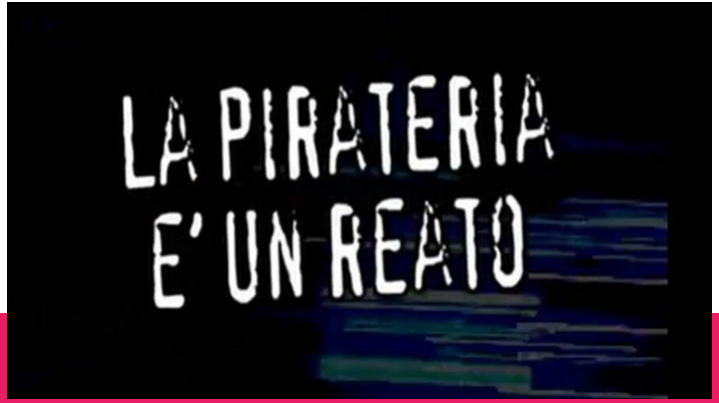


DISCLAIMER: ACCEDERE A SISTEMI INFORMATIVI SENZA AUTORIZZAZIONE E' UN REATO

$> whoami

- Ex Unifi
- Principal Security Consultant @ WithSecure
- Lead of Global Purple Team Service
- Lead of Active Directory Security Review

Come Rapinare Una Banca

E non andare in galera

Chi vuol essere milionario?

Chi vuol essere milionario?

- A: Tu
- B: Io
- C: La Corea del Nord

Chi vuol essere milionario?

- ~~A: Tu~~
- ~~B: Io~~
- C: La Corea del Nord

Chi vuol essere milionario?

Parte del programma di “raccolta fondi” della Corea del Nord consiste nel commettere cyber crimini verso altri stati con lo **scopo di rubare denaro.**

Causa: Non hanno introiti a causa delle sanzioni internazionali

Chi vuol essere milionario?

Il caso più famoso e’ quello che da molti viene definita la più grande cyber rapina di tutti i tempi ai danni della Banca del Bangladesh nel Febbraio 2016. Si stima che la perdita si aggiri attorno agli **80 milioni di dollari**.

Ma come hanno fatto?

Come Rapinare Una Banca

- La compromissione di account utenti di home banking e' il modo più comune di rubare soldi, **ma e' anche il piu efficiente?**
- Society for Worldwide Interbank Financial Telecommunications (**SWIFT**) e' una rete informatica chiusa, partecipata dalle più grosse istituzioni finanziarie al mondo per facilitare **trasferimenti internazionali** di fondi fra oltre 11000 banche.

Come Rapinare Una Banca

- Il 4 Febbraio 2016, varie richieste vengono inoltrate dalla banca del Bangladesh verso la Federal Reserve per spostare circa **800 milioni** dal conto che la banca del Bangladesh ha nella FR verso le Filippine.

Come Rapinare Una Banca

- Per un errore degli attaccanti, il 6 Febbraio la banca del Bangladesh si accorge di un anomalia. Tutto questo grazie ad **una stampante che non funzionava**.

Come Rapinare Una Banca

- La Federal Reserve aveva tentato di contattare la banca per le varie transazioni sospette, ma l'attacco era stato coordinato con un weekend **in Bangladesh**. Tutto per un errore di spelling!!
- La banca del Bangladesh e' andata **totalmente nel panico** e ha tentato di contattare la Federal Reserve
- Ma gli attaccanti erano riusciti a prevedere anche questo, dato che **in America era già il weekend** e nessuno stava lavorando!

Come Rapinare Una Banca

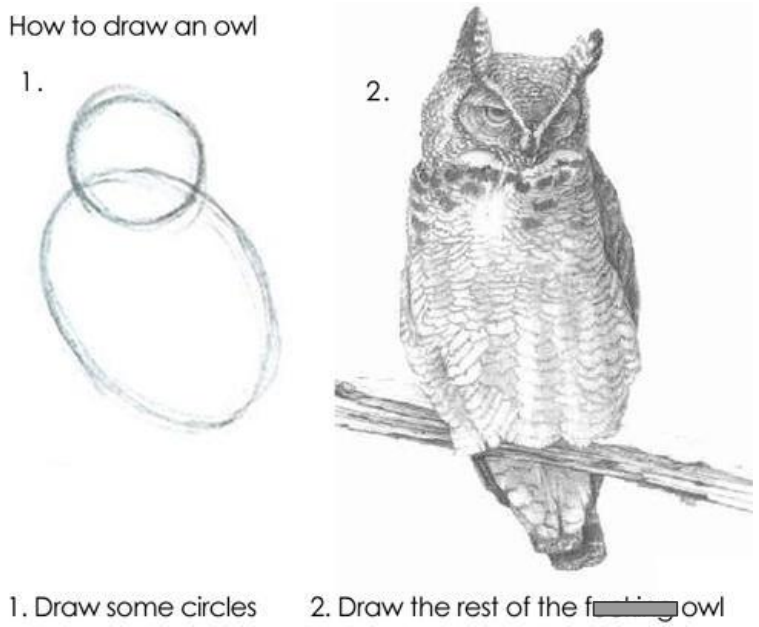
- Quando ormai la truffa e’ stata svelata, gli attaccanti sono riusciti a rubare **la modesta cifra di 80 milioni** di dollari in totale.
- Fun fact: I soldi sono stati riciclati in un **casinò nelle Filippine**, giocando a caso ad un gioco che ha circa il 50% di possibilità di vincita.

Come Rapinare Una Banca

- Questo e’ stato uno degli “incident” piu famosi della storia e **ha aperto gli occhi a tante organizzazioni** su quali fossero le loro difese contro attaccanti motivati e con molte risorse.
  - Sicurezza delle rete SWIFT
  - Casino nelle Filippine

Quindi, come si rapina una banca?

- Comprometti il perimetro esterno
  - Falle nelle applicazioni web esposte
  - Comprometti un dipendente tramite phishing
- Eleva i tuoi privilegi nella rete
  - Misconfigurazioni
  - Pratiche di cattiva amministrazione di sistema
- Identifica le postazioni critiche
  - SWIFT
  - ATM
- Hackerale
- Trasferisci i soldi



Come mai non sono in galera?

- Non si sa bene chi sono i responsabili, sospettata Corea del Nord
- Attaccanti sponsorizzati dallo stato, non hanno motivo di essere messi in galera. La **scarsa cooperazione** fra stati rende l’estradizione impossibile.

Quindi, cosa possiamo fare?

Red Team

- Analista **esperto** di sicurezza offensiva
- Responsabile per **emulare minacce avanzate**, come Nord Corea o simili
- **RAPINARE BANCHE**
- Creare software per **evadere** i vari prodotti di security
- La maggior parte dell’azienda del cliente e’ all'oscuro delle sue attività
- Il team di difesa dell’azienda sarà **costretto a rispondere alla minaccia** come se fosse reale

Penetration Tester

- Analista di sicurezza offensiva, responsabile per **identificare proattivamente vulnerabilità** nei sistemi usando tecniche simili ai veri attaccanti
- Dove ho iniziato io
- Corsi: Practical Ethical Hacking, PEN-200: Penetration Testing with Kali Linux

Blue Team: Security Operation Center

Persone responsabili per il **monitoraggio continuo** dei sistemi di sicurezza.

- Analizzare gli eventi e i log dei vari AV, EDR, Firewall, Proxy, Mail etc..
- Se un evento risulta un incidente di sicurezza, escalare a chi si occupa di Incident Response
- Corsi: Blue Team Level 1

Blue Team: Incident Response

- Ultima linea di difesa
- Responsabili per il **contenimento** e l'**eradicazione** della minaccia dalla rete
- Devono ricostruire tutte le azioni dell'attaccante e assicurarsi che ogni backdoor sia rimossa
- Corsi: Practical Windows Forensics

Blue Team: Threat Intelligence

- Hanno la responsabilità di **monitorare** il cyberspazio e identificare le minacce più probabili data una particolare azienda
- Possono anche attribuire incidenti a varie entità, come un altro caso della Corea del Nord
- Corsi: ATT&CK® Cyber Threat Intelligence Certification, Hunting Adversary Infrastructure

Domande?

careers @ WithSecure