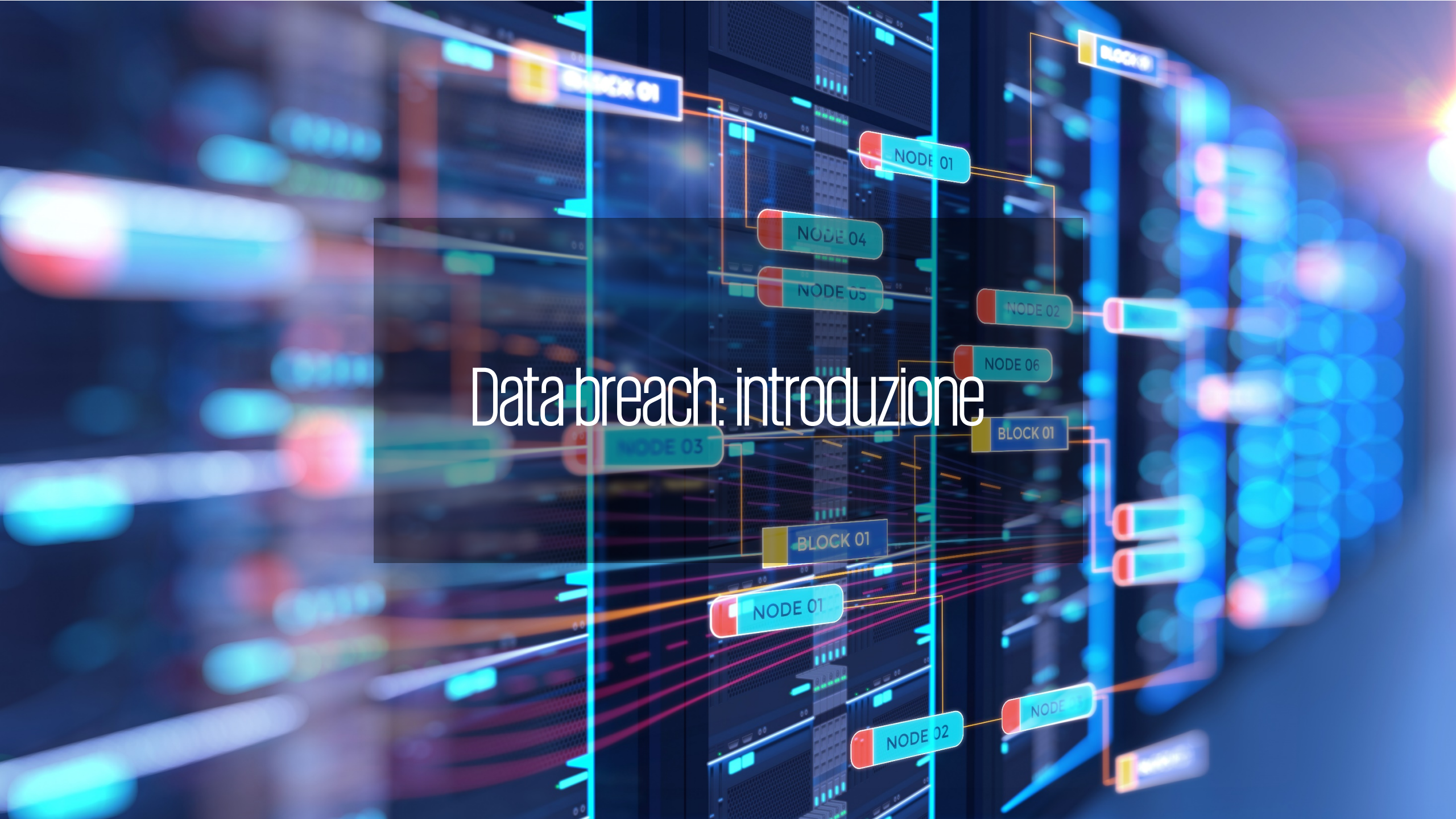
Data breach: real world adversary tactics and techniques

30/11/2019 - Torino

Chi siamo

Dario Amoruso è Senior Manager in KPMG Advisory ed opera nella linea di servizi che si occupa di Cyber Security, ha conseguito la laurea Specialistica in Ing, Informatica presso Università di Pisa. Le sue competenze si sviluppano da un lato verso tematiche di Governance Risk e Compliance e dall'altro verso tematiche tecnologiche legate ad attività di Security Testing e Red and Blue teaming. Negli ultimi anni ha sviluppato notevoli esperienze in ambito tematiche di Industrial Control System (ICS) Security

Matteo Ranalli è un consulente appassionato di sicurezza, laureato in Ingegneria Informatica, con una forte curiosità verso tutti gli aspetti legati all'informatica. Attualmente lavora nel gruppo di Cyber Security di KPMG Advisory, ove mette a disposizione le proprie competenze ed esperienze maturate in ambito di Blue Teaming e Red Teaming, insieme ad altre tematiche inerenti la sicurezza dei dati e delle aziende.



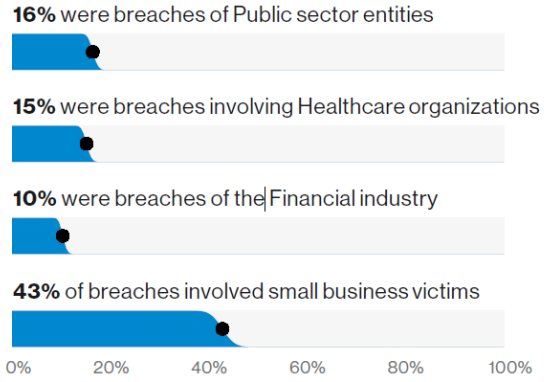
Data breach: introduzione

Data breach - Introduzione

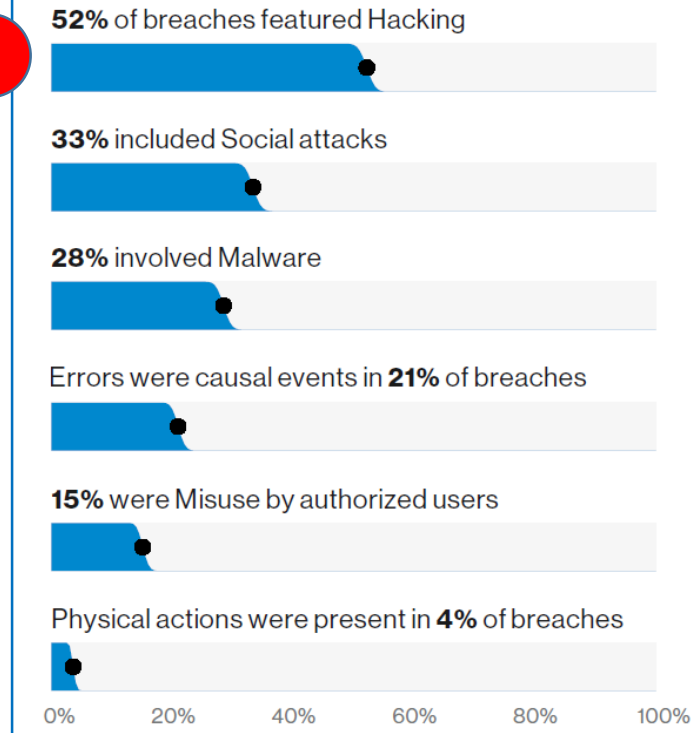
Con il termine **data breach** si intende un incidente di sicurezza in cui dati sensibili, protetti o riservati vengono consultati, copiati, trasmessi, rubati o utilizzati da un soggetto non autorizzato. Solitamente il data breach si realizza con una divulgazione di dati riservati o confidenziali all'interno di un ambiente privo di misure di sicurezze (da esempio, su web) in maniera involontaria o volontaria. Tale divulgazione può avvenire in seguito a:

- **perdita accidentale**: ad esempio, data breach causato da smarrimento di una chiavetta USB contenente dati riservati
- **furto**: ad esempio, data breach causato da furto di un notebook contenente dati confidenziali
- **infedeltà aziendal**e: ad esempio, data breach causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia distribuita in ambiente pubblico
- **accesso abusivo**: ad esempio, data breach causato da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite

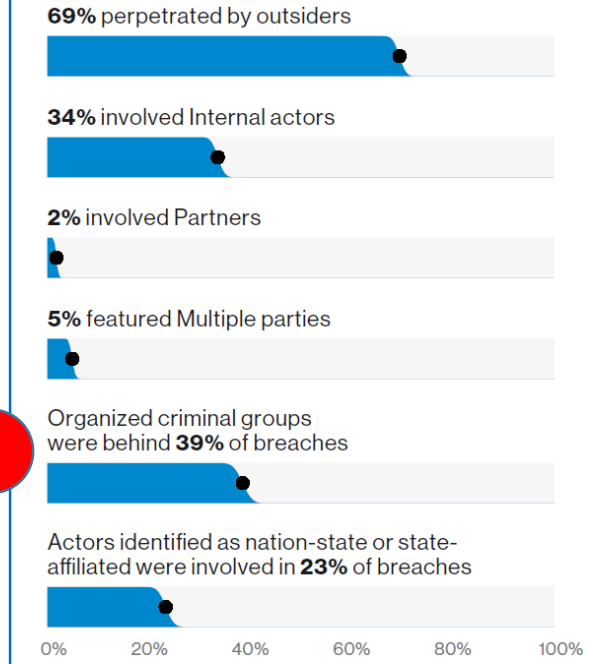
Data breach - Un po' di statistiche



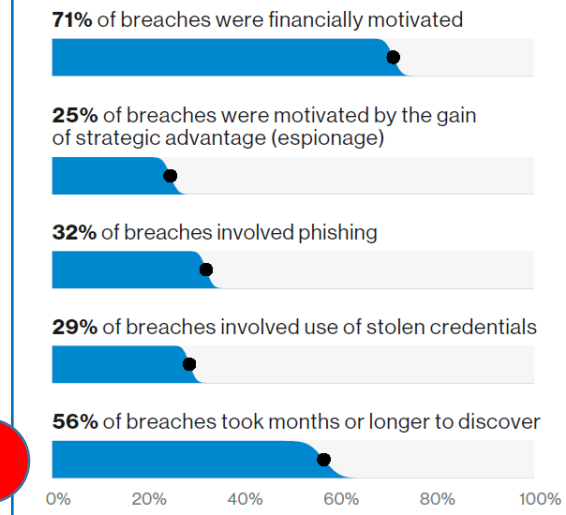
Chi sono le vittime



Quali tattiche sono utilizzate



Chi li effettua



Altri fattori comuni

The data set for this report totals over 100,000 incidents, 101,168 to be exact!

Fonte: Verizon - 2019 Data Breach Investigations

Data breach - La top 10 del 21° secolo

1. Yahoo
Date: 2013-14
Impact: 3 billion user accounts

2. Marriott International
Date: 2014-18
Impact: 500 million customers

3. Adult Friend Finder
Date: October 2016
Impact: More than 412.2 million accounts

4. eBay
Date: May 2014
Impact: 145 million users compromised

5. Equifax
Date: July 29 2017
Impact: Personal information of 143 million consumers

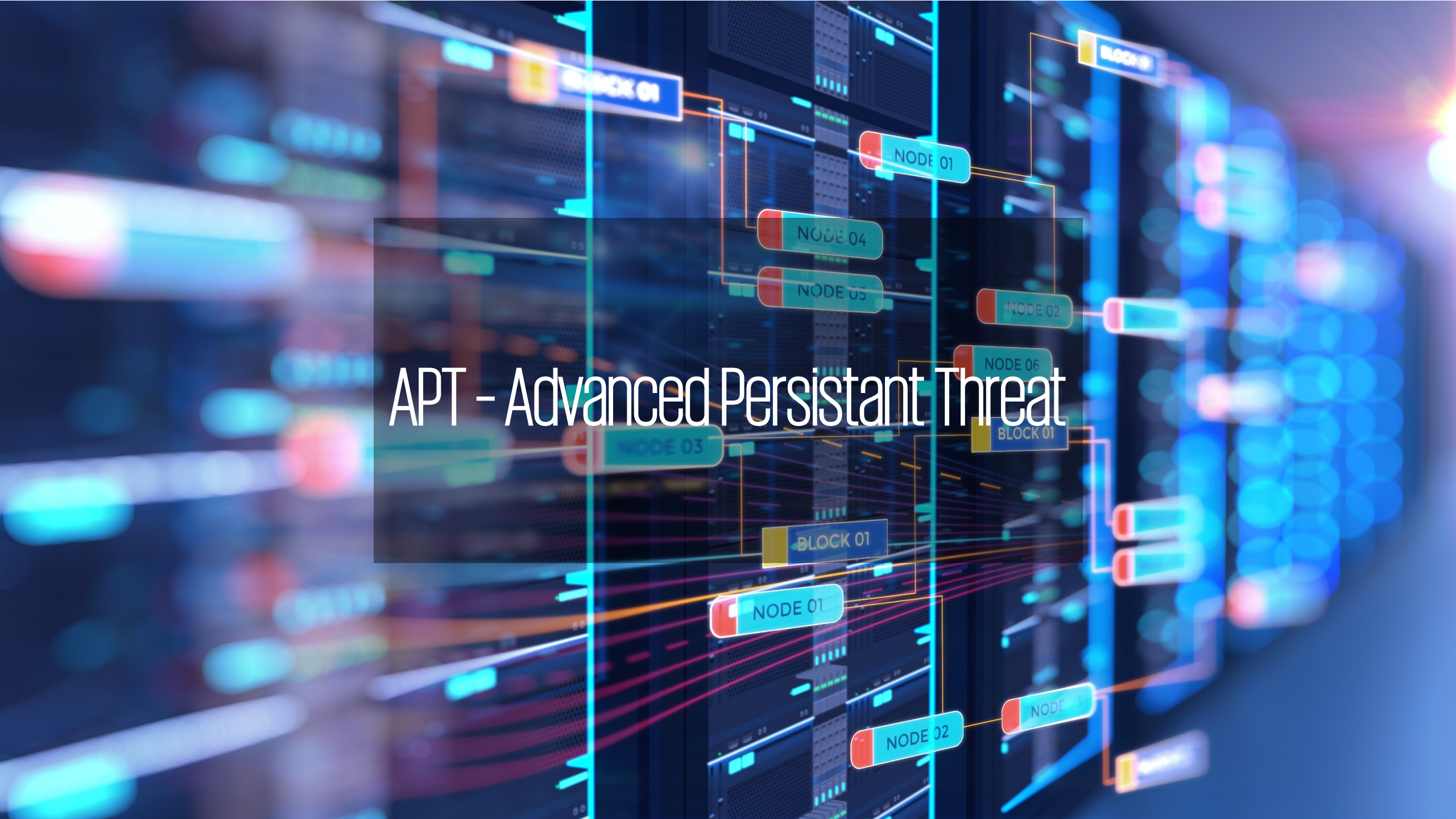
6. Heartland Payment Systems
Date: March 2008
Impact: 134 million credit cards exposed through SQL injection to install spyware on Heartland's data systems.

7. Target Stores
Date: December 2013
Impact: Credit/debit card information and/or contact information of up to 110 million people compromised

8. Uber
Date: Late 2016
Impact: Personal information of 57 million Uber users and 600,000 drivers exposed.

9. JP Morgan Chase
Date: July 2014
Impact: 76 million households and 7 million small businesses

10. Sony's PlayStation Network
Date: April 20, 2011
Impact: 77 million PlayStation Network accounts hacked; estimated losses of $171 million while the site was down for a month.

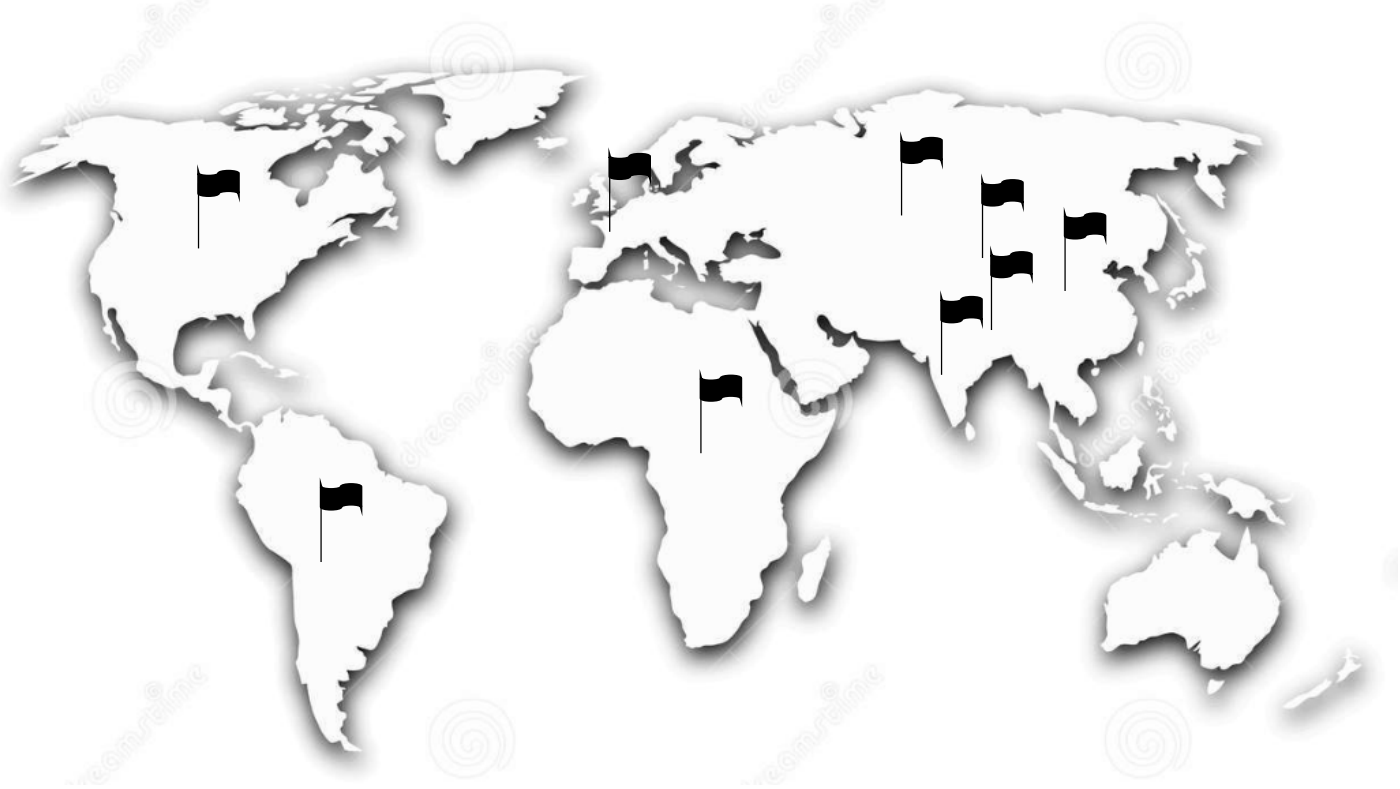


APT - Advanced Persistant Threat

APT - Advanced Persistent Threat

L'acronimo **APT, Advanced Persistent Threat**, rappresenta una **minaccia portata avanti da un avversario dotato di notevole expertise tecnico e grandi risorse**, in grado di effettuare attacchi su vasta scala, utilizzando molteplici vettori, e per periodi di tempo molto estesi.

La maggior parte delle APT, ma non tutte, sono gestite da gruppi organici a stati sovrani.



APT – Gruppi criminali famosi

Di seguito sono rappresentati una serie non esaustiva di alcuni dei maggiori gruppi APT rilevati nel mondo, che si sono distinti per le loro capacità, motivazioni e target preferiti.

APT28 – Fancy Bear

Lazarus Group (aka Hidden Cobra)

MuddyWater

Deep Panda

Ulteriori gruppi conosciuti:

- APT18
- APT41
- Axiom
- BlackOasis
- Carbanak
- Charming Kitten
- Cobalt Group
- CopyKittens
- Elderwood
- Group5
- Honeybee
- Leafminer
- Leviathan
- Magic Hound
- Night Dragon
- Patchwork
- PittyTiger
- Poseidon Group
- Putter Panda
- Rancor
- RTM
- Sandworm Team
- Scarlet Mimic
- Soft Cell
- Stealth Falcon
- Stolen Pencil
- Strider

E molti altri…

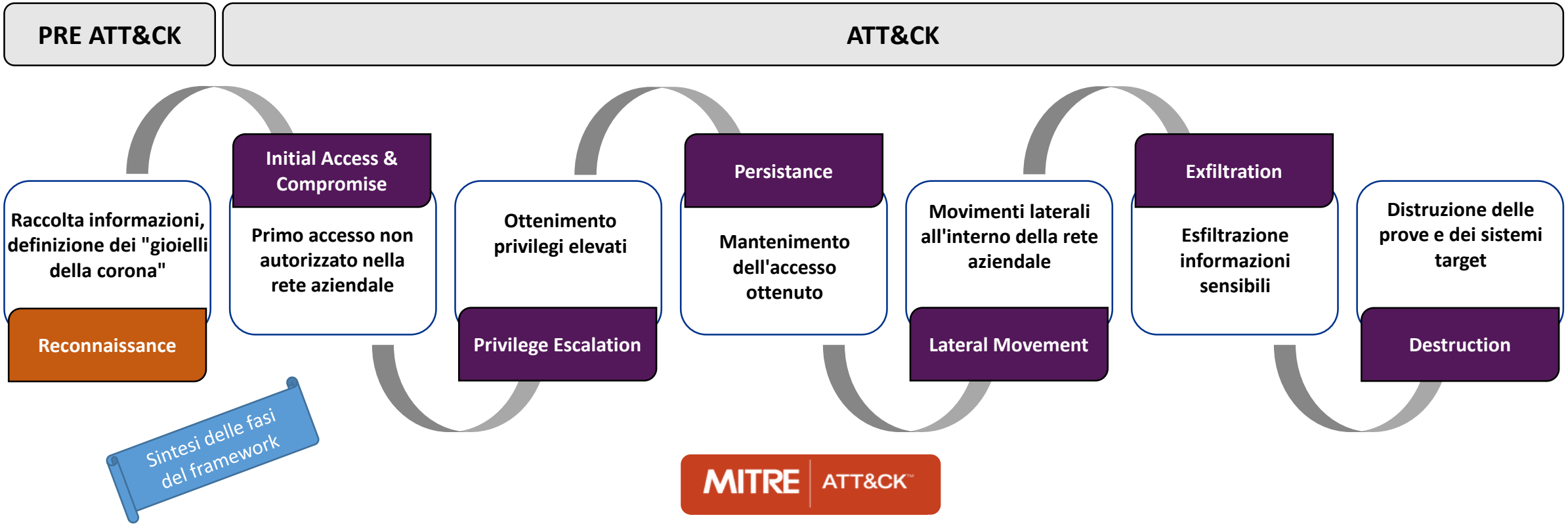
Mitre Att&ck - Tattiche e tecniche degli APT

Mitre Att&ck - Un framework open source

Il **Mitre Att&ck** (Adversarial Tactics, Techniques & Common Knowledge) è un framework nato per descrivere e categorizzare i comportamenti e le tecniche utilizzate dagli attori criminali internazionali nell'esecuzione di attacchi informatici complessi.

È suddiviso in due fasi: **PRE-ATT&CK** e **ATT&CK**.

- La prima fase definisce tecniche e metodologie usate per raccogliere quante più informazioni sul target designato;
- la seconda fase definisce tecniche e metodologie che vengono usate dopo aver ottenuto un primo accesso non autorizzato sul target designato.



Mitre Att&ck - Un linguaggio unificato

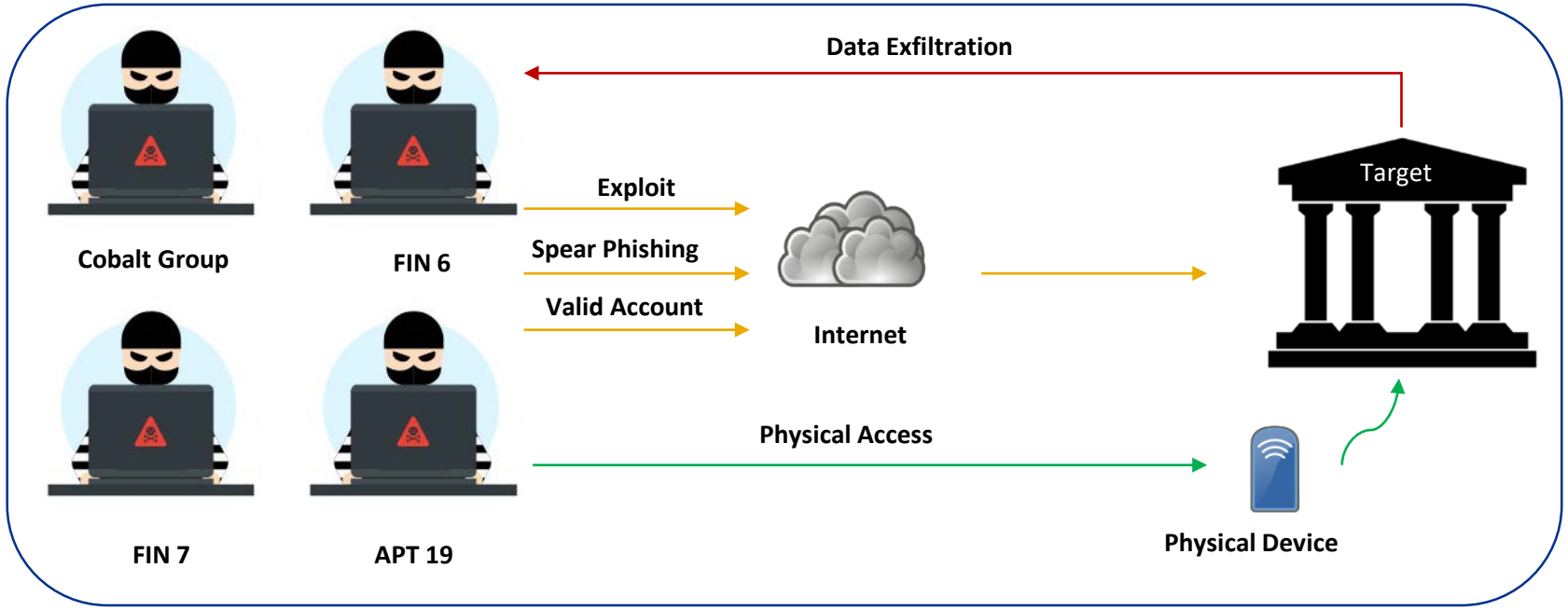
L'utilizzo di un framework come questo ha molteplici vantaggi:

- tenere traccia del comportamento degli avversari a un livello dettagliato;
- comunicare con i difensori e con altre organizzazioni comportamenti specifici usando un linguaggio unificato;
- evidenziare le eventuali lacune o punti di forza del proprio perimetro difensivo.

Di seguito viene riportata una porzione della matrice **ATT&CK** che illustra le capacità del framework di tracciare in maniera chiara ed esplicativa i comportamenti osservati durante una compromissione.

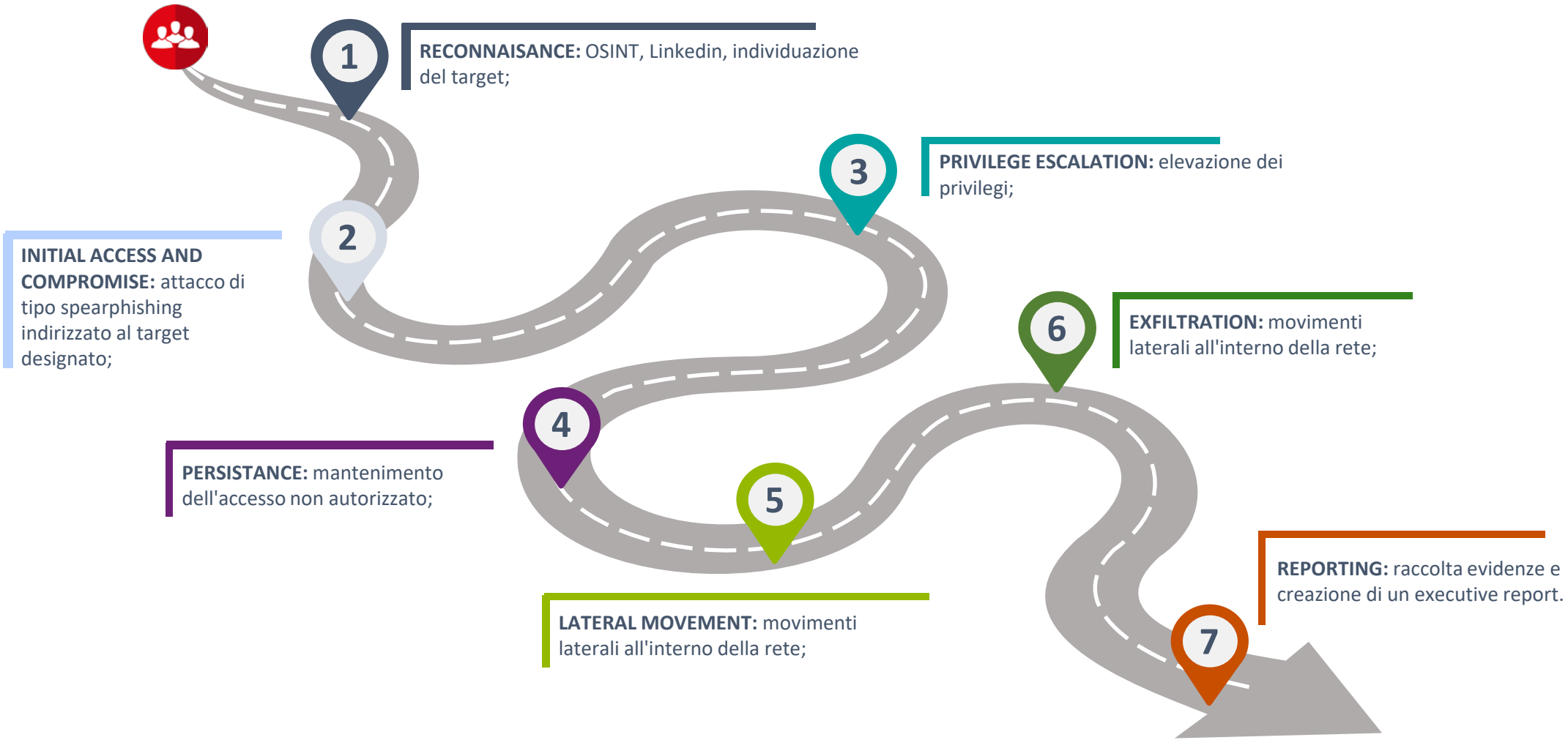
Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Accessibility Features	Accessibility Features	Binary Padding	Brute Force	Account Discovery	Application Deployment Software	Command-Line	Automated Collection	Automated Exfiltration	Commonly Used Port
AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Application Window Discovery	Exploitation of Vulnerability	Execution through API	Clipboard Data	Data Compressed	Communication Through Removable Media
Basic Input/Output System	Bypass User Account Control	Code Signing	Credential Manipulation	File and Directory Discovery	Logon Scripts	Graphical User Interface	Data Staged	Data Encrypted	Custom Command and Control Protocol
Bootkit	DLL Injection	Component Firmware	Credentials in Files	Local Network Configuration Discovery	Pass the Hash	PowerShell	Data from Local System	Data Transfer Size Limits	Custom Cryptographic Protocol
Change Default File Handlers	DLL Search Order Hijacking	DLL Injection	Exploitation of Vulnerability	Local Network Connections Discovery	Pass the Ticket	Process Hollowing	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	Data Obfuscation
Component Firmware	Exploitation of Vulnerability	DLL Search Order Hijacking	Input Capture	Network Service Scanning	Remote Desktop Protocol	Rundll32	Data from Removable Media	Exfiltration Over Command and Control Channel	Fallback Channels
DLL Search Order Hijacking	Legitimate Credentials	DLL Side-Loading	Network Sniffing	Peripheral Device Discovery	Remote File Copy	Scheduled Task	Email Collection	Exfiltration Over Other Network Medium	Multi-Stage Channels
Hypervisor	Local Port Monitor	Disabling Security Tools	Two-Factor Authentication Interception	Permission Groups Discovery	Remote Services	Service Execution	Input Capture	Exfiltration Over Physical Medium	Multiband Communication
Legitimate Credentials	New Service	Exploitation of Vulnerability		Process Discovery	Replication Through Removable Media	Third-party Software	Screen Capture	Scheduled Transfer	Multilayer Encryption
						Windows Management			

Mitre Att&ck - Tecniche e tattiche reali



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery
External Remote Services	CMSTP	Application Shimming	Application Shimming	Bypass User Account Control	Credential Dumping	Account Discovery
Spearphishing Attachment	Command-Line Interface	External Remote Services	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning
Spearphishing Link	Dynamic Data Exchange	Logon Scripts	Exploitation for Privilege Escalation	Code Signing	Input Capture	Network Sniffing
Valid Accounts	Exploitation for Client Execution	New Service	New Service	Obfuscated Files or Information	Input Prompt	Permission Groups Discovery
Hardware Additions	User Execution	Redundant Access	Process Injection	Process Injection	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery
	Mshta	Registry Run Keys / Startup Folder	Scheduled Task	Signed Binary Proxy Execution	Network Sniffing	Security Software Discovery

Mitre Att&ck - Un esempio di scenario per le aziende

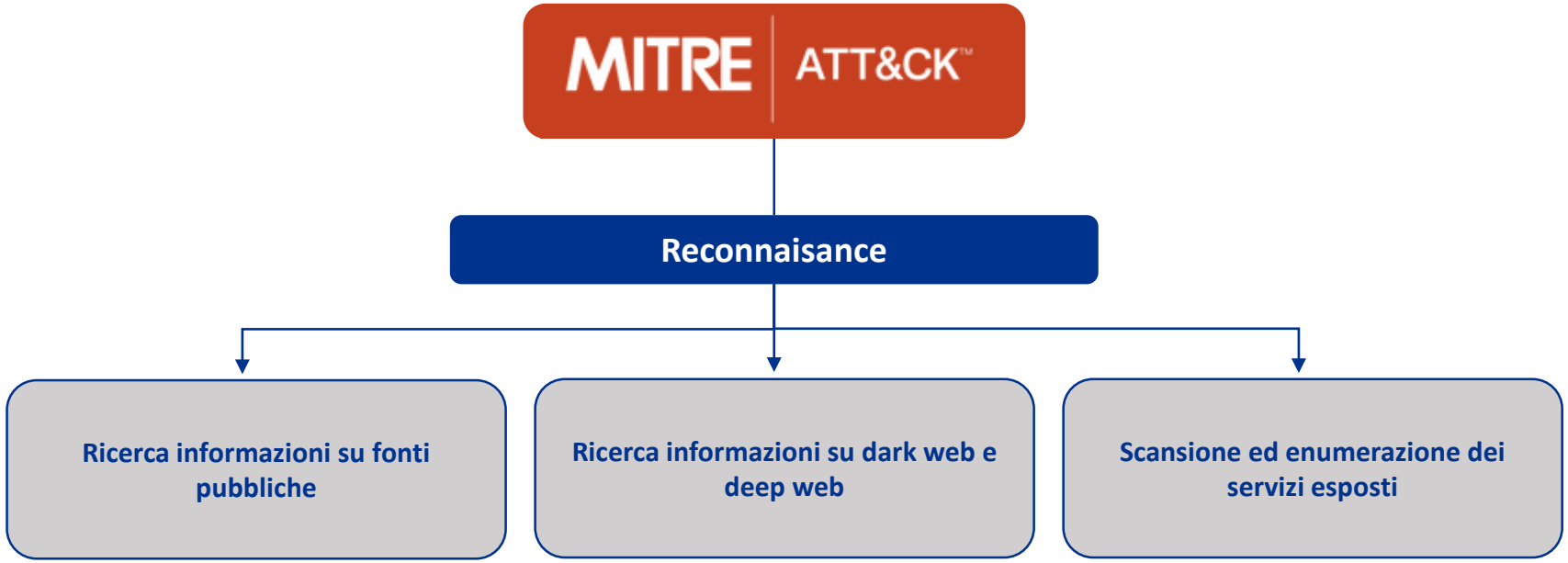


Mitre Att&ck - Recoinnaissance

La prima fase consiste nel raccogliere quante più informazioni possibile sul target designato in modo da individuare eventuali punti deboli e/o vulnerabili, sfruttabili per un successivo acceso non autorizzato.

Queste informazioni possono riguardare ad esempio email del personale, numeri di telefono, personale di gestione, ubicazione fisica degli edifici, fornitori di terze parti.

Per raggiungere questi scopi vengono utilizzate diverse tecniche di ricognizione, di seguito alcuni dei metodi che vengono utilizzati:

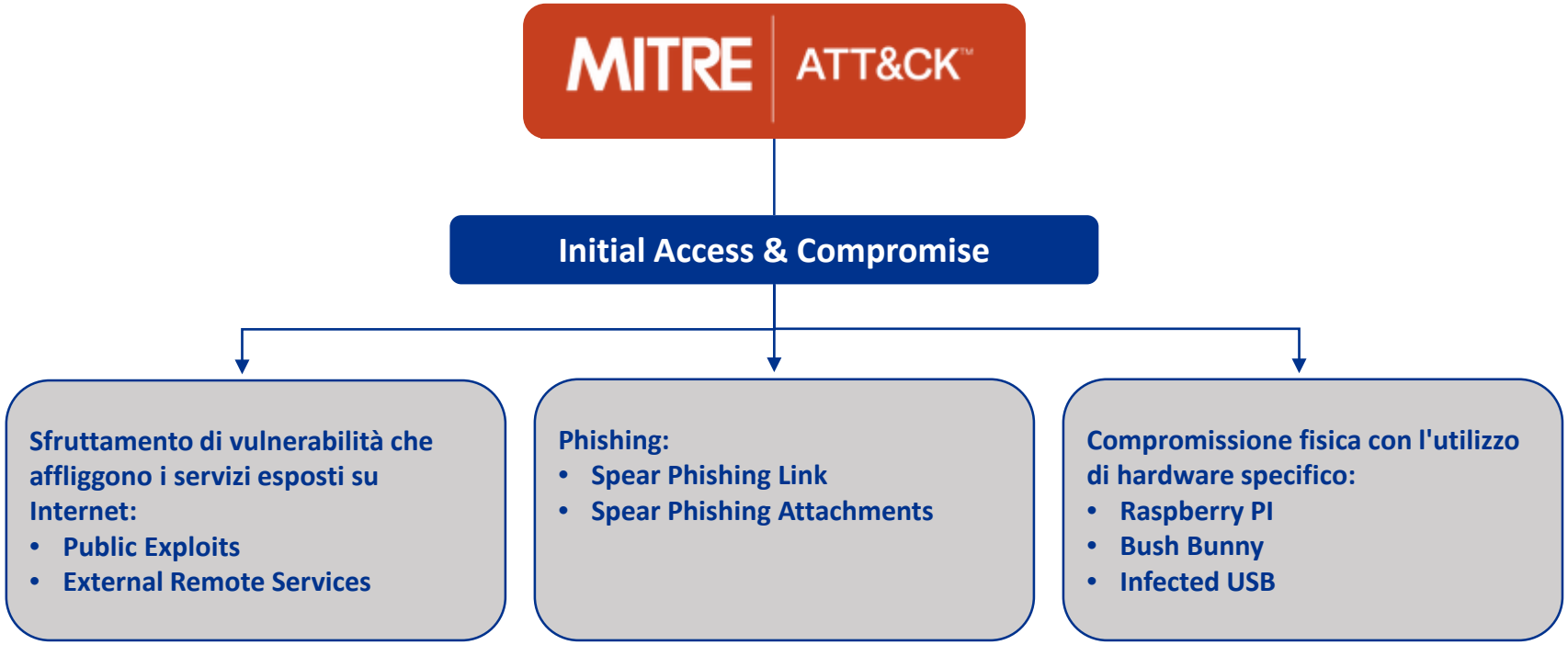


Mitre Att&ck - Initial access & compromise

Sulla base delle informazioni raccolte nella fase precedente, viene pianificato ed eseguito un primo accesso non autorizzato all'interno della rete aziendale.

Esistono molteplici tattiche proposte nel framework **Mitre Att&ck**, che vengono utilizzate in questa fase.

Di seguito ne vengono elencate alcune:

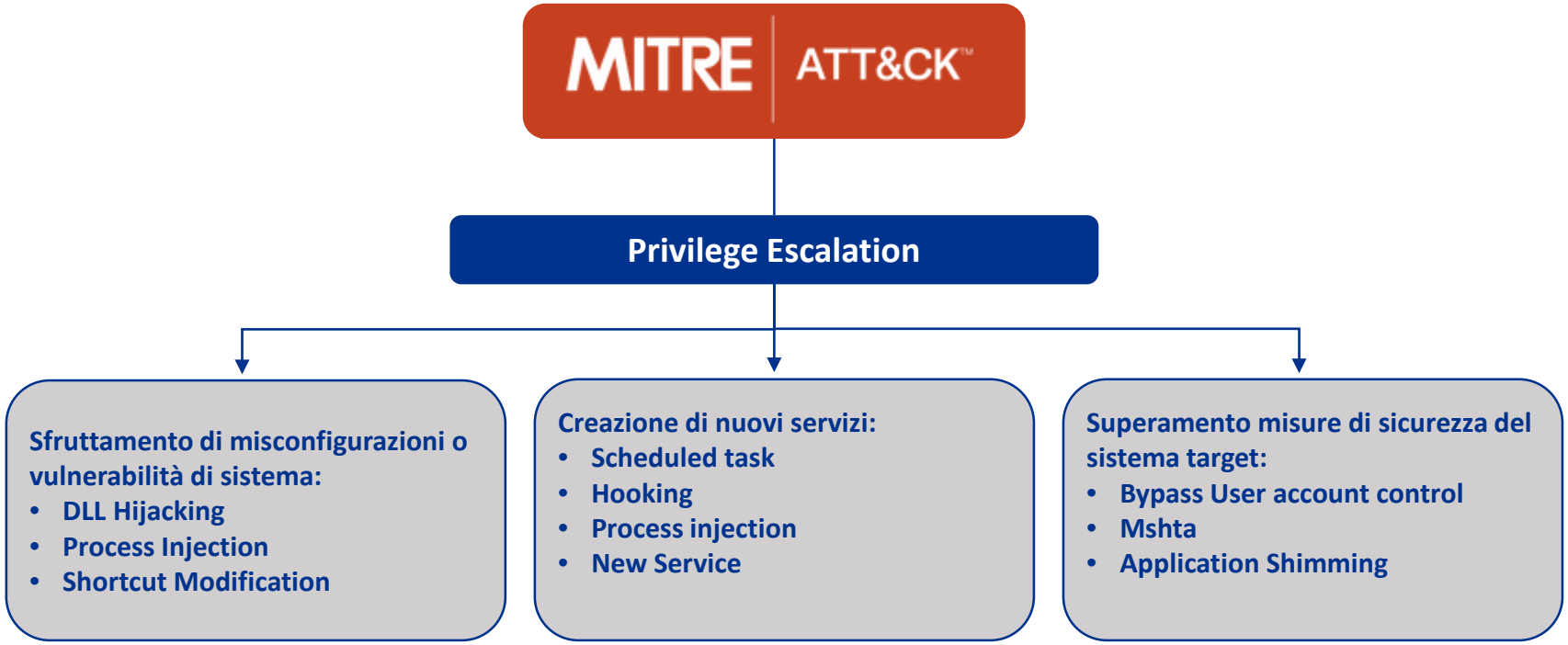


Mitre Att&ck - Privilege escalation

Per stabilire un accesso persistente, è necessario attuare delle tecniche che permettano di elevare i privilegi sulla macchina appena compromessa.

Questo passaggio risulta essere necessario per raccogliere ulteriori informazioni riguardo alla macchina stessa, come ad esempio le password di sistema.

Alcune delle attività proposte dal framework **Mitre Att&ck** per questa specifica fase, sono le seguenti:

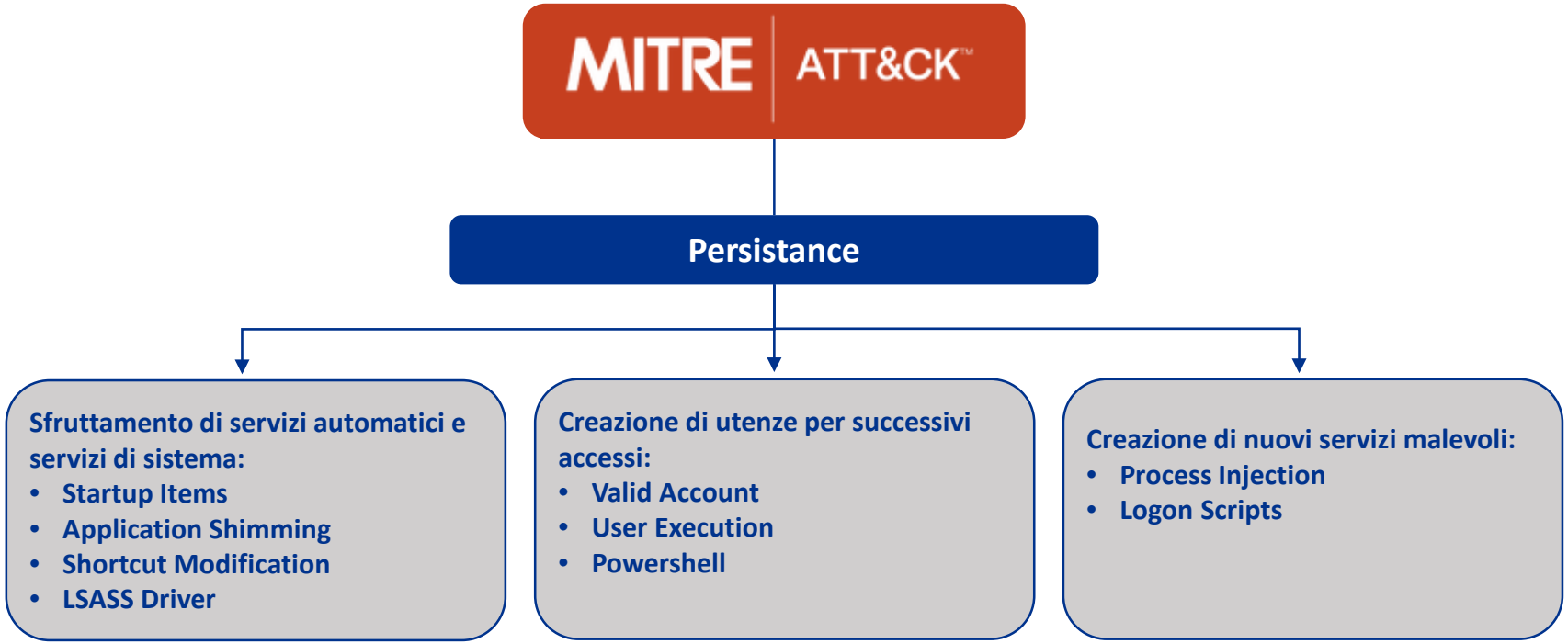


Mitre Att&ck - Persistance

Una volta ottenuto il primo accesso non autorizzato all'interno della rete aziendale, comincia la terza fase, dedicata al mantenimento prolungato di questo accesso, anche in caso di riavvii di sistema.

Questa fase risulta essere fondamentale per procedere successivamente con l'esfiltrazione dei dati sensibili.

Alcune delle attività che vengono svolte in questa fase sono:

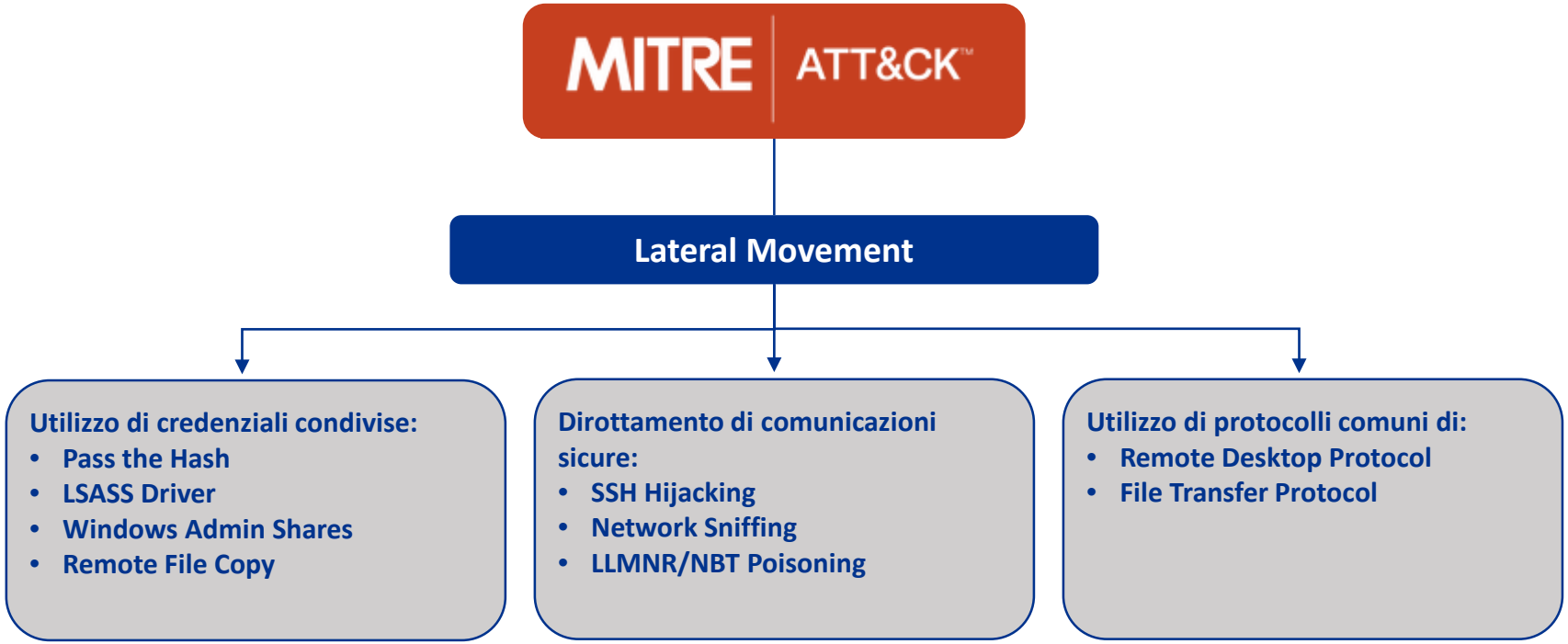


Mitre Att&ck - Lateral movement

In questa fase del **Mitre Att&ck** framework vengono attuate delle tecniche avanzate che permettono di muoversi lateralmente all'interno della rete, in modo da ottenere una maggiore visibilità della stessa.

Questo tipo di "movimento laterale" risulta fondamentale nel caso di presenza di reti segregate, o di informazioni accessibili solo da determinati computer.

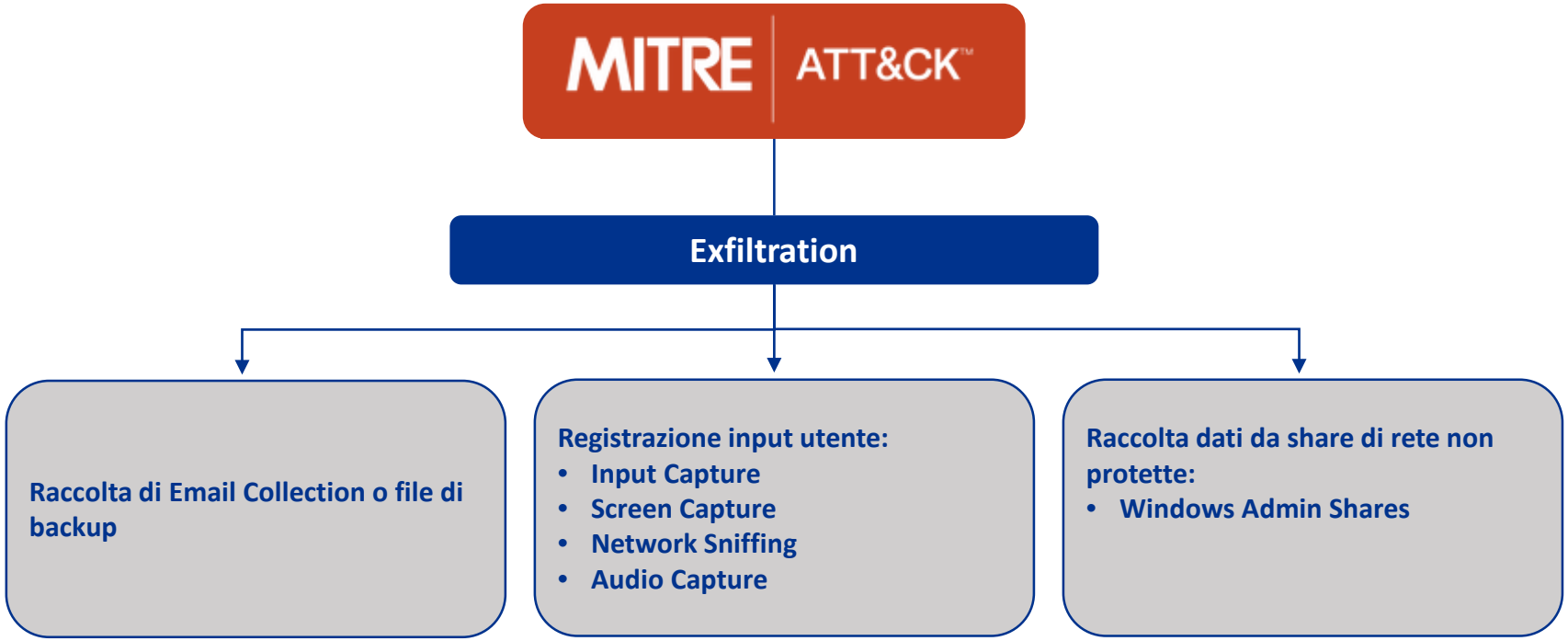
Di seguito vengono elencate alcune delle tecniche che possono essere utilizzate per il raggiungimento degli scopi sopra descritti:



Mitre Att&ck - Exfiltration

In quest'ultima fase, dopo aver localizzato in quelle precedente le potenziali informazioni sensibili, verranno eseguiti dei tentativi di esfiltrazione di dati critici.

A supporto di queste operazioni, il framework **Mitre Att&ck** propone diverse tecniche, di seguito ne vengono elencate alcune:



Mitre Att&ck - The end

Un malintenzionato, a seguito dell'esfiltrazione dei dati, distruggerà tutte le prove (alle volte compresi i sistemi target), in modo da non essere rintracciato.

Un professionista di sicurezza informatica, a seguito dell'esfiltrazione dei dati, provvederà a redigere un report dettagliato con le azioni effettuate.

The dark side is cool…

But the bright side is way better!!

Choose carefully!


NODE 01
NODE 04
NODE 02
NODE 06
BLOCK 01
BLOCK 01
NODE 01
NODE 02

Grazie