UNIVERSITÀ DI PAVIA
Area Sistemi Informativi

n 10 Luglio 2023

Attacchi informatici: le misure di difesa dell'Ateneo nell'ultimo mese

I tentativi di intrusione nei sistemi informatici o di raccolta illecita di informazioni sono un fenomeno da monitorare e fronteggiare quotidianamente in Ateneo.

Ad oggi non ci sono state perdite di dati grazie alle misure di protezione adottate che hanno ben anticipato le intenzioni malevole e messo al sicuro il lavoro interno svolto.

La sicurezza collettiva dipende molto anche dalla responsabilità del singolo nell'utilizzare i propri dispositivi, tenerli aggiornati e relazionarsi con l'Area Sistemi Informativi qualora non si senta adeguatamente protetto.

I numeri sotto riportati evidenziano infatti ancora margini di miglioramento nel comportamento di ciascuno di noi oltre alla necessità di un costante lavoro interno ad ogni struttura al fine di acquisire consapevolezza dei rischi e quindi di adottare comportamenti adeguati alle condizioni di sicurezza.

In questo mese abbiamo avuto 11 pc infetti che sono stati segnalati e bonificati e circa 151 comunicazioni C&C rilevate e bloccate. Il drastico calo di comunicazioni C&C. Il perdurare dei test di Cisco Umbrella che permette un blocco delle comunicazioni malevoli a livello di risoluzioni DNS si sta rivelando uno strumento fondamentale per ridurre i rischi di attacchi.

Queste tipologie di attacchi rappresentano uno dei primi fenomeni da monitorare poiché potrebbero nascondere malware, cryptolocker o altri fenomeni malevoli che approfondiremo nei successivi numeri di questa newsletter.

In questo numero della newsletter relativa alla cybersecurity tratteremo delle tecniche di attacco "Man-in-the-Middle".

Malware and Attacks

11
Computers Infected with Bots

151
Communications with C&C* Sites

* C&C - Command and Control.
If proxy is deployed, there might be additional infected computers.

4 Known Malware Downloaded by

10 Users

2 Zero-Days Downloaded

Zero-days downloaded present a unique count of old or new malware variant with un-known anti-virus signature.

123
Unique Software Vulnerabilities were Attempted to be Exploited

Indicates potential attacks on computers on your network.

High Risk Web Access

6
High Risk Web Applications

19.4MB

Potential risks: opens a backdoor to your network, hides user activity, causes data leakage or malware infections.

0
High Risk Web Sites

0 hits

Potential risks: Exposure to web-based threats and network infection. Examples: Spam, malicious, phishing web sites.

SaaS Applications

0
SAAS Applications Seen

1
Users Using SAAS Application

Applications that have integration with our Harmony Email & Collaboration solution and can be fully protected by our Threat Prevention engines.

Data Loss

0
potential data loss incidents

0
sensitive data categories

Indicates information sent outside the company or to unauthorized internal users. Information that might be sensitive. See GDPR Article 5

Attacchi “Man-in-the-Middle”.

Un attacco “Man-in-the-Middle” (MITM) è una forma di attacco informatico in cui una terza parte “malintenzionata” si posiziona tra due sistemi che stanno comunicando, intercettando e potenzialmente manipolando la comunicazione tra di esse senza che le parti coinvolte ne siano consapevoli.

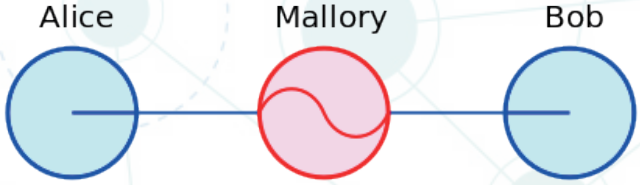
Il funzionamento dell’attacco Man-in-the-Middle avviene tipicamente in questo modo:

1. Il mittente invia i suoi dati a un destinatario.
2. Il malintenzionato, posizionandosi tra il mittente e il destinatario, intercetta i dati trasmessi.
3. Il malintenzionato può decidere di passare semplicemente i dati ricevuti al destinatario, in modo che sembri che la comunicazione sia avvenuta senza intoppi.
4. In alternativa, il malintenzionato può anche manipolare i dati prima di inviarli al destinatario, al fine di alterare la comunicazione o svolgere altre azioni dannose.
5. Il destinatario riceve i dati, senza rendersi conto che sono stati intercettati o manipolati.

Questo tipo di attacco può essere eseguito su diversi ambiti, tra cui reti Wi-Fi, reti cablate, messaggi e comunicazioni web. L’obiettivo principale di un attacco Man-in-the-Middle può essere quello di intercettare e raccogliere informazioni sensibili, come credenziali di accesso, informazioni finanziarie o dati personali.

Facendo un esempio concreto:

Supponiamo che Alice voglia comunicare con Bob e che Mallory voglia spiare la conversazione e, se possibile, consegnare a Bob dei falsi messaggi. Per iniziare, Alice deve chiedere a Bob la sua chiave pubblica. Se Bob invia la sua chiave pubblica ad Alice, ma Mallory è in grado di intercettarla, può iniziare un attacco “Man in the middle”. Mallory può semplicemente inviare ad Alice una chiave pubblica della quale possiede la corrispondente chiave privata. Alice poi, credendo che questa sia la chiave pubblica di Bob, cifra i suoi messaggi con la chiave di Mallory ed invia i suoi messaggi cifrati a Bob. Mallory quindi li intercetta, li decifra, ne tiene una copia per sé, e li re-cifra (dopo averli alterati se lo desidera) usando la chiave pubblica che Bob aveva originariamente inviato ad Alice. Quando Bob riceverà il messaggio cifrato, crederà che questo provenga direttamente da Alice.



1. Alice invia un messaggio a Bob, il quale viene intercettato da Mallory:
   Alice *“Ciao Bob, sono Alice. Dammi la tua chiave.”* → Mallory Bob

2. Mallory ritrasmette il messaggio a Bob, Bob non può sapere che non si tratta realmente di Alice:
   Alice Mallory *“Ciao Bob, sono Alice. Dammi la tua chiave.”* → Bob
3. Bob risponde con la propria chiave:
   Alice Mallory ← [chiave di Bob] Bob
4. Mallory sostituisce la chiave di Bob con la propria e la ritrasmette ad Alice, sostenendo sia la chiave di Bob:
   Alice ← [chiave di Mallory] Mallory Bob
5. Alice cripta un messaggio con quella che crede essere la chiave di Bob, pensando che solo Bob potrà leggerlo:
   Alice *“Incontriamoci in piazza!”* [criptato con la chiave di Mallory] → Mallory Bob
6. Ora Mallory può decriptare il messaggio, essendo stata usata la sua chiave, leggerlo, modificarlo se lo desidera, criptarlo con la chiave di Bob e infine inviarlo a Bob:
   Alice Mallory *“Incontriamoci in stazione!”* [criptato con la chiave di Bob] → Bob
7. Bob crede che questo messaggio provenga da una comunicazione sicura con Alice.

Entrando più nel dettaglio un attacco Man-in-the-Middle (MITM) può avvenire secondo le seguenti tipologie:

1. **Interposizione:** Un attaccante cerca di interporre se stesso tra il mittente (A) e il destinatario (B) durante la comunicazione. Ciò può avvenire sia su reti cablate che wireless, come ad esempio sulle reti Wi-Fi o Ethernet.
2. **Intercezione:** Una volta posizionato tra A e B, l’attaccante intercetta il traffico che fluisce tra le due parti. Questo può essere realizzato mediante l’uso di software o dispositivi specializzati, noti come “sniffing tools”, che consentono di catturare e analizzare i pacchetti di dati scambiati tra A e B.
3. **Spoofing:** Dopo aver intercettato il traffico, l’attaccante può impersonare sia A che B per entrambe le parti coinvolte. In altre parole, l’attaccante farà credere ad A di essere B e a B di essere A. In questo modo, le due parti non si accorgono che c’è un intruso tra di loro.
4. **Manipolazione:** Un attacco Man-in-the-Middle può anche prevedere la manipolazione dei dati scambiati tra A e B. L’attaccante può modificare il contenuto dei messaggi, inserire informazioni false o addirittura bloccare alcuni messaggi. Questo tipo di manipolazione mira spesso a indurre in errore o ingannare le due parti coinvolte.

Scenari di attacco Man-in-the-Middle.

1. **Wi-Fi pubbliche non sicure:** Le reti Wi-Fi pubbliche, come quelle presenti in caffetterie, aeroporti o hotel, spesso non offrono una protezione adeguata. Gli attaccanti possono utilizzare queste reti per posizionarsi tra gli utenti e i servizi online a cui si connettono.

2. **Phishing:** Un attacco Man-in-the-Middle può essere utilizzato come parte di un attacco di phishing. L'attaccante può intercettare le credenziali di accesso dell'utente mentre quest'ultimo tenta di effettuare il login su un sito Web contraffatto, creando una pagina falsa simile a quella legittima.
3. **Siti Web non sicuri:** Gli attaccanti possono sfruttare vulnerabilità nei siti Web non sicuri o non crittografati per intercettare e manipolare le informazioni sensibili scambiate tra gli utenti e il sito.
4. **Attacchi a reti aziendali:** In un ambiente aziendale, un attacco Man-in-the-Middle può essere utilizzato per monitorare e intercettare il traffico tra i dipendenti e i server dell'azienda, compromettendo dati aziendali sensibili.

Modalità di difesa.

Per proteggersi da questo tipo di attacchi, è consigliabile utilizzare connessioni sicure e crittografate, come il protocollo HTTPS per i siti web. Inoltre, si sconsiglia l'uso reti Wi-Fi pubbliche non sicure e assicurarsi di avere un software di sicurezza aggiornato sui propri dispositivi.

Proteggersi da un attacco Man-in-the-Middle richiede una combinazione di precauzioni tecniche e comportamentali. Ecco alcuni suggerimenti dettagliati per ridurre il rischio di essere vittima di questo tipo di attacco:

1. **Utilizzare connessioni crittografate:**
   - Quando si accede a siti Web, assicurarsi di connettersi a quelli che utilizzano il protocollo HTTPS. La presenza del lucchetto e il prefisso "https://" nell'URL del sito indicano che la connessione è crittografata.
   - Evitare di accedere a siti che richiedono informazioni sensibili tramite connessioni non crittografate (HTTP).
   - Utilizzare una VPN (Virtual Private Network) quando ci si connette a reti Wi-Fi pubbliche o non sicure. La VPN crittografa tutto il traffico di rete tra il dispositivo e il server VPN, proteggendo le comunicazioni da eventuali intercettazioni.
2. **Verificare l'autenticità dei siti Web:**
   - Prima di inserire dati sensibili su un sito Web, verificare attentamente l'URL per accertarsi di essere sul sito corretto. Gli attacchi di phishing possono trarre in inganno utilizzando URL simili a quelli legittimi.
   - Utilizzare password manager o funzioni di autocompletamento dei browser per evitare di digitare le credenziali su siti contraffatti.
3. **Aggiornare e proteggere i dispositivi:**
   - Mantenere sempre aggiornato il sistema operativo, il software e le applicazioni sul proprio dispositivo. Le versioni più recenti spesso correggono vulnerabilità note.
   - Attivare il firewall e utilizzare un software antivirus e anti-malware per rilevare e prevenire eventuali minacce informatiche.
4. **Evitare reti Wi-Fi non sicure:**

- Evitare di connettersi a reti Wi-Fi pubbliche o non sicure, come quelle in aeroporti, caffetterie o hotel, quando si tratta di attività sensibili, come il banking online o l'accesso a informazioni personali.
- Se necessario, utilizzare una VPN per cifrare il traffico Wi-Fi e proteggere le comunicazioni.

5. **Verificare i certificati:**
   - Quando si accede a siti Web crittografati, è possibile verificare il certificato digitale del sito per assicurarsi che sia valido e corrisponda al sito che si sta visitando.
   - Verificare che il certificato sia stato rilasciato da un'autorità di certificazione attendibile e che non siano presenti errori o avvisi di sicurezza nel browser.
6. **Sensibilizzazione e formazione:**
   - Educarsi e sensibilizzare se stessi e gli altri sui rischi degli attacchi Man-in-the-Middle e delle pratiche di sicurezza informatica in generale.
   - Essere cauti e sospettosi riguardo a e-mail, messaggi o link sospetti che potrebbero essere collegati a attacchi di phishing o di intercettazione.

Seguendo queste misure precauzionali e praticando la consapevolezza delle minacce informatiche, sarà possibile ridurre notevolmente il rischio di essere vittima di un attacco Man-in-the-Middle. La sicurezza informatica è un impegno continuo, quindi è importante rimanere sempre informati sulle nuove minacce e adottare le migliori pratiche di sicurezza disponibili.

Per saperne di più...

- per informazioni: **https://trasformazionedigitale.unipv.it**
- per contattare l'Area Sistemi Informativi: **https://sos.unipv.it**
- se sei uno studente scrivi a questo indirizzo: **smart@ unipv.it** oppure contatta un tecnico del tuo dipartimento per ottenere informazioni
- informazioni in tempo reale su attacchi informatici: **https://www.csirt.gov.it**

Fonti

- Wikipedia portale sicurezza informatica - *Attacco "Man-in.-the-Middle"*
- Kaspersky Lab - *"Man-in.-the-Middle"*