La Threat Intelligence e il contrasto agli Advanced Persistent Threats

Giorgio Di Tizio

Dipartimento di Ingegneria e Scienza dell'Informazione

Universita' degli Studi di Trento

Attacco informatico

E’ un attivita’ malevola che ha come obiettivo di collezionare, distruggere o degradare sistemi informatici o informazioni presenti in essi

- Rendere inaccessibile il sito web di un azienda attraverso attacchi DDoS
- Accedere a dati sensibili per rivenderli o renderli illeggibili attraverso attacchi ransomware

Principali motivazioni alla base di un attacco informatico:

1. Economiche
2. Spionaggio
3. Ideologiche
4. Divertimento

Attacco Targeted vs Untargeted

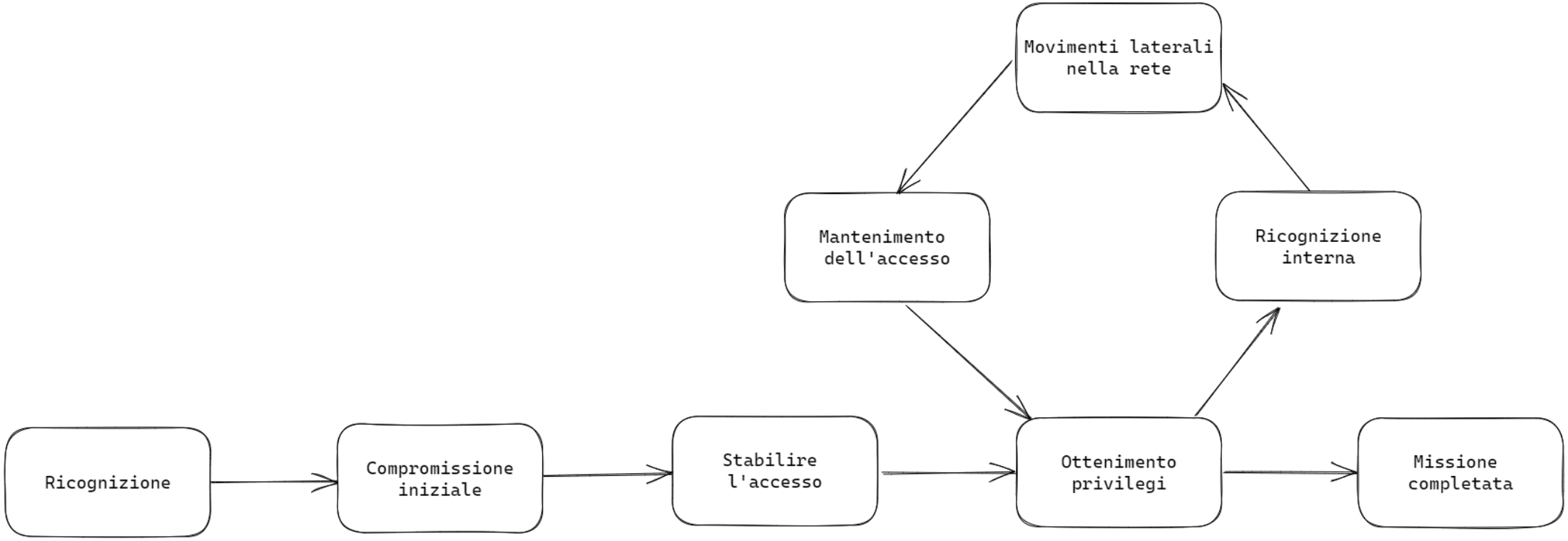
Attacco targeted → attacco informatico rivolto a una specifica organizzazione o persona. Es. Un azienda, un'ente governativo o un giornalista

- Richiede un'attivita' di ricognizione e scanning per identificare i punti deboli dell'obiettivo

Attacco untargeted → attacco informatico opportunistico rivolto a un non definito insieme di utenti o organizzazioni

- Richiede la distribuzione di trappole generiche per la compromissione iniziale

La Kill chain di un attacco informatico



Compromissione iniziale

- Vettore di attacco → tecnica utilizzata dagli attaccanti per entrare in una rete o un sistema
- Esistono diversi vettori di attacco utilizzati per l'accesso iniziale, non necessariamente permettono il mantenimento dell'accesso alla macchina o alla rete
- Esempi:
  - USB contenente malware
  - Phishing
  - Exploitation di Web applications
  - Drive-by
  - Supply-chain

Attacco Phishing

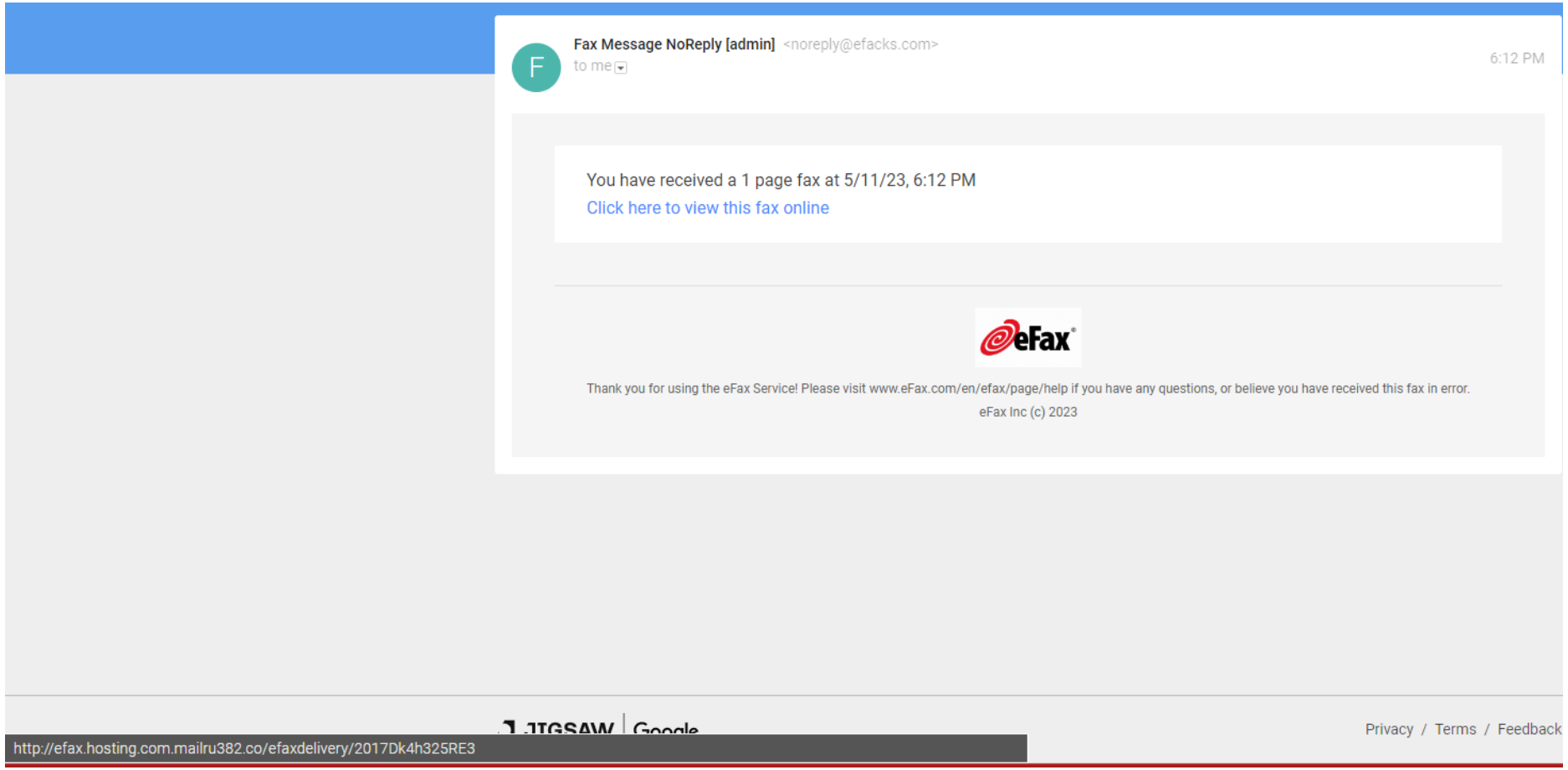
Invio di messaggi ingannevoli ad un utente con l'obiettivo di indurlo a:

- rivelare dati sensibili (es. password, carta di credito)
- eseguire codice malevolo (es. lanciare un eseguibile, visitare un sito web compromesso)

Tipicamente utilizza tecniche di social engineering per spingere l'utente ad eseguire un'azione che normalmente non farebbe

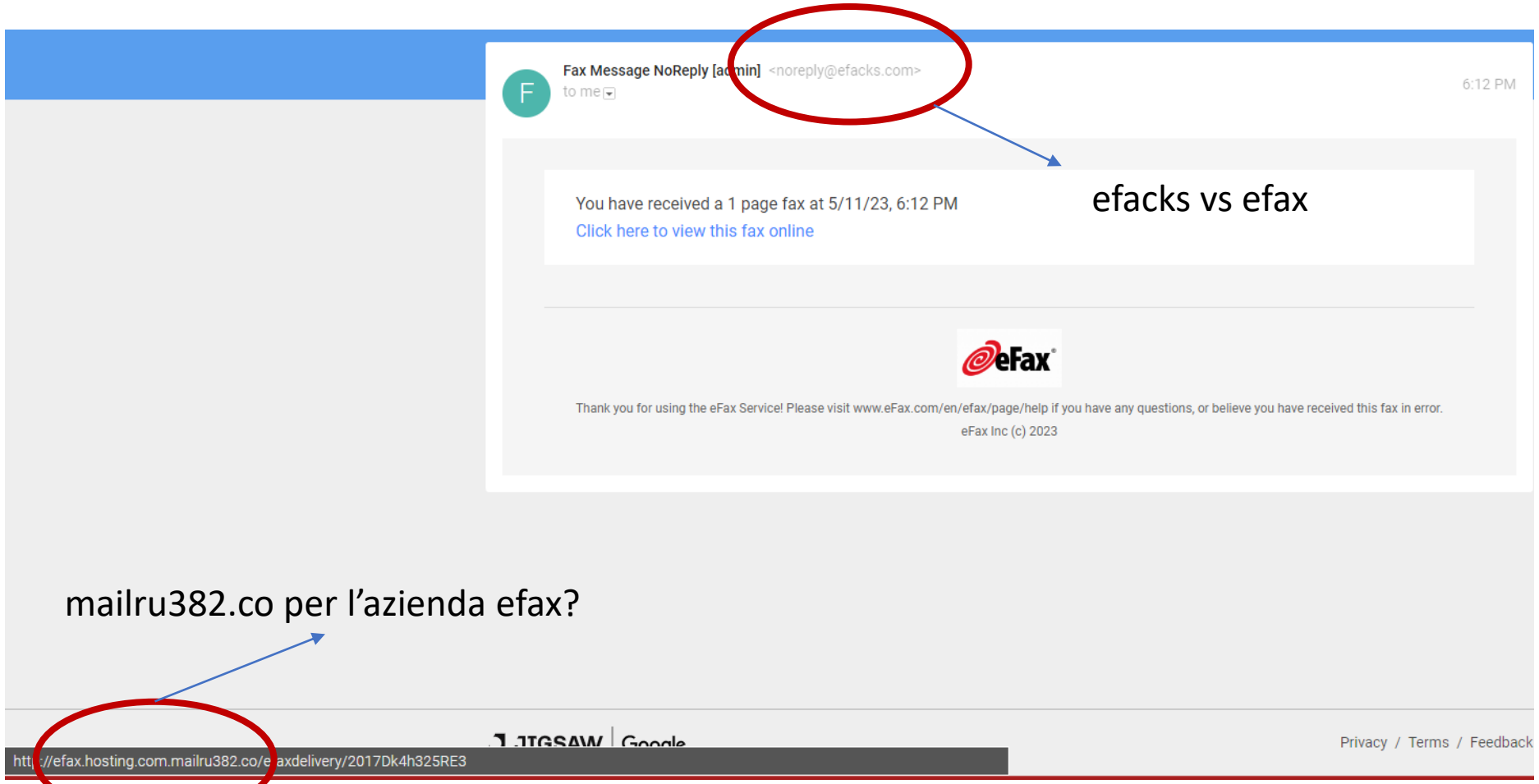
Diversi vettori utilizzati: email, social network, SMS

Legittima o Phishing?



https://phishingquiz.withgoogle.com/

Legittima o Phishing?



https://phishingquiz.withgoogle.com/

Alcune regole per proteggersi

- In generale: prendere ogni comunicazione con un po' di circospezione
- Non cadere nella trappola del social engineering: urgenza, curiosita', etc.
- Controllare l'email e i links rispetto a piccole variazioni. Es. *www.confindustria.tn.it* vs *www.confindustria.tn.com*
- Contesto: e' la richiesta realistica? Es. ho comprato qualcosa, ho fatto il login, questo utente e' noto per inviarmi documenti di un certo tipo, etc.

Vulnerabilita’ software

Falla nella logica di un programma che se utilizzata risulta in un impatto negativo alla confidenzialita’, integrita’ o disponibilita’ dei dati o del servizio stesso

Una vulnerabilita’ e’ detta 0-day se non e’ nota agli sviluppatori del software ma e’ attualmente sfruttata da un’attaccante

Esistono diverse tipologie di vulnerabilita’ software:

- SQL
- Buffer Overflow
- XSS
- …

Aggiornamenti software

Tipicamente includono risoluzione di vulnerabilita' software, bugs e aggiunta/modifica di funzionalita' gia' presenti

Aggiornare il software non e' sempre immediato → puo' richiede tempo e risorse per verificare che le funzionalita' utilizzate non siano state modificate dall'aggiornamento

Database delle vulnerabilita’ software

Esistono diversi database che collezionano informazioni riguardo alle vulnerabilita’ **note** (es. National Vulnerability Database, Snyk Database)

Contengono informazioni che identificano la vulnerabilita’ (CVE ID) e le possibili mitigazioni (es. Patch, PoC)

Il numero di vulnerabilita’ riportate pubblicamente ogni anno e’ enorme

- 2022 → 25K CVE
- 2021 → 20K CVE
- 2020 → 18.3K CVE

Tenere traccia e risolvere ogni vulnerabilita’ e’ impossibile → bisogna concentrarsi su quello che gli attaccanti utilizzano (~6% del totale)

Cyber Threat Intelligence

Informazioni riguardanti minacce informatiche e il loro comportamento applicabili immediatamente nel processo decisionale di un'organizzazione per aiutarla a ridurre l'impatto degli attacchi informatici

Permette di:

- Essere proattivi nei confronti delle minacce → es. Prioritizzare vulnerabilita' software
- Rilevare e rispondere piu' velocemente agli attacchi → es. Investigare determinati eventi presenti nei log di un sistema

Dati utilizzati dalla Threat Intelligence

L’analisi utilizza diverse fonti:

- Feeds di sicurezza: IoC, vulnerabilita’ software, report di malware, social network e underground forums
- Community di condivisione di informazioni: es. MISP, ma anche social network come Twitter
- Log interni all’azienda

Underground Forums

Forums dove si discutono attivita' criminali: dal Denial of Service, passando per lo sviluppo di malware, l'accesso agli accounts, e lo scambio di valute.

Le discussioni sono divise in categorie (boards) e argomenti (threads)

Non solo condivisione di informazioni riguardo l'hacking ma anche vendita e acquisto di prodotti (es. malware) e servizi (es. affitto di server, stress testers, etc.). Marketplaces in stile Ebay con descrizioni dei prodotti e recensioni dei clienti

Cybercrime-as-a-Service

Modello di business dove servizi illegali sono offerti negli underground forums per condurre le diverse fasi di un attacco

I criminali sono entrepreneurs che acquistano competenze specialistiche, infrastrutture e strumenti per il loro “business”

E’ possible acquistare un malware per il controllo remoto di una macchina (Malware-as-a-service), codice per sfruttare una vulnerabilita’ software per l’infezione (Exploit-as-a-service), e il traffico degli utenti (Traffic-as-a-service) per ricreare l’intera kill chain dell’attacco

Advanced Persistent Threats (APTs)

Cosa sono:

- Malware?
- Attacchi targeted?
- Attaccanti statuali?

NIST: “Un avversario che possiede avanzata esperienza e risorse che permettono di ottenere i propri obiettivi attraverso diversi vettori di attacco. Gli obiettivi degli APTs tipicamente includono l’instaurazione di accesso e movimento laterale nella infrastruttura IT da compromettere per finalita di esfiltrazione di dati o per l’impedimento delle funzionalita’ critiche dell’organizzazione. Gli APTs si dedicano all’obiettivo per un lungo periodo di tempo adattandosi alle difese”

Classi di APTs

Gruppi di attivisti:

- Gaza Cybergang,...

Gruppi e-crime:

- FIN5, FIN6, FIN7, Cobalt group,…

Gruppi statuali:

- China: APT30, APT18, APT1,…
- Russia: APT29, APT28,…
- North Korea: Lazarus Group,APT38

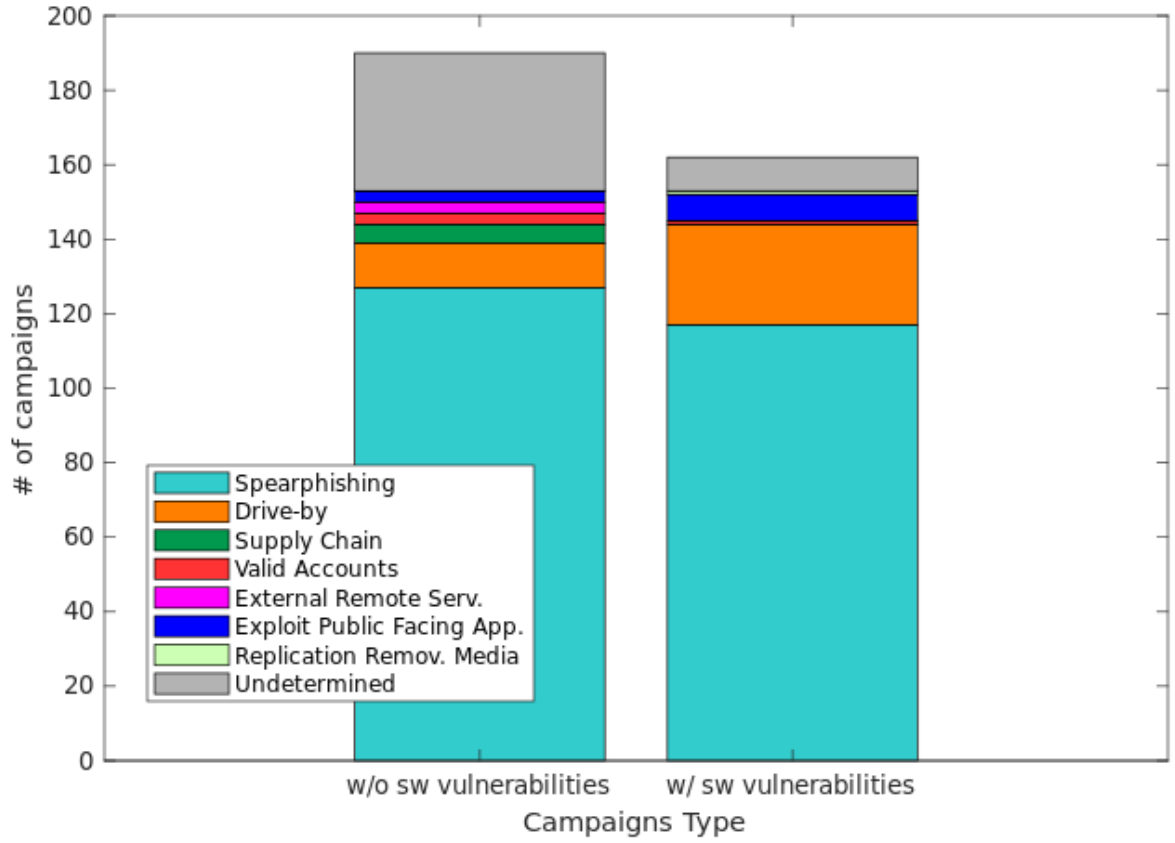
Perche’ gli APTs?

La differenza tra attacchi untargeted e targeted sta diventando molto labile → gli attacchi informatici sono un vero e proprio lavoro

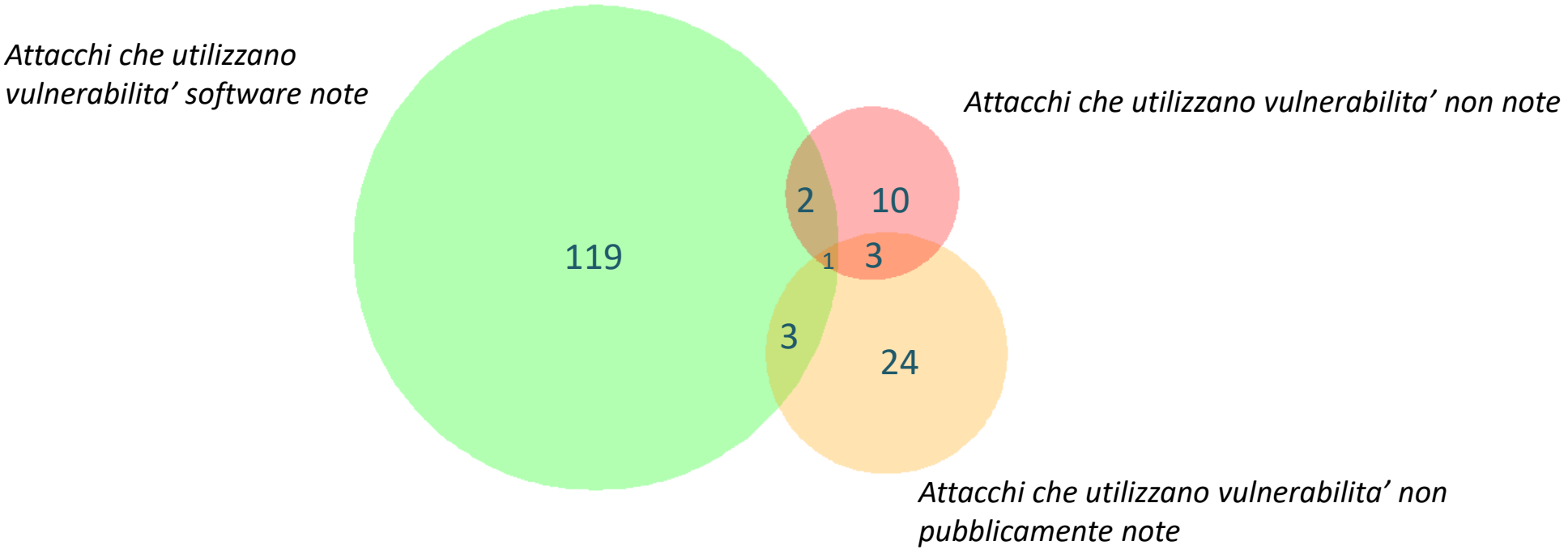
Sempre piu’ attacchi sono effettuati da gruppi organizzati con un livello di sofisticatezza comparabile ad attacchi APTs

Anche se i target principali rimangono grandi aziende o enti governativi, anche piccole e medie imprese sono attaccate da APTs es. come parte di una supply chain

Le caratteristiche degli APTs: vettori di attacco



Le caratteristiche degli APTs: vulnerabilita' software



Analisi costi ed efficacia degli aggiornamenti software

L’aggiornamento **immediato** dei prodotti software in un azienda permette di ridurre il rischio di essere compromessi da un attacco APTs

- Non sempre possible o conveniente

Una strategia che e’ reattiva sulle vulnerabilita’ software pubbliche o che sono attivamente utilizzate dai criminali (es. PoC o underground forums) ha la stessa efficacia di cercare di aggiornare il software ad ogni release ma costa meno

La Threat Intelligence e il contrasto agli APTs

La Kill chain di un attacco informatico

Attacco Phishing

Invio di messaggi ingannevoli ad un utente con l'obiettivo di indurlo a:

- rivelare dati sensibili (es. password, carta di credito)
- eseguire codice malevolo (es. lanciare un eseguibile, visitare un sito web compromesso)

Tipicamente utilizza tecniche di social engineering per spingere l'utente ad eseguire un'azione che normalmente non farebbe

Diversi vettori utilizzati: email, social network, SMS

Vulnerabilita' software

Falla nella logica di un programma che se utilizzata risulta in un impatto negativo alla confidenzialita', integrita' o disponibilita' dei dati o del servizio stesso

Una vulnerabilita' e' detta 0-day se non e' nota agli sviluppatori del software ma e' attualmente sfruttata da un'attaccante

Esistono diverse tipologie di vulnerabilita' software:

- SQL
- Buffer Overflow
- XSS
- ...

Cyber Threat Intelligence

Informazioni riguardanti minacce informatiche e il loro comportamento applicabili immediatamente nel processo decisionale di un'organizzazione per aiutarla a ridurre l'impatto degli attacchi informatici

Permette di:

- Essere proattivi nei confronti delle minacce → es. Prioritizzare vulnerabilita' software
- Rilevare e rispondere piu' velocemente agli attacchi → es. Investigare determinati eventi presenti nei log di un sistema

Underground Forums

Forums dove si discutono attivita' criminali: dal Denial of Service, passando per lo sviluppo di malware, l'accesso agli accounts, e lo scambio di valute.

Le discussioni sono divise in categorie (boards) e argomenti (threads)

Non solo condivisione di informazioni riguardo l'hacking ma anche vendita e acquisto di prodotti (es. malware) e servizi (es. affitto di server, stress testers, etc.). Marketplaces in stile Ebay con descrizioni dei prodotti e recensioni dei clienti

Advanced Persistent Threats (APTs)

Cosa sono:

- Malware?
- Attacchi targeted?
- Attaccanti statuali?

NIST: "Un avversario che possiede avanzata esperienza e risorse che permettono di ottenere i propri obiettivi attraverso diversi vettori di attacco. Gli obiettivi degli APTs tipicamente includono l'instaurazione di accesso e movimento laterale nella infrastruttura IT da compromettere per finalita di esfiltrazione di dati o per l'impedimento delle funzionalita' critiche dell'organizzazione. Gli APTs si dedicano all'obiettivo per un lungo periodo di tempo adattandosi alle difese"