WHITE PAPER

Comprendere gli autori delle minacce odierni

Insights dagli Incident Responders e suggerimenti su come proteggere la tua organizzazione

Executive Summary

Il panorama delle minacce informatiche è in costante mutamento, ponendo sfide significative ai professionisti della sicurezza. Gli autori delle minacce spesso eludono i tradizionali controlli di sicurezza orientati alla prevenzione. Durante la prima metà del 2023, gli autori di minacce informatiche hanno frequentemente sfruttato credenziali valide per infiltrarsi nelle reti aziendali. Una volta dentro, hanno abilmente neutralizzato le difese per operare di nascosto. [1] Questa strategia ha fornito loro ampio margine di manovra per esplorare la rete, spostarsi lateralmente tra i vari sistemi e rastrellare dati sensibili. Solo dopo aver raccolto quanto desideravano, hanno proceduto a esfiltrare e criptare le informazioni, assicurandosi così un furto di dati indisturbato. Se da un lato le attività sempre più sofisticate degli aggressori dovrebbero far suonare un campanello d'allarme, dall'altro questa stessa sofisticazione offre alle organizzazioni ampie possibilità di bloccare questi attacchi prima che gli autori delle minacce possano raggiungere i loro obiettivi.

Nella prima metà del 2023, due terzi dei criminali informatici hanno utilizzato credenziali valide per ottenere l'accesso iniziale a una rete.[2]

L'evoluzione del panorama delle minacce tiene svegli i professionisti della sicurezza

In un sondaggio condotto da Enterprise Strategy Group, ai partecipanti è stato chiesto che cosa rende le operazioni di sicurezza più complesse oggi rispetto a due anni fa. La risposta principale è stata la rapida evoluzione del panorama delle minacce informatiche.[3]

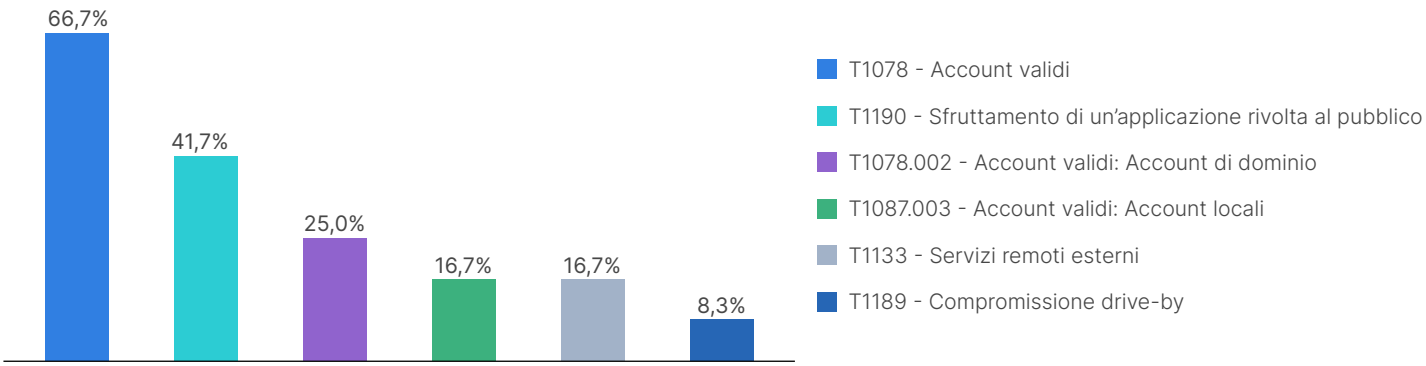
Per fornire ai difensori informazioni strategiche sulle tattiche più comuni utilizzate dagli autori delle minacce, Fortinet ha recentemente pubblicato il Fortinet FortiGuard Incident Response Report 1H 2023. Nel report, abbiamo condiviso i modi più comuni in cui gli avversari possono ottenere e mantenere l'accesso alle organizzazioni, cosa fanno di solito dopo aver ottenuto l'accesso e gli obiettivi più comuni degli autori delle minacce che abbiamo osservato.

Questo documento sintetizza i principali risultati del report al fine di assistere le organizzazioni nel valutare le proprie capacità di sicurezza informatica. L'obiettivo è individuare eventuali lacune esistenti e stabilire le azioni e gli investimenti prioritari per colmarle, fornendo così un solido approccio alla gestione del rischio informatico.

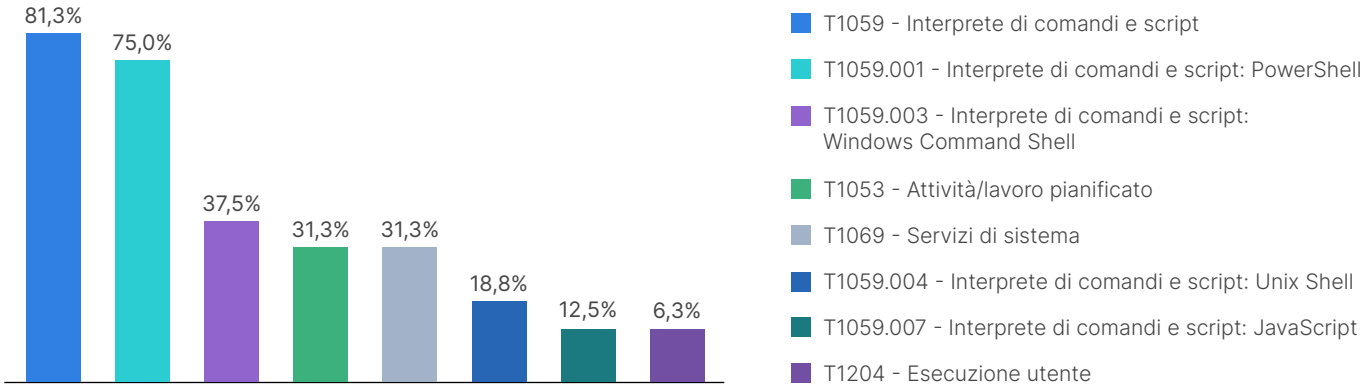
In che modo gli autori delle minacce ottengono e mantengono l'accesso alla tua rete

Con tutti gli investimenti compiuti negli anni in capacità di sicurezza informatica orientate alla prevenzione, le organizzazioni spesso si chiedono in che modo gli autori delle minacce continuino a farsi strada nelle reti aziendali. I controlli di sicurezza stabiliti sono stati inefficaci? Ci sono state lacune tra questi controlli che hanno consentito agli avversari di sfuggire alle falle? I dipendenti sono stati indotti a scaricare file che hanno permesso a un cybercriminale di accedere alla rete?

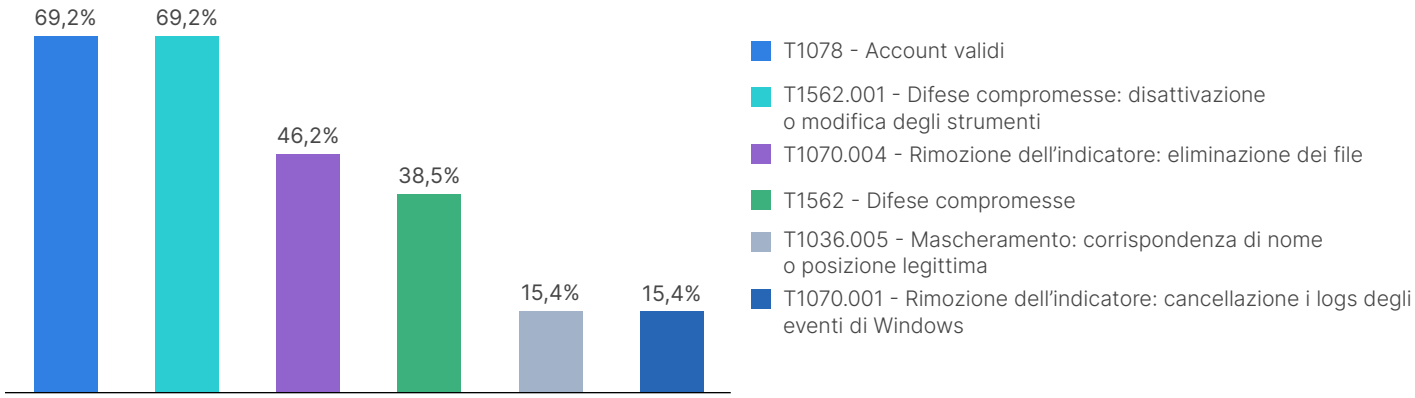
Sebbene la risposta a queste domande sia talvolta affermativa, gli autori delle minacce hanno spesso utilizzato credenziali valide come meccanismo di ingresso, seguite dallo sfruttamento di applicazioni rivolte al pubblico. Negli ultimi sei mesi, infatti, più di due terzi delle violazioni che abbiamo analizzato sono state causate da avversari che hanno utilizzato account validi per ottenere l'accesso.[4] Le credenziali valide sono facilmente reperibili e rese disponibili sul dark web a questo scopo. Esiste un'intera categoria di "initial access brokers" che forniscono mezzi di ingresso, compreso l'accesso con credenziali.



Non solo, quando il codice dannoso veniva eseguito, veniva innescato automaticamente tramite creazione di script, come PowerShell o shell dei comandi. Anche se l'istinto iniziale potrebbe essere quello di incolpare gli utenti finali, l'esecuzione da parte degli utenti non è entrata nell'elenco dei principali metodi di compromissione.

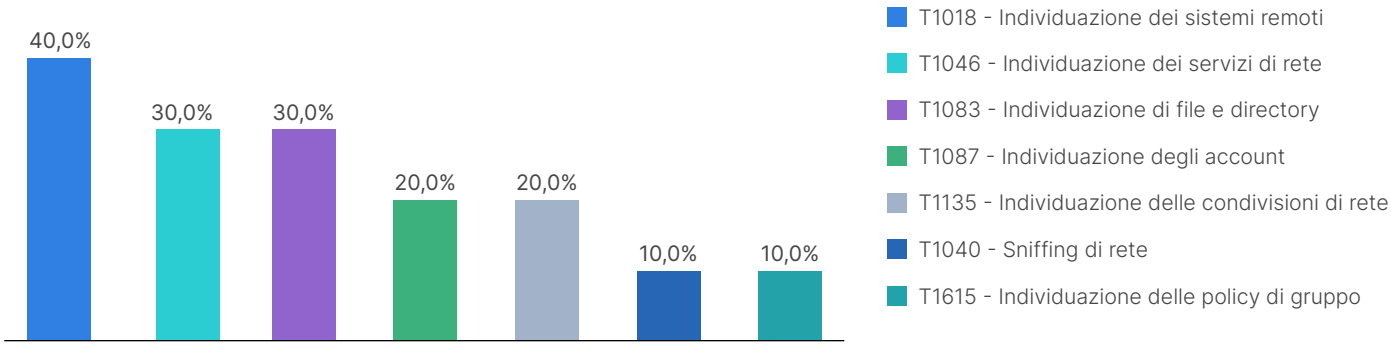


Infine, una volta ottenuto l'accesso a un'organizzazione, gli autori delle minacce hanno in genere adottato misure per rimanere inosservati per un periodo prolungato, in media 26 giorni, mentre continuavano a svolgere le loro attività.[5] Questo è il risultato dell'utilizzo di account validi, della disattivazione degli strumenti di difesa e della rimozione dei segnali dell'intrusione iniziale.

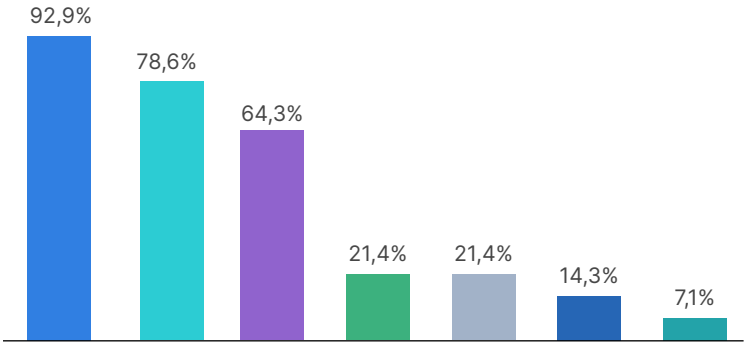


Uno sguardo più ravvicinato all'individuazione, al movimento laterale e all'ulteriore istruzione

Una volta ottenuto l'accesso, in previsione di rimanere inosservati per un periodo prolungato, gli autori delle minacce hanno in genere preso tempo per pianificare la mossa successiva, concentrandosi sull'individuazione di sistemi remoti, servizi di rete, file, directory, account e persino condivisioni di rete.[6]



Grazie a queste informazioni dettagliate, spesso riportate all'autore delle minacce tramite comunicazioni Command&Control (C&C), le campagne si muovevano lateralmente per aumentare al massimo la loro portata all'interno dell'organizzazione. Il più delle volte, questo è avvenuto utilizzando i sistemi e i servizi remoti che gli autori delle minacce hanno individuato una volta ottenuto l'accesso alla rete.

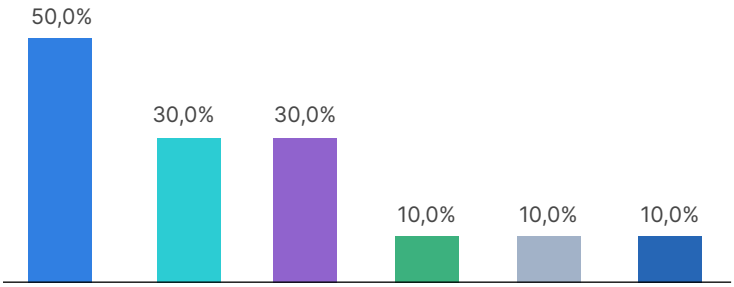


È interessante notare che, mentre nella comunità della sicurezza si discute del fatto che gli autori delle minacce spesso utilizzino il traffico crittografato per aggirare le ispezioni di sicurezza, la metà delle volte il traffico C&C utilizza protocolli del livello di applicazione standard. L'uso di canali crittografati è stato osservato solo nel 15% dei casi.[7]

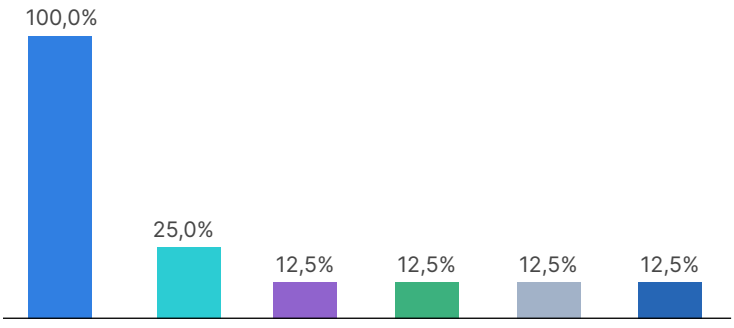
Nel 25% dei casi, i criminali informatici hanno crittografato i dati e compromesso i sistemi di ripristino.[9]

Uno sguardo più ravvicinato alla raccolta, all'esfiltrazione e all'impatto

Con una conoscenza approfondita dell'organizzazione, dei suoi sistemi e dei suoi dati, gli autori delle minacce sono stati regolarmente in grado di raccogliere i dati sia dalle unità di condivisione della rete che dai sistemi locali (rispettivamente il 70% e il 50%) prima di esfiltrare i dati attraverso gli stessi canali C&C, o addirittura tramite protocolli alternativi o servizi web.[8]



È interessante notare che in tutti i casi in cui Fortinet è stata chiamata a indagare, i dati sono stati crittografati per aumentare al massimo l'impatto e, in un quarto dei casi, anche il ripristino del sistema è stato compromesso.[10]



Conclusioni

Cosa significa questo per i difensori?

Innanzitutto, smettere di dare la colpa ai controlli di sicurezza installati per non aver protetto le risorse dell'organizzazione. Quando gli aggressori utilizzano account validi per accedere a una rete, è necessario essere in grado di identificare le attività anomale o non autorizzate degli utenti validi e delle loro credenziali. Pertanto, le organizzazioni devono investire maggiormente in tecnologie e servizi di rilevamento e risposta per salvaguardare efficacemente la propria azienda.

Inoltre, i segni di attività dopo l'intrusione sono spesso disponibili, ma solo per i team e gli strumenti preparati a identificarli. Gli strumenti di registrazione e monitoraggio delle attività possono individuare l'installazione automatica, l'evasione, il rilevamento, il movimento laterale, le comunicazioni C&C e altro ancora, se correttamente configurati e monitorati.

Infine, per aumentare il ritorno sull'intrusione, gli autori delle minacce spesso procedono attraverso più fasi di azione. Questa è una buona notizia per i difensori, in quanto è sufficiente rilevare e interrompere tali attività in una sola fase per sventare l'attacco. Tuttavia, questo è possibile solo se l'organizzazione ha definito i processi e addestrato i suoi team ad eseguirli, che trasformeranno i singoli segnali in indicatori di incidenti a più alta fedeltà e attiveranno le azioni di contenimento e correzione. Idealmente, ciò assume la forma di playbook documentati, ripetibili e praticati per guidare il personale che potrebbe non avere le competenze, il tempo o la diligenza necessari per gestire un flusso costante di avvisi spesso banali. Detto questo, tali informazioni spesso tracciano un quadro importante degli attacchi in corso.

Per ulteriori approfondimenti sulle attività degli aggressori e sui suggerimenti per proteggere efficacemente la tua organizzazione, scarica una copia gratuita del report completo.

[1] FortiGuard Incident Response Report, 1H 2023, Fortinet, 17 ottobre 2023.

[2] Ibid.

[3] SOC Modernization and the Role of XDR, Enterprise Strategy Group, 24 ottobre 2022.

[4] FortiGuard Incident Response Report, 1H 2023, Fortinet, 17 ottobre 2023.

[5] Ibid.

[6] Ibid.

[7] Ibid.

[8] Ibid.

[9] Ibid.

[10] Ibid.

febbraio 16, 2024 10:27 AM

2451968-0-0-IT