TD SYNNEX

Initial Access Broker

Il commando d’assalto del Cyber Crime

27 Settembre 2024

Webinar

Andrea Pezzoni – Security Presales Specialist – TD SYNNEX

Le 7 fasi di attacco

Reconnaissance

Weaponisation

Delivery

Exploitation

Installation

Command and control

Actions on objectives

Initial Access Broker

- Password Reuse
- Email Hacks
- VPN Profiles
- Exposed RDP Servers
- Social Engineering

Gli Initial Access Broker sono Cyber Threats Actors(CTA) che cercano di ottenere l'accesso alle reti informatiche con l’obiettivo di venderlo ad altri CTA.

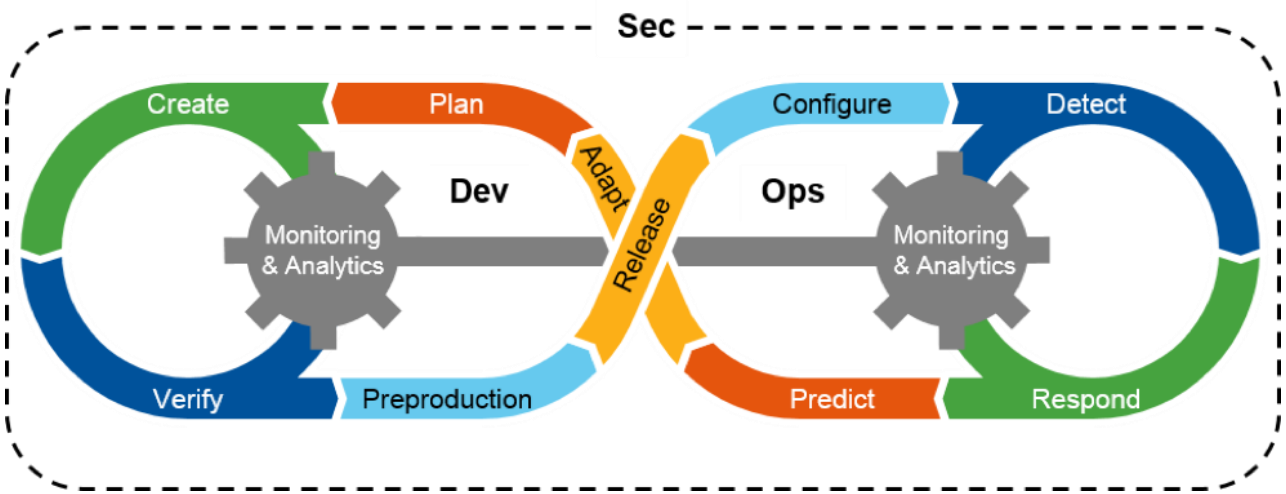
Initial Access Broker

Vulnerability Scanning

La Vulnerability Scanning, detta anche Vulnerability Assessment,
è il processo di valutazione delle reti o delle risorse informatiche alla ricerca di vulnerabilità di sicurezza,
ovvero di difetti o punti deboli che gli attori esterni o interni possono sfruttare.
La scansione delle vulnerabilità è la prima fase del più ampio ciclo di vita della gestione delle vulnerabilità.

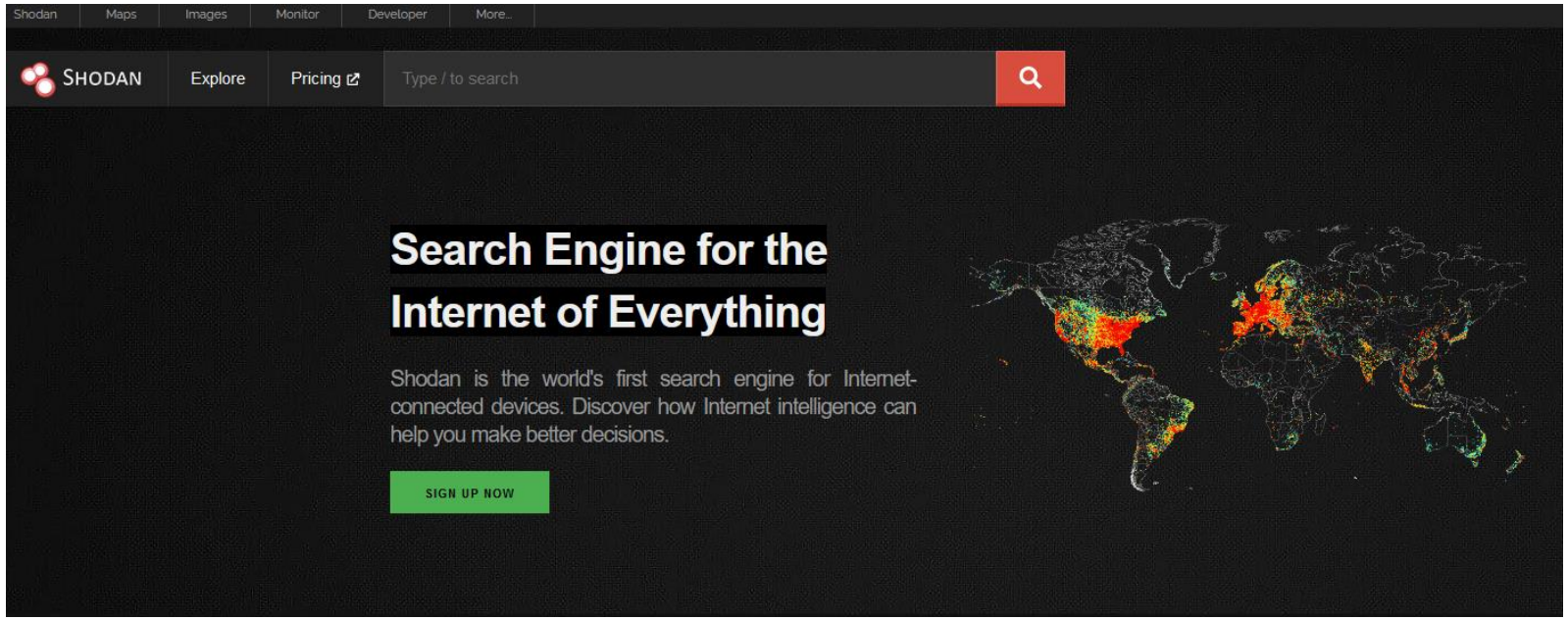
IBM

11% degli host esposti nei Public Cloud registrano vulnerabilità di grado High o Critical



TD SYNNEX

Tool di analisi



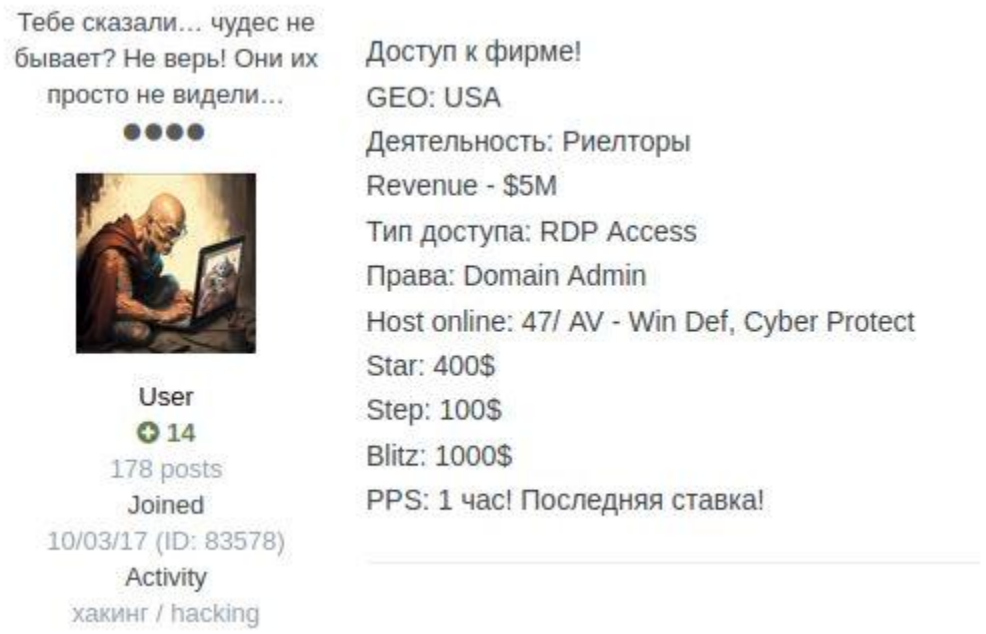
NMAP . ORG

who.is

APT – Advanced Persistent Threat

Gli Advanced Persistent Threat sono attacchi eseguiti manualmente, non automatizzati e indiscriminati, che prendono di mira tutta la rete di un target specifico, spesso studiato per molti mesi.

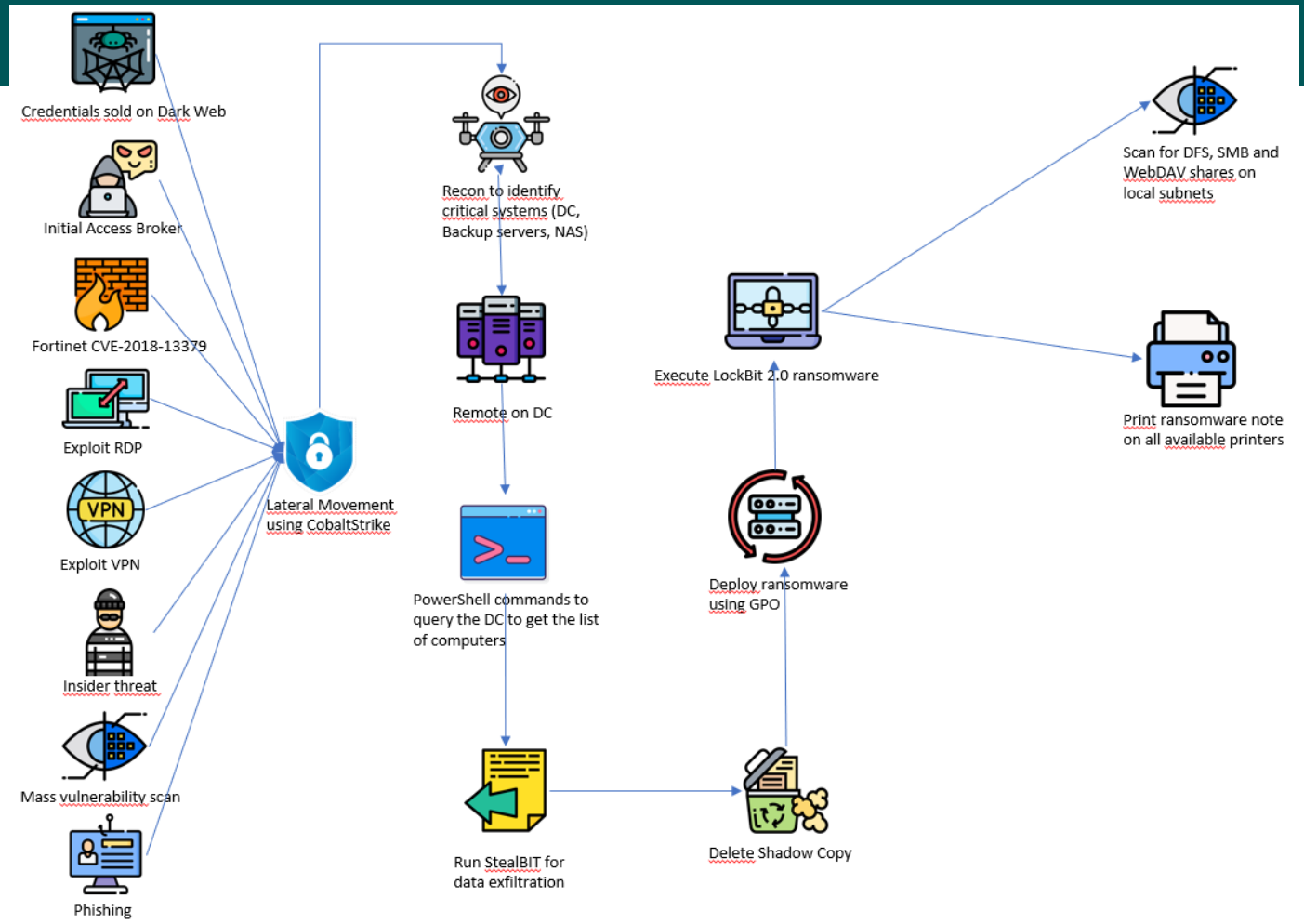
IAB – Esempio di compravendita



Come ogni sito di e-commerce, nei forum underground che vendono gli accessi, sono elencate le caratteristiche dell'accesso:

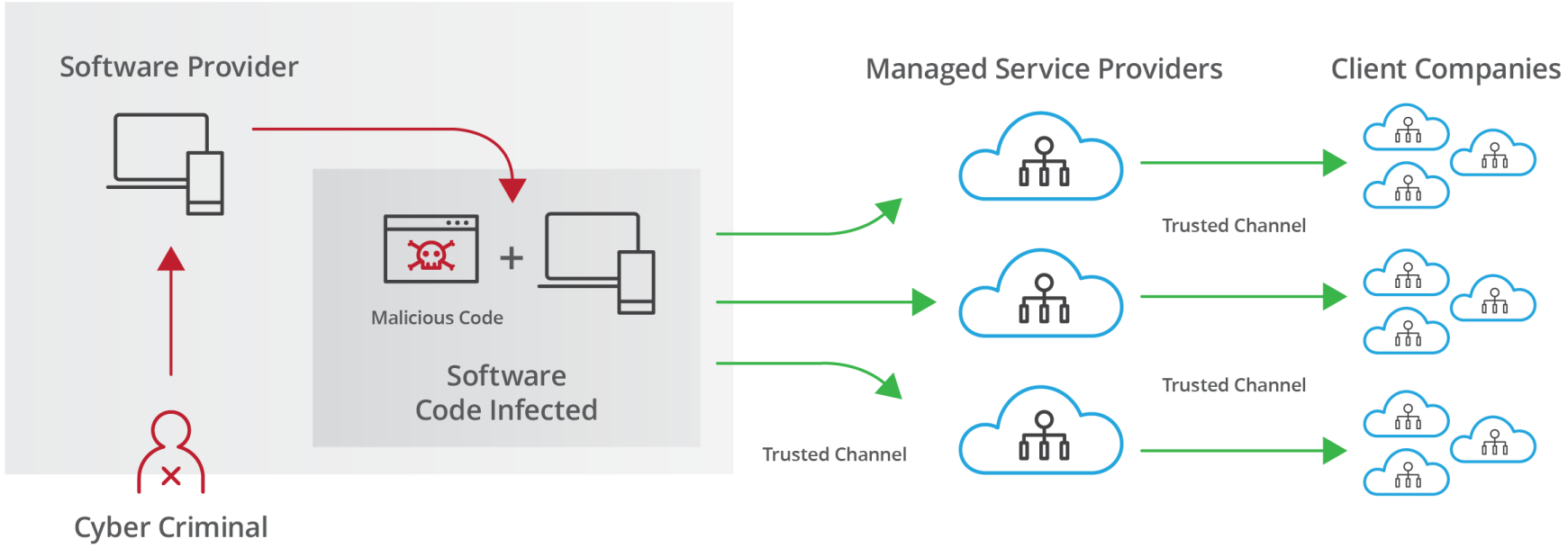
- Geolocalizzazione
- Industria di riferimento (Real Estate)
- Fatturato
- Tipo di Accesso
- Livello di autorizzazione
- Caratteristiche della rete e antivirus
- Base d'asta
- Cifra di rilancio
- Prezzo di acquisto immediato

Lockbit attack

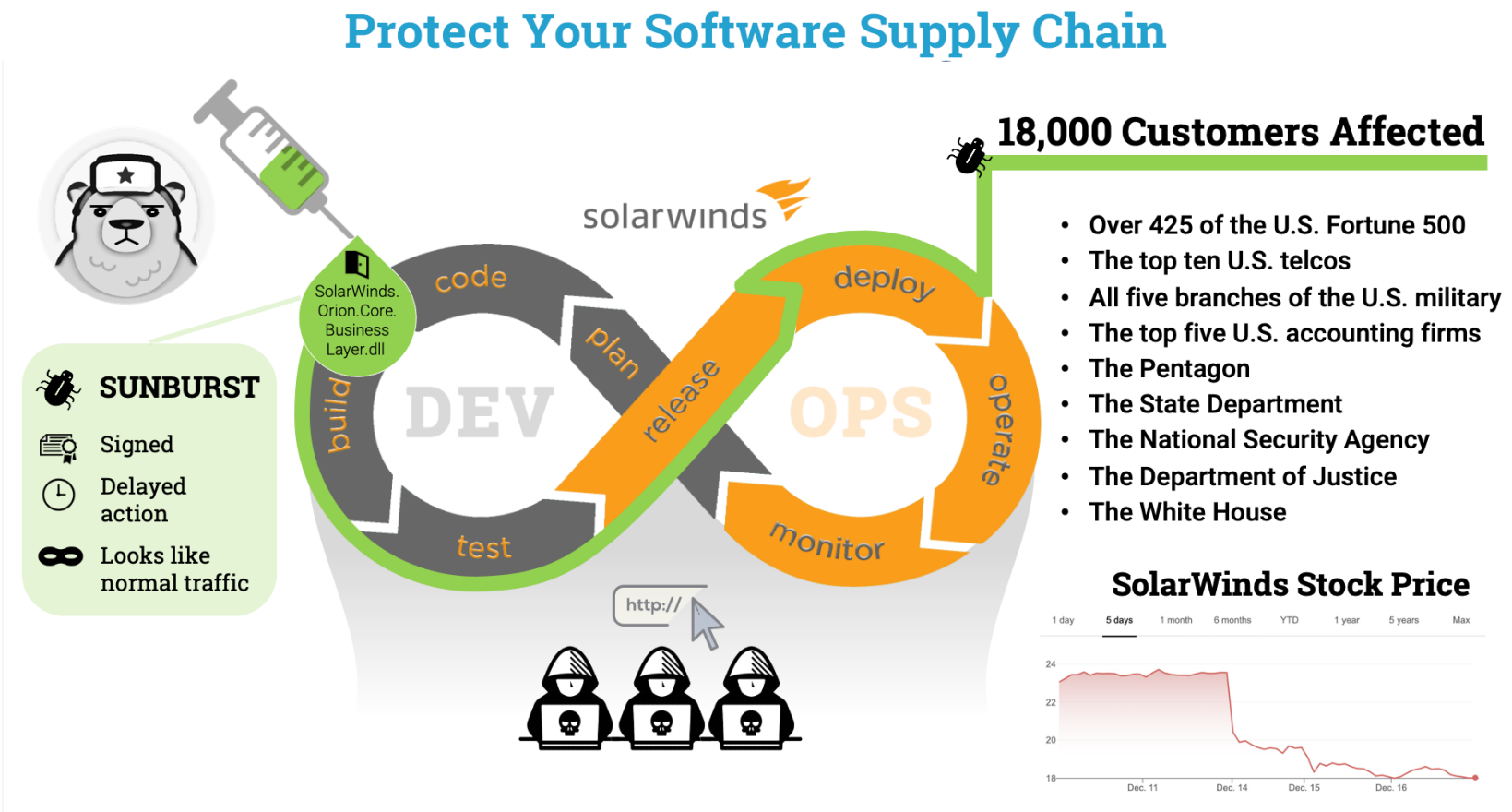


Supply Chain Attack

Attacchi volti a colpire i fornitori software o di servizi terzi per poi fare escalation verso reti clienti aziendali inconsapevoli



Caso Solarwinds



Campagne Phishing

Da: news <admin@pc-mediation.com>
Inviato:
A:
Oggetto: Licenza 534238623
Allegati: inform_1852.zip

Agenzia Entrate

Direzione Centrale Gestione Tributi

Gentile contribuente,
dall'esame dei fatti e dei versamenti relativi alla Comunicazione delle liquidazioni periodiche Iva, da voi mostrata per l'ultimo trimestre 2020, sono emerse alcune incoerenze.
Le informazioni relative alle incoerenze sono visionabili nel documento in allegato o nel "Cassetto fiscale" (sezione L'Agenzia scrive) e nel servizio "Fatture e Corrispettivi (sezione Consultazione - L'Agenzia scrive),
entrambi accessibili dal sito web dell'Agenzia delle entrate (www.agenziaentrate.gov.it).

Password: gov2021

Questa e-mail è stata figliata automaticamente, pertanto la preghiamo di non reagire a questo indirizzo di posta elettronica.

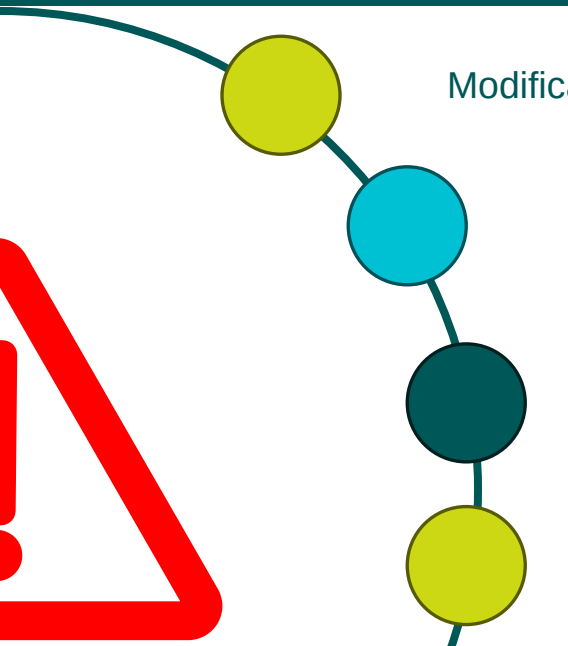
Il Phishing rimane uno dei metodi più utilizzati per accedere alle risorse aziendali.
In Italia circa il 9% degli attacchi riguarda campagne di Phishing

Piccolo Gioco:
mybank.com o mybank.com

RaaS – Ransomware As A Service

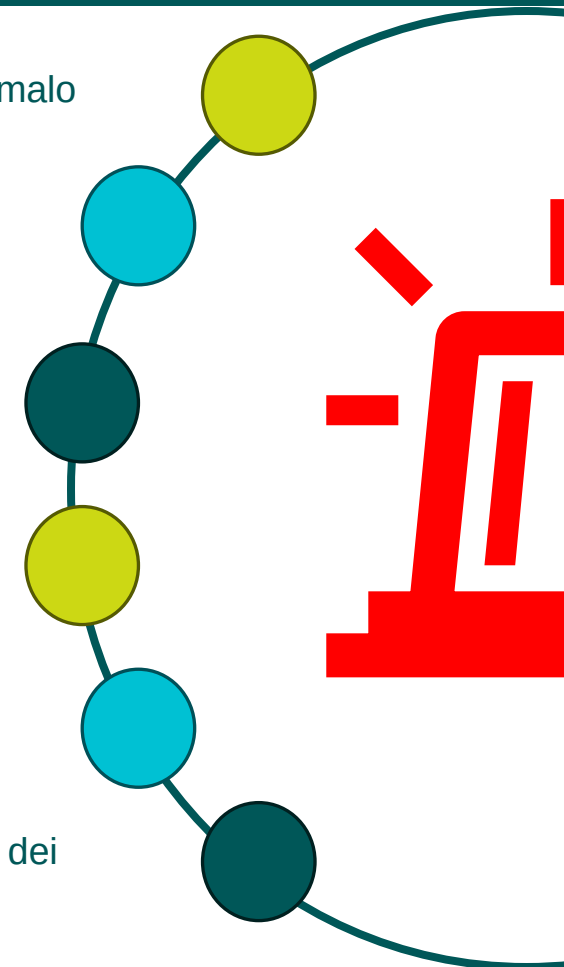
Il RaaS funziona alla stregua di legittimi modelli di business software-as-a-service (SaaS) . Gli sviluppatori di ransomware, detti anche operatori RaaS, si occupano dello sviluppo e del mantenimento di strumenti e infrastrutture ransomware. Confezionano i propri strumenti e servizi in kit RaaS che vendono ad altri hacker, detti affiliati RaaS.

Indicatori di Compromissione



- Modifica dei registri di sistema
- Modifiche dei DNS dei sistemi
- Modifiche sulle Group Policy
- Riavvii anomali dei sistemi critici
- Compressione e copia di grandi volumi di file
- Uso di tool di sniffing o network analysis

- Traffico Network anomalo
- Geolocalizzazione sospetta
- Nuove App sui dispositivi
- Comportamenti strani utenti Admin
- Volumi di accesso anomali
- Copia e lettura anomala dei database



TD SYNNEX

”A breach alone is not a disaster, but mishandling it is.”

Serene Davis

https://www.cisecurity.org/insights/blog/initial-access-brokers-how-theyre-changing-cybercrime
https://www.curatedintel.org/2021/09/lockbit-20-ransomware-attack-analysis.html
https://ransomware.org/blog/initial-access-brokers-everything-you-need-to-know/
https://syslogic.ca/blog/cybersecurity-101-how-to-keep-your-business-safe-from-iabs/
https://www.fastweb.it/fastweb-plus/digital-dev-security/...
https://www.hbs.net/blog/how-software-supply-chain-attacks-work/
https://blog.adolus.com/three-things-the-solarwinds-supply-chain-attack-can-teach-us
https://www.redhotcyber.com/post/killsec-annuncia-la-nuova-piattaforma-ransomware-as-a-service-raas/
https://www.ibm.com/it-it/topics/ransomware-as-a-service
https://www.shodan.io/
https://nmap.org/
https://www.paloaltonetworks.com/state-of-cloud-native-security
https://www.ibm.com/topics/vulnerability-scanning
https://startupitalia.eu/tech/cybersecurity/devsecops-lo-sviluppo-software-agile-attento-alla-sicurezza/

TD SYNNEX

Q&A

Your Opinion Counts!

Scarica la presentazione cliccando sul codice QR

PROSSIMI APPUNTAMENTI

4 OTTOBRE: Zero Trust Security Policies

11 OTTOBRE: NGFW e la protezione perimetrale

18 OTTOBRE: IPS e IDS

25 OTTOBRE: TBD

TEAM SECURITY: security.it@tdsynnex.com
SPEAKER: andrea.pezzoni@tdsynnex.com