il 17% e il BEC (Business Email Compromise) con il 6%. Documenti dannosi (maldoc), campagne di spam, strumenti di accesso remoto e server di accesso sono stati rilevati ognuno nel 5% dei casi.

Principali azioni per raggiungere gli obiettivi, 2022

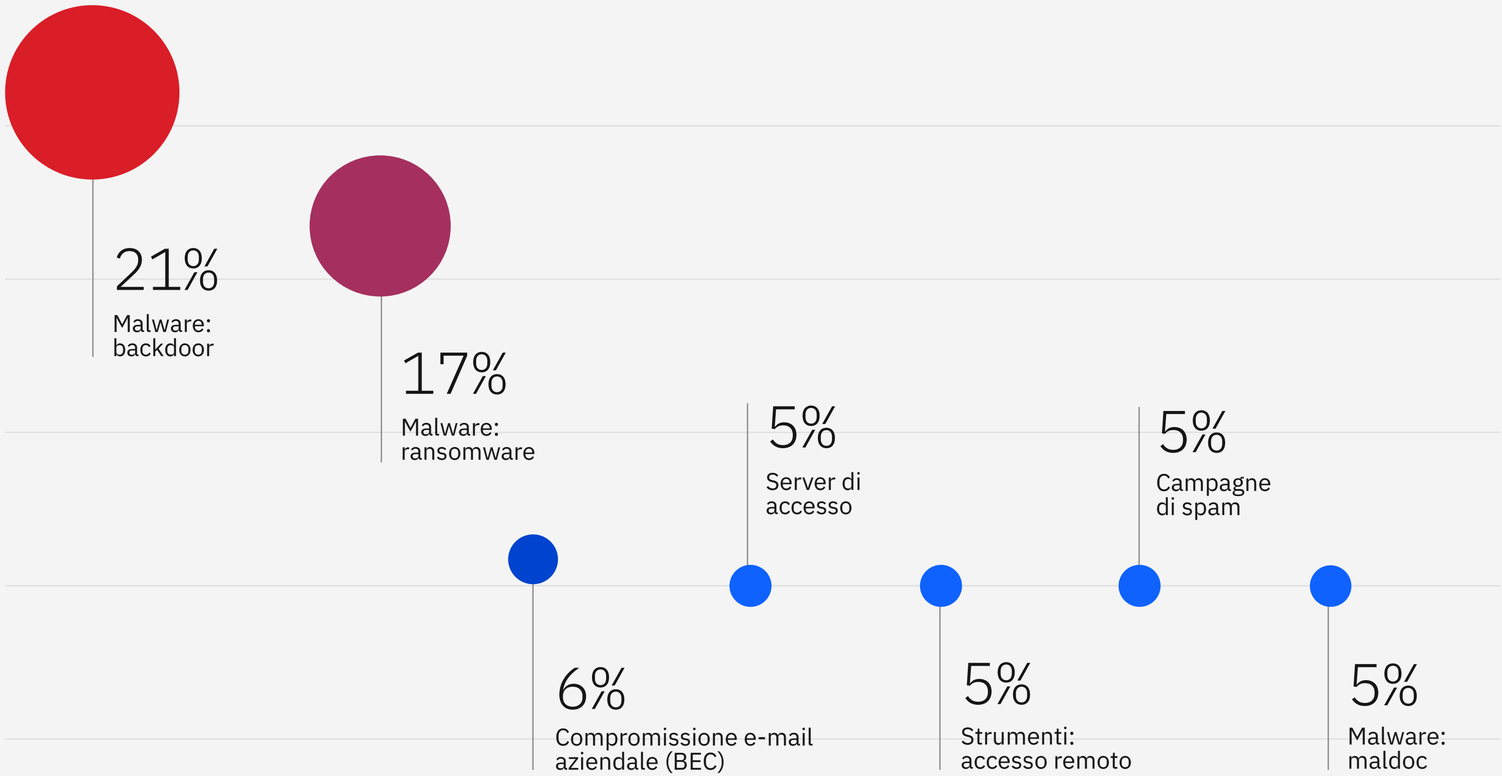


Figura 7: Principali azioni per raggiungere gli obiettivi rilevate da X-Force nel 2022. Fonte: X-Force

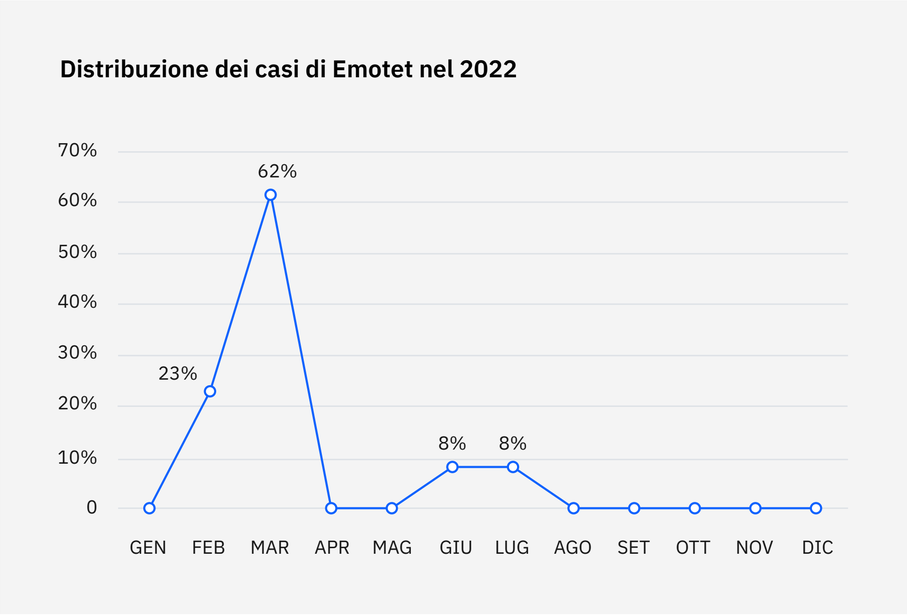


Figura 8: Grafico sui picchi di casi di Emotet nei primi mesi del 2022. Fonte: X-Force

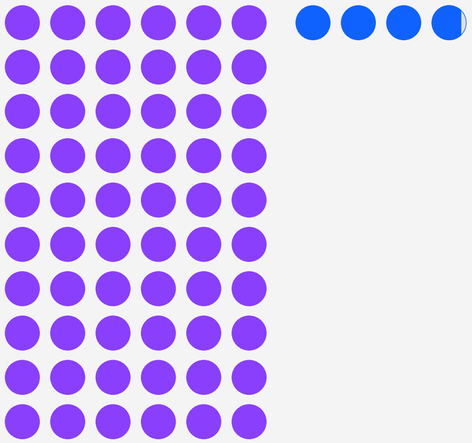
Nei casi in cui una distribuzione di backdoor è stata classificata come azione per raggiungere l'obiettivo, è probabile che l'autore della minaccia avesse ulteriori piani per quando la backdoor sarebbe diventata operativa. Ulteriori obiettivi dell'aggressore sono stati probabilmente evitati dall'efficace intervento dei team di sicurezza o di una risposta all'incidente. Un'ulteriore attività dannosa avrebbe probabilmente incluso l'utilizzo di ransomware, poiché circa due terzi dei casi di backdoor in questione mostravano i tipici segnali di un attacco ransomware.

L'aumento della diffusione di backdoor può essere giustificato anche dalla quantità di denaro che questo tipo di accesso può generare sul dark web. L'accesso a una rete aziendale compromessa da un initial access broker (broker di accesso iniziale) in genere viene venduto per diverse migliaia di dollari americani. Questo tipo di accesso può essere ricercato da malintenzionati che vogliono ottenere un rapido profitto evitando problemi con il mantenimento dell'accesso mentre si spostano lateralmente e violano dati di alto valore. Possono mettersi alla ricerca di backdoor anche i malintenzionati che non dispongono del malware necessario per stabilire un accesso al sistema.

Generalmente, i broker di accesso iniziale cercano di mettere all'asta gli accessi di cui dispongono. X-Force ha visto lievitare tali prezzi tra i 5.000 e i 10.000 dollari, sebbene il prezzo finale possa essere minore. Altri hanno segnalato accessi venduti per 2.000-4.000 dollari, e in un caso si sono raggiunti i 50.000 dollari. Si tratta di cifre nemmeno paragonabili con prezzi significativamente più bassi come, per esempio, quello di una singola carta di credito, offerta per meno di 10 dollari.

In febbraio e marzo, le backdoor hanno portato a un notevole aumento dei casi di Emotet. Un picco che ha gonfiato in modo significativo la classifica dei casi di backdoor, poiché quelli distribuiti durante questo lasso di tempo rappresentano il 47% di tutte le backdoor globalmente individuate nel corso del 2022. In seguito alla pausa di Emotet tra luglio e novembre, dopo la quale si è ripreso per quasi due settimane a un volume molto inferiore, il numero di casi di backdoor è diminuito in modo significativo.

Durata media dell’attacco ransomware



Ransomware

Anche in quello che per alcune delle bande di ransomware più prolifiche è stato un anno caotico, i ransomware hanno rappresentato la seconda azione per raggiungere l’obiettivo più diffusa, immediatamente dopo le distribuzioni backdoor, continuando a interrompere le attività aziendali. La percentuale di incidenti ransomware è scesa dal 21% del 2021 al 17% del 2022.

Uno studio IBM X-Force ha rivelato che, tra il 2019 e il 2021, la durata media degli attacchi ransomware ha registrato una riduzione del 94,34%, passando da oltre due mesi a poco meno di quattro giorni. Ciò nonostante, i ransomware costituiscono un pericolo evidente e attuale che presenta solo segnali di sviluppo, non di rallentamento.

Un modo particolarmente dannoso in cui gli operatori di ransomware distribuiscono il proprio carico utile (payload) attraverso una rete è compromettendo i controller di dominio. Un piccola percentuale, circa il 4%, dei risultati relativi a test di penetrazione non autorizzata condotti da X-Force Red ha rivelato entità dalle configurazioni errate in Active Directory che potrebbero rimanere esposte all’escalation dei privilegi o al controllo totale del dominio. Nel 2022, X-Force ha osservato anche attacchi di ransomware più aggressivi a infrastrutture sottostanti, come ESXi e Hyper-V. Il potenziale elevato impatto di questi metodi di attacco sottolinea l’importanza di proteggere adeguatamente controller di dominio e hypervisor.

Varianti ransomware

Poiché i gruppi di ransomware e i relativi broker di accesso vanno e vengono, X-Force ha registrato un regolare abbandono dei principali gruppi attivi in questo spazio. Nel 2022, X-Force si è imbattuto in 19 ransomware, rispetto ai 16 del 2021. Le varianti LockBit costituivano il 17% degli incidenti ransomware osservati complessivamente, contro il 7% del 2021. Seguono a pari merito Phobos e WannaCry che costituivano l’11% degli incidenti. I principali gruppi del 2022 hanno scalzato dalla vetta REvil, al primo posto nel 2021, noto anche come Sodinokibi, con il 37% dei casi nel 2021, e dal secondo posto Ryuk con il 13%, entrambi scesi al 3%.

LockBit 3.0 è l’ultimissima variante della famiglia di ransomware LockBit, parte di un’operazione di ransomware-as-a-service (RaaS) associata a LockerGoga e MegaCortex. LockBit è operativo dal settembre 2019, mentre LockBit 3.0 è stato rilasciato nel 2022. Una buona parte del codice sorgente di LockBit 3.0 sembra essere stata presa in prestito dal ransomware BlackMatter.

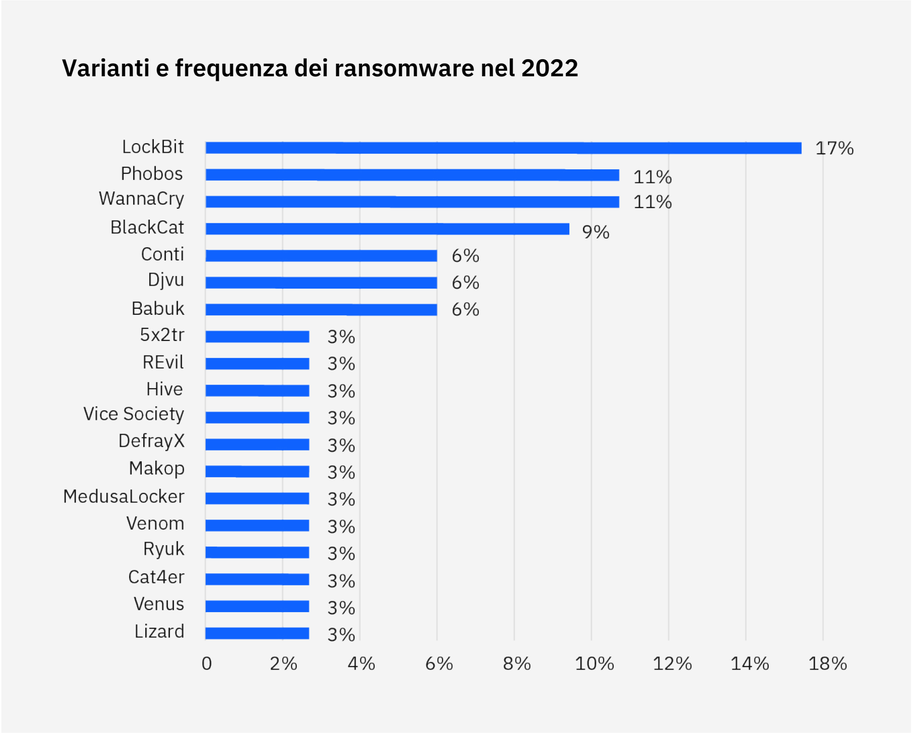


Figura 9: Varianti ransomware e frequenza con cui sono state rilevate durante le attività di risposta agli incidenti condotte da X-Force nel 2022. Fonte: X-Force

I ricercatori hanno rilevato il ransomware Phobos per la prima volta agli inizi del 2019. In base a somiglianze di codice, meccanismi di diffusione, tecniche di sfruttamento e alle richieste di riscatto, Phobos è stato ritenuto un fork delle già note famiglie di ransomware Crysis e Drama. Phobos è stato comunemente usato per attacchi in scala più piccola, che implicavano richieste di riscatto più contenute. I principali metodi riscontrati per la distribuzione di Phobos sono campagne di phishing via e-mail e sfruttamento di porte RDP (Remote Desktop Protocol) vulnerabili.

WannaCry, comparso per la prima volta nel 2017, si è diffuso utilizzando EternalBlue per sfruttare la vulnerabilità del server (MS17-010) Microsoft Server Message Block 1.0 (SMBv1). Diversi casi di WannaCry o Ryuk osservati da X-Force nel 2022 sono stati conseguenza di infezioni avvenute da tre a cinque anni prima e si sono verificati su apparecchiature datate e prive di patch, mettendo in luce l'importanza di un'adeguata ripulitura (cleanup) dopo tali eventi.

Compromissione e-mail aziendale (BEC)

Nel 2022, BEC ha conservato il terzo posto con il 6% degli incidenti a cui X-Force ha dovuto rispondere. Si tratta di un dato leggermente inferiore rispetto all'8% degli attacchi nel 2021 e al 9% del 2020, anno in cui si piazzava al quinto posto. BEC ha preso il posto degli attacchi di accesso al server, al secondo posto nel 2021. Questo tipo di attacchi si verificano quando un aggressore ottiene l'accesso a un server per obiettivi finali sconosciuti, e nel 2022 è stato classificato in maniera più dettagliata in base al tipo di accesso ottenuto dagli autori. Nel 50% dei casi di BEC affrontati da X-Force sono stati utilizzati link di spear phishing. Allegati malevoli e violazioni di account validi sono stati utilizzati ognuno nel 25% dei tentativi di abilitare BEC.

Impatti principali

Per comprendere meglio l'impatto che gli autori di minacce cercavano di produrre, X-Force ha esaminato più da vicino le conseguenze degli incidenti sulle aziende vittime di attacchi. Si tratta di informazioni che consentono alle aziende di comprendere meglio le conseguenze principali di un attacco e pianificare in modo più efficace le risposte a eventuali incidenti futuri.

L'analisi ha rilevato che oltre un incidente su quattro puntava a estorcere denaro alle aziende vittime, impatto principale degli incidenti corretti da X-Force. I casi di estorsione osservati sono stati perpetrati soprattutto attraverso ransomware o BEC e, spesso, includevano l'utilizzo di strumenti di accesso da remoto, cryptominer, backdoor, dispositivi per il download e web shell.

Impatti principali nel 2022

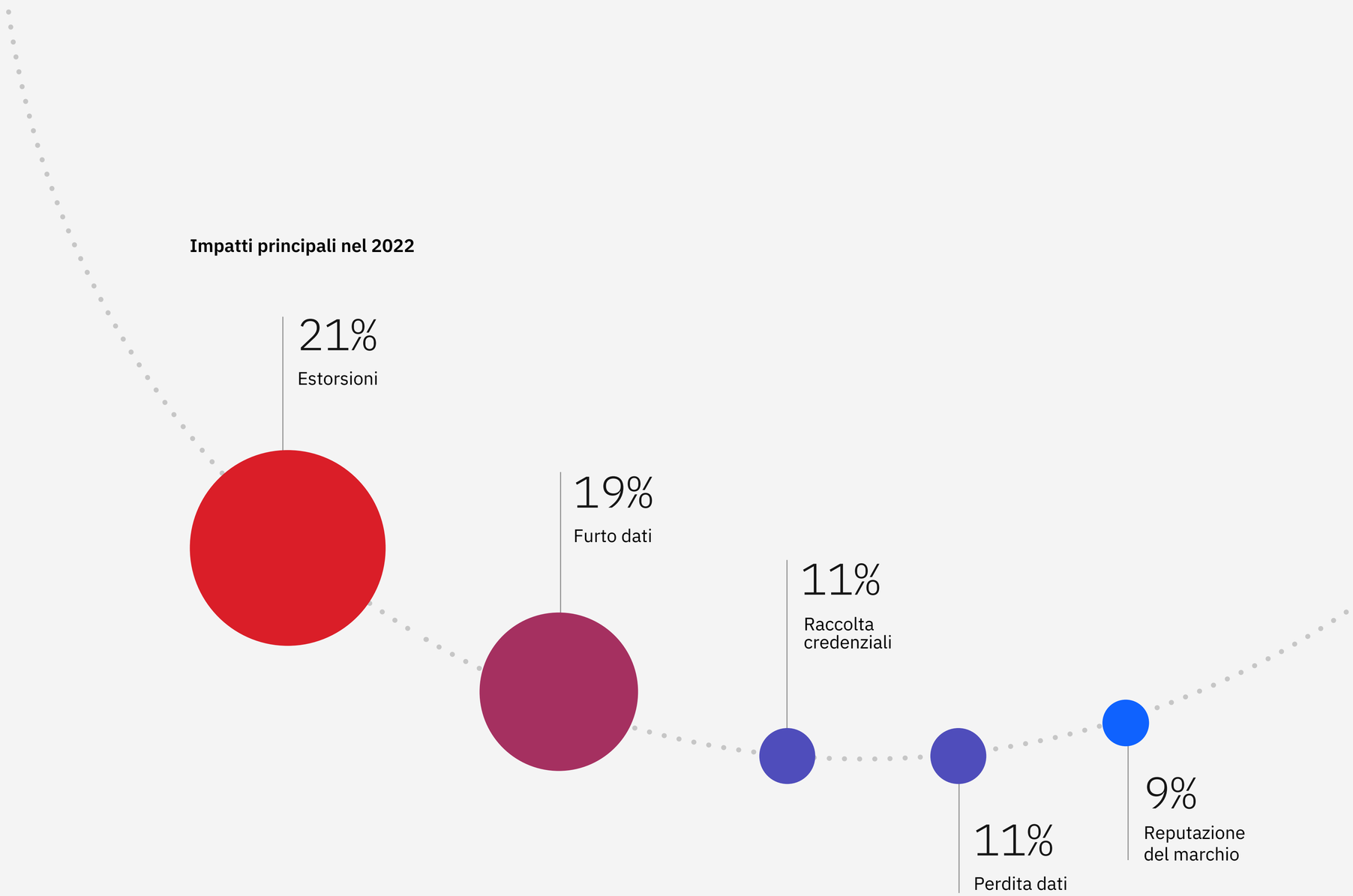


Figura 10: Principali impatti osservati da X-Force in risposta agli incidenti nel 2022. Fonte: X-Force

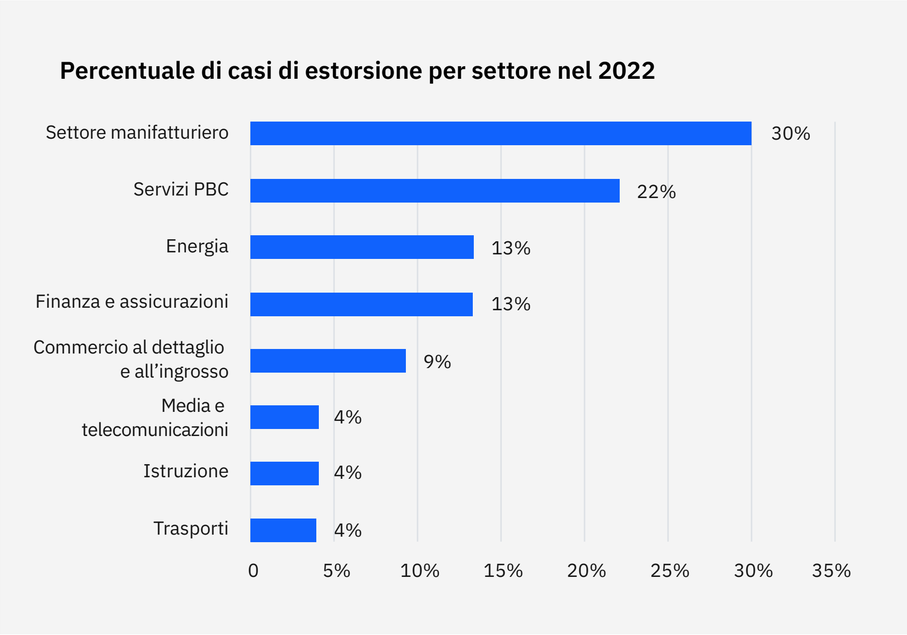


Figura 11: Percentuale dei casi di estorsione per settore osservati da X-Force in risposta agli incidenti nel 2022. La somma totale non equivale al 100% per via degli arrotondamenti. Fonte: X-Force

Il furto di dati si è piazzato secondo e ha rappresentato il 19% di tutti gli incidenti corretti da X-Force. Le mitigazioni successive a raccolte di credenziali, che hanno comportato il furto di nomi utente e password, hanno rappresentato l'11% dei casi. Gli incidenti in cui X-Force è riuscita a individuare informazioni effettivamente perdute dopo il furto sono stati meno comuni rispetto al furto stesso di dati, rappresentando l'11% dei casi. Gli impatti sulla reputazione del marchio, come l'interruzione dei servizi ai clienti, hanno contato nel 9% degli incidenti. Consulta l'Appendice per una lista completa degli impatti rilevati da X-Force. Gli incidenti che hanno impattato sulla reputazione del marchio sono stati soprattutto attacchi DDoS (distributed denial of service), che sono spesso utilizzati anche per estorcere denaro alle vittime che vogliono fermare un attacco.

Sviluppi rilevanti nelle estorsioni online[1-9]

Anno	Evento	Tattica
2013	Cryptolocker: uno delle prime grandi ondate di ransomware	Crittografia dei dati
2014	DDoS 4 Bitcoin, Armada Collective	Ransom DDoS
2015	Il Ransomware Chimera aggiunge la minaccia di fuga dei dati rubati online	Doppia estorsione
2017-18	BitPaymer e SamSam	Big game hunting (caccia grossa)
2020	Il caso Vastaamo	Tripla estorsione

Estorsioni

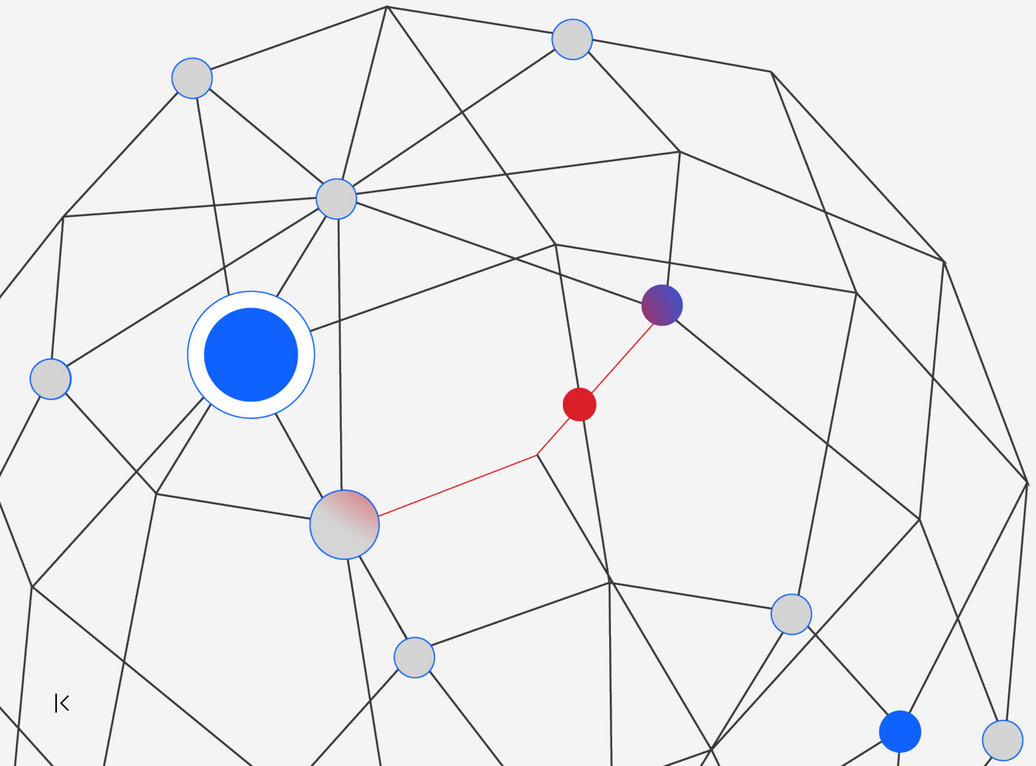
Sebbene le estorsioni oggi siano generalmente associate ai ransomware, le campagne di estorsione comprendono una varietà di metodi per mettere pressione alle vittime. Tra questi annoveriamo minacce DDoS, crittografia dei dati e, più di recente, minacce di doppia e tripla estorsione che combinano diversi elementi citati in precedenza.

Un'altra tattica sperimentata da almeno un gruppo di ransomware a partire dal 2022 è stata quella di rendere i dati rubati più accessibili alle vittime a valle. In questo modo le vittime di secondo livello, individuando i propri dati tra quelli fuoriusciti, eserciteranno pressioni sull'organizzazione obiettivo del gruppo ransomware o sui loro affiliati. X-Force prevede che, nel 2023, gli autori di minacce sperimenteranno nuove o avanzate tecniche di notifica alle vittime a valle, in modo da aumentare i possibili costi legali e reputazionali di un'intrusione.

Spesso, sia chi si deve difendere che le vittime di attacchi informatici si concentrano sugli impatti prodotti sulla loro organizzazione dagli autori della minaccia. Tuttavia, è importante considerare le intenzioni degli autori stessi, le loro possibilità e come si evolvono nel tempo. Tale approccio consente di valutare con maggior criterio quali potrebbero essere le prossime evoluzioni. Dato il ventaglio sempre più grande di opzioni di estorsione, e che l'obiettivo principale degli autori di ransomware è il guadagno economico, il team di X-Force valuta che gli autori di minacce continueranno a evolversi e ad estendere le loro metodologie di estorsione per trovare nuovi modi per spingere le vittime a pagare.

07

Sviluppi informatici della guerra russa in Ucraina



Al momento di questa pubblicazione, le attività informatiche sostenute dal governo Russo in seguito all'invasione dell'Ucraina non hanno determinato gli attacchi ampiamente diffusi e ad alto impatto originariamente temuti dai governi occidentali. Tuttavia, la Russia ha distribuito contro obiettivi ucraini un numero di wipers mai visto in precedenza, evidenziando il suo continuo investimento nei malware distruttivi. Inoltre, l'invasione ha comportato una recrudescenza delle attività di hacktivist, perseguite da gruppi schierati dall'una o dall'altra parte, e un nuovo ordine del panorama criminale informatico dell'Europa orientale.

Nell'aprile del 2022, considerato il potenziale avanzato della Russia in termini di attacchi informatici contro infrastrutture critiche dimostrato sin dal 2015, le agenzie di sicurezza informatica internazionali hanno lanciato un allarme. Questo metteva in guardia da operazioni informatiche potenzialmente significative e conseguenti interruzioni in Ucraina e altrove. Tra le minacce più significative emerse dalla valutazione di X-Force ci sono il ritorno dell'hacktivism, il malware wiper e importanti cambi di rotta nel mondo della criminalità informatica. La maggior parte di tali operazioni ha preso di mira entità presenti in Ucraina, Russia e Paesi confinanti, ma alcune si sono diffuse anche in altre aree.

In alternativa, chi si deve difendere sta sfruttando abilmente i progressi compiuti negli ultimi anni in termini di rilevamento, risposta e condivisione delle informazioni. Molti degli attacchi wiper della prima ora sono stati individuati, analizzati e resi pubblici rapidamente. Questi attacchi includono almeno otto wiper individuati e la scoperta, e l'interruzione, di un attacco informatico russo pianificato alla rete elettrica ucraina nell'aprile 2022.

Nel cyberspazio, gli effetti più sentiti della guerra in corso provengono da autoproclamati gruppi di attivisti informatici che operano a sostegno degli interessi nazionali ucraini o russi. Mentre molti gruppi si sono formati a partire dall'invasione della Russia e stanno operando contro le reti sia russe che ucraine facendone una questione politica, Killnet è uno dei più prolifici gruppi simpatizzanti per la Russia. Ha rivendicato attacchi DDoS contro servizi pubblici, governi, ministeri, aeroporti, banche e compagnie energetiche con sede presso i Paesi membri della NATO, i paesi alleati in Europa, oltre che in Giappone e Stati Uniti. Gli enti il cui profilo rientra negli obiettivi di Killnet dovrebbero valutare di tutelarsi mettendo in atto azioni di mitigazione, come l'acquisizione dei servizi di un provider di misure di mitigazione DDoS di terze parti.

Timeline degli eventi hacktivist selezionati nel 2022

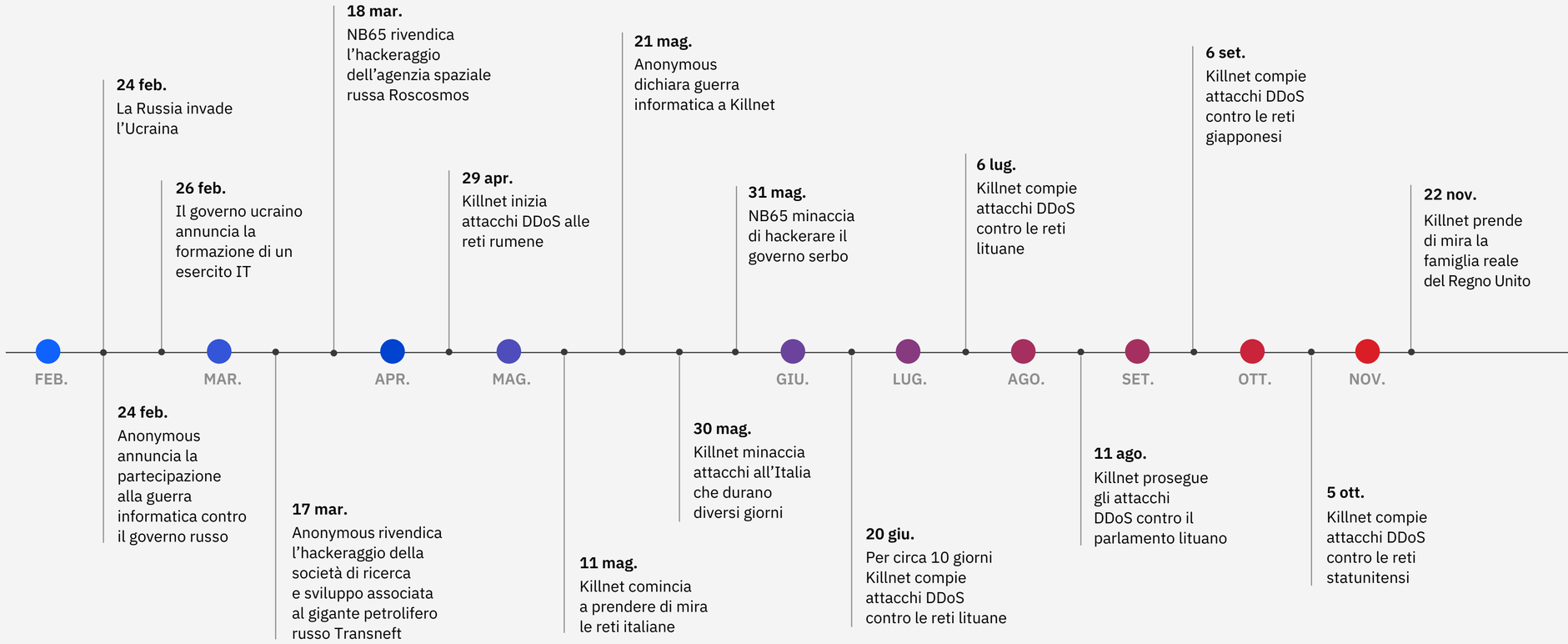


Figura 12: Immagine degli eventi hacktivist osservati finora durante il conflitto in Ucraina.
Fonte: Analisi del rapporto open source di X-Force

Wiper protagonisti nella guerra russa in Ucraina

La guerra russa in Ucraina emerge per l'utilizzo di numerose famiglie wiper distribuite contro obiettivi multipli in rapida successione e su scala mai vista prima, oltre che per il ricorso a malware contemporaneamente a operazioni militari di tipo cinetico.

Tali distribuzioni comprendono almeno nove nuovi wiper: AcidRain, WhisperGate, HermeticWiper, IsaacWiper, CaddyWiper, DoubleZero, AwfulShred, OrcShred e SoloShred. Si tratta di wiper utilizzati soprattutto contro reti ucraine da prima dell'invasione fino alle prime fasi della guerra, da gennaio a marzo 2022. Sebbene i wiper siano stati utilizzati anche in passato, si trattava per lo più di campagne autonome contro un numero limitato di obiettivi. Tuttavia, le evidenti eccezioni di WannaCry e NotPetya, che si sono diffuse indiscriminatamente dopo gli effetti sulle loro vittime iniziali, sollevano la preoccupazione che tali wiper si diffondano ulteriormente o vengano riutilizzati altrove per operazioni malevoli.

X-Force continua a ritenere che gli autori di minacce informatiche sostenuti dal governo russo costituiscano ancora un'importante minaccia a reti di computer e infrastrutture critiche di tutto il mondo. Tale opinione è motivata dalla lunga durata delle operazioni informatiche russe mirate alle reti ucraine, europee, NATO e statunitensi e dagli attacchi portati dai gruppi di minaccia russi a partire sin dal 2015.

Scontri tra gruppi di criminalità informatica russi

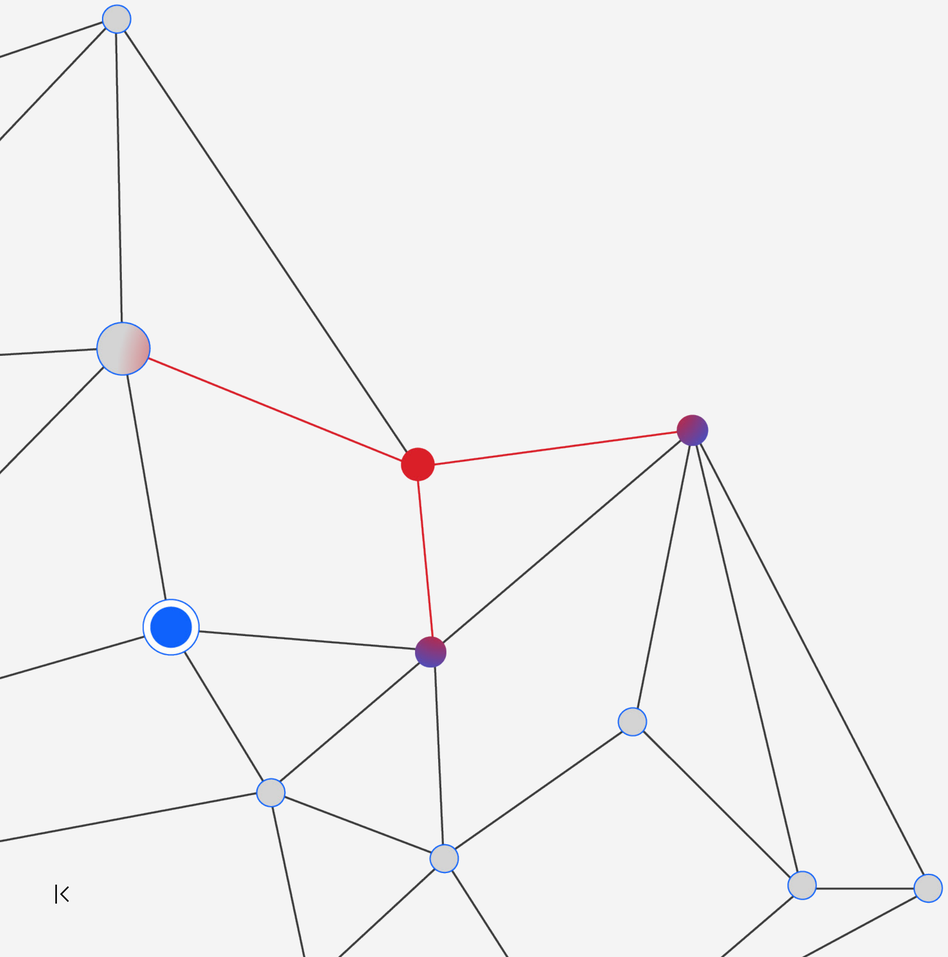
Il 2022 è stato un anno frenetico per ITG23, una delle più note organizzazioni di criminali informatici russi, conosciuta soprattutto per aver sviluppato il trojan bancario Trickbot e il ransomware Conti. All'inizio del 2022, dopo essersi pubblicamente schierato a favore della guerra russa, il gruppo ha subito una serie di importanti perdite. Conosciute come ContiLeaks e TrickLeaks, tali perdite hanno determinato la pubblicazione di migliaia di messaggi di chat e il doxing di numerosi membri del gruppo. X-Force ha comprovato come ITG23 abbia avviato i propri attacchi sistematici a partire da metà aprile fino ad almeno metà giugno del 2022, un cambiamento senza precedenti, poiché il gruppo non aveva mai preso di mira l'Ucraina prima.

Inoltre, il gruppo ha apparentemente ritirato due delle sue famiglie di malware di più alto profilo, Trickbot e Bazar, e ha interrotto l'operazione ransomware Conti. Numerosi rapporti hanno suggerito che all'interno del gruppo potrebbe verificarsi un significativo rimpasto del personale, con scissioni in diverse fazioni e alcuni membri che si trasferiscono del tutto.

L'interruzione di Trickbot e Bazar, responsabili di un importante numero di infezioni nel 2021, ha comportato un vuoto rapidamente colmato da famiglie di malware come Emotet, IcedID, Qakbot e Bumblebee. Prima della sua chiusura, ITG23 stava ancora distribuendo il ransomware Conti in modo prolifico, rappresentando un terzo di tutti i ransomware a cui X-Force si è trovato a rispondere durante il primo trimestre del 2022.

Il gruppo ha rilasciato anche una nuova versione del suo malware Anchor, una backdoor furtiva tradizionalmente schierata contro obiettivi di alto profilo. La versione aggiornata rilevata da X-Force, e chiamata AnchorMail, è caratterizzata da un nuovo meccanismo di comunicazione di comando e controllo (C2) basato su e-mail. Il server C2 usa i protocolli Simple Mail Transfer Protocol Secure (SMTPS) e Internet Message Access Protocol Secure (IMAPS), e il malware comunica con il server inviando e ricevendo messaggi di posta elettronica appositamente realizzati.

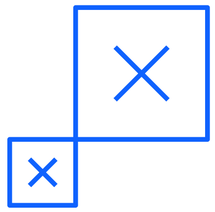
Il panorama dei malware



Aumento dei worm diffusi via USB

In seguito ai tentativi di infezioni Raspberry Robin osservati da X-Force mentre tentavano di colpire le organizzazioni a metà maggio 2022, il misterioso worm ha iniziato a diffondersi rapidamente all'interno delle reti delle vittime da utenti che condividevano dispositivi USB (Universal Serial Bus). Agli inizi di giugno le infezioni hanno registrato un'impennata ed entro i primi di agosto Raspberry Robin ha raggiunto il picco del 17% dei tentativi di infezione rilevati da X-Force. Tale picco è stato individuato nei settori di olio e gas, manifatturiero e dei trasporti. Per questi settori il 17% dei tentativi di infezione rappresenta un numero importante, dato che la stessa varietà di malware è stata registrata da meno dell'1% di tutti i clienti X-Force. X-Force ha osservato una maggiore attività di Raspberry Robin anche tra settembre e novembre 2022.

La diffusione di worm basati su USB è abilitata attraverso il social engineering e, per infettare efficacemente, richiede accesso fisico a una rete o a un endpoint da parte di un utente legittimo o attraverso altri mezzi. X-Force consiglia di assicurarsi che i propri strumenti di sicurezza blocchino i malware basati su USB, implementando formazione di sensibilizzazione sulla sicurezza e disabilitando le funzionalità di esecuzione automatica per qualsiasi supporto rimovibile. In ambienti particolarmente sensibili, come OT o dove esistono interruzioni di flusso, sarebbe più sicuro proibire del tutto l'uso di unità flash USB. Se non è possibile farlo, oltre a quanto suggerito più sopra, controllare con estrema attenzione il numero di dispositivi portatili che possono essere utilizzati nel proprio ambiente.



Aumentano i malware basati su linguaggio Rust

Durante il 2022, la popolarità del linguaggio di programmazione Rust è cresciuta costantemente tra gli sviluppatori di malware, per via del suo supporto cross-platform e dei bassi tassi di rilevamento antivirus rispetto ad altri linguaggi più comuni. In maniera simile al linguaggio Go, il malware trae vantaggio da un processo di compilazione più complicato che può richiedere più tempo all'analisi da parte dei reverse engineer. Alcuni sviluppatori di ransomware hanno rilasciato versioni Rust dei loro malware, tra questi BlackCat, Hive, Zeon e più di recente RansomExx. Inoltre, X-Force ha analizzato un ITG23 crypter scritto in Rust, insieme alla famiglia CargoBay di backdoor e downloader.
La crescente popolarità di Rust evidenzia come, all'interno dell'ecosistema ransomware, si presti costante attenzione all'innovazione per eludere i sistemi di rilevamento delle minacce.

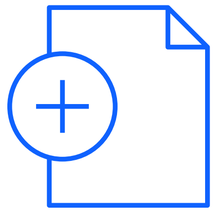
Vidar InfoStealer

X-Force ha notato un improvviso flusso di malware Vidar InfoStealer, cominciato a giugno 2022 e continuato fino ai primi mesi del 2023. Osservato per la prima volta nel 2018, Vidar è un Trojan ruba-informazioni distribuito come MaaS (malware as a service). Solitamente il Trojan viene eseguito quando l'utente clicca su un link, un allegato o uno spam malevolo (malspam). A causa del suo ampio set di funzionalità, Vidar può essere utilizzato per recuperare un'ampia varietà di informazioni presenti sul dispositivo, tra cui informazioni relative a carte di credito, nomi utente, password e file, nonché per acquisire schermate del desktop dell'utente. Vidar può anche sottrarre portafogli di cripto-valuta Bitcoin o Ethereum.

Tipicamente, dietro gli attacchi attraverso info-stealer (malware che rubano informazioni) ci sono motivazioni economiche. I dati rubati vengono analizzati e qualsiasi informazione di valore viene raccolta e organizzata in un database. Successivamente, tale database può essere venduto sul dark web o tramite l'app di messaggistica privata Telegram. Le informazioni possono essere utilizzate per compiere diversi tipi di frodi, come la richiesta di prestiti bancari o carte di credito, l'acquisto di articoli online, oppure avanzare richieste di risarcimento fraudolente all'assicurazione sanitaria.

Gli autori di minacce possono utilizzare le credenziali di accesso compromesse per entrare in account aziendali e servizi da remoto. Il costo medio per l'utilizzo di un info stealer è di circa 250 dollari al mese e sono gli utenti a distribuire il malware scelto. X-Force registra regolarmente trattative di mercato in cui si tenta di vendere gli accessi rubati dai malware info stealer per un prezzo che va dai 10 ai 75 dollari. Una volta ottenuto l'accesso, gli autori di minacce possono facilmente utilizzare i privilegi dell'account violato come punto di partenza per avviare ulteriori attività malevoli.

L’evoluzione dei meccanismi per veicolare i malware



Sono sempre più comuni i malware veicolati attraverso documenti infetti di Microsoft Office, solitamente allegati a e-mail di phishing. Gli sviluppatori di programmi malware hanno creato dei documenti contenenti macro dannose progettate per eseguire malware una volta aperti. L’utilizzo di macro a tali propositi è divenuto così diffuso che i prodotti Microsoft Office sono arrivati a includere messaggi di sicurezza ogni volta che si aprono documenti con attivazione macro. Nel luglio 2022, Microsoft ha iniziato a bloccare l’esecuzione predefinita delle macro nei documenti ricevute via e-mail o attraverso la rete.

Man mano che i sistemi di difesa hanno aumentato le proprie capacità di rilevamento e prevenzione, gli autori di minacce hanno sentito la necessità di abbandonare le applicazioni Visual Basic (VBA, Visual Basic Application) per spostarsi verso un format macro più datato all’interno di Excel, conosciuto come Macro 4.0. I documenti Excel malevoli sono stati utilizzati per diverso tempo. Tuttavia, la maggior parte dei meccanismi di sicurezza sono stati realizzati intorno alle macro VBA interne a un documento Excel. Per un certo periodo, le macro di Excel Macro 4.0 hanno rappresentato un buon mezzo per eludere i sistemi di rilevamento. Nello stesso periodo, alcuni autori di minacce hanno iniziato a inviare e-mail i cui collegamenti rinviavano le vittime a un sito dropper dove scaricare i documenti infetti, invece di inviarli come allegato di posta elettronica. Quando Microsoft ha apportato le modifiche che consentivano agli amministratori di disabilitare Macro 4.0 e bloccare anche l’esecuzione delle macro scaricate da Internet, gli autori di minacce sono stati costretti a cambiare di nuovo tattica.

In seguito alle modifiche apportate da Microsoft, ci sono ancora molti programmatori di malware che continuano ad affidarsi a documenti Microsoft Office con attivazione macro, ma i gruppi più sofisticati hanno adottato una catena infettiva più evoluta e complessa. Queste tattiche più recenti si affidano a una combinazione di file HTML che all’interno presentano un file binario incorporato, o un file compresso protetto da password. Questi file contengono anche un’immagine ISO che a sua volta può contenere un file LNK, CMD o di altro tipo che è poco probabile possa essere inviato a un destinatario di posta elettronica o scaricato da Internet. Altri includono l’inserimento di template o lo sfruttamento delle vulnerabilità da remoto. CVE-2021-40444, una vulnerabilità in Microsoft HTML (MSHTML) legata all’esecuzione da remoto dei codici, è un esempio di componente software utilizzato per eseguire il rendering di pagine Web in Microsoft Windows in modo da eseguire il malware, anziché fare affidamento sulle macro.

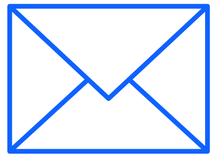
I dati sullo spamming evidenziano la minaccia ransomware e illustrano ulteriormente le tendenze macro

X-Force ha analizzato le tendenze delle e-mail di phishing e spam per comprendere meglio la loro efficacia complessiva e l'uso che ne fanno gli autori di minacce. L'indagine ha scoperto che le e-mail di spam sono state regolarmente utilizzate durante tutto l'anno per veicolare malware come Emotet, Qakbot, IcedID e Bumblebee, che determinavano spesso infezioni ransomware.

Malware[10-18]	**Ransomware**
Trickbot	*Conti*
Bazarloader	*Conti*, Diavol
IcedID	*Conti*, Quantum
Bumblebee	*Conti*, Diavol, Quantum
Emotet	*Conti*, BlackCat, Quantum
Qakbot	*REvil*, *Conti*, Black Basta
SocGholish	LockBit

I dati di questa tabella riguardano il periodo che va da fine 2021 alla pubblicazione di questo report. I caratteri corsivi indicano che il malware o il ransomware sono stati visti nel 2022, ma non sono stati osservati da X-Force almeno da ottobre 2022.

Nel settembre 2022, X-Force ha individuato un'ondata di attività Qakbot che per compromettere le vittime utilizzava attacchi smuggling HTML. Tali infezioni sono collegate a un'ampia serie di attività che seguono la compromissione, tra cui ricognizione, raccolta di informazioni e distribuzione di playload aggiuntivi. Durante il 2022, le infezioni Qakbot non controllate hanno portato a numerose infezioni da Black Basta. X-Force ha visto gli attacchi ransomware rivendicati sul sito del gruppo di ransomware Black Basta diminuire notevolmente durante l'interruzione delle attività di phishing di Qakbot nell'estate del 2022. Allo stesso modo, X-Force prevede che una ripresa delle attività di Qakbot sarà correlata all'aumento delle vittime di ransomware.



L’aggiramento delle macro

In seguito alle modifiche alle macro apportate da Microsoft a partire dall’ottobre 2021, l’utilizzo di file ISO e LNK è risultato essere una tattica piuttosto diffusa per infettare le organizzazioni vittime di attacchi. Tattica che include sia la consegna diretta dei payload attraverso quei file contenitore, sia l’offuscamento dei file con attivazione macro al loro interno.

- I file ISO e i file compressi sono stati utilizzati per aggirare l’attributo MOTW (mark of the web) utilizzato da Microsoft per consentire agli obiettivi di attivare macro dannose. Mentre i file ISO o compressi risulteranno essere scaricati da Internet, non accadrà lo stesso per l’allegato con attivazione macro al suo interno, consentendo agli autori di minacce di perseguire l’attacco.
- Un altro metodo per aggirare le restrizioni alle macro è di includere i playload direttamente nei file LNK che, una volta cliccati, lanciano i comandi arbitrari perlopiù usati per scaricare o caricare gli stage successivi. Prima del 2022, si era registrata una sola campagna che utilizzava questa tattica, nel febbraio 2021. X-Force l’ha vista ripresentarsi per la prima volta tra febbraio e marzo 2022 e attualmente continua a osservarla con regolarità.

Ulteriori tendenze rilevate da X-Force nelle campagne di spam degli autori di minacce includono l’aumentato utilizzo degli archivi compressi crittografati inviati come allegato e del thread hijacking.

- Le estensioni compresse crittografate, che il software antivirus riesce a rilevare e segnalare come dannose con più difficoltà, nel 2022 sono state scoperte più di frequente. Nel 2022, il numero medio delle e-mail di spam contenenti simili allegati e consegnate ogni settimana è aumentato di nove volte rispetto ai dati a partire da aprile 2021.
- Il thread hijacking, attraverso cui gli autori di minacce si inseriscono nei thread di posta elettronica già esistenti, è una tattica di lunga data utilizzata per aumentare la credibilità degli spam e indurre le vittime ad agire. Rispetto alla gran parte del 2021, nel 2022 tale tattica ha registrato una decisa crescita, affievolendosi in primavera: una tendenza che X-Force stima essere in gran parte riconducibile allo spamming di Emotet.

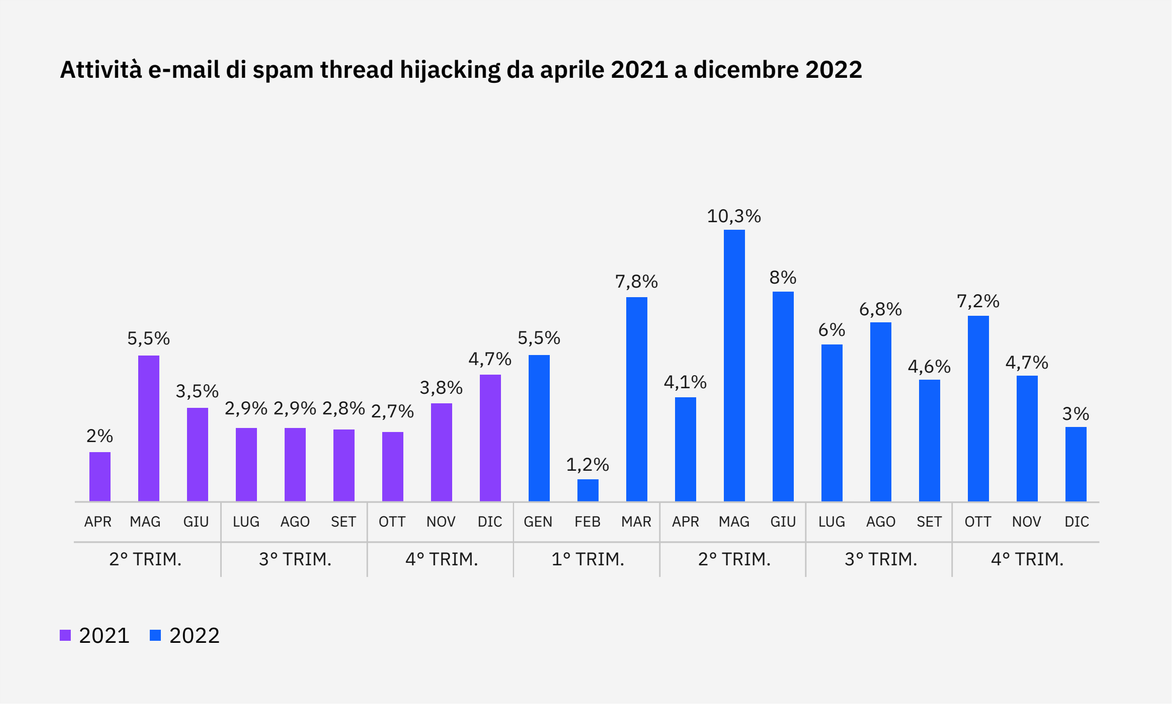


Figura 13: Il grafico mostra la percentuale mensile di tutti i tentativi di thread hijacking rilevati nei dati X-Force a partire da aprile 2021. Fonte: X-Force

- Dopo l'interruzione del gennaio 2021, Emotet ha fatto il suo ritorno nel novembre 2021. Ha proseguito la propria attività nel 2022, prendendosi una pausa di quasi quattro mesi a partire da metà luglio, ed è ricomparso per quasi due settimane nel novembre 2022.

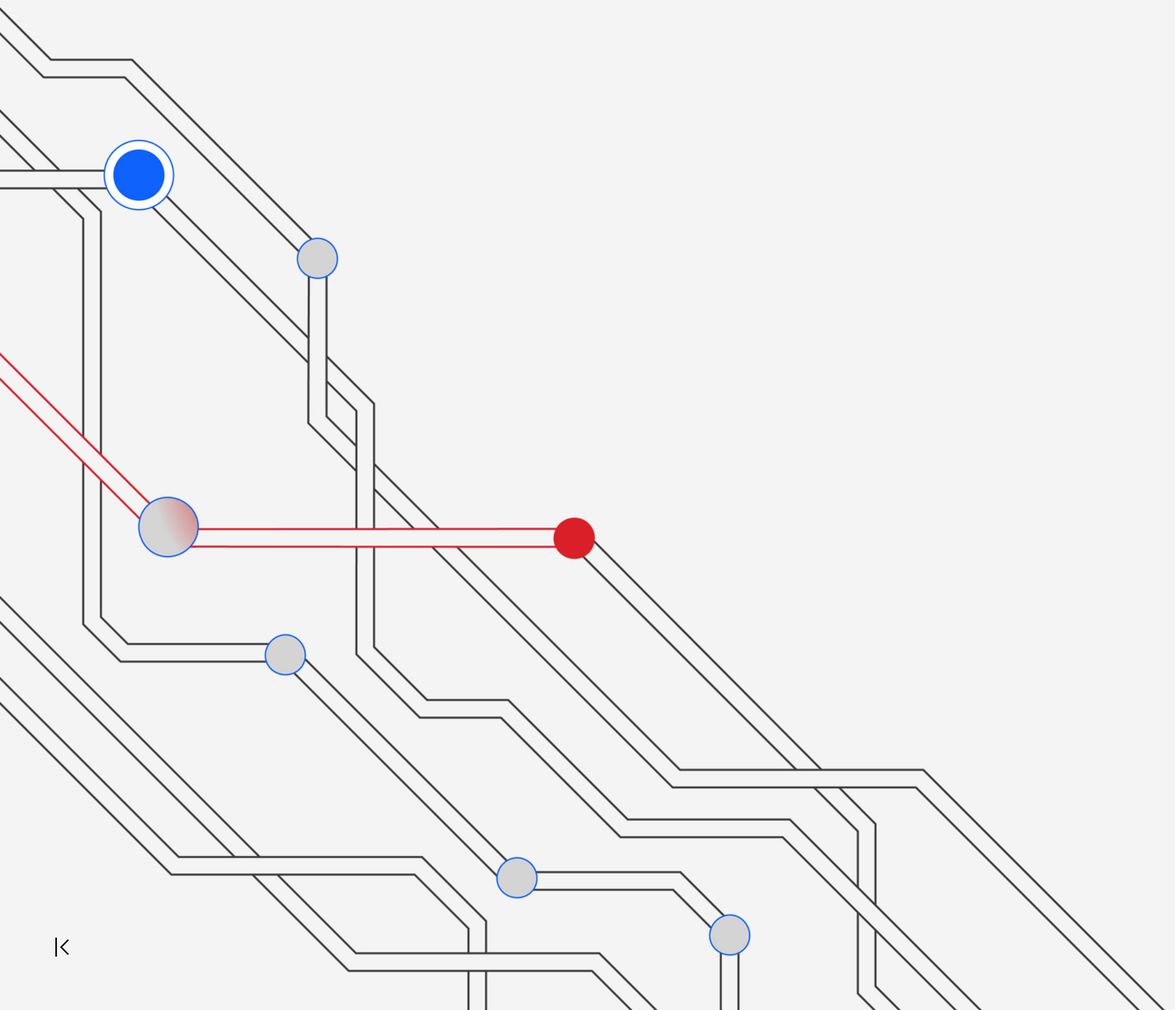
- Nel 2022, i dati hanno mostrato quasi il doppio dei tentativi regolari ogni mese, rispetto ai dati disponibili a partire da aprile 2021. Il thread hijacking ha avuto un andamento instabile fino a maggio 2022 e il suo declino nella seconda metà dell'anno coincide grossomodo con l'inattività di Emotet.

- E-mail spam portatrici di Emotet, Qakbot e IcedID hanno fatto largo impiego di thread hijacking. La ricomparsa di Emotet nel novembre 2021 ha contribuito all'instabile aumento registrato fino a maggio 2022. Il generale declino nella tarda metà dell'anno coincide con l'interruzione di Emotet da luglio fino a ottobre e al breve ritorno nel novembre 2022.

- Tenere traccia dei thread hijacking e distinguerli accuratamente dalle istanze dei malintenzionati semplicemente aggiungendo un'intestazione di risposta all'oggetto di un'e-mail di spam è difficile e probabilmente lo diventerà ancora di più. Per esempio, alcuni autori di minacce hanno cominciato a rimuovere l'intestazione "Re:" davanti all'oggetto delle e-mail, probabilmente perché consapevoli che tale intestazione può essere utilizzata per tracciare la loro attività.

09

Minacce a tecnologie operative (OT) e sistemi di controllo industriali



Minacce alle tecnologie operative

Il 2022 ha registrato la scoperta di due nuovi malware specifici per OT, Industroyer2 e INCONTROLLER, conosciuto anche come PIPEDREAM, e la divulgazione di molte vulnerabilità OT chiamate OT: ICEFALL. Il panorama delle minacce informatiche contro OT si sta espandendo drammaticamente e i proprietari e gli operatori di asset OT devono essere profondamente consapevoli dei cambiamenti in corso.

Per ottenere maggiori informazioni su come gli autori di minacce stiano cercando di compromettere i clienti dei settori che implicano l'uso di sistemi OT, X-Force ha esaminato più da vicino gli attacchi di rete specificamente rivolti a OT e i dati IR. I dati sugli attacchi in rete mostrano che, negli ambienti IT e OT di questi settori, aggressioni di forza bruta, utilizzo di standard di crittografia deboli e obsoleti e password deboli o predefinite costituiscono allarmi diffusi.

Tra i dati riferiti agli attacchi di rete specifici di ICS (Incident Command System), gli avvisi di probabili tentativi di forza bruta sono stati i più comuni, subito dopo sono risultati quelli di crittografia debole. Gli avvisi di crittografia debole più frequenti riguardavano l'uso continuato di Transport Layer Security (TLS) 1.0, un metodo di crittografia obsoleto e non sicuro disapprovato nel marzo 2021. Sebbene il governo degli Stati Uniti raccomandi una riconfigurazione per utilizzare TLS 1.2 o 1.3, le linee guida del National Institute of Standards and Technology (NIST) affrontano la realtà in modo più approfondito. La realtà è che i sistemi più datati, per garantire un funzionamento continuo, potrebbero aver bisogno di utilizzare una versione di crittografia più debole. Sono stati numerosi anche gli avvisi di password deboli o predefinite, soprattutto considerando che si tratta di procedure elementari

Vulnerabilità che facilitano gli attacchi di forza bruta. La scansione diffusa e probabilmente indiscriminata delle vulnerabilità interne ed esterne è stata il tentativo di attacco più comune contro i settori che implicano l'uso di sistemi OT. I dati hanno rivelato che tutt'oggi vecchie vulnerabilità e minacce sono ancora rilevanti. Un gruppo di vulnerabilità scoperte nel 2021 da Cisco Talos nel software di monitoraggio Advantech R-SeeNet ha innescato, nel 2022, un'esigua maggioranza di avvisi in seguito alla scansione delle vulnerabilità nei settori OT. Tali vulnerabilità potevano consentire agli aggressori di eseguire codici o comandi arbitrari.

La seconda vulnerabilità più comune, tuttavia, risale al 2016, una vulnerabilità di by-pass del filtro nell'applicazione Trihedral VTScada, CVE-2016-4510, che poteva permettere agli utenti non autenticati di inviare richieste HTTP per accedere ai file. A evidenziare ulteriormente il rischio rappresentato dalle minacce di vecchia data sono alcuni attacchi, come WannaCry e Confickern, che rappresentano ancora una significativa minaccia per OT.

Il manifatturiero è ancora il settore OT più bersagliato

Osservando il sottoinsieme degli incidenti nei settori che implicano l'uso di sistemi OT, i dati affermano che il settore più attaccato nel 2022 è stato quello della produzione manifatturiera. Questo settore è stato preso di mira nel 58% degli incidenti corretti da X-Force La distribuzione di backdoor è stata la principale azione per raggiungere l'obiettivo, individuata nel 28% dei casi nel settore manifatturiero. Settore particolarmente appetibile per gli autori di ransomware, probabilmente per la sua bassa tolleranza ai tempi di indisponibilità.

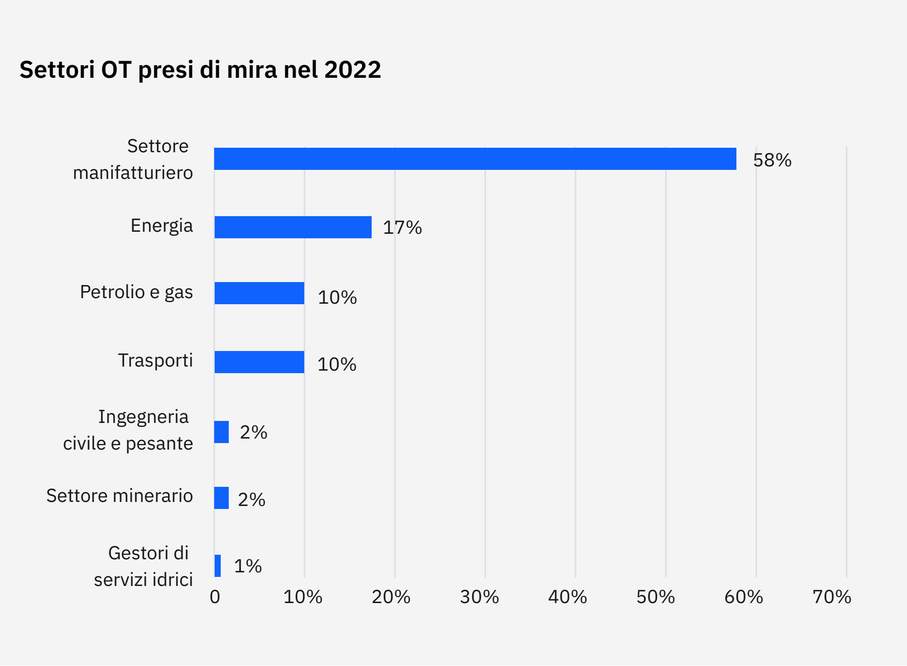


Figura 14: Percentuali di casi IR per settori a uso di sistemi OT a cui X-Force ha risposto nel 2022.
Fonte: X-Force

Osservando i vettori di accesso iniziale nei casi riguardanti i settori a uso di sistemi OT, lo spear phishing è risultato nel 38% dei casi, tra i quali l'utilizzo di allegati costituiva il 22% dei casi, l'uso di link il 14%, mentre lo spear phishing come servizio il 2% dei casi. Lo sfruttamento di applicazioni rivolte al pubblico ha occupato il secondo posto con il 24% dei casi, seguendo la più ampia tendenza del settore. Tra gli incidenti relativi a questi settori ci sono stati anche numerosi rilevamenti di backdoor, nel 20%, e di ransomware, nel 19% dei casi. A livello di impatto al primo posto rimangono le estorsioni, con il 29% dei casi, con il furto di dati subito dietro con il 24% dei casi.

Un'altra importante vulnerabilità sfruttata contro le OT è stata la mancanza di una corretta segmentazione tra le reti OT e IT. Per ottenere accesso ad ambienti OT isolati, il team di X-Force Red Adversary Simulation Services prende regolarmente di mira la segmentazione debole. Questi ambienti includono il targeting di server di passaggio, workstation con host dual-homed e server di report, come storici dei dati che espongono servizi Web e SQL da OT alle reti IT aziendali. Segmentare in maniera corretta queste porzioni delle reti e monitorare da vicino le comunicazioni tra di esse può contribuire a proteggere gli asset.

Tendenze geografiche

Nel 2022, per il secondo anno di fila, la regione Asia-Pacifico detiene il primo posto come regione più attaccata, totalizzando il 31% degli incidenti a cui X-Force ha dovuto rispondere. Subito dietro, l'Europa con il 28% degli attacchi e il Nord America con il 25% degli incidenti. Asia-Pacifico ed Europa hanno registrato le percentuali più elevate di casi, crescendo rispettivamente di cinque e quattro punti percentuali rispetto ai dati del 2021, mentre nel Medio Oriente si è registrato un significativo calo dal 14% al 4%.

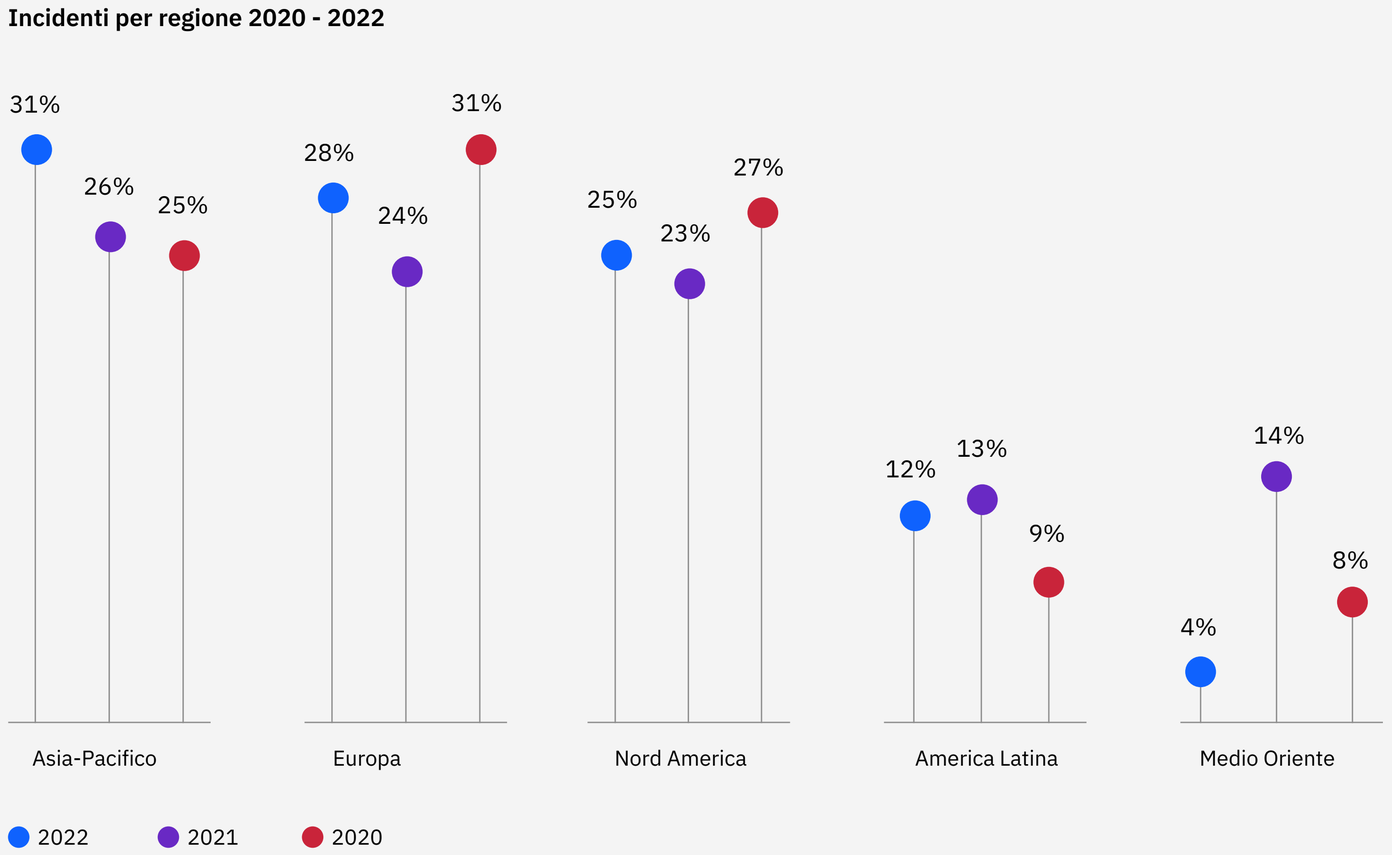


Figura 15: Percentuale di casi IR a cui X-Force ha risposto dal 2020 al 2022 (per regione). Fonte: X-Force

#1 | Asia-Pacifico

La regione Asia-Pacifico, e in special modo il Giappone, ha rappresentato l'epicentro del picco di Emotet nel 2022. Seppur non direttamente connessa alla guerra in Europa, l'ondata dei casi di Emotet in Giappone è avvenuta in concomitanza con l'invasione russa in Ucraina, che altri ricercatori della cybersecurity community ritengono abbia contribuito alla significativa attività di Emotet in quel periodo. Le campagne di spamming sono state individuate in diversi settori, con la maggior parte dei casi registrati nei settori manifatturiero e finanziario-assicurativo. Emotet viene veicolato soprattutto attraverso campagne di spamming, utilizzando titoli e oggetti capaci di catturare l'attenzione.

In questa regione il manifatturiero è in cima alla lista dei settori attaccati, 48% dei casi; distaccato, al secondo posto, il settore finanziario-assicurativo con il 18%.

Nella regione, lo spear phishing attraverso allegati è stato il principale vettore di infezione, con il 40% dei casi, seguito dallo sfruttamento di applicazioni rivolte al pubblico al 22%. I casi relativi a servizi remoti esterni e collegamenti di spear phishing occupano a pari merito il terzo posto con il 12% dei casi.

Le distribuzioni di backdoor sono state le più comuni azioni per raggiungere l'obiettivo, con il 31% dei casi nella regione. Al secondo posto i Ransomware con il 13% e al terzo i maldoc con il 10% dei casi. L'impatto più frequente è rappresentato dall'estorsione, osservata nel 28% dei casi. Al secondo posto le conseguenze sulla reputazione del marchio, con il 22%, seguite al terzo dal furto di dati nel 19%.

In Giappone sono stati totalizzati il 91% dei casi di tutta la regione Asia-Pacifico, nelle Filippine il 5% e in Australia, India e Vietnam l'1,5% ciascuno.

La regione Asia-Pacifico ha registrato il maggior numero di attacchi nel settore manifatturiero, con il 48% dei casi.

#2 | Europa

L’Europa ha registrato un significativo aumento nella distribuzione di backdoor, a cominciare dal marzo 2022, subito dopo l’invasione russa in Ucraina. Nella regione la distribuzione di backdoor ha totalizzato il 21% dei casi, con i ransomware all’11%. Gli strumenti di accesso da remoto sono stati individuati nel 10% degli incidenti a cui X-Force ha dovuto rispondere. Per quanto riguarda l’impatto sui clienti, il 38% dei casi osservati in Europa da X-Force erano relativi a estorsione, il 17% a furto dati e il 14% a raccolta dati. L’Europa è stata la regione più colpita dai casi di estorsione, rappresentando il 44% di tutti i casi di estorsione osservati.

Lo sfruttamento di applicazioni rivolte al pubblico è stato il principale vettore di infezioni utilizzato contro le organizzazioni europee, gravando sul 32% di tutti gli incidenti corretti da X-Force nella regione, alcuni dei quali avevano causato infezioni ransomware. Al secondo posto, la violazione di account locali validi, con il 18%, seguita dallo spear phishing con il 14%, decisamente in calo rispetto al 42% del 2021. Tale diminuzione dei link di spear phishing potrebbe essere conseguenza di una maggiore consapevolezza da parte degli utenti, migliori sistemi di sicurezza e-mail, o sistemi di difesa più efficaci nel bloccare i malware dopo l’installazione.

Per quanto riguarda i settori più attaccati, servizi professionali, aziendali e per i consumatori a pari merito con finanza e assicurazioni rappresentano ognuno il 25% dei casi a cui X-Force ha risposto. Al secondo posto il settore manifatturiero con il 12% dei casi, mentre energetico e sanitario si assestano entrambi al terzo posto con il 10%.

Il Regno Unito è risultato il Paese più attaccato in Europa, totalizzando il 43% dei casi. La Germania ha totalizzato il 14%, il Portogallo il 9%, l’Italia l’8% e la Francia il 7% dei casi. “X-Force ha risposto a un più piccolo numero di casi anche in Norvegia, Danimarca, Svizzera, Austria, Grecia, Groenlandia, Spagna e Serbia.

Il Regno Unito è risultato il Paese più attaccato in Europa, totalizzando il 43% dei casi.

#3 | Nord America

X-Force ha osservato un leggero aumento nel numero di incidenti verificatisi nel Nord America, che è passato dal 23% dei casi totali nel 2021 al 25% nel 2022.

Le compagnie energetiche sono salite in cima all'elenco delle principali vittime in Nord America, avendo subito il 20% di tutti gli attacchi a cui X-Force ha dovuto rispondere nel 2022. Al secondo posto, seguono i settori manifatturiero e del commercio al dettaglio e all'ingrosso con il 14% dei casi ciascuno. Mentre il commercio al dettaglio e all'ingrosso ha mantenuto una posizione simile a quella del 2021, rispetto allo stesso anno i numeri che riguardano la manifattura hanno rappresentato un calo del 50%. Nel 2022, i servizi professionali, aziendali e per i consumatori si sono posizionati al terzo posto con il 12%, tra incrementi dei casi di ransomware e altri casi correlati a malware.

I principali vettori di infezione individuati sono stati lo sfruttamento di applicazioni rivolte al pubblico, nel 35%, e gli allegati spear phishing nel 20% dei casi. Gli incidenti ransomware hanno rappresentato il 23% dei casi, alcuni dei quali sono risultati rilevamenti di infezioni persistenti di WannaCry o Ryuk risalenti al 2018 o al 2019, fatto che evidenzia l'importanza di una corretta pulizia a seguito di certi eventi. Nella regione, il 12% dei casi sono stati costituiti da botnet, con backdoor e BEC entrambi al terzo posto con il 10% ciascuno.

Per quanto riguarda i principali impatti causati dagli autori di minacce, il primo posto è occupato dalla raccolta di credenziali, che ha rappresentato il 25% degli incidenti corretti da X-Force in Nord America. Secondo posto, a pari merito, perdita e furto di dati, con il 17% ciascuno, seguiti dalle estorsioni con il 13% dei casi.

Gli Stati Uniti hanno totalizzato l'80% degli attacchi nella regione, contro il 20% del Canada.

Con il 20% dei casi, le organizzazioni più attaccate in Nord America sono state le compagnie energetiche.

#4 | America Latina

Ai fini di questo report, per America Latina IBM intende Messico, Centro e Sud America.

Gli incidenti in America Latina vanno in controtendenza rispetto alle tendenze globali, riportando il commercio al dettaglio e all'ingrosso come il settore più attaccato, con il 28% dei casi corretti da X-Force, in risalita rispetto al secondo posto del 2021. Il secondo settore più bersagliato è stato quello finanziario-assicurativo, con il 24% dei casi, seguito dall'energetico con il 20%.

I ransomware hanno distanziato per numero le altre tipologie di attacco, totalizzando il 32% dei casi a cui X-Force ha dovuto rispondere. La distribuzione di backdoor è stata la seconda azione per raggiungere l'obiettivo più individuata, con il 16% dei casi, mentre BEC e thread hijacking via e-mail si sono piazzati al terzo posto con l'11% ciascuno. Estorsioni e furto dati sono stati gli impatti più osservati nella regione, con il 27%, mentre le perdite finanziarie hanno segnato il 20% dei casi. Al terzo posto pari merito, perdita e distruzione dei dati entrambi con il 13% dei casi.

Tra i principali vettori di accesso, troviamo i servizi esterni da remoto, con il 30%, e lo sfruttamento delle applicazioni rivolte al pubblico con il 20% dei casi. Compromissioni delle unità rimovibili, hardware aggiuntivi, account di dominio validi, account locali validi e allegati di spear phishing hanno rappresentato ciascuno il 10% dei casi.

Tra tutti i casi a cui X-Force si è trovato a rispondere in America Latina, il Brasile ha inciso per il 67%, la Colombia per il 17% e il Messico per l'8%. Perù e Cile si dividono il restante 8%.

In America Latina, il Brasile ha totalizzato il 67% dei casi corretti da X-Force.

#5 | Medio Oriente e Africa

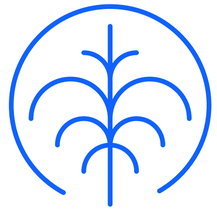
Ai fini di questo report, IBM considera la regione Medio Oriente e Africa inclusiva di Levante, Penisola Arabica, Egitto, Iran, Iraq e dell'intero continente africano.

X-Force ha individuato la distribuzione di backdoor nel 27% dei casi a cui ha dovuto rispondere in questa regione durante il 2022. Il secondo attacco più utilizzato vede ransomware e worm pari merito con il 18% ciascuno. Estorsioni e perdite finanziarie rappresentano ognuna metà degli impatti riconducibili agli incidenti individuati nella regione nel 2021.

Per ottenere accesso iniziale, i link di spear phishing sono stati utilizzati nei due-terzi dei casi, mentre i supporti rimovibili hanno inciso per il restante terzo degli incidenti corretti da X-Force in Medio Oriente e Africa. Nel 2022, in Medio Oriente e Africa il settore più colpito è risultato quello finanziario-assicurativo, che ha totalizzato il 44% degli incidenti con un leggero calo rispetto al 48% del 2021. I servizi professionali, aziendali e per i consumatori hanno subito il 22% degli attacchi, con il manifatturiero e l'energetico al terzo posto con l'11% ciascuno.

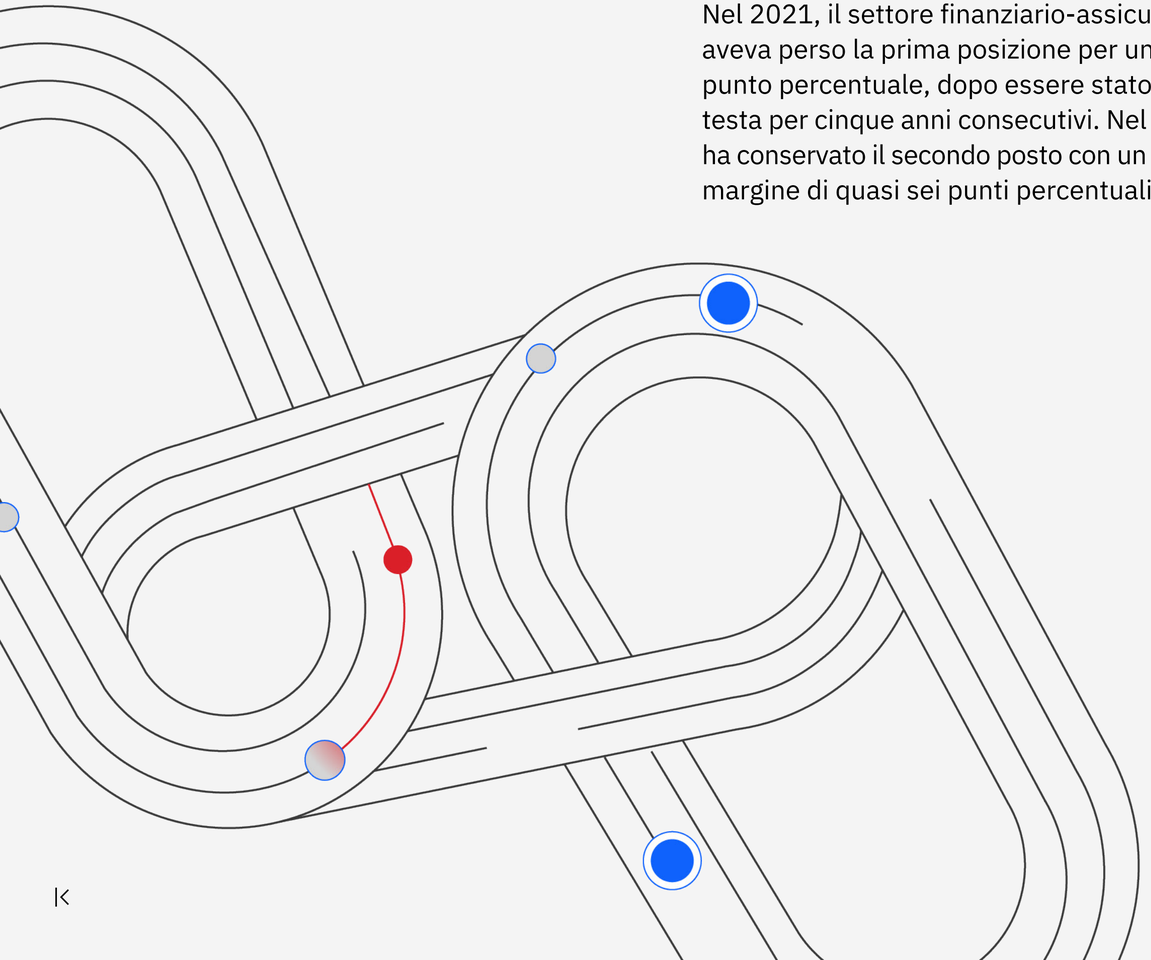
L'Arabia Saudita ha registrato due terzi dei casi a cui X-Force ha dovuto rispondere. Qatar, Emirati Arabi Uniti e Sudafrica si dividono i restanti casi.

La distribuzione di backdoor è risultato l'attacco più diffuso nella regione, con il 27% dei casi.



Tendenze settoriali

Secondo i dati di risposta di X-Force, per il secondo anno consecutivo il settore manifatturiero è risultato il più attaccato. Nel 2021, il settore finanziario-assicurativo aveva perso la prima posizione per un solo punto percentuale, dopo essere stato in testa per cinque anni consecutivi. Nel 2022, ha conservato il secondo posto con un ampio margine di quasi sei punti percentuali.



Percentuali di attacchi per settore, 2018 - 2022

Settore	2022	2021	2020	2019	2018
Produzione manifatturiera	24,8%	23,2	17,7	8	10
Finanza e assicurazioni	18,9%	22,4	23	17	19
Servizi professionali, aziendali e per il consumatore	14,6%	12,7	8,7	10	12
Energia	10,7%	8,2	11,1	6	6
Commercio al dettaglio e all'ingrosso	8,7%	7,3	10,2	16	11
Istruzione	7,3%	2,8	4	8	6
Sanità	5,8%	5,1	6,6	3	6
Pubblica Amministrazione	4,8%	2,8	7,9	8	8
Trasporti	3,9%	4	5,1	13	13
Media e telecomunicazioni	0,5%	2,50	5,7	10	8

24,8%

dei casi corretti da X-Force è avvenuto nel settore manifatturiero.

#1 | Produzione manifatturiera

La produzione manifatturiera è stata il settore più attaccato, con un margine leggermente superiore rispetto al 2021. Nel 2022, nel 28% degli incidenti sono state distribuite backdoor, superando i ransomware apparsi nel 23% degli incidenti corretti da X-Force. La percentuale di distribuzione delle backdoor è stata spinta anche dall'impennata di infezioni Emotet. Alcuni casi avrebbero potuto comportare attacchi ransomware, oltre ad altre attività dannose, ma sono stati individuati sufficientemente in tempo per essere corretti.

I primi due vettori di infezione, a pari merito, sono stati gli allegati di spear phishing e lo sfruttamento di applicazioni rivolte al pubblico, con il 28% dei casi ciascuno. Al secondo posto, con il 14%, i servizi esterni da remoto, seguiti al terzo da link di spear phishing e account di default validi, con ciascuno il 10% dei casi di accesso iniziale.

Le estorsioni sono risultate essere l'impatto principale per le aziende manifatturiere, con il 32% dei casi. Notoriamente, i produttori manifatturieri tollerano molto poco, se non affatto, i tempi di indisponibilità, rendendo le estorsioni una strategia molto redditizia per gli aggressori. Il furto dei dati è risultato al secondo posto tra gli incidenti più comuni, con il 19% dei casi, seguito dalle perdite di dati con il 16%. La regione Asia-Pacifico ha osservato il maggior numero di incidenti nel settore manifatturiero, circa il 61% dei casi. Seguono, a pari merito, Europa e Nord America con il 14%, poi America Latina con l'8% e Medio Oriente e Africa con il 4%.

18,9%

dei casi corretti da X-Force è avvenuto nel settore finanziario-assicurativo.

#2 | Finanza e assicurazioni

Le organizzazioni finanziario-assicurative hanno totalizzato meno di un attacco su cinque, tra tutti quelli a cui X-Force ha risposto nel 2022, piazzandosi al secondo posto. Tale percentuale indica una leggera diminuzione negli ultimi anni, in quanto hanno cominciato ad attirare l'attenzione degli aggressori anche altri settori, in particolare quello manifatturiero.

Rispetto ad altri settori, le organizzazioni finanziario-assicurative tendono a essere più all'avanguardia sia nelle trasformazioni digitali che nell'adozione del cloud. Di conseguenza, gli aggressori potrebbero aver bisogno di lavorare più duramente per condurre un attacco di successo contro tali organizzazioni.

Gli attacchi backdoor sono stati l'azione per raggiungere l'obiettivo osservata più spesso, nel 29% dei casi, seguiti da ransomware e maldoc, con l'11% dei casi. Il principale vettore di infezioni sono risultati gli allegati di spear phishing, utilizzati nel 53% degli attacchi contro il settore. Al secondo posto, lo sfruttamento di applicazioni rivolte al pubblico, con il 18% degli attacchi. Terzi i link di spear phishing con il 12% dei casi.

Il più alto volume di attacchi a organizzazioni finanziario-assicurative si è registrato in Europa, con il 33% circa degli attacchi complessivi; subito dopo la regione Asia-Pacifico con circa il 31%. L'America Latina ha subito circa il 15% degli incidenti a cui X-Force si è trovato a rispondere, mentre Nord America e Medio Oriente e Africa hanno subito ognuno il 10% circa degli attacchi.

14 , 6%

dei casi corretti da X-Force è avvenuto nel settore dei servizi professionali, aziendali e per consumatori.

#3 | Servizi professionali, aziendali e per il consumatore

L'industria dei servizi professionali include consulenze, compagnie di gestione e studi legali. Tali servizi hanno totalizzato il 52% delle vittime di questo segmento. Di contro, i servizi aziendali includono aziende IT e servizi tecnologici, pubbliche relazioni, pubblicità e comunicazione. Questi servizi rappresentano il 37% delle vittime. I servizi per i consumatori, che comprendono costruzioni edili, immobili, arte, intrattenimento e ricreazione, rappresentano l'11% dei casi. Insieme, costituiscono la categoria dei servizi professionali, aziendali e per il consumatore dell'X-Force Threat Intelligence Index 2023.

I servizi professionali, aziendali e per il consumatore hanno subito in primo luogo attacchi ransomware e backdoor, con il 18% dei casi ciascuno. I primi due vettori di infezione sono stati lo sfruttamento di applicazioni rivolte al pubblico e i servizi esterni da remoto, con il 23% ciascuno. Gli allegati di spear phishing e gli account locali validi hanno causato ognuno il 15% degli attacchi.

Le estorsioni hanno rappresentato l'impatto più comune, con il 28% dei casi, mentre furto di dati, raccolta di credenziali e fughe di dati hanno impattato ognuno nel 17% dei casi. X-Force ha risposto al 47% dei casi in Europa, al 33% in Nord America, al 10% in Asia-Pacifico, al 7% in Medio Oriente e Africa e al 3% in America Latina.

10,7%

dei casi corretti da X-Force è avvenuto nel settore energetico.

#4 | Energia

Come nel 2021, le compagnie energetiche, tra le quali servizi elettrici e compagnie petrolifere e del gas, hanno rappresentato il quarto settore più attaccato, con il 10,7% dei casi. Il vettore di infezione più diffuso è stato lo sfruttamento delle applicazioni rivolte al pubblico, nel 40% dei casi. I link di spear phishing e i servizi esterni da remoto hanno inciso ciascuno per il 20% dei casi. L'azione per raggiungere l'obiettivo più comune coincide con i botnet, nel 19% dei casi, con ransomware e BEC secondi con il 15%.

Furto dei dati ed estorsioni sono stati registrati nel 23% dei casi, seguiti da raccolta di credenziali e infezioni botnet nel 15% dei casi ciascuno. Tra tutti i casi a cui X-Force si è trovata a rispondere nel mondo, le organizzazioni nordamericane sono risultate le vittime più comuni, con il 46% dei casi, rispetto ad Europa e America Latina, con il 23% ciascuna; appena sotto il 5% Asia-Pacifico e Medio Oriente e Africa.

L'industria energetica rimane sotto la pressione di un gran numero di forze globali, specialmente quelle esasperate dalla guerra russa in Ucraina e da come questa abbia condizionato il già agitato mercato mondiale dell'energia.

8,7%

dei casi corretti da X-Force è avvenuto nel settore del commercio al dettaglio e all'ingrosso.

#5 | Commercio al dettaglio e all'ingrosso

I rivenditori al dettaglio sono responsabili del commercio di beni verso consumatori e grossisti. Generalmente, i grossisti sono responsabili del trasporto e della distribuzione di tali beni dai produttori direttamente verso i rivenditori o i consumatori. Secondo i dati X-Force IR, il settore dei rivenditori al dettaglio e grossisti è risultato essere il quinto più bersagliato, esattamente come nel 2021.

Negli attacchi a questo settore il vettore di accesso iniziale più comune sono state le e-mail di phishing con link malevoli, con il 33% dei casi. Servizi esterni da remoto compromessi, spear phishing con allegati malevoli e hardware aggiunti hanno inciso ognuno nel 17% dei casi.

Ransomware, backdoor e BCE sono state le azioni per raggiungere l'obiettivo più comuni, costituendo ognuna il 19% delle attività intraprese dagli aggressori. I worm sono stati individuati nel 10% dei casi. Le vittime hanno subito estorsioni nel 50% dei casi, mentre raccolta delle credenziali e perdite finanziarie nel 25% dei casi ciascuno. Nord America e America Latina hanno registrato la maggior parte dei casi, il 39% ciascuno, rispetto al 22% europeo.

7,3%

dei casi corretti da X-Force è avvenuto nel settore dell' istruzione.

#6 | Istruzione

Nel settore dell'istruzione si sono registrati casi di backdoor nel 20% degli attacchi a cui X-Force ha dovuto rispondere. Ransomware, adware e spam hanno inciso per il 13% ciascuno. Nel 42% dei casi, si è osservato che l'accesso iniziale più sfruttato è stato lo sfruttamento di applicazioni rivolte al pubblico, seguito dagli allegati di spear phishing, con il 25%. Le violazioni di phishing tramite servizio, link e account valido cloud e locale hanno rappresentato vettori di accesso iniziale ognuno per l'8% dei casi. Furto e perdita di dati, estorsioni e ricognizione hanno rappresentato i principali impatti, ognuno con il 25% dei casi. La regione Asia-Pacifico ha totalizzato il 67% dei casi, il Nord America il 27% e l'America Latina il 6%.

5,8%

dei casi corretti da X-Force è avvenuto nel settore dell'assistenza sanitaria.

#7 | Assistenza sanitaria

Tra i primi 10 settori, l'assistenza sanitaria è scesa al settimo posto, un ulteriore calo rispetto al sesto posto del 2021. Negli ultimi tre anni, la percentuale di casi riguardanti il settore sanitario a cui X-Force ha dovuto rispondere è rimasto invariata al 5%-6% circa. Gli attacchi backdoor si sono registrati nel 27% dei casi, mentre quelli web shell nel 18%. Adware, BEC, cryptominer, programmi di caricamento, strumenti di ricognizione, scansione e accesso remoto hanno costituito ognuno il 9% dei casi. La ricognizione ha rappresentato il maggior numero di impatti osservati, 50% dei casi, mentre il furto di dati e il mining di valuta digitale sono stati individuati ciascuno nel 25% dei casi.

Gli obiettivi con sede in Europa hanno totalizzato il 58% degli incidenti, il restante 42% è stato registrato in Nord America.

4,8%

dei casi corretti da X-Force è avvenuto nel settore della Pubblica Amministrazione.

#8 | Pubblica Amministrazione

Un altro grande obiettivo delle backdoor è stata la Pubblica Amministrazione, con il 25% dei casi X-Force IR. Questa percentuale è uguale a quella degli attacchi DDoS, anche loro responsabili di un quarto dei casi. Le informazioni particolarmente sensibili presenti nelle reti del settore pubblico sono un obiettivo comune delle campagne di spionaggio informatico. Tali informazioni possono includere ampi database PII e altre informazioni che potrebbero essere utilizzate da gruppi sostenuti dagli stati o vendute a scopo di lucro dai criminali informatici. Nel 17% dei casi sono stati individuati maldoc, mentre cryptominer strumenti di acquisizione delle credenziali, ransomware e web shell si dividono il restante 83% dei casi.

Dei casi in questo settore, X-Force è stata in grado di ricollegare gli incidenti, in percentuali uguali, a: criminali informatici, minacce interne che hanno portato alla distruzione di dati, hacktivist e gruppi di minaccia sostenuti dallo stato per condurre attività di spionaggio.

Sfruttamento di applicazioni rivolte al pubblico e allegati di spear phishing sono stati i principali vettori di infezione, ognuno con il 40% dei casi, mentre la violazione degli account di default validi ha inciso per il 20%. Gli enti pubblici più bersagliati sono stati quelli della regione Asia-Pacifico, con il 50% dei casi, con l'Europa al 30% e il Nord America al 20%.

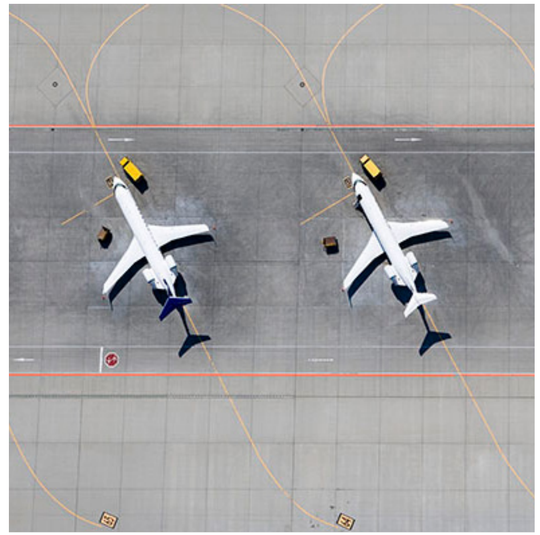
3,9%

dei casi corretti da X-Force è avvenuto nel settore dei trasporti.

#9 | Trasporti

Al settimo posto nel 2021, il settore dei trasporti è tornato alla nona posizione del 2020. Tuttavia, il settore ha conservato la stessa percentuale di incidenti a cui X-Force ha dovuto rispondere. Il vettore di accesso iniziale più diffuso è stato il phishing, con il 51% dei casi, parimenti suddiviso tra link, allegati e spear phishing come servizio. La violazione di account locali validi ha rappresentato il 33% dei vettori di accesso iniziale, mentre gli account cloud validi hanno costituito un punto di ingresso nel 17% dei casi. Le principali azioni per raggiungere l'obiettivo sono state accesso ai server e distribuzione di strumenti di accesso da remoto, nel 25% dei casi ciascuno, seguiti da campagne di spam, ransomware, backdoor e defacing, ciascuno con il 13% dei casi.

Il furto di dati ha rappresentato l'impatto più diffuso, con il 50% dei casi, mentre l'estorsione e le conseguenze sul marchio hanno impattato nel 25% dei casi ognuno. Le compagnie di trasporto europee sono state le più prese di mira, contando il 62% dei casi, al secondo posto la regione Asia-Pacifico, appena sopra il 37%.



0,5%

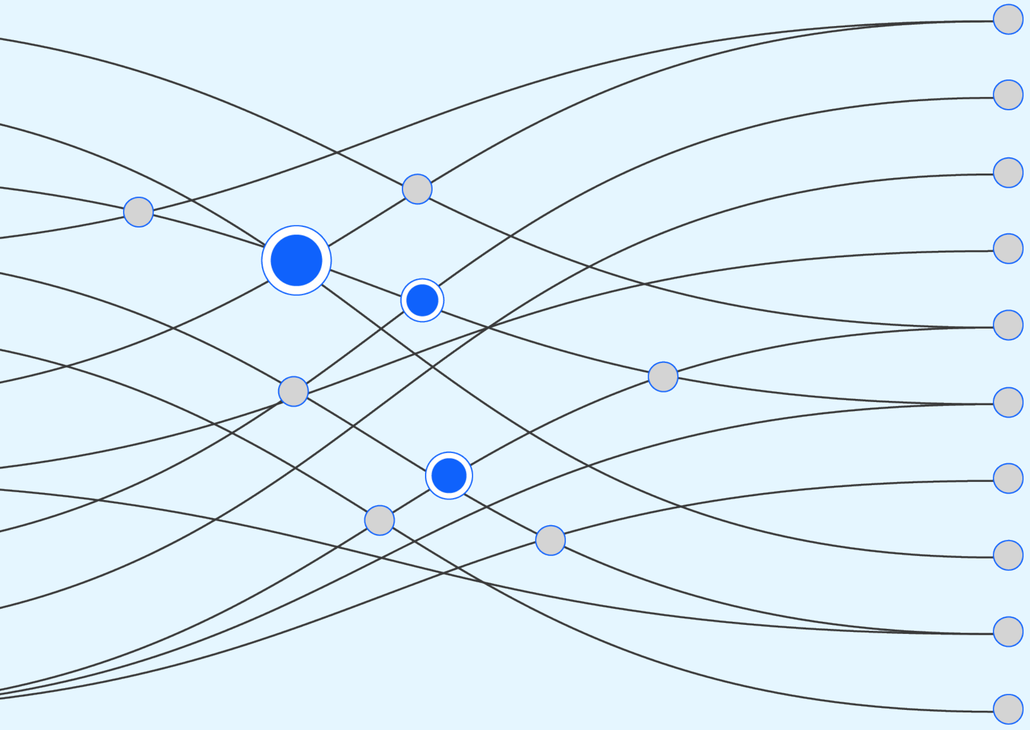
dei casi corretti da X-Force è avvenuto nel settore media e telecomunicazioni.

#10 | Media e telecomunicazioni

Il settore media e telecomunicazioni ha riguardato una piccola frazione degli incidenti corretti da X-Force, piazzandosi in ultima posizione per il secondo anno consecutivo. Violazioni di servizi esterni da remoto, come VPN e altri meccanismi di accesso, e account di dominio validi sono i vettori di infezione osservati. Questi vettori hanno condotto ad attacchi ransomware. Le azioni osservate in questi casi includevano distribuzione di ransomware e strumenti di esfiltrazione dei dati. A loro volta, queste azioni hanno portato a furto, perdita e distruzione di dati e ad estorsione.

12

Suggerimenti



I suggerimenti che seguono sono le azioni da compiere per proteggere le organizzazioni contro minacce malevoli, comprese quelle presentate in questo report.

Gestire gli asset: “Cosa abbiamo? Cosa dobbiamo difendere? Quali sono i dati più importanti per la nostra attività?” Queste sono le prime domande a cui ogni team addetto alla sicurezza dovrebbe rispondere per costruire un sistema di difesa efficace. Dare priorità all’individuazione degli asset sul proprio perimetro, comprendere quanto si è esposti agli attacchi di phishing e ridurre le superfici suscettibili ad attacchi contribuiscono ulteriormente alla sicurezza olistica. Infine, le organizzazioni dovrebbero estendere i propri programmi di gestione degli asset fino a includere codici sorgente, credenziali e altri dati che già potrebbero esistere su Internet o sul dark web.

Conoscere il nemico: sebbene molte organizzazioni abbiano un’ampia visuale sul panorama delle minacce, X-Force raccomanda di adottare una posizione che enfatizzi gli autori delle minacce specifiche che più probabilmente potrebbero puntare al proprio settore, organizzazione e/o area geografica. Una tale prospettiva include la comprensione di come operano gli autori di minacce, individuando il loro livello di sofisticatezza e sapendo quali tattiche, tecniche e procedure potrebbero utilizzare per i loro attacchi.

Gestire la visibilità: dopo aver compreso meglio quali nemici potrebbero attaccarle più probabilmente, le organizzazioni devono essere certe di avere la giusta visibilità dei data source che potrebbero rivelare la presenza di un aggressore. Mantenere visibilità dei punti chiave in tutta l’azienda e garantire che gli avvisi di sicurezza siano generati e attivati in modo tempestivo sono condizioni fondamentali per fermare gli aggressori prima che possano causare interruzioni.

Misurarsi con le supposizioni: le organizzazioni devono supporre di essere già state compromesse. In tal modo, i team possono riesaminare continuamente i seguenti aspetti:

- Il modo in cui gli aggressori possono penetrare il sistema
- Quanto siano efficaci le proprie capacità di rilevamento e risposta rispetto a tattiche, tecniche e procedure emergenti
- Il livello di difficoltà che un possibile nemico troverebbe nel compromettere i dati e i sistemi più critici.

I team di sicurezza più efficaci eseguono regolarmente test di natura offensiva, tra cui individuazione delle minacce, test di penetrazione e attacchi mirati di red team per rilevare o confermare percorsi di attacchi opportunisti nei propri ambienti.

Lavorare sull'intelligence: attivare l'intelligence sulle minacce ovunque. L'effettiva attivazione dell'intelligence sulle minacce consentirà di analizzare i comuni percorsi di attacco e individuare le possibilità chiave di mitigare gli attacchi più diffusi, oltre a sviluppare nuove opportunità di rilevamento ad alta fedeltà. L'attivazione dell'intelligence sulle minacce dovrebbe essere associata alla comprensione dei nemici e del loro modo di agire.

Essere preparati: gli attacchi sono inevitabili, vietato commettere errori. Le organizzazioni dovrebbero sviluppare piani di risposta agli incidenti su misura per i propri ambienti. Questi piani dovrebbero essere regolarmente analizzati e modificati man mano che l'organizzazione cambia, con particolare attenzione al miglioramento dei tempi di risposta, correzione e ripristino.

Ingaggiare un fornitore di servizi IR (incident response) riduce il tempo necessario per reagire in modo qualificato e mitigare un attacco. Inoltre, includere un fornitore IR nello sviluppo e nei test del piano di risposta è fondamentale e contribuisce a garantire una risposta più efficiente. I migliori piani IR prevedono una risposta inter-organizzativa, includono le parti interessate al di fuori dell'IT e testano le linee di comunicazione tra i team tecnici e l'alta dirigenza. Infine, testare il proprio piano attraverso un'esercitazione cyber range immersiva e pressante può migliorare considerevolmente la capacità di rispondere a un attacco.

Azioni per aumentare la sicurezza:

- [ ] Gestire gli asset
- [ ] Conoscere il nemico
- [ ] Gestire la visibilità
- [ ] Misurarsi con le supposizioni
- [ ] Lavorare sull'intelligence
- [ ] Essere preparati

Chi siamo

IBM Security X-Force

IBM Security X-Force è un team di hacker, responder, ricercatori e analisti incentrato sulle minacce informatiche. Il nostro portfolio include prodotti e servizi di attacco e difesa, alimentato da una visione a 360 gradi delle minacce.

In un periodo di attacchi informatici implacabili, in cui tutto è connesso e i mandati normativi sono in aumento, le organizzazioni hanno bisogno di un approccio alla sicurezza mirato. X-Force ritiene che le minacce debbano essere il punto focale. Attraverso servizi di test di penetrazione, gestione delle vulnerabilità e simulazioni avversario, il team di hacker X-Force Red assume il ruolo di aggressore malintenzionato per trovare le vulnerabilità nella sicurezza che mettono a rischio i tuoi asset più importanti. Attraverso la preparazione agli incidenti, il rilevamento, la risposta e i servizi di gestione delle crisi, il team IR di X-Force sa dove possono nascondersi le minacce e come fermarle.

I ricercatori di X-Force creano tecniche offensive per rilevare e prevenire le minacce, mentre gli analisti con X-Force raccolgono e traducono i dati delle minacce in informazioni utilizzabili per ridurre il rischio.

Con una profonda comprensione di come gli attori delle minacce pensano, pianificano e colpiscono, X-Force può aiutarti a prevenire, rilevare, rispondere e riprenderti dagli incidenti, concentrandoti sulle priorità aziendali.

Se la tua organizzazione desidera ricevere supporto per rafforzare la sua posizione in fatto di sicurezza, pianifica una consulenza one-on-one con un esperto IBM Security X-Force.

Prenota una consulenza →

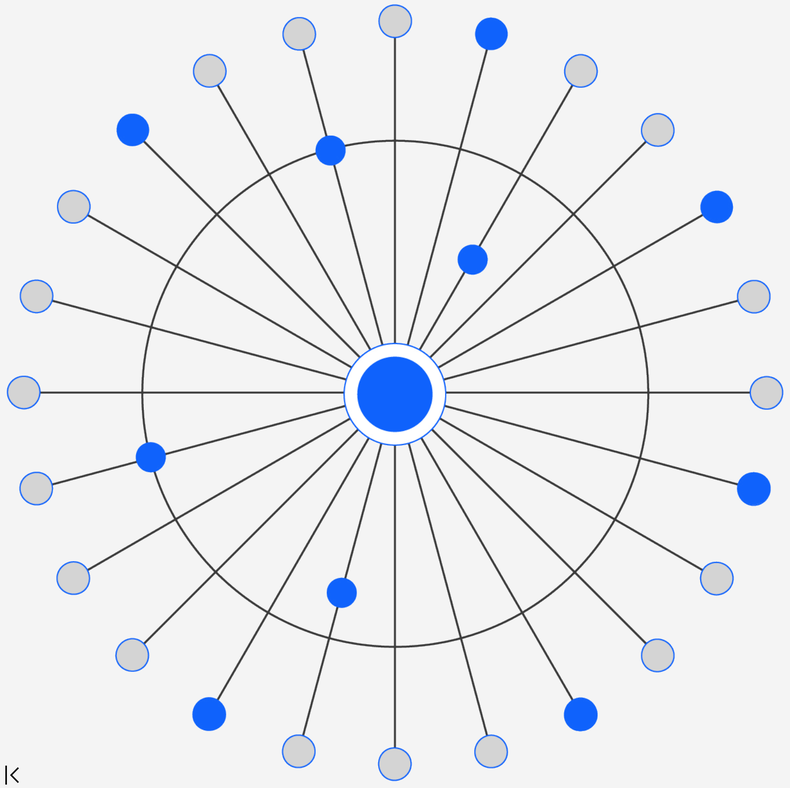
IBM Security

IBM Security si adatta al tuo spazio in continua espansione e lavora al tuo fianco per mantenerti sulla strada giusta. Grazie alle nostre funzionalità AI e di automazione dinamica, ti aiutiamo a stare sempre un passo avanti, con maggiore velocità e maggiore precisione. Assicurati di fare sempre la mossa giusta, oggi come domani, grazie agli insight del nostro fidato team di esperti leader del settore. Dalla previsione delle minacce, alla protezione dei dati, lavorando con fornitori diversi o in tutto il mondo, non importa dove sia diretta la tua azienda, IBM Security può aiutarti a raggiungere gli obiettivi di business più ambiziosi, esplorando nuove fondamentali tecnologie e contribuendo a ridurre al minimo le minacce impreviste.

Scopri di più →

14

Contributi



Michael Worley
Christopher Caridi
Michelle Alvarez
Karlina Bakken
Yannick Bedard
Michele Brancati
Christopher Bedell
Joshua Chung
Scott Craig
Joseph DiRe
John Dwyer
Emmy Ebanks
Richard Emerson
Charlotte Hammond
Kevin Henson
Guy-Vincent Jourdan
Vio Onut
Mitch Mayne
Dave McMillen
Kat Metrick
Scott Moore
Golo Mühr
Andy Piazza
Benjamin Shipley
Christopher Thompson
Ole Villadsen
Reginald Wong
John Zorabedian

Appendice

Lista degli impatti

Impatti	Impatti
Botnet	Mining di valuta digitale
Reputazione del marchio	Spionaggio
Raccolta credenziali	Estorsioni
Distruzione dati	Perdita finanziaria
Perdita dati	Interruzione della produzione (OT)
Furto dati	Ricognizione

1. “A timeline of the biggest ransomware attacks,” CNET, 15 novembre 2021
2. “International action against DD4BC cybercriminal group,” Europol, 12 gennaio 2016
3. “DD4BC, Armada Collective, and the Rise of Cyber Extortion,” Recorded Future, 7 dicembre 2015
4. “A Brief History of Ransomware.” Varonis, 10 novembre 2015
5. “Inside Chimera Ransomware - the first ‘doxingware’ in wild,” MalwardBytes Labs, 8 dicembre 2015
6. “Big Game Hunting: The Evolution of INDRIK SPIDER From Dridex Wire Fraud to BitPaymer Targeted Ransomware,” Crowdstrike, 14 novembre 2018
7. “Operators of SamSam Continue to Receive Significant Ransom Payments,” Crowdstrike, 11 aprile 2018
8. “Triple Extortion Ransomware: The DDoS Flavour,” PacketLabs, 12 maggio 2022
9. “They Told Their Therapists Everything. Hackers Leaked It All,” Wired, 4 maggio 2021
10. “BazarCall to Conti Ransomware via Trickbot and Cobalt Strike,” The DFIR Report, 1 agosto 2021
11. “Diavol Ransomware,” The DFIR Report, 13 dicembre 2021
12. “Quantum Ransomware,” The DFIR Report, 25 aprile 2022
13. “Bumblebee Loader Linked to Conti and Used In Quantum Locker Attacks,” Kroll, 6 giugno 2022
14. “This isn’t Optimus Prime’s Bumblebee but it’s Still Transforming,” Proofpoint, 28 aprile 2022,
15. “Understanding REvil: REvil Threat Actors May Have Returned (Updated),” Unit 42, 3 giugno 2022
16. “AdvIntel’s State of Emotet aka “SpmTools” Displays Over Million Compromised Machines Through 2022,” AdvIntel, 13 settembre 2022
17. “Back in Black: Unlocking a LockBit 3.0 Ransomware Attack,” NCC Group, 19 agosto 2022
18. “Back in Black: Unlocking a LockBit 3.0 Ransomware Attack,” NCC Group, 19 agosto 2022.

IBM Italia S.p.A.
Circonvallazione Idroscalo
20054 Segrate (Milano)
Italia

Prodotto negli Stati Uniti d’America
Febbraio 2023