proofpoint.

SCHEDA SULLE MINACCE

Violazione e takeover degli account cloud

In breve

DESCRIZIONE

La violazione degli account cloud consiste nell'ottenere il controllo dell'account cloud di un servizio email di un utente legittimo o di un servizio di collaborazione, al fine di ottenere l'accesso a una vasta gamma di dati, contatti, voci di calendario, email e altri strumenti di sistema. Oltre ai dati dell'utente compromesso, il criminale informatico può utilizzare l'account per impersonare l'utente in attacchi di social engineering come la violazione delle email aziendali (BEC, Business Email Compromise), sia all'interno che all'esterno dell'azienda. I criminali informatici possono accedere a dati sensibili, convincere utenti o partner commerciali esterni a inviare denaro o danneggiare la reputazione e le finanze di un'azienda. Possono anche installare backdoor per mantenere l'accesso per attacchi futuri.

STRUMENTI UTILIZZATI

- Attacchi di phishing, incluso il phishing dei token OAuth
- Attacchi di forza bruta che automatizzano la ricerca sistematica delle credenziali di accesso, come Aircrack-ng e Jack the Ripper
- Riciclo delle credenziali di accesso, o stuffing, che utilizza coppie di nome utente e password precedentemente rubate
- Malware, inclusi i keylogger e stealer delle credenziali come PunkeyOS e Spyrix

TIPI

- Furto delle credenziali di accesso: i criminali informatici sfruttano password deboli, sistemi di sicurezza non efficaci e password riutilizzate provenienti da altri siti per violare i sistemi.
- Applicazioni OAuth dannose: i criminali informatici utilizzano il phishing dei token OAuth e lo spoofing delle applicazioni per manipolare i proprietari degli account e spingerli a delegare i permessi di accesso alle risorse di sistema.
- Minacce interne: un comportamento negligente o intenti dolosi possono portare alla perdita delle credenziali d'accesso.
- Malware: il software dannoso installato nei sistemi può passare inosservato per lunghi periodi di tempo. Tale malware può rubare le credenziali e comunicare con i criminali informatici.

FATTORI DI RISCHIO

- Utilizzo di applicazioni e servizi informatici o cloud non approvati (Shadow IT) senza l'approvazione del dipartimento IT
- Strumenti inadeguati per il monitoraggio della sicurezza di email e cloud
- Condivisione delle credenziali d'accesso tra i dipendenti o con partner esterni
- Scarsa sensibilizzazione degli utenti in merito alle buone pratiche di sicurezza e alle tecniche comuni del phishing

La maggior parte delle aziende ha migrato le proprie risorse nel cloud. Lo stesso hanno fatto i criminali informatici. A partire da email e webmail in hosting, applicazioni di produttività cloud come Microsoft 365 e Google Workspace, fino agli ambienti di sviluppo cloud come AWS e Azure, i criminali informatici hanno capito il valore inestimabile delle credenziali di accesso e le hanno rese l'obiettivo di innumerevoli campagne di phishing. Poiché il single sign-on offre un accesso laterale a molti sistemi diversi all'interno di un'azienda, un singolo account compromesso può causare danni considerevoli.

La violazioni degli account cloud nei media

Capital One riceve una multa di 80 milioni di dollari per la violazione di 100 milioni di richieste di carte di credito nel 2019

Il Dipartimento di giustizia degli Stati Uniti ha arrestato Paige Thompson, un ex progettista software di Amazon, accusandola di frode telematica e abuso per il presunto accesso ai dati di Capital One. Utilizzando un attacco di falsificazione delle richieste lato server (SSRF, Server-Side Request Forgery), ha ottenuto le credenziali di accesso di qualcuno che aveva accesso a informazioni sensibili memorizzate nel servizio di archiviazione dei file Amazon S3. Secondo l'accusa, la Thompson si è vantata dei suoi exploit sul suo canale Slack e ha pubblicato le istruzioni su GitHub per replicare l'attacco[1].

NSA e FBI accusano la Russia di attacchi di forza bruta su larga scala contro Microsoft 365

Un rapporto congiunto pubblicato dal servizio di intelligence britannico, dalla National Security Agency degli Stati Uniti, dall'FBI e dal Dipartimento della Sicurezza Nazionale degli Stati Uniti ha identificato il gruppo di criminali informatici russo "Fancy Bear" come responsabile di una campagna di lunga durata per violare gli account Microsoft 365. Il gruppo ha fatto ricorso alla tecnica del "password spraying," un attacco cui i computer cercano di accedere a un account più volte in successione utilizzando diverse combinazioni di password [2].

1 Devling Barrett *(The Washington Post)*, "Capital One Fined $80 Million for 2019 Hack of 100 Million Credit Card Applications." (Capital One riceve una multa di 80 milioni di dollari per la violazione di 100 milioni di richieste di carte di credito nel 2019), agosto 2020.

2 Thomas Brewster *(Forbes),* "NSA and FBI Blame Russia for Massive 'Brute Force' Attacks On Microsoft 365." (NSA e FBI accusano la Russia di attacchi di forza bruta su larga scala contro Microsoft 365), luglio 2021.

Anatomia di un takeover degli account cloud

Ecco come si svolge la maggior parte degli attacchi di takeover degli account cloud.

1. **Furto delle credenziali d'accesso.** I criminali informatici ottengono l'accesso alle credenziali di accesso degli utenti tramite il phishing delle credenziali, attacchi di forza bruta contro le password, stuffing/riciclo delle credenziali di accesso, applicazioni OAuth dannose o malware che ruba le credenziali di accesso (consultare **"Strumenti utilizzati"** a pagina 1).
2. **Infiltrazione.** Una volta entrato nell'account dell'utente, il criminale informatico ha accesso all'email, ai contatti, al calendario e ai file della vittima. Il criminale informatico può rubare questi dati direttamente o usarli per impersonare l'utente in modo convincente.
3. **Persistenza e propagazione.** Alcuni truffatori rispondono a thread email esistenti o inviano email che contengono malware o URL non sicuri a colleghi e partner commerciali esterni. Fingendo di essere l'utente compromesso, il criminale informatico può quindi prendere di mira altre persone all'interno e all'esterno dell'azienda inviando loro fatture false o istruzioni per il reindirizzamento dei pagamenti. Il criminale informatico può anche caricare malware nelle condivisioni di file aziendali o sabotare l'azienda in altri modi. Spesso, il criminale informatico imposta regole di inoltro automatico che gli permetteranno di accedere all'email dell'utente anche se l'utente modifica la password. Avendo accesso a tutte le email in entrata e gli inviti del calendario, il criminale informatico ottiene dettagli chiave che potrà sfruttare per attacchi futuri.
4. **Monetizzazione.** Se una violazione dell'account non viene rilevata in tempo, può portare al furto di denaro o dati preziosi come record finanziari o proprietà intellettuale.

Gli attacchi portano a perdite di dati, bonifici bancari fraudolenti e violazioni del sistema

1	**RICOGNIZIONE**
	Phishing delle credenziali d'accesso
	Perdita o svuotamento
	Keylogger o malware
	Personale interno ostile
	Social Engineering
2	**INFILTRAZIONE**
	Ricerca sistematica delle credenziali d'accesso
	Login diretto
	Malware cloud (applicazioni di terze parti)
3	**PROPAGAZIONE, PERSISTENZA E APPRENDIMENTO**
	Mantenimento dell'accesso • Creazione di regole per il trasferimento delle email • Modifica dei permessi • Creazione di account amministrativi • Disabilitazione dell'autenticazione a più fattori • Creazione di un accesso di terze parti
	Utilizzo di account fidati per lanciare gli attacchi • Invio di email di phishing interne ed esterne • Caricamento e condivisione di malware
	Misurazione del potenziale • Visualizzazione di email e file • Esplorazione della struttura organizzativa • Studio dei processi aziendali
4	**MONETIZZAZIONE**
	Violazione dell'email aziendale / Frodi via email • Bonifici bancari fraudolenti • Frode degli stipendi • Frode delle carte regalo • Frode della supply chain
	Esfiltrazione dei dati • Email • Download • Condivisione
	Sabotaggio • Ransomware cloud • Distruzione
	Violazione dei sistemi • Spam • Frodi come servizio • Estrazione di criptovalute

Fattori di rischio e conseguenze associate con il takeover degli account cloud

Come proteggere la tua azienda

- Evita che le email di phishing delle credenziali di accesso raggiungano le caselle email dei tuoi utenti.
- Trasforma i tuoi utenti in una solida linea di difesa grazie alla formazione sulle best practice per le password e insegnando loro come riconoscere le email di phishing. Idealmente, dovrebbero essere in grado di segnalare in modo semplice i messaggi sospetti.
- Prendi in considerazione una soluzione CASB (Cloud Access Security Broker) per ottenere una vista consolidata dei servizi cloud della tua azienda. Questa soluzione dovrebbe includere i dettagli degli utenti e delle applicazioni OAuth con accesso ai dati nei servizi cloud da qualsiasi dispositivo o luogo.
- Adotta un approccio Zero Trust per l'accesso alla rete e alle applicazioni per limitare i danni da parte di un account compromesso.
- Analizza le email interne, non solo i messaggi in arrivo, per minacce come il malware e le frodi via email.
- Abilita un'autenticazione a più fattori. Sebbene non sia sempre la soluzione definitiva contro il takeover degli account, rende più difficile il compito di un criminale informatico.
- Identifica gli utenti più a rischio e monitora gli incidenti.
- Imposta e assegna le priorità agli incidenti in base ai fattori di rischio più critici per la tua azienda.
- Correla le minacce per email e cloud per rilevare con precisione gli account compromessi.
- Assicura la governance delle applicazioni OAuth e revoca le applicazioni dannose o pericolose.
- Previeni i clic sugli URL dannosi e i download malware isolando la navigazione sul web.
- Analizza gli incidenti di sicurezza con una soluzione che fornisce analisi forensi dettagliate e report personalizzabili.
- Blocca l'accesso non autorizzato alle applicazioni e ai servizi cloud tramite controlli adattivi degli accessi, specialmente per i dispositivi non gestiti.
- Automatizza la risposta agli incidenti di sicurezza con controlli delle policy flessibili che attivano un allarme quando si verifica un incidente o la modifica del profilo di rischio degli utenti. Gli utenti sotto attacco o che rappresentano un rischio maggiore a causa delle loro abitudini digitali o accesso ai privilegi si devono ri-autenticare regolarmente.

Osservazioni della ricerca

Proofpoint ha monitorato migliaia di tenant cloud e oltre 20 milioni di utenti cloud attivi. In uno studio del 2020 sui dati delle minacce cloud, abbiamo rilevato quanto segue:

95% delle aziende è stato colpito.

52% delle aziende ha subito la violazione di almeno un account.

32% delle aziende violate ha riscontrato un'attività post-violazione: manipolazione dei file, inoltro delle email e attività all'interno di applicazioni OAuth.

10% delle aziende aveva autorizzato applicazioni OAuth dannose.

Secondo l'86% dei responsabili IT intervistati per un report 2021 del Ponemon Institute commissionato da Proofpoint, la violazione degli account cloud costa alle aziende oltre 500.000 dollari all'anno[3].Gli intervistati hanno anche segnalato una media di 64 violazioni degli account cloud all'anno, il 30% delle quali ha portato alla divulgazione di dati sensibili[4].

Quasi il 60% degli intervistati ha indicato che gli account Microsoft 365 e Google Workspace sono duramente colpiti da attacchi di phishing e forza bruta nel cloud.

Complessivamente, oltre il 50% ha affermato che il phishing è il metodo che i criminali informatici utilizzano più frequentemente per acquisire credenziali di accesso al cloud legittime.

3 Ponemon Institute, "Cost of Cloud Compromise and Shadow IT." (Il costo delle violazioni cloud e della Shadow IT), aprile 2021.
4 Ibid.

Per saperne di più

Per contrastare la violazione degli account cloud, le aziende devono assicurarsi di disporre di solide misure di sicurezza. Le piattaforme di sicurezza devono fornire crittografia end-to-end e monitoraggio continuo dei dati oltre a rilevare rapidamente gli incidenti per permettere agli amministratori di limitare e porre rimedio a qualsiasi danno.

Per scoprire come contrastare la violazione degli account cloud in modo efficace, visita il sito **www.proofpoint.com/it**.

INFORMAZIONI SU PROOFPOINT

Proofpoint è un'azienda leader nella cybersecurity e nella conformità, che protegge dai rischi il patrimonio più importante di un'azienda: le persone. Con una suite integrata di soluzioni basate su cloud, Proofpoint aiuta le aziende di tutto il mondo a bloccare le minacce mirate, a salvaguardare i propri dati e a proteggere gli utenti dagli attacchi IT. Aziende di ogni dimensione, tra cui più della metà delle Fortune 1000, si affidano alle soluzioni di sicurezza e di conformità incentrate sulle persone di Proofpoint per mitigare i rischi di sicurezza veicolati via email, cloud, social media e web. Per ulteriori informazioni: **www.proofpoint.com/it**.

©Proofpoint, Inc. Proofpoint è un marchio commerciale di Proofpoint, Inc. negli Stati Uniti e negli altri Paesi. Tutti gli altri marchi qui menzionati appartengono ai rispettivi proprietari.