ICT POWER.IT

Microsoft

#POWERCON2023

Hacker point of view: i dettagli fanno la differenza

Domenico Caldarelli

Head of Cybersecurity

domenico.caldarelli@itisistemi.it

/domenicocaldarelli

Speaker

Domenico Caldarelli

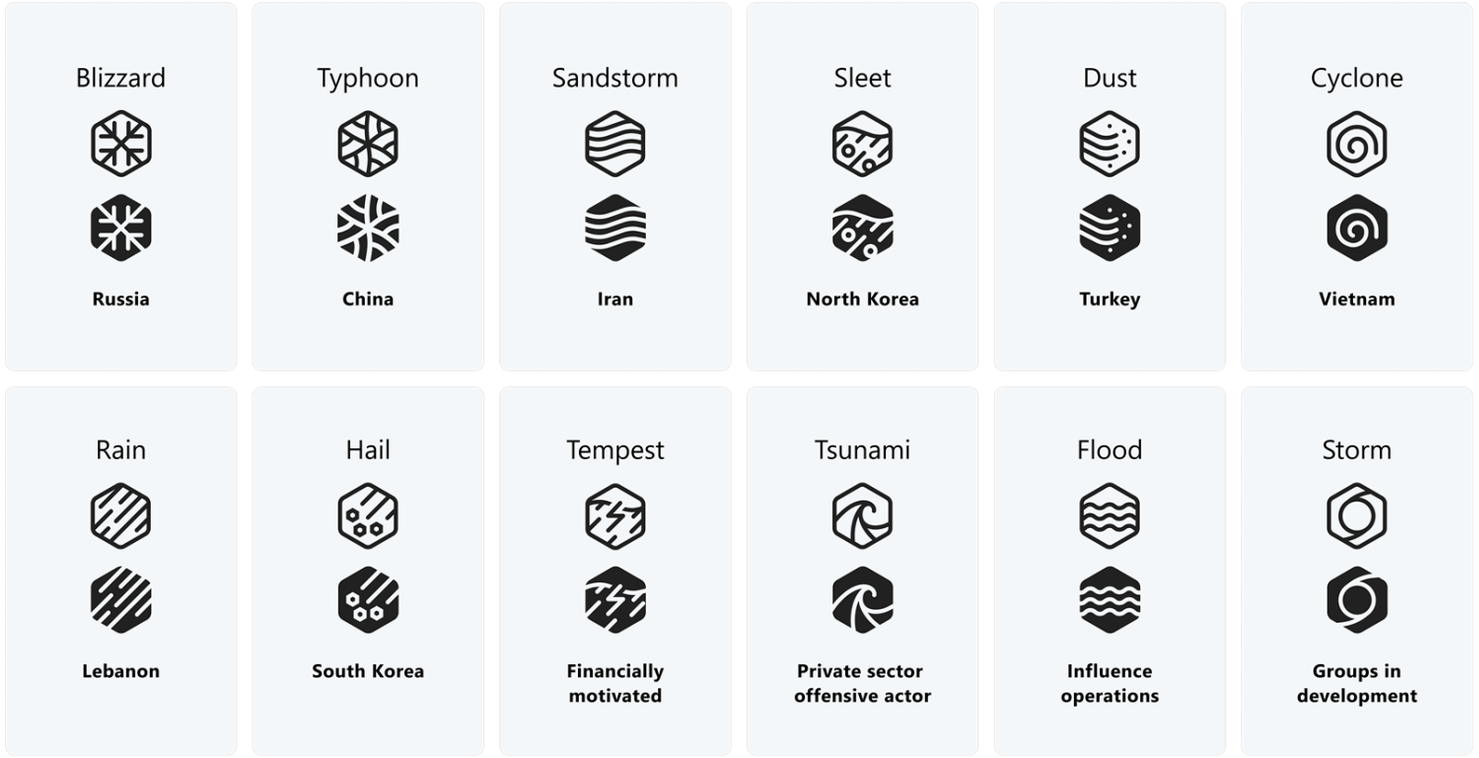
Head of Cyber Security, ITI srl

- Ethical Hacker
- OSCP, OSWA, CRTP

Agenda

- APT Groups
- Lateral Movement / Pivoting
- Command & Control
- Phishing

APT Groups



Attori nazione-stato
Attori motivati dal punto di vista finanziario
Attori offensivi del settore privato (PSOA)
Operazioni di influenza
Gruppi in fase di sviluppo

https://learn.microsoft.com/it-it/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Statistics

38% increase in Cybercrime-as-a-Service targeting business email observed between 2019 and 2022

35 million business email compromise attempts, with an average of 156,000 attempts daily, detected and investigated by Microsoft Threat Intelligence between April 2022 and April 2023

} *Microsoft* [1]

Ransomware attacks occur roughly every 11 seconds, and 94% of them now target backups

---> *NetworkComputing* [2]

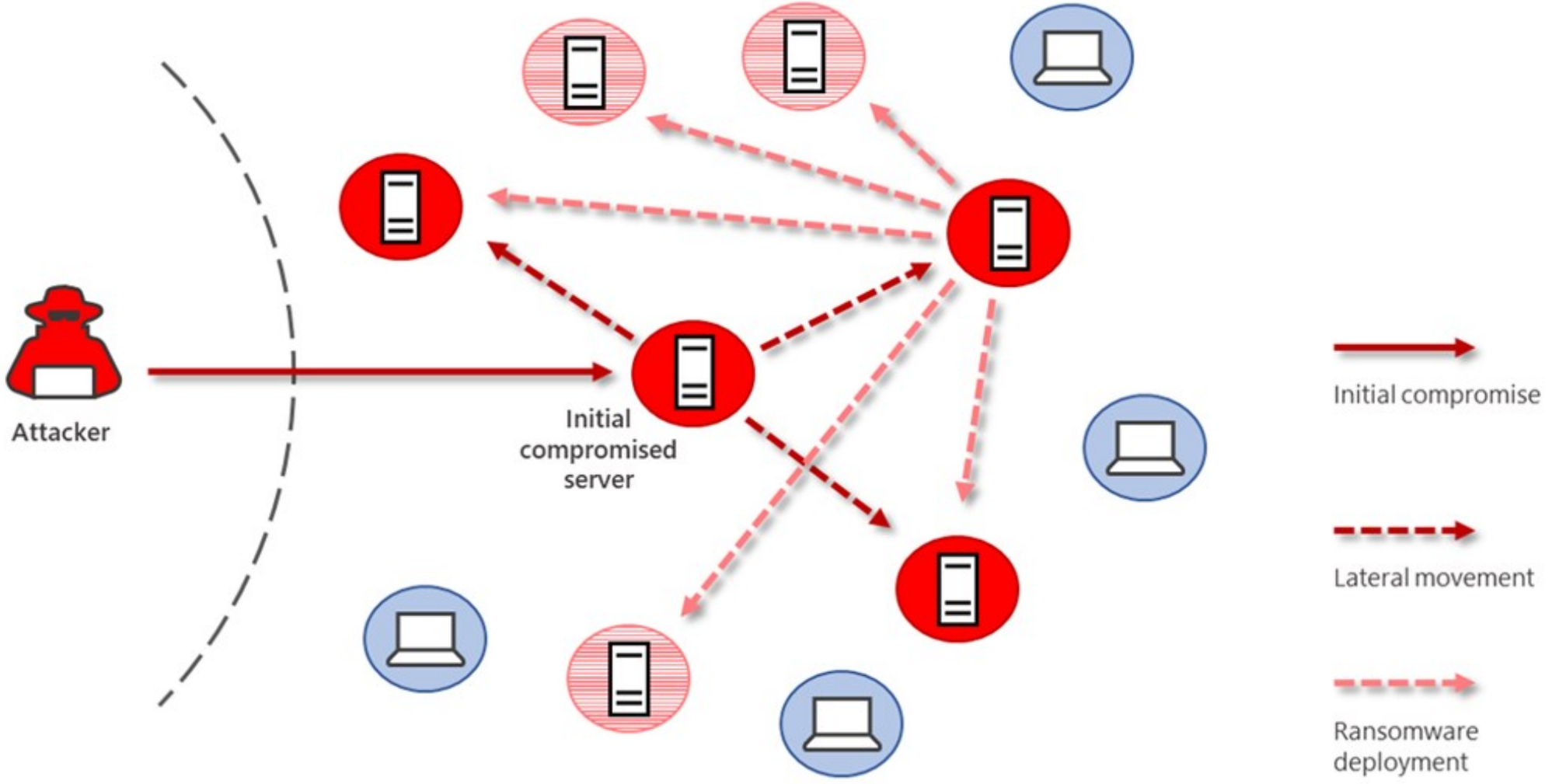
21% Share of incidents that saw backdoors deployed

62% Percentage of phishing attacks using spear phishing attachments

} *IBM* [3]

1. https://shorturl.at/cpxN6
2. https://www.networkcomputing.com/network-security/structured-success-4-architectural-pillars-cyber-resilience
3. https://www.ibm.com/downloads/cas/DB4GL8YM

Lateral Movement / Pivoting



Persistence

Con persistenza si intende la possibilità di accedere ad un server, o eventualmente ai dati della vittima, ogni volta che l'attaccante lo ritiene necessario.

Una persistenza viene creata dopo aver eseguito un accesso ad un sistema, e può essere fatta in vari modi: tramite l'esecuzione di comandi all'avvio delle macchine, tramite task schedulati creati appositamente, con l'aggiunta di codice appositamente scritto ed ubicato opportunamente nel sistema, ecc…

Un difensore potrebbe correggere la vulnerabilità (o la misconfiguration) utilizzata dall'attaccante per eseguire l'accesso, impedendogli di poterlo eseguire nuovamente. Di conseguenza, per un attaccante è importante effettuare tali azioni al fine di mantenere l'accesso ed avere il tempo necessario per i suoi scopi.

Il command and control (C2) è un server esposto su rete internet che rimane in ascolto sulle porte definite dall'attaccante in attesa che la macchina vulnerabile lo contatti.

Solitamente un attaccante preferisce l'utilizzo di un Cloud Provider (Microsoft Azure, Google Cloud, Amazon AWS, ecc…) per essere più anonimo possibile. Questa modalità facilita anche determinate azioni consentendo di evitare alcune difese che potrebbero essere presenti all'interno dell'infrastruttura della vittima.

https://www.ictpower.it/sicurezza/blue-team-experience-detection-and-mitigation.htm

Phishing

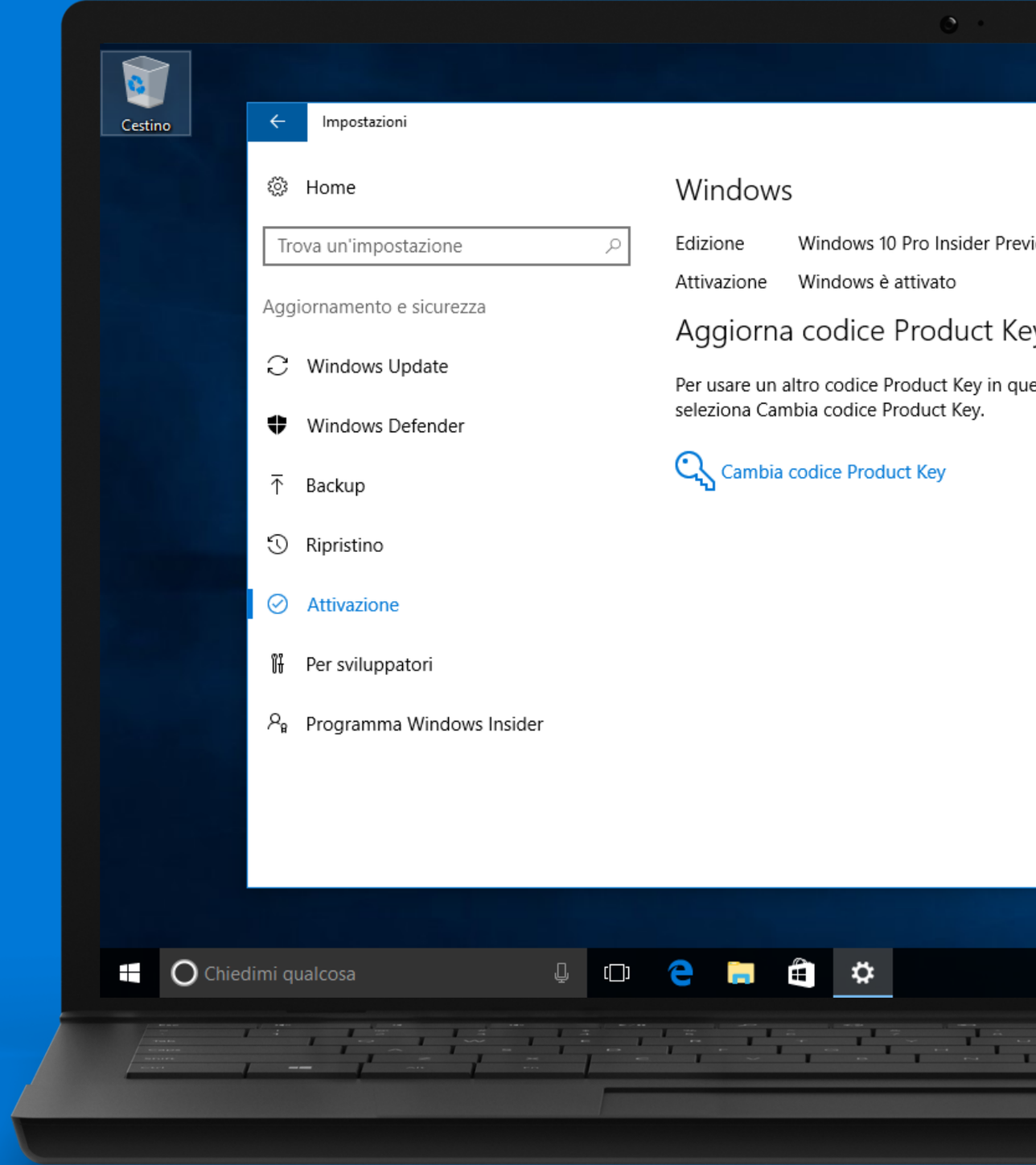
Il phishing è una forma di attacco informatico in cui gli aggressori cercano di ingannare le vittime al fine di ottenere informazioni sensibili come username, password, dettagli finanziari o altre informazioni personali.

Questo tipo di attacco viene effettuato solitamente attraverso e-mail e messaggi di testo oppure effettuando chiamate telefoniche o attraverso siti web fraudolenti che si presentano come legittimi e affidabili, assumendo varie denominazioni (ad esempio: Vishing).

Può anche assumere forme più mirate, come lo **spear phishing**, in cui gli aggressori raccolgono informazioni specifiche sulla vittima per personalizzare l'attacco e renderlo più credibile. Ad esempio, potrebbero utilizzare il nome, il ruolo o i dettagli personali della vittima per creare un messaggio che sembra autentico e convincente.

Le organizzazioni legittime, è bene ricordarlo, non chiedono mai password, informazioni personali o finanziarie sensibili tramite e-mail. In caso di dubbio, è meglio contattare direttamente l'organizzazione in questione per verificare l'autenticità delle richieste.

DEMO


Cestino
Impostazioni
Home
Trova un'impostazione
Aggiornamento e sicurezza
Windows Update
Windows Defender
Backup
Ripristino
Attivazione
Per sviluppatori
Programma Windows Insider
Windows
Edizione
Windows 10 Pro Insider Previ
Attivazione
Windows è attivato
Aggiorna codice Product Key
Per usare un altro codice Product Key in que
seleziona Cambia codice Product Key.
Cambia codice Product Key
Chiedimi qualcosa

Grazie

Domenico Caldarelli
Head of Cybersecurity
domenico.caldarelli@itisistemi.it

/domenicocaldarelli