Seminario a cura di (ISC)2

Attacchi ransomware e business email compromise
un'analisi dei casi più frequenti del 2024 e
uno sguardo al 2025

Filadelfio Emanuele | CISO, *Elmec Informatica SpA*
Marco Misitano| Founder Member and Board Member, *(ISC)2 Italy Chapter*

Marco Misitano
Founder Member and Board Member, (ISC)2 Italy Chapter

Introduzione: l'associazione e le attività

ISC2 CHAPTER | ITALY

Filadelfio Emanuele
CISO Elmec Informatica SpA
BU Director CybergON

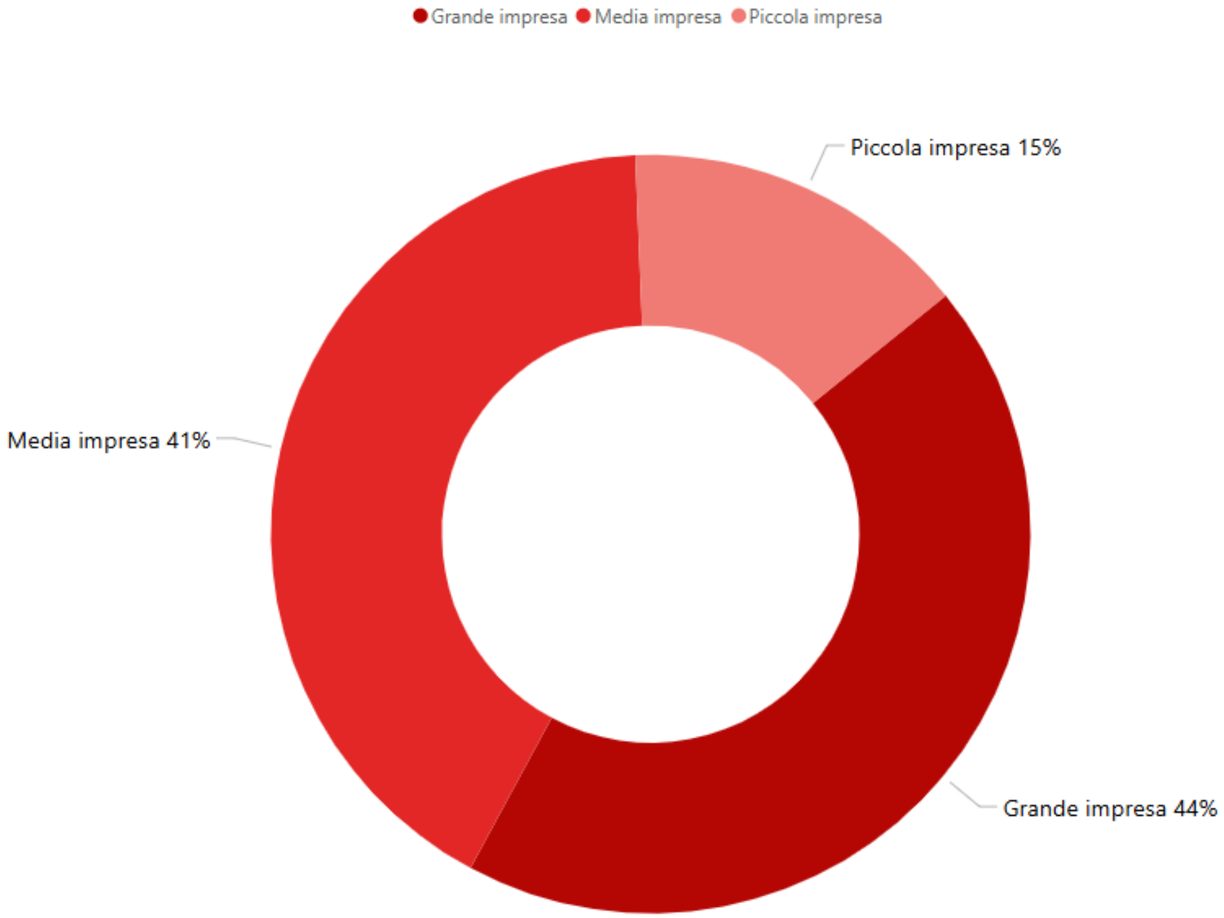
Gli attacchi più frequenti del 2024 (e uno sguardo al 2025)

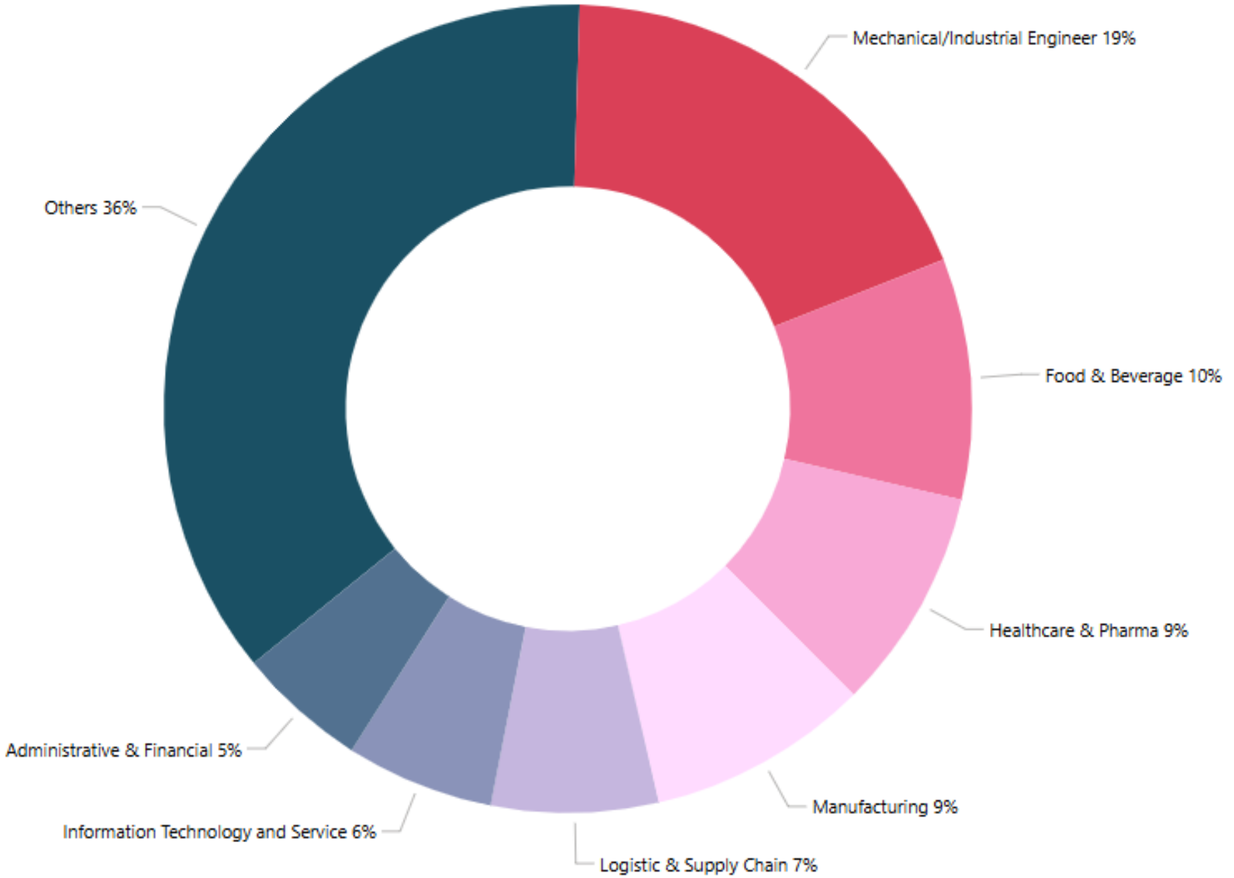
Condivisione di esperienze reali vissute sul campo:

Lo scenario
Analisi degli attacchi
Lesson learned

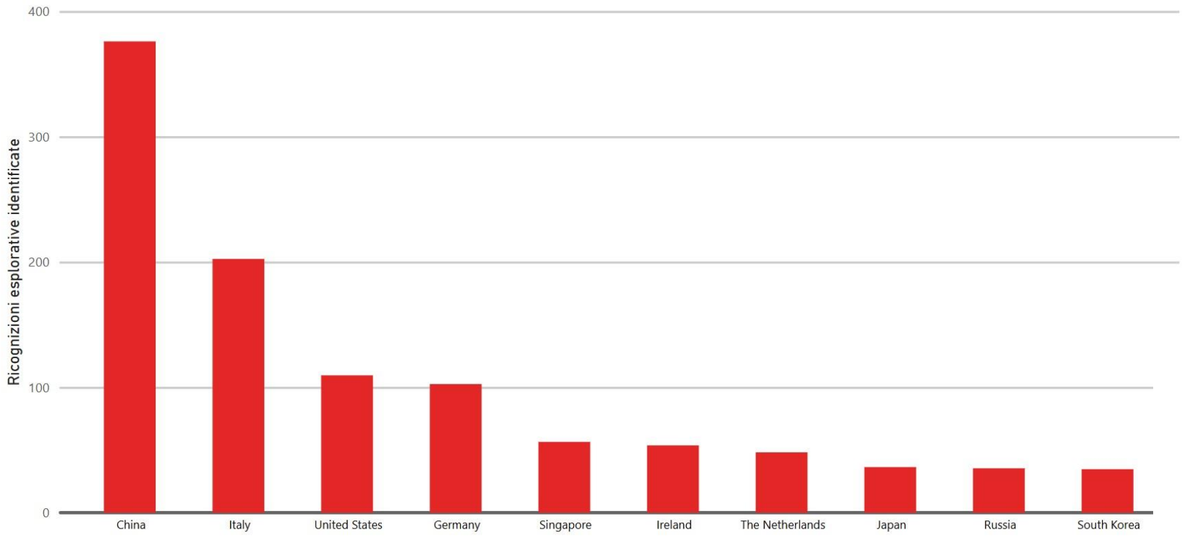
LO SCENARIO

Lo scenario – Bacino di osservazione





Lo scenario – Da dove arrivano gli attacchi? (2024)

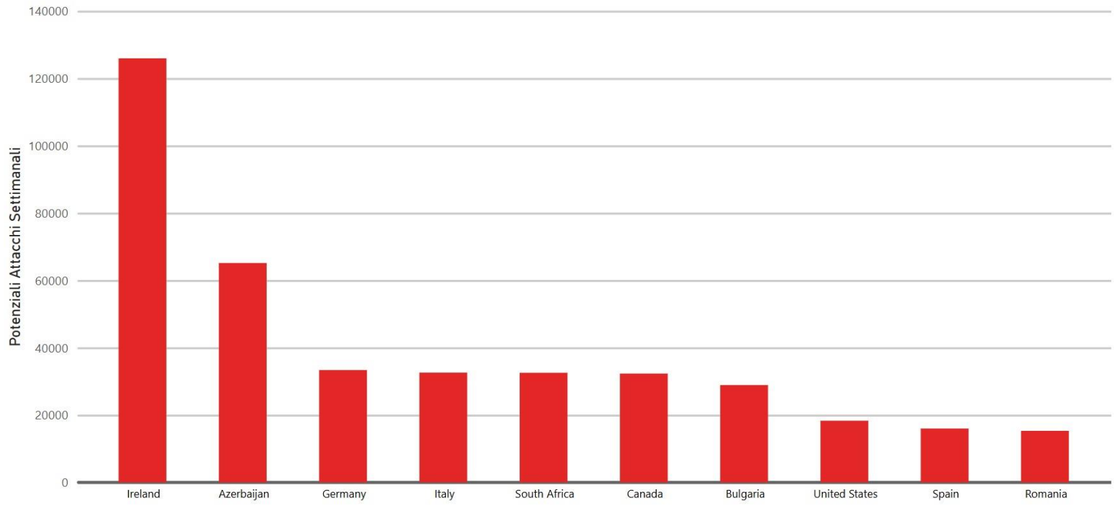


Attacchi intercettati:

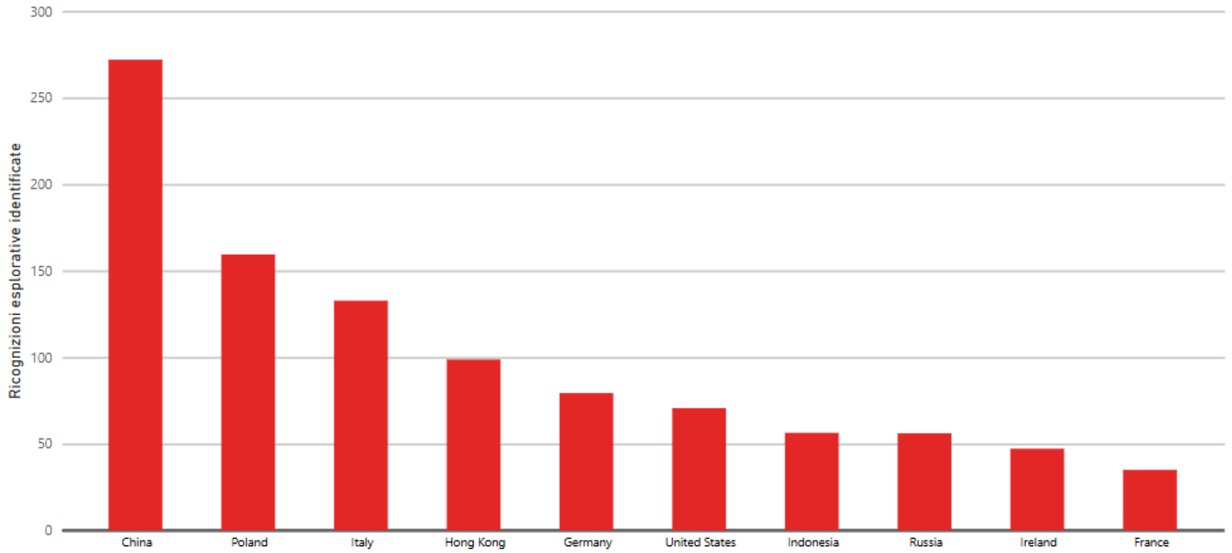
- *Irland*
- *Azerbajian*
- *Germany*
- *Italy*

Esplorative eseguite:

- *China*
- *Italy*
- *United States*
- *Germany*



Lo scenario – Da dove arrivano gli attacchi? (2025)

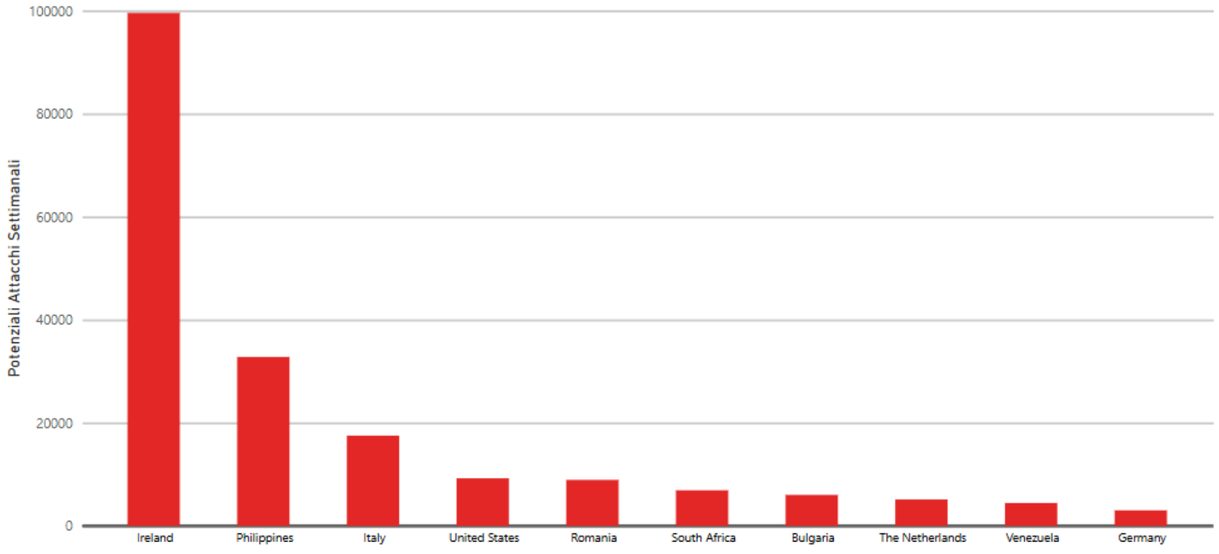


Esplorative eseguite:

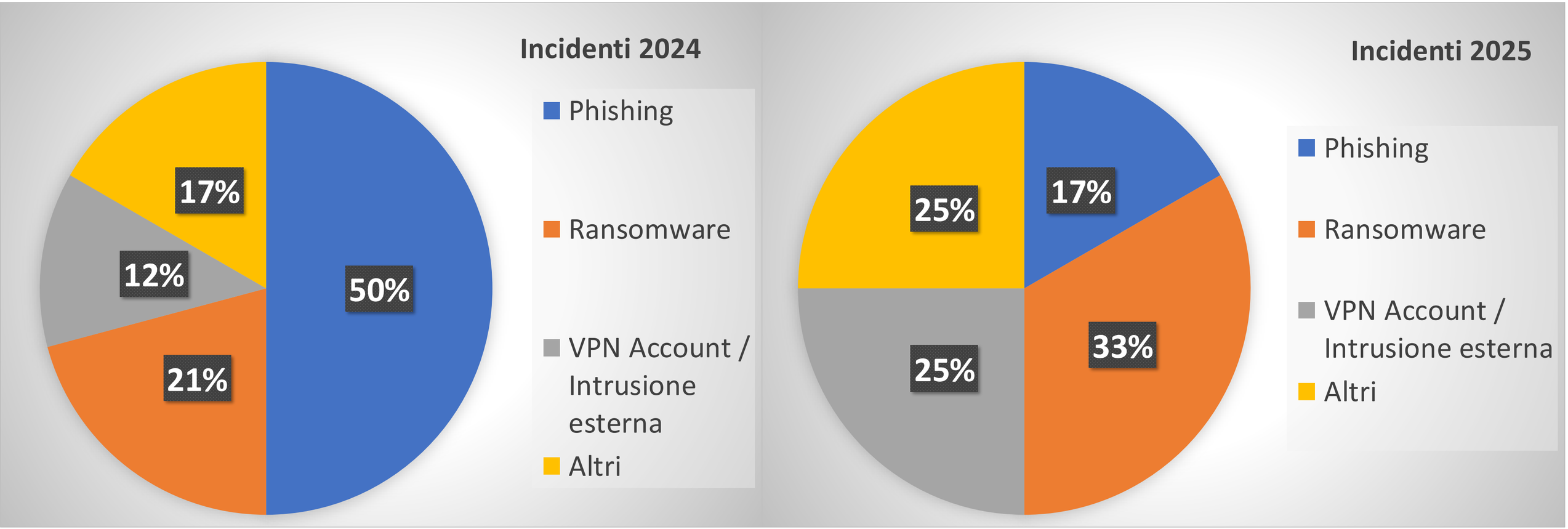
- *China*
- ***Poland***
- *Italy*
- ***Hong Kong***

Attacchi intercettati:

- *Irland*
- ***Philippines***
- *Italy*
- ***United States***



Lo scenario – Incidenti gestiti



Trend 2025

Tipologia di attacchi

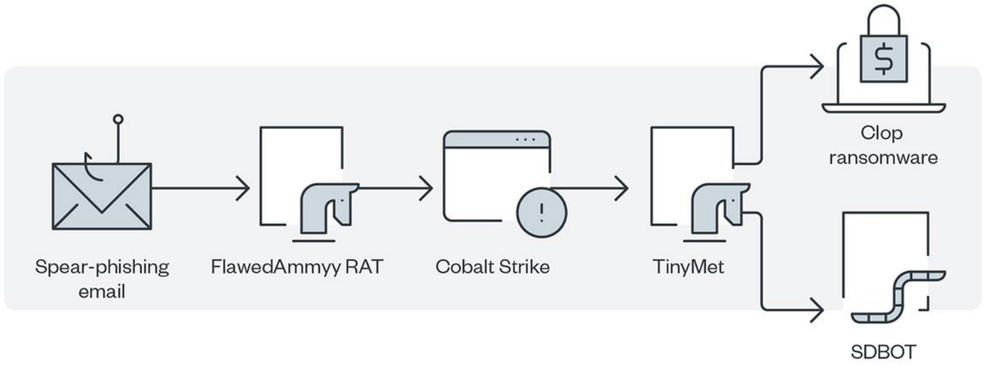
- *Phishing* *stabile*
- ***Intrusione esterna*** ***+200%***
- ***Ransomware*** ***+180%***

Gang criminali più attive

Info & status	N. rivendicazioni	2025	2024
clop	982	399	74
ransomhub	690	159	531
akira	632	157	315

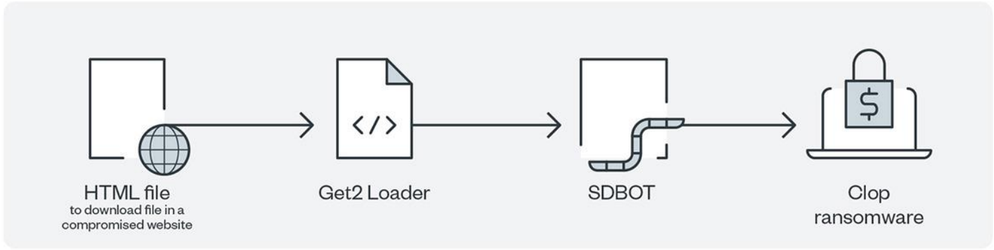
ANALISI DEGLI ATTACHI

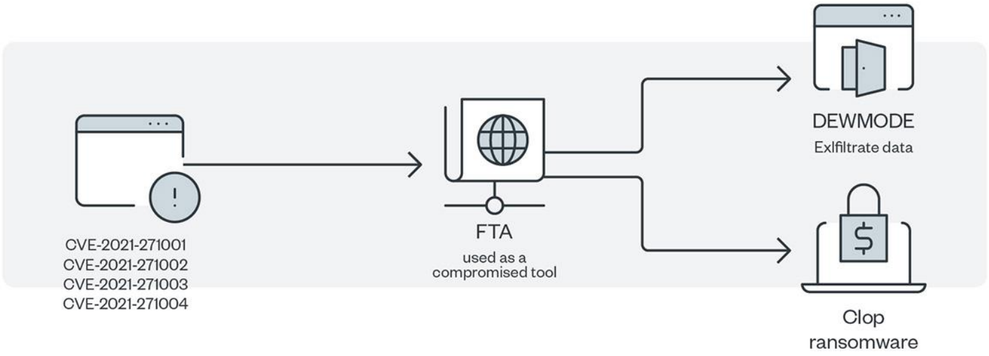
RANSOMWARE - Analisi dei punti di ingresso



Campagna di phishing

Sito internet compromesso





Vulnerabilità infrastrutturali

Furto credenziali VPN

RANSOMWARE – Conoscerlo per difendersi

Tattiche	***Strategia di difesa***
Ricognizione e persistenza	*Monitoraggio rete interna (IDS)* *Sistemi di protezione avanzata (XDR)* *Monitoraggio H24 (SOC)*
Esfiltrazione informazioni	*Segregazione rete* *VPN con doppio fattore di autenticazione* *Monitoraggio traffico in uscita* *Blocco del traffico malevolo*
Backup dei dati	*Gestione delle vulnerabilità continuative* *Backup a prova di ransomware* *Test di ripristino* *Resilienza operativa (non solo DR)*
Crittografia dei dati	*Monitoraggio delle terze parti* *Fiducia dei fornitori*

RANSOMWARE – Lesson learned

Le prime 24 ore

Definire il comitato di crisi
Isolare i sistemi e reset credenziali
Gestire comunicazione interna ed esterna
Ingaggio fornitori (cyber, IT, comunicazione, legale)

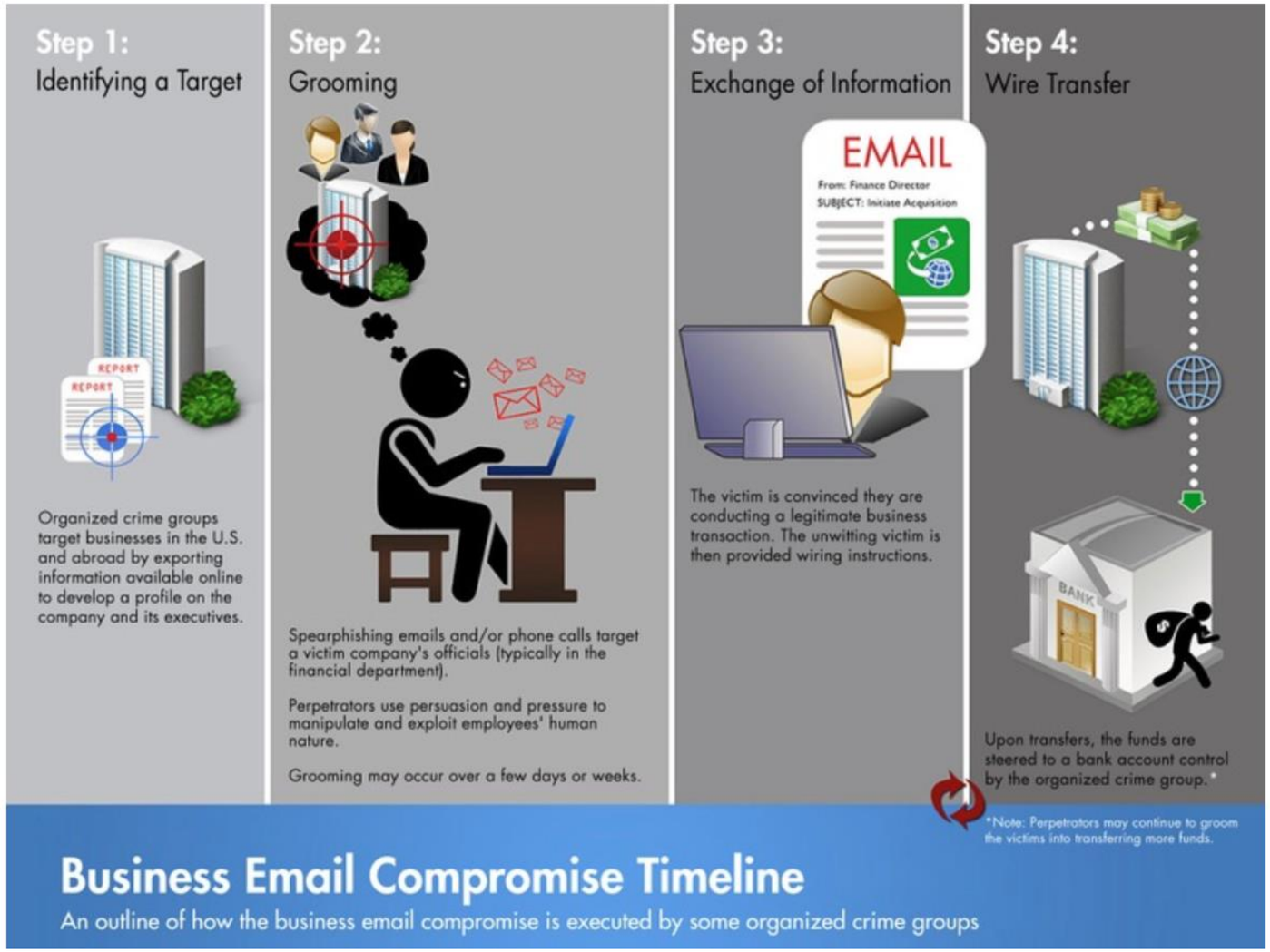
Giorni successivi

Gestire dipendenti e fornitori
Prepararsi all'eventuale pubblicazione dell'incidente
Ripartire in sicurezza (essere pronti ad un nuovo attacco)

Valutazione impatti

Valutare impatti dell'incidente (tecnico, reputazionale, verso i fornitori/clienti, legale, normativo)

Business Email Compromise



Business Email Compromise – Conoscerlo per difendersi

Tattiche

Ricerca informazioni sulla vittima

Furto delle credenziali

Monitoraggio mail e creazione regole di «replica»

Utilizzo della casella (pagamenti, esfiltrazioni, etc)

Strategia di difesa

Monitorare in modo continuativo l'esposizione pubblica dell'azienda (OSINT, dati disponibili, darkweb)
Attivare protezione avanzata posta (DKIM, SPF, etc.)

Attivare doppio fattore di autenticazione
Definire password policy

Monitorare gli accessi alle caselle di posta
Gestire gli allarmi dei service provider

Formazione e awareness

Q&A

Contatti:

ISC2 ITALY CHAPTER

https://www.isc2chapter-italy.it

Roberto Bonalumi

https://www.linkedin.com/in/robertobonalumi/

Filadelfio Emanuele

https://www.linkedin.com/in/filadelfio/