TD SYNNEX

Cyber Kill Chain

Le 7 fasi di attacco e gli indicatori di compromissione

26 Luglio 2024

Webinar

Andrea Pezzoni – Security Presales Specialist – TD SYNNEX

Le 7 fasi di attacco

Reconnaissance

Weaponisation

Delivery

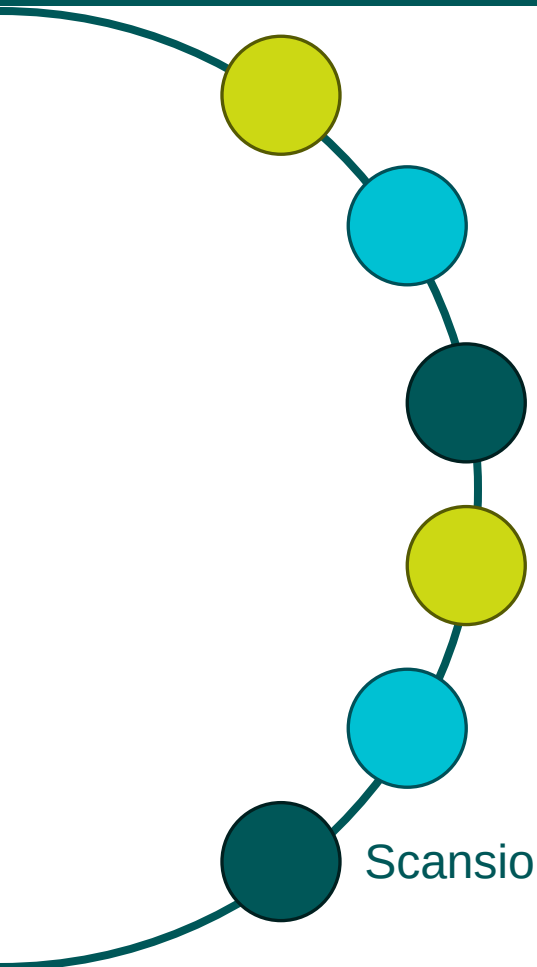
Exploitation

Installation

Command and control

Actions on objectives

Reconnaissance



Analisi Social Networks

Analisi Siti Istituzionali

Ricerca informazioni da DNS

Scansione vulnerabilità

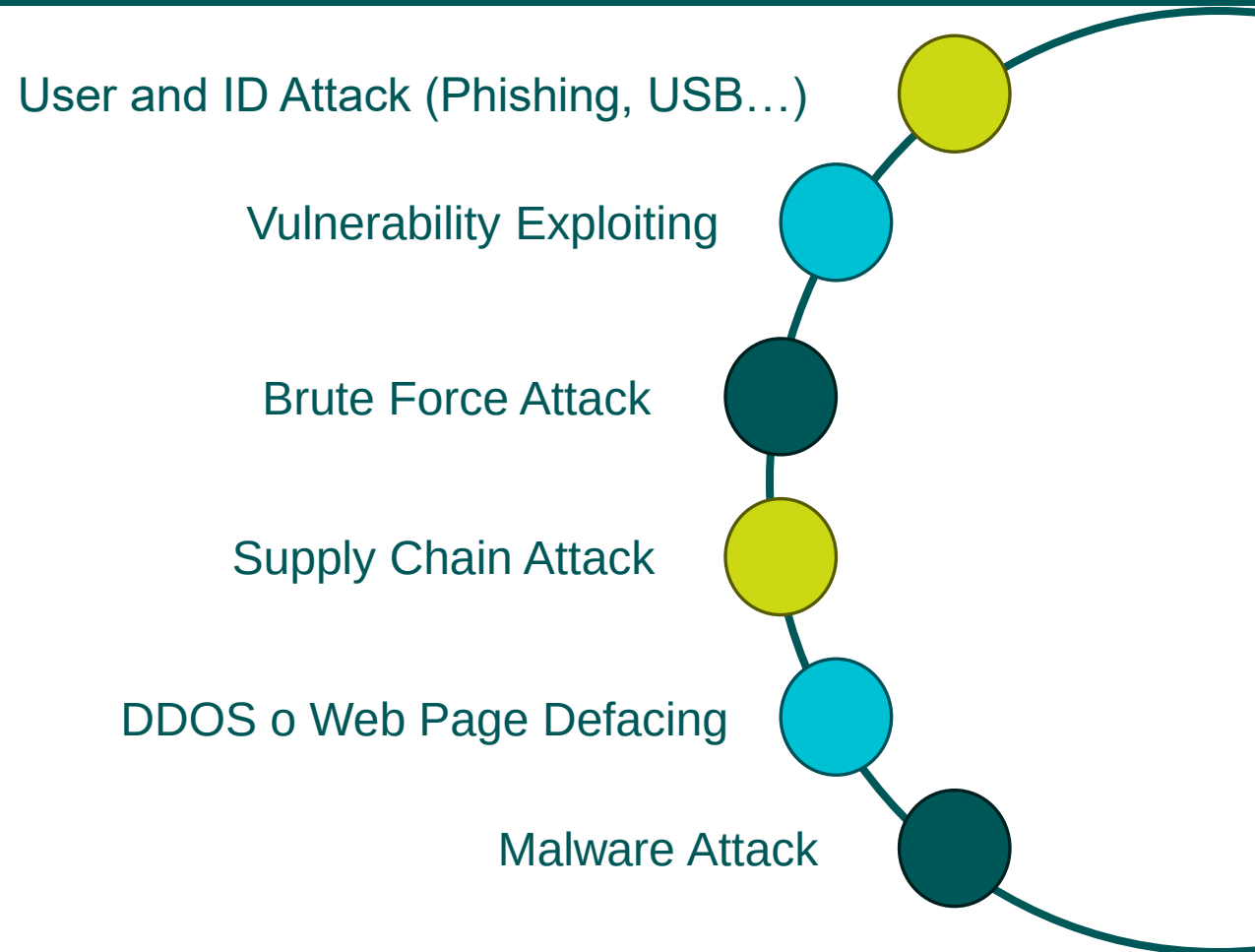
Ricerca di Aziende Supply Chain

Scansione superficie ed enumerazione

Weaponisation

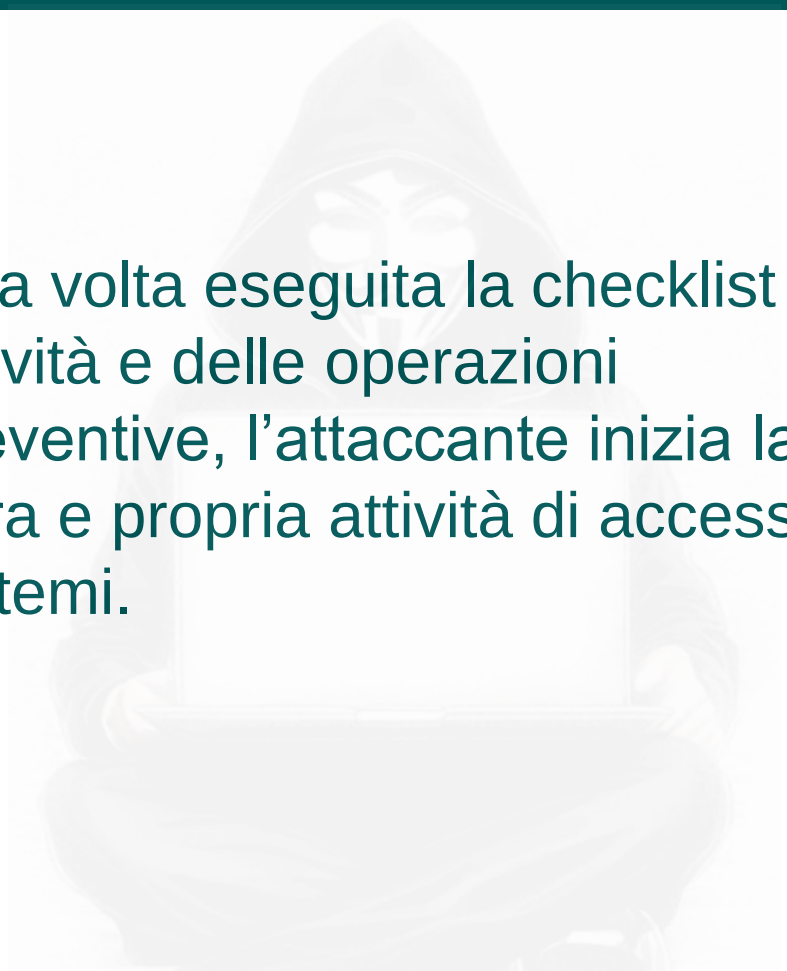
La fase di armamento viene utilizzata per organizzare le informazioni ottenute e scegliere il metodo di attacco.

In aggiunta, in questa fase viene creata l'infrastruttura di appoggio dell'attacco, la rete C&C e i repository del codice.



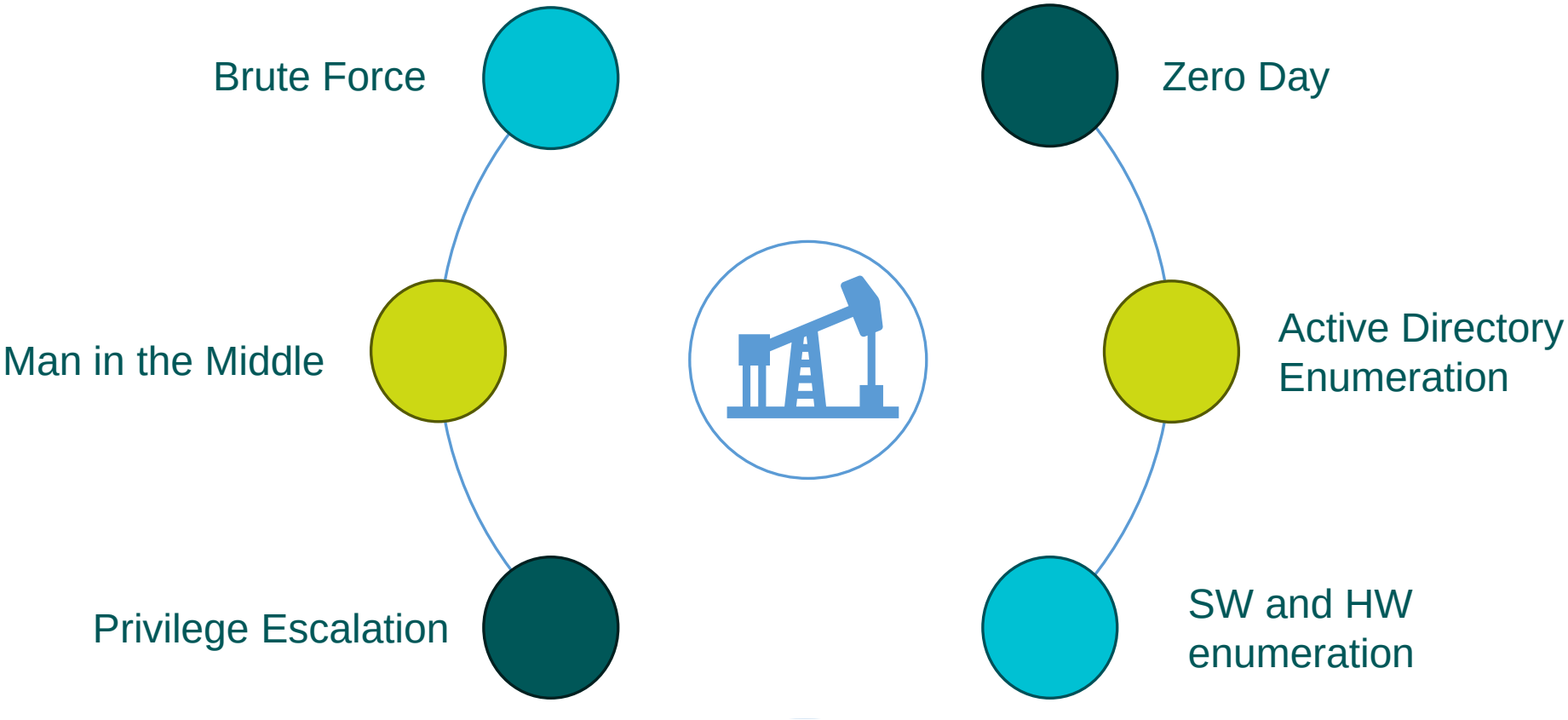
Delivery

Una volta eseguita la checklist delle attività e delle operazioni preventive, l'attaccante inizia la vera e propria attività di accesso ai sistemi.



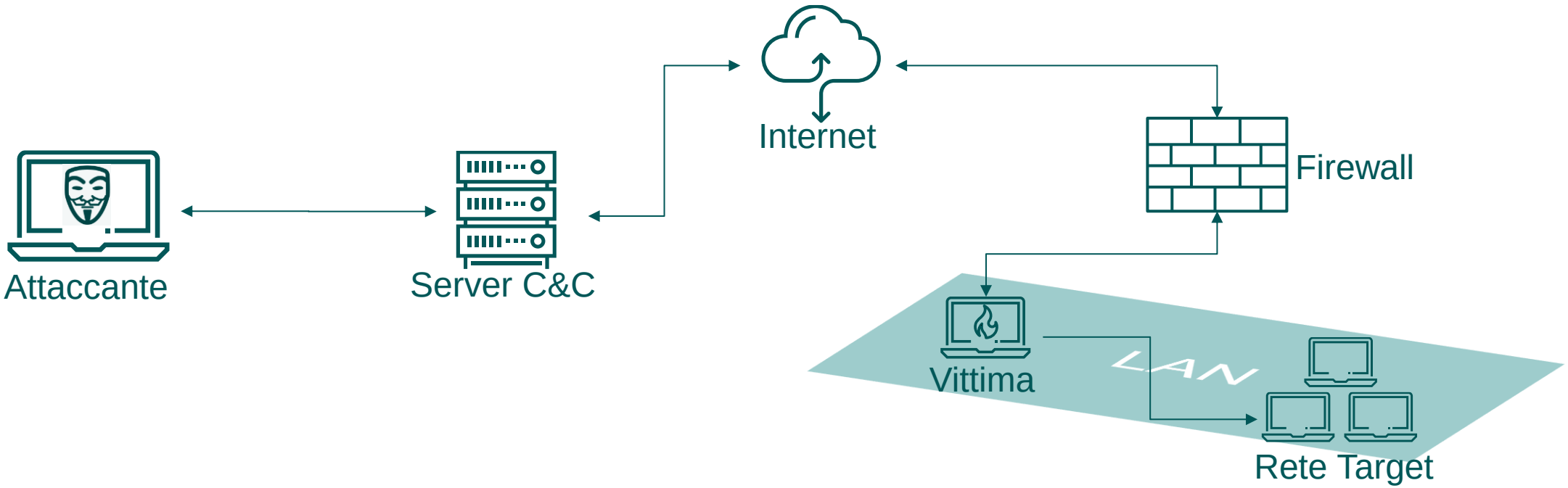
- Obiettivo
- Enumerazione delle risorse
- Vulnerabilità
- Metodo di attacco

Exploitation



Installation

Command and Control



Fase di esfiltrazione dei dati e iniezione del codice malevolo.

Actions on objectives

Motivazioni Economiche

Estorsione

Doppia Estorsione

Tripla Estorsione

Hacktivism Espionage

Motivazione politica

Attivismo

Spionaggio internazionali

Spionaggio industriale

Sabotaggio

Motivazioni personali

Concorrenza

Vendetta

Le 7 fasi di attacco

Considerazioni dopo averne approfondito le fasi

Targeted Attack

Reconnaissance

Weaponisation

Delivery

Opportunistic attack

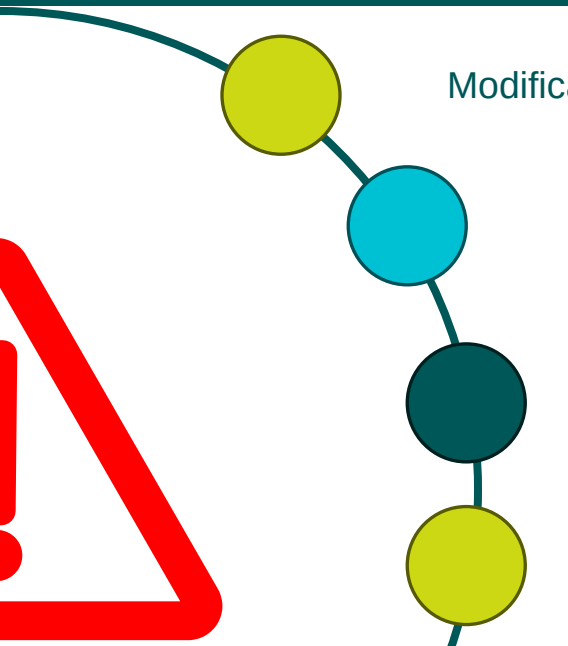
Exploitation

Installation

Command and control

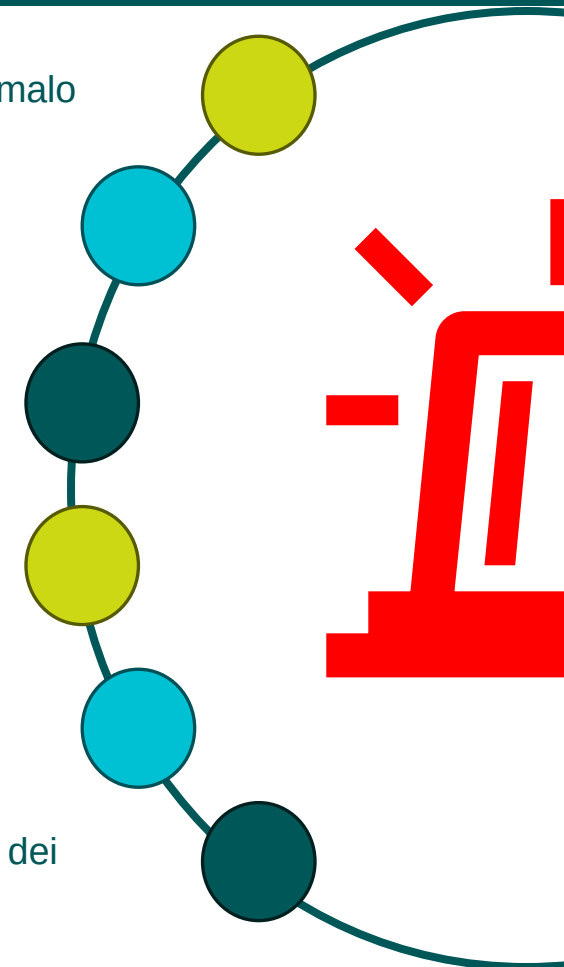
Actions on objectives

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

“Security is always excessive until it’s not enough.”

Robbie Sinclair

Sitografia

https://www.difesaonline.it/evidenza/cyber/che-cos%C3%A8-la-cyber-kill-chain
https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
https://www.crowdstrike.com/cybersecurity-101/cyber-kill-chain/
https://www.sentinelone.com/cybersecurity-101/cyber-kill-chain/

https://www.cybersecurity360.it/soluzioni-aziendali/cyber-kill-chain-ecco-come-identificare-un-attacco-informatico-e-adottare-le-giuste-contromisure/
https://www.trendmicro.com/vinfo/us/security/definition/indicators-of-compromise
https://www.microsoft.com/en-us/security/business/security-101/what-are-indicators-of-compromise-ioc

TD SYNNEX

Q&A

Your Opinion Counts!

Scarica la presentazione cliccando sul codice QR

PROSSIMI APPUNTAMENTI

TORNEREMO IN ONDA A **SETTEMBRE**!

18 SETTEMBRE: Cyber Unit: Speciale Acronis Advanced Security + XDR

27 SETTEMBRE: Initial Access Broker

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