DOCUMENTO DI SINTESI

CROWDSTRIKE

GLOBAL THREAT REPORT 2025

Avversari intraprendenti e organizzati come imprese

Ogni anno, il Global Threat Report di CrowdStrike fornisce un'analisi completa del settore della sicurezza informatica sul panorama delle minacce relative all'anno precedente, oltre che sul comportamento e sulle attività di spionaggio degli avversari. Comprendi i trend e gli eventi che hanno definito il 2024, i metodi utilizzati dagli avversari e le misure che le organizzazioni devono adottare per proteggersi dalle minacce in continua evoluzione.

Per tutto il 2024, gli avversari hanno adottato un approccio intraprendente, perfezionando e scalando le proprie strategie di successo e sperimentando nuove tecnologie per ottenere velocità ed efficienza sempre maggiori. Gli avversari moderni sono determinati e professionali. Imparano velocemente e si adattano ai mutamenti della difesa senza perdere d'occhio i loro obiettivi.

Bisogna conoscerli per fermarli. Apprendere dai comportamenti, dalle motivazioni e dalle tecniche degli avversari consente di comprendere meglio le loro attività e, da ultimo, difendersi meglio.

Il Global Threat Report 2025 di CrowdStrike offre una panoramica del 2024, in modo tale da avere un quadro completo delle minacce da affrontare. Il report include le osservazioni dell'esclusivo team CrowdStrike Counter Adversary Operations, il quale combina la potenza della threat intelligence con la velocità di team di threat hunting dedicati e trilioni di eventi di telemetria generati dalla piattaforma AI-native CrowdStrike Falcon®.

Questo documento di sintesi fornisce un quadro generale dei risultati principali del report, evidenziando quello che i team di sicurezza devono sapere (e fare) per riuscire ad affrontare il panorama sempre più complesso delle minacce.

PER ULTERIORI INFORMAZIONI SU QUALSIASI AVVERSARIO MENZIONATO NEL PRESENTE DOCUMENTO DI SINTESI O SU QUELLI CHE PUNTANO IL TUO SETTORE O REGIONE, CONSULTA CROWDSTRIKE ADVERSARY UNIVERSE®.

Overview sul panorama delle minacce

Gli avversari sono sempre più rapidi: il breakout time medio, ovvero il tempo impiegato da un avversario per passare da un host inizialmente compromesso a un altro all'interno dell'organizzazione target, è sceso a **48 minuti** nel 2024, mentre il breakout time più veloce registrato è stato di **51 secondi**.

Le modalità di accesso si stanno evolvendo: gli avversari impiegano il phishing vocale (vishing), il callback phishing e l'help desk social engineering per entrare nelle reti target. Inoltre, si affidano alle credenziali compromesse: gli annunci degli access broker, ovvero i venditori di credenziali rubate valide, sono aumentati del **50% su base annua**.
Più della metà (52%) delle vulnerabilità osservate da CrowdStrike nel 2024 erano legate all'accesso iniziale.

La furtività rimane una priorità: le minacce moderne vedono la predominanza di tecniche di intrusione interattive, in cui gli avversari usano le azioni hands-on-keyboard per raggiungere i loro obiettivi. Nel 2024, **il 79% dei casi rilevati erano privi di malware**, mentre CrowdStrike ha osservato un **aumento del 35% rispetto all'anno precedente** delle campagne di intrusione interattiva.

L'IA generativa è inclusa nella cassetta degli attrezzi degli avversari: l'uso dell'IA generativa (genAI) è cresciuto nel 2024 per affinare le tecniche di social engineering, accelerare le operazioni di disinformazione e supportare l'attività dannose sulla rete.

Le attività informatiche della Cina sono aumentate: le attività associate alla Cina sono aumentate del **150% in tutti i settori**, con un'incredibile impennata del **200-300%** in settori chiave quali i servizi finanziari, i media, la produzione e l'industria/ingegneria.

Gli ambienti cloud sono sotto attacco: il il cloud continua a essere un obiettivo primario per via della vastità dei suoi dati, della scalabilità e delle configurazioni errate che è possibile sfruttare. Nel 2024, CrowdStrike ha registrato un **aumento del 26%** delle nuove intrusioni nel cloud non attribuite, segno che i servizi cloud sono presi di mira da un numero maggiore di avversari.

CONVENZIONI DI DENOMINAZIONE

AVVERSARIO	NATION-STATE O CATEGORIA DI AFFILIAZIONE
 BEAR	RUSSIA
 BUFFALO	VIETNAM
 CHOLLIMA	DPRK (COREA DEL NORD)
 CRANE	ROK (REPUBBLICA DI COREA)
 HAWK	SIRIA
 JACKAL	HACKTIVISTA
 KITTEN	IRAN
 LEOPARD	PAKISTAN
 LYNX	GEORGIA
 OCELOT	COLOMBIA
 PANDA	REPUBBLICA POPOLARE CINESE
 SAIGA	KAZAKISTAN
 SPHINX	EGITTO
 SPIDER	eCRIME
 TIGER	INDIA
 WOLF	TURCHIA

Intrusioni interattive per regione

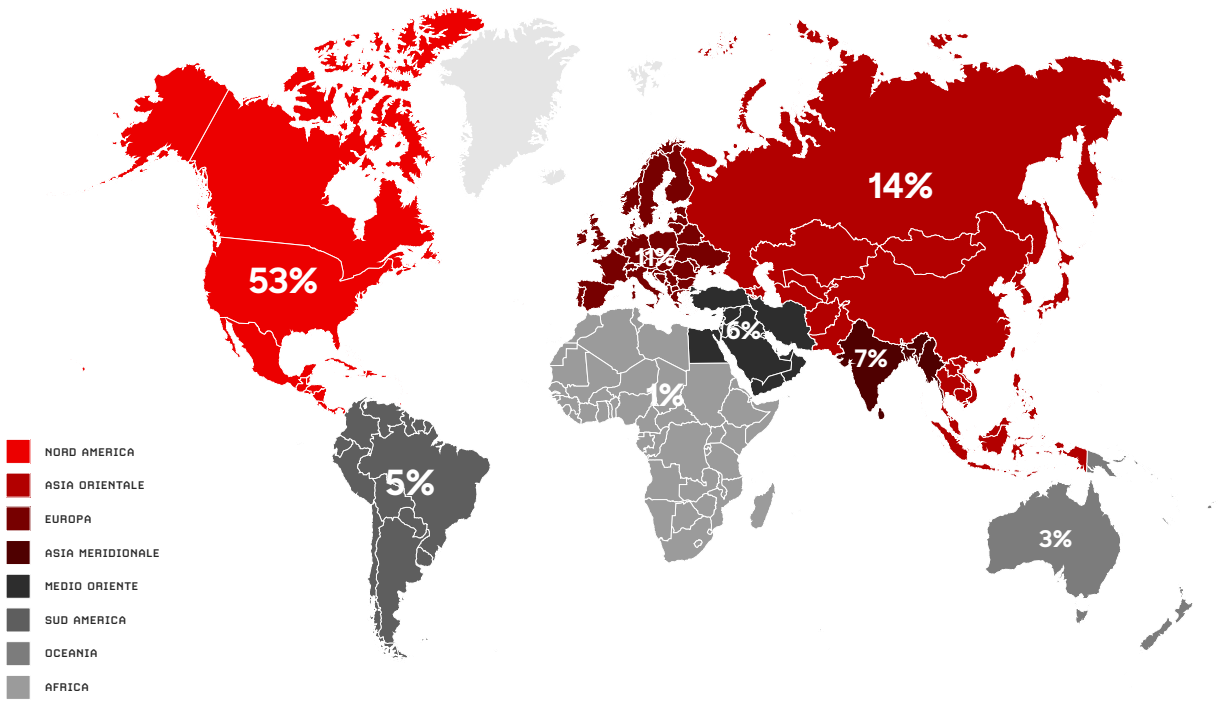

Figura 1. Intrusioni interattive per regione, gennaio-dicembre 2024

I 10 principali settori presi di mira dalle intrusioni interattive

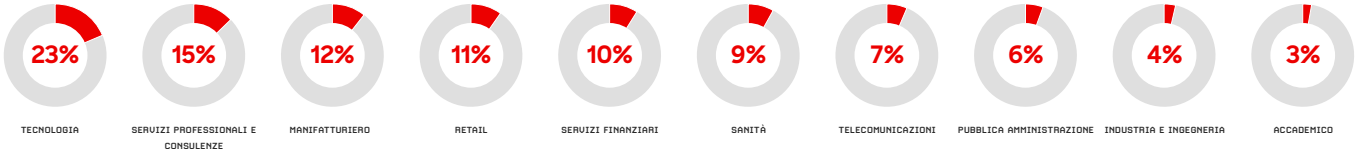

Figura 1. I 10 principali settori presi di mira dalle intrusioni interattive, gennaio-dicembre 2024

Le statistiche evidenziano la portata globale delle operazioni degli avversari e la necessità di strategie di sicurezza cross-domain che tengano conto delle compromissioni dell'identità, dei movimenti laterali e dei vettori di attacco basati su cloud.

Il passaggio a tecniche di attacco prive di malware è stata una tendenza determinante negli ultimi cinque anni. Nel 2024, le attività senza malware hanno rappresentato il 79% dei casi rilevati, segnando un aumento significativo rispetto al 40% del 2019.

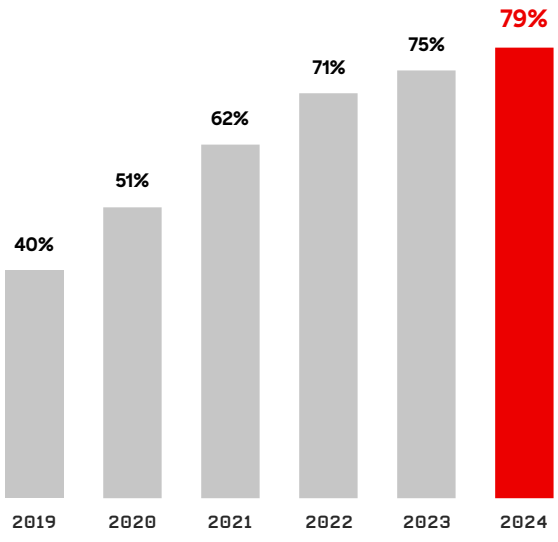

Figura 3. Percentuale dei casi rilevati privi di malware, 2019-2024

Temi principali sugli avversari

IL BUSINESS DEL SOCIAL ENGINEERING

Nel 2024, le tecniche di accesso iniziali sono cambiate e gli avversari hanno iniziato a prendere di mira le debolezze umane, utilizzando credenziali compromesse e social engineering per accedere e muoversi lateralmente all'interno delle organizzazioni. CrowdStrike ha osservato un'impennata delle campagne telefoniche di social engineering e della manipolazione dell'help desk, segnalando un'evoluzione delle tattiche di eCrime.

- Le operazioni di vishing hanno segnato un aumento del 442% tra la prima e la seconda metà del 2024.
- Sofisticati gruppi di eCrime come CURLY SPIDER, CHATTY SPIDER e PLUMP SPIDER hanno utilizzato queste tattiche per rubare credenziali, stabilire sessioni remote ed eludere il rilevamento.
- Nel corso del 2024, CrowdStrike ha monitorato almeno sei campagne analoghe ma probabilmente distinte in cui cybercriminali che si spacciavano per personale IT chiamavano le potenziali vittime e cercavano di convincerle a iniziare sessioni di supporto da remoto.

CASO DI STUDIO

CURLY SPIDER

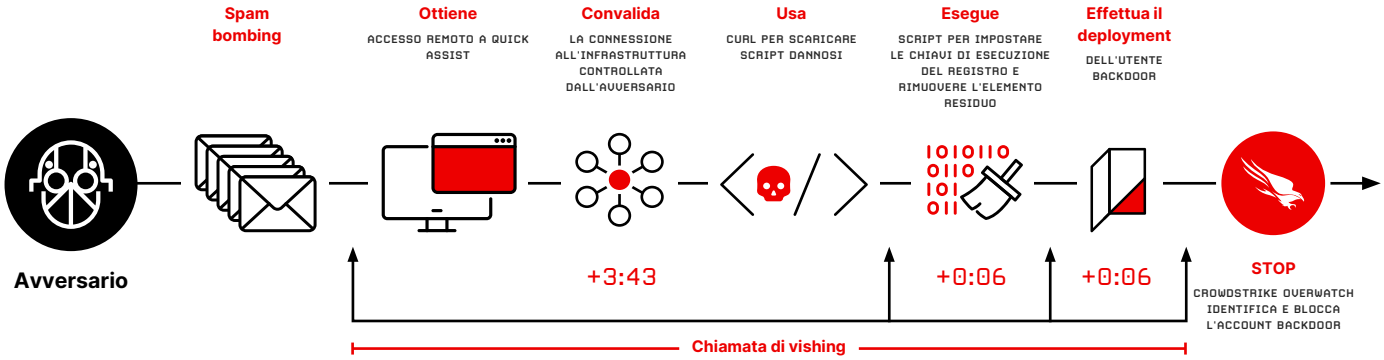

Figura 4. Cronologia che mostra come CrowdStrike OverWatch si muova più velocemente di CURLY SPIDER per bloccare un attacco di social engineering in meno di quattro minuti

Nel 2024, CURLY SPIDER è stato uno degli avversari eCrime più veloci e adattabili. In questo caso, ha tentato di raggiungere il proprio obiettivo senza dover passare a un altro dispositivo. L'intera catena di attacco, dall'interazione iniziale con l'utente e il social engineering all'introduzione di un account backdoor per stabilire la persistenza, ha impiegato meno di quattro minuti.

Una volta che CURLY SPIDER ha ottenuto l'accesso iniziale, le sue opportunità sono limitate; l'accesso dura solo il tempo della chiamata con la vittima. Per un maggiore controllo, l'avversario cerca subito di stabilire un accesso permanente prima della fine della sessione.

Grazie all'accesso remoto protetto, CURLY SPIDER può muoversi rapidamente, spesso mentre interagisce attivamente con la vittima, per distribuire la propria carica distruttiva e stabilire la persistenza. La maggior parte del tempo di intrusione viene impiegato per garantire la connettività e risolvere i problemi di accesso al fine di raggiungere gli script dannosi ospitati nel cloud.

L'IA generativa e l'avversario intraprendente

Nonostante la relativa novità della genAI, CrowdStrike ha individuato diversi tipi di avversario che la utilizzano. Le basse barriere all'ingresso e le potenti capacità della GenAI la rendono uno strumento molto interessante. Consente ai cybercriminali di creare e-mail di phishing convincenti, condurre campagne a scopo di inganno e sviluppare script dannosi, una tendenza prevista proseguire nel 2025.

- I modelli linguistici di grandi dimensioni (LLM) e i modelli di genAI in grado di creare immagini foto realistiche possono generare contenuti convincenti su larga scala senza bisogno di grandi competenze. Possono supportare le attività di social engineering o le operazioni di informazione.
- CrowdStrike ha risposto all'attività di FAMOUS CHOLLIMA in **304 incidenti nel corso dell'anno**, di cui il **40% era rappresentato da minacce interne**. In alcuni casi, l'avversario ha utilizzato la genAI per creare falsi profili LinkedIn.
- NITRO SPIDER ha utilizzato siti web generati mediante l'IA per campagne di malvertising, selezionando le vittime attraverso annunci dannosi prima di reindirizzarle a pagine false create con l'IA.

La crescente attività informatica della Cina

Nel 2024, le capacità di spionaggio informatico della Cina hanno raggiunto un punto di svolta critico, con attacchi sempre più audaci, tattiche più furtive e una maggiore capacità operativa. Questi progressi riflettono le priorità strategiche dell'intelligence cinese, tra cui l'influenza a livello regionale, l'acquisizione di tecnologia e la soppressione delle minacce percepite ai fini della stabilità del regime.

- Per tutto il 2024, gli avversari associati alla Cina hanno continuato a operare in ogni settore e regione su scala globale, mantenendo le finalità delle operazioni e aumentandone la portata.
- CrowdStrike ha identificato sette nuovi avversari associati alla Cina nel 2024, evidenziando un passaggio a intrusioni più mirate e con scopi più specifici. Cinque di questi gruppi sono unici per specializzazione e sofisticazione.
- LIMINAL PANDA, LOCKSMITH PANDA e OPERATOR PANDA sono avversari molto abili con mandati e set di strumenti unici per prendere di mira le reti di telecomunicazioni; VAULT PANDA si concentra sul settore dei servizi finanziari globali; mentre ENVOY PANDA, inizialmente dotato di una scarsa capacità, ha aumentato notevolmente la propria postura di sicurezza delle operazioni (OPSEC).

I cybercriminali cloud-conscious continuano a innovarsi

Gli avversari che si concentrano sul cloud sfruttano configurazioni errate, credenziali rubate e strumenti di gestione del cloud per infiltrarsi nei sistemi, spostarsi lateralmente e mantenere l'accesso permanente per attività come il furto di dati e il deployment di ransomware. Gli avversari associati alla Cina e alla Corea del Nord hanno esteso i loro attacchi alle piattaforme cloud, mentre i gruppi eCrime hanno adottato tattiche avanzate come l'abuso dei rapporti di fiducia e le minacce interne per compromettere le risorse cloud.

- L'abuso di account validi è diventato la principale tattica di accesso iniziale, rappresentando il **35% degli incidenti cloud** nella prima metà del 2024. Gli aggressori utilizzano sempre più tattiche orientate alla furtività e cercano di accedere alle credenziali per prendere di mira account validi.
- Nel 2023, l'avversario eCrime SCATTERED SPIDER ha rappresentato ilil **30% di tutte le intrusioni cloud.** Questo numero è sceso al **13% nel 2024**, in parte perché molti cybercriminali nation-state e opportunistici prendono sempre più di mira il piano di controllo cloud.
- Nel **75% dei casi osservati**, i cybercriminali cloud-conscious hanno rimosso gli indicatori dai file di log nel tentativo di eludere il rilevamento.

Sfruttamento intraprendente delle vulnerabilità

Gli avversari prendono sempre più di mira le appliance di rete esposte a Internet, sfruttando le loro debolezze di sicurezza intrinseche per ottenere l'accesso iniziale, dove la visibilità per il rilevamento e la risposta agli endpoint (EDR) è limitata. L'esecuzione di codice da remoto (RCE) è possibile grazie a tecniche come il chaining, l'exploit o l'abuso di funzionalità legittime del prodotto e spesso vengono riutilizzate vulnerabilità note per compromettere ripetutamente gli stessi dispositivi. Gli avversari continuano a prendere di mira le appliance alla fine del loro ciclo di vita utile, poiché i sistemi obsoleti con vulnerabilità prive di patch offrono dei punti d'appoggio negli ambienti target.

- I cybercriminali prendono di mira le vulnerabilità all'interno del sistema operativo proprietario dell'appliance di rete. Queste vulnerabilità sono dei bersagli interessanti perché potenzialmente consentono agli aggressori di utilizzare un difetto per prendere di mira più prodotti che eseguono lo stesso sistema operativo.
- Il chaining di più vulnerabilità offre agli aggressori maggiori vantaggi. In primo luogo, rende possibile l'RCE senza autenticazione combinando più exploit in un unico attacco. In secondo luogo, il chaining di exploit mina il processo di applicazione di patch basato sul punteggio di gravità seguito da molte aziende.
- Per scoprire nuove vulnerabilità o abusare di funzionalità legittime del prodotto, l'avversario probabilmente utilizzerà blog tecnici e renderà operativo l'exploit di proof-of-concept (POC) pubblici più velocemente rispetto al passato.

Gli exploit SaaS continueranno

Nel corso del 2024, CrowdStrike Intelligence ha osservato che diversi eCrime e intrusioni mirate utilizzavano l'accesso ad applicazioni software as a service (SaaS) basate su cloud per ottenere dati al fine di facilitare i movimenti laterali, le estorsioni e prendere di mira terze parti. I cybercriminali spesso accedevano a queste applicazioni tramite identità compromesse single sign-on (SSO). Con l'adozione crescente del cloud, si prevede che nel 2025 gli avversari perfezionino la propria attività di spionaggio, rendendo gli exploit SaaS una minaccia critica e in continua evoluzione.

- Nella prima metà del 2024, i cybercriminali cloud-conscious hanno spesso preso di mira Microsoft 365, nello specifico **SharePoint nel 22% delle intrusioni e Outlook nel 17%.**
- SCATTERED SPIDER ha sfruttato gli account SSO compromessi per accedere a un'ampia gamma di applicazioni SaaS integrate, tra cui strumenti per chat, gestione delle relazioni con i clienti, gestione delle credenziali, archiviazione dei documenti, produttività e sicurezza.
- In molte intrusioni, gli avversari hanno cercato nelle applicazioni SaaS le seguenti informazioni: 1) le credenziali dell'account e la documentazione dell'architettura di rete per permettere il movimento laterale e 2) la polizza assicurativa contro gli attacchi informatici e i dati sui ricavi per ottenere informazioni da usare nelle estorsioni.

Conclusioni

Nel corso del 2025, il panorama della sicurezza informatica sta continuando e continuerà a evolversi rapidamente, presentando sfide notevoli per le organizzazioni di tutti i settori e aree geografiche. Considerata la resilienza, la capacità d'innovazione e l'adattabilità degli avversari, è necessario avere una comprensione completa delle minacce odierne su tutti gli aspetti del paesaggio.

Il social engineering si è diffuso nel corso del 2024 con nuovi metodi di accesso iniziale da parte degli avversari per aggirare le difese di sicurezza. La genAI è diventata uno strumento chiave per l'avversario, soprattutto come supporto delle campagne di social engineering e IO (operazioni di intelligence a ritmo elevato). CrowdStrike prevede che continuerà ad essere impiegata nelle operazioni degli avversari durante tutto il 2025.

Gli avversari che si dedicano all'eCrime restano una minaccia per alcuni settori. Per tutto il 2024, si sono dimostrati tenaci nei loro attacchi mirati, spesso compensando alla minore sofisticazione mediante l'acquisizione di una conoscenza approfondita del settore, dell'area geografica e delle tecnologie correlate alla vittima.

Le intrusioni mirate degli avversari sono state attive e innovative nel 2024, adattando le tattiche per raggiungere obiettivi geopolitici e strategici ed eludendo al contempo le difese potenziate. Si prevede che gli avversari associati alla Russia continuino nella loro lotta per la vittoria in Ucraina, concentrandosi sulle operazioni di raccolta di informazioni contro l'Ucraina e i membri della NATO. Gli avversari associati alla Cina beneficeranno probabilmente di investimenti a lungo termine in programmi informatici, con un conseguente aumento delle pratiche OPSEC, delle operazioni a ritmo sostenuto e di una prolifica attività di intrusioni a livello globale.

Il panorama degli exploit delle vulnerabilità rimane un problema critico. I cybercriminali continueranno ad attaccare i dispositivi alla periferia della rete, in particolare le appliance di rete. Anche le applicazioni SaaS sono nel mirino. Dopo aver osservato nel 2024 come gli avversari specializzati in eCrime e intrusioni mirate utilizzino l'accesso alle applicazioni SaaS basate su cloud per ottenere dati per i movimenti laterali, l'estorsione e l'attacco a terze parti, CrowdStrike prevede che l'exploit SaaS sarà una minaccia da tenere d'occhio nel 2025.

Nel corso del 2024, gli avversari hanno conseguito una maggiore maturità e sofisticazione delle operazioni in tutti i settori e aree geografiche. Nonostante l'evolversi di queste minacce nel 2025, il team Counter Adversary Operations di CrowdStrike continua a lavorare per identificare, tracciare e bloccare i cybercriminali quando e dove possibile.

Raccomandazioni

1 Proteggi l'intero ecosistema di identità

Gli avversari prendono sempre più di mira le identità attraverso il furto di credenziali, l'autenticazione a più fattori (MFA) e il social engineering, spostandosi lateralmente tra ambienti on-premise, cloud e SaaS tramite rapporti di fiducia. Ciò consente loro di impersonare utenti legittimi, aumentare il livello di accesso ed eludere il rilevamento.

Le organizzazioni devono adottare soluzioni MFA a prova di phishing, come le chiavi di sicurezza hardware, per impedire gli accessi non autorizzati. Sono essenziali solide policy per identità e accessi, tra cui l'accesso just-in-time, le revisioni periodiche degli account e i controlli di accesso condizionale. Gli strumenti di rilevamento delle minacce all'identità devono monitorare i comportamenti negli endpoint e negli ambienti on-premise, cloud e SaaS per segnalare casi di privilege escalation, accessi non autorizzati o creazione di account backdoor. Integrando questi strumenti con la piattaforma Extended Detection and Response (XDR), è possibile ottenere una visibilità completa e una difesa unificata contro gli avversari.

Inoltre, le organizzazioni devono educare gli utenti a riconoscere i tentativi di vishing e phishing, mantenendo al contempo un monitoraggio proattivo per rilevare e rispondere alle minacce basate sull'identità.

2 Elimina le lacune nella visibilità cross-domain

L'uso crescente da parte degli avversari di tecniche hands-on-keyboard e di strumenti legittimi rende più difficile il rilevamento e la risposta. A differenza del malware tradizionale, questi metodi consentono agli aggressori di aggirare le misure di sicurezza tradizionali eseguendo comandi e utilizzando software legittimi per imitare le normali operazioni.

Per contrastare questo problema, le organizzazioni devono modernizzare le loro strategie di rilevamento e risposta. Le soluzioni SIEM (gestione delle informazioni e degli eventi di sicurezza) e XDR di nuova generazione forniscono una visibilità unificata su endpoint, reti, ambienti cloud e sistemi di identità, consentendo agli analisti di creare correlazioni tra comportamenti sospetti e scoprire il percorso completo dell'attacco.

Il threat hunting e la threat intelligence proattivi migliorano ulteriormente il rilevamento, identificando potenziali pattern di attacco e fornendo approfondimenti su tattiche, tecniche e procedure. Grazie all'intelligence in tempo reale, le organizzazioni possono rimanere informate sulle minacce emergenti, anticipare gli attacchi e dare priorità alle attività essenziali per la sicurezza.

3 Difendi il cloud come infrastruttura fondamentale

Gli avversari che si concentrano sul cloud sfruttano configurazioni errate, credenziali rubate e strumenti di gestione del cloud per infiltrarsi nei sistemi, spostarsi lateralmente e mantenere l'accesso permanente per attività malevole come il furto di dati e il deployment di ransomware.

Le CNAPP (piattaforme per la protezione delle applicazioni cloud native) con funzionalità CDR (rilevamento e risposta cloud) sono fondamentali per contrastare tali minacce.

Queste soluzioni forniscono una visione unificata della postura di sicurezza cloud, aiutando a rilevare, assegnare priorità e rimediare rapidamente a configurazioni errate, vulnerabilità e minacce degli avversari. Inoltre, l'applicazione di rigorosi controlli di accesso, come l'accesso basato sui ruoli e le policy condizionali, limita l'esposizione ai sistemi critici e garantisce il monitoraggio continuo delle anomalie, compresi gli accessi da posizioni impreviste.

Inoltre, gli audit regolari sono fondamentali ai fini della sicurezza. Gli strumenti automatizzati possono rivelare impostazioni di archiviazione eccessivamente permissive, API esposte e vulnerabilità prive di patch. Mediante revisioni frequenti degli ambienti cloud, è possibile risolvere tempestivamente autorizzazioni inutilizzate e configurazioni obsolete.

4 Assegna la priorità alle vulnerabilità mediante un approccio incentrato sull'avversario

Gli avversari sfruttano sempre più le vulnerabilità diffuse pubblicamente e ricorrono al chaining degli exploit, combinando più vulnerabilità per ottenere un accesso rapido, ottenere maggiori privilegi e aggirare le difese. Spesso, questi attacchi in più fasi si basano su risorse pubbliche come l'exploit di POC e i blog tecnici, consentendo all'avversario di ottenere una carica distruttiva efficace e difficile da rilevare.

Per contrastare queste minacce, le organizzazioni devono dare massima importanza all'applicazione regolare di patch o all'aggiornamento dei sistemi critici, in particolare dei servizi online presi di mira più di frequente come i server web e i gateway VPN. Il monitoraggio dei segnali impercettibili di chaining degli exploit, come arresti anomali imprevisti o tentativi di privilege escalation, può essere d'aiuto per rilevare gli attacchi prima del loro progredire.

Strumenti come CrowdStrike Falcon® Exposure Management, creati con funzionalità di assegnazione delle priorità con IA nativa, consentono ai team di ridurre il rumore di fondo e concentrarsi sulle vulnerabilità più importanti, in particolare quelle che interessano i sistemi critici e ad alto rischio. Grazie ad approcci proattivi alla sicurezza, alla scoperta delle esposizioni su tutta la superficie di attacco e all'uso dell'automazione, le organizzazioni possono mitigare le minacce sofisticate e limitare le opportunità per gli avversari.

5 Conosci il tuo avversario e preparati

Quando un attacco informatico si svolge in pochi minuti, o addirittura secondi, essere preparati può essere determinante per riuscire a contenerlo. Un approccio basato sull'intelligence consente ai team di sicurezza di andare oltre la difesa reattiva, in modo da capire quale avversario sta attaccando, come opera e quali sono i suoi obiettivi. Con la threat intelligence, la profilazione dell'avversario e l'analisi dell'attività di spionaggio, i team di sicurezza possono dare priorità alle risorse, adattare le difese e andare attivamente in cerca delle minacce per scovarle sul nascere. La threat intelligence di CrowdStrike non si limita a rilevare le minacce note, ma anticipa le attività di spionaggio nuove e in evoluzione, facendo sì che i responsabili della difesa siano sempre un passo avanti. Integrando perfettamente l'intelligence nei flussi di lavoro di sicurezza, le organizzazioni possono accelerare i tempi di risposta, bloccare gli avversari e trasformare l'intelligence in azione.

Sebbene la tecnologia sia fondamentale per rilevare e bloccare le intrusioni, l'utente finale rimane un anello cruciale della catena per fermare le compromissioni. Le organizzazioni devono adottare programmi di sensibilizzazione degli utenti per contrastare le continue minacce di phishing e le tecniche di social engineering correlate. Per quanto riguarda i team di sicurezza, la pratica li rende perfetti. Occorre promuovere un ambiente che esegua regolarmente simulazioni di attacco ed esercitazioni red team/blue team per identificare le lacune ed eliminare i punti deboli nelle proprie strategie e risposte di sicurezza informatica.

Scarica il report completo

Il Global Threat Report 2025 di CrowdStrike presenta un'analisi completa degli eventi e delle tendenze più importanti nel panorama delle minacce informatiche nel 2024. Scarica una copia gratuita del report all'indirizzo https://www.crowdstrike.com/global-threat-report/.

Informazioni su CrowdStrike

CrowdStrike (Nasdaq: CRWD), leader globale della sicurezza informatica, ha ridefinito la sicurezza moderna con la piattaforma nativa in cloud più avanzata al mondo per la protezione delle aree critiche del rischio aziendale: endpoint e workload cloud, identità e dati.

Con la tecnologia CrowdStrike Security Cloud e l'intelligenza artificiale di prima classe, la piattaforma CrowdStrike Falcon® sfrutta gli indicatori di attacco in tempo reale, le informazioni sulle minacce, lo spionaggio degli avversari in evoluzione e la telemetria arricchita proveniente da tutta l'azienda per fornire rilevamenti estremamente accurati, protezione e ripristino automatici, threat hunting d'élite e osservabilità prioritaria delle vulnerabilità.

Costruita appositamente nel cloud con un'architettura basata su un unico agent leggero, la piattaforma Falcon assicura un deployment rapido e scalabile, protezione e prestazioni superiori, complessità ridotta e un time-to-value immediato.

CrowdStrike: We stop breaches.

Ulteriori informazioni: https://www.crowdstrike.com/it-it/

Seguici: Blog | X | LinkedIn | Facebook | Instagram | YouTube

Inizia oggi stesso la prova gratuita: www.crowdstrike.com/free-trial-guide/