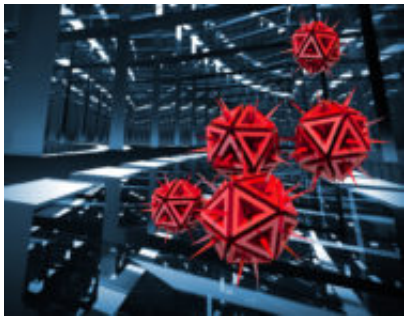
Insider Threat: Tecniche di Exfiltration

Author : Mattia Reggiani

Date : 26 settembre 2018



In questo articolo verranno trattate alcune tecniche esercitate dagli attaccanti interni per trasferire dati e informazioni al di fuori della rete aziendale. Nella seconda parte dell'articolo verrà approfondito un approccio di monitoraggio e simulazione d'attacco con il fine di prevedere gli eventi avversi più comuni.

Introduzione

E' credenza comune che la maggior parte delle minacce informatiche siano riconducibili a fattori esogeni, con la visione stereotipata dell'attaccante che cerca di penetrare la rete aziendale da una postazione remota. Questa limitazione porta a trascurare i rischi di natura endogena, alle quali un'azienda è sottoposta quotidianamente.

Contribuiscono inoltre ad alimentare un illusorio senso di sicurezza i vari componenti tecnologici quali firewall e antivirus; la tendenza è quella di fidarsi della propria infrastruttura al punto che nello svolgere le analisi di rischio, le minacce interne vengono spesso associate a probabilità di accadimento basse e trascurabili.

Non esiste una definizione unica di insider: ai fini dell'articolo considereremo "insider threat" un individuo o un programma che sfrutta la sua posizione interna al sistema per commettere azioni malevole. Nello specifico, l'articolo si focalizzerà unicamente su minacce interne di natura colposa.

E' possibile delineare due principali macro-categorie di insider:

- Personale dipendente e terze parti che, da un account aziendale, hanno la possibilità di effettuare attacchi informatici alla rete.
- Malware, un programma informatico usato per condurre attività indesiderate. L'attacco di un software malevolo è solitamente considerato un fattore rischio esogeno, tuttavia in questa sede considereremo il caso in cui il malware si sia già insidiato nell'infrastruttura aziendale.

Il patrimonio aziendale che può rientrare nel mirino degli insider è molto vasto. Nel mondo digitale, il dato è una risorsa strategica fondamentale: le informazioni aziendali riservate, proprietà intellettuale, dati personali di clienti e di dipendenti, potrebbero facilmente costituire un obiettivo di alto valore per qualsiasi attaccante. In termini di asset aziendali, i database ed i file server sono quelli più colpiti, essendo per loro natura una fonte significativa di dati digitali.

Tecniche di Exfiltration

Con il termine “exfiltration”, si fa riferimento all'insieme di tecniche utilizzate al fine di trasferire dati e informazioni da una rete, o più in generale da un elaboratore, verso un’infrastruttura governata dall'attaccante, in modo non autorizzato. L’esportazione può avvenire principalmente in due approcci:

- Manuale, ad esempio tramite accesso fisico a un elaboratore utilizzando device quali external hard drive, USB drive, o altri dispositivi di memoria rimovibili.
- Seguendo una procedura semi-automatizzata attraverso l’utilizzo di un programma malevolo. Tale tecnica sfrutta il canale di comunicazione di rete esistente e non richiede alcun accesso fisico. In questo caso, la trasmissione dei dati potrebbe avvenire adoperando connessioni cablate, WiFi, Bluetooth o un altro canale di radiofrequenza.

Approfondiremo di seguito l’approccio più diffuso illustrando le tecniche di exfiltration semi-automatizzate, tramite quindi canali di comunicazione digitali.

Negli ultimi anni, i protocolli di rete sfruttati dagli attori malevoli per trasferire informazioni sono stati: ICMP (Internet Control Message Protocol), UDP (User Datagram Protocol) e TCP (Transmission Control Protocol).

ICMP

Il protocollo ICMP è utilizzato generalmente dagli amministratori di rete per trasmettere informazioni tra gli elaboratori di una rete, come per esempio malfunzionamenti o dati di controllo. Le ragioni per le quali viene abilitato questo protocollo possono essere varie, tra cui manutenzione facilitata della rete.

Questo protocollo potrebbe essere impiegato per veicolare dati all'interno dei singoli pacchetti e trasportare quindi informazioni: abusando della funzionalità echo request[1], è possibile iniettare dati in uno spazio di qualche byte riservato al payload. Nel dettaglio, il pacchetto basato su IPv4[2] è composto da 20 bytes per lo IPv4 header, 8 byter per lo ICMP header e una dimensione di byte arbitraria (fino a raggiungere il massimo valore consentito dalla MTU[3] per l’intero pacchetto) per il ICMP payload dove concretamente sono inseriti i dati da exfiltrare.

UDP

I protocolli UDP e TCP non sono protocolli di amministrazione, ma sono designati per trasferire dati tra gli elaboratori tramite le applicazioni software.

Nelle reti aziendali, l'utilizzo più comune del protocollo UDP è per il servizio DNS (Domain Name System): un sistema utilizzato per la risoluzione di nomi dei nodi della rete in indirizzi IP. Tali indirizzi IP sono essenziali per inviare e ricevere i pacchetti di rete, tramite le applicazioni. Infatti, per poter far funzionare un normale browser web, è necessario abilitare questo servizio nel firewall perimetrale e risulta usuale trovare questo canale di comunicazione abilitato nelle reti aziendali.

Anche in questo caso è possibile abusarne per veicolare dati da exfiltrare, utilizzando appunto la risoluzione dei nomi di dominio: anzichè risolvere il hostname, è possibile inserire una sequenza di byte arbitrari, opportunamente codificati per rispettare i caratteri consentiti[4], al fine di inviare dati. Mentre per la ricezione di dati, è consigliato utilizzare il campo DNS TXT in quanto può ospitare diversi byte.

Tale canale di comunicazione, come ICMP è molto limitato in termini di quantità di byte che si possono far veicolare in un singolo pacchetto. Questo è uno dei motivi per cui TCP risulta essere più idoneo e che si presta meglio all'invio di dati, considerata inoltre la sua caratteristica di trasferire i pacchetti in modo affidabile.

TCP

Molti software, inclusi i browser di navigazione web, sono basati sul protocollo TCP. Nel dettaglio, il protocollo TCP supporta diverse applicazioni, tra cui appunto i servizi web HTTP (Hypertext Transfer Protocol) e HTTPS (Hyper Text Transfer Protocol Secure), ma anche altre implementazioni tra cui FTP[5] (File Transfer Protocol) e Email[6].

Il servizio FTP è stato creato per trasferire file, quindi chiaramente un'interessante via per veicolare dati, però é assai probabile che questo utilizzo venga prevenuto, disattivandolo oppure chiudendo la connessione di uscita. Mentre invece il protocollo di posta elettronica risulta generalmente abilitato, specialmente per le reti aziendali. Tale sistema potrebbe essere tranquillamente utilizzato per trasferire dati e informazioni, sotto forma di testo o allegato. In particolar modo se si utilizzano servizi email di terze parti, il monitoraggio delle informazioni passanti per i server di posta risulta molto complicato.

HTTP(S)

Analizzando in dettaglio il servizio HTTP, basato sul protocollo TCP, è possibile capire il motivo per cui è diventato uno dei migliori metodi utilizzato per exfiltrare informazioni. Tale servizio web è difatti adoperato principalmente per la navigazione Internet e quindi abilitato verosimilmente in tutte le reti aziendali. L'attaccante che vorrà trasferire informazioni potrà fare affidamento sicuro a questo canale.

La versione HTTPS aggiunge inoltre un canale di comunicazione cifrato: in questo caso, specialmente per quelle organizzazioni che non intercettano il traffico TLS (Transport Layer Security), è pressoché improbabile decifrare il traffico passante sulla rete analizzando i pacchetti, e quindi venire a conoscenza di quale dato stia lasciando la rete interna.

Negli ultimi anni si sono viste diverse mitigazioni a questa minaccia, tra cui consentire o meno la connessione web ai siti non trusted e con reputazione bassa. Questo meccanismo di prevenzione si potrebbe eludere facilmente utilizzando i servizi cloud di terze parti, i quali hanno guadagnato un'alta reputazione (quindi meno monitorati nelle reti aziendali) e solitamente sono sempre consentiti nelle policy aziendali.

Prevenzione: monitoring e proactive assessment

L'elaborazione di una strategia di sicurezza dei dati efficace e un sistema di controllo interno é essenziale al fine di prevenire attacchi informatici, individuarli e bloccarli.

Un buon approccio per fronteggiare questi tipi di minacce è la defence-in-depth, che utilizza vari livelli e strati di tecnologie, processi e personale per una protezione totale. Al giorno d'oggi dal punto di vista tecnologico, la forma di detection e mitigation più utilizzata nelle medio e grandi organizzazioni sono i sistemi di Data Loss Prevention (DLP), seguite delle soluzioni SIEM (Security Incident Event Management) incaricati di correlare ad analizzare i log. Possono essere poi configurati ulteriori tecnologie quali Identity Access Management (IAM), Intrusion Detection e Prevention Systems (IDS e IPS).

Secondo le best practices e gli standard industriali di settore, quali NCSC[7] e CSC[8], il monitoraggio degli eventi di sicurezza è un elemento chiave della sicurezza aziendale. Generalmente il monitoraggio e correlazione degli eventi di sicurezza è l'attività principale del SOC (Security Operation Centre), per poi rispondere prontamente agli incidenti informatici.

L'attività successiva alla definizione di un consolidato defence-in-depth, è quella di eseguire delle simulazioni d'attacco quanto piu realistiche per misurare i tempi di risposte ed i tempi di intervento alla minaccia. Considerata la notevole evoluzione degli attacchi reali su ampia scala, le organizzazioni hanno la necessità di evolvere i propri approcci al security testing, con l'ottica di valutare l'effettiva resilienza contro gli attacchi di natura "cyber" e colmare il divario tra security testing dell'infrastruttura e scenari d'attacco reali. Partendo da tale aspetto, le attività di red teaming utilizzano le tattiche, le tecniche e gli strumenti allo stato dell'arte per simulare un attacco reale contro un'organizzazione e verificarne la reale resilienza, valutando inoltre l'efficacia e la capacità di detection delle strutture SOC.

Al fine di testare l'effettiva resilienza e preparazione agli attacchi informatici, e specialmente le minacce insider, la simulazione d'attacco deve prevedere di emulare le tecniche di exfiltration precedentemente descritte, sia in termini di canali sfruttati che di tipologie di dato carpito.

La parte critica di un' operazione di adversary simulation, è fare in modo che il team attaccante rimanga quanto più invisibile e trasparente al team interno di difesa dell'organizzazione attaccata, evitando pertanto di far scattare gli alert ed essere rilevati da vari meccanismi di sicurezza (Firewall, IDS/IPS e AV).

Infine, uno degli indicatori più importanti di questo esercizio è rappresentato dalla durata del tempo medio da rilevazione MTTD (Mean Time To Detect) e dal tempo medio di recovery MTTR (Mean Time To Recover) per la squadra di difesa, che dovrebbero essere migliorati per

ogni attacco eseguito.

Conclusione

Negli ultimi anni sono cresciuti in modo quasi esponenziale nuovi tipi di attacchi informatici, più complessi, comunemente chiamati APT (Advanced Persistence Threat) che sono in grado di creare e personalizzare i vettori di attacco per essere pienamente funzionanti con l'ambiente di destinazione. Le semplici attività di valutazione delle vulnerabilità ed i penetration test non sono più sufficienti a soddisfare e mitigare la minaccia di un attacco informatico, poiché in molti casi l'anello più debole nella catena di sicurezza è il fattore umano e l'uso appropriato delle tecnologie.

In questo contesto, le simulazioni d'attacco focalizzate sulle attività che un'attaccante compie una volta inserito nella rete interna, consentono di ottenere una comprensione della resilienza dell'organizzazione contro tali vettori, il miglioramento delle capacità investigative e di risposta del team di sicurezza della difesa, permettendo infine di valutare il ritorno degli investimenti di un'organizzazione sulla sicurezza delle informazioni.

Riferimenti

Understanding the insider threat & how to mitigate it - NCC Group
https://www.nccgroup.trust/uk/our-research/understanding-the-insider-threat-and-how-to-mitigate-it/

MITRE ATT&CK
https://attack.mitre.org/

Wikipedia, the free encyclopedia
https://wikipedia.org

Insider Threat Report: 2018 - CA Technologies
https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf

Note

1. Anche conosciuta come “ping”, è una funzionalità del protocollo ICMP con i seguenti parametri: Type 8 eCode 0. Si veda RFC 792 (https://tools.ietf.org/html/rfc792).
2. Internet Protocol version 4, è la quarta revisione dell'Internet Protocol. Si veda RFC 791 (https://tools.ietf.org/html/rfc791).
3. Maximum Transmission Unit, rappresenta il datagramma di dimensioni massime che può essere trasmesso attraverso la rete, generalmente 1500 byte.
4. Ogni sottodomino può avere una dimensione massima di 63 caratteri, e l'intero hostname 253 caratteri. I caratteri accettati possono essere lettere dalla “a” alla “z”, numeri dallo ‘0’ al ‘9’ e il segno meno ‘-‘.
5. Nelle sue versioni cifrate SCP (Secure Copy Protocol) e SFTP (SSH File Transfer

Protocol o Secure File Transfer Protocol).
6. Con i protocolli SMTP (Simple Mail Transfer Protocol), IMAP (Internet Message Access Protocol) e POP3 (Post Office Protocol 3).
7. National Cyber Security Centre (https://www.ncsc.gov.uk/guidance/10-steps-cyber-security)
8. CIS Critical Security Controls (https://learn.cisecurity.org/20-controls-download?f=CSC-MASTER-VER%25206.0%2520CIS%2520Critical%2520Security%2520Controls%2520%252010.15.2015)

Articolo a cura di **Mattia Reggiani**