Cyber Threat Intelligence e Threat Hunting nel settore dell'energia

CSP006_S_E

PRESENTAZIONE DA PARTE DI:
DR. STEFAN SCHAUER
DR. ABDELKADER SHAABAN
AIT ISTITUTO AUSTRIACO DI TECNOLOGIA

Riconoscimento

- *Co-finanziato dall'Unione Europea. I punti di vista e le opinioni espresse sono tuttavia esclusivamente quelli dell'autore o degli autori e non riflettono necessariamente quelli dell'Unione Europea o di HADEA. Né l'Unione Europea né l'autorità che ha concesso il finanziamento possono essere ritenute responsabili.*
- *Accordo di progetto n. 101083594*

Cyber Threat Intelligence e Threat Hunting nel settore dell'energia

Panoramica

- Argomento-1: Introduzione all'intelligence delle minacce e alla caccia alle minacce
- Argomento-2: Fonti e raccolta dei dati
- Argomento 3: Attori e tattiche di minaccia
- Argomento 4: Modellazione pratica delle minacce e indagini sulla sicurezza

Ordine del giorno

o1. Perché la mia azienda dovrebbe essere un obiettivo di un cyber-attacco?

o2. Attori della minaccia

o3. Esercizio: Catena di morte informatica

Perché la mia azienda dovrebbe essere bersaglio di un attacco informatico?

Perché?

Perché la mia azienda dovrebbe essere bersaglio di un attacco informatico?

... perché i vostri dati sono preziosi

- Database di clienti, profili, dati di carte di credito
- Piani strategici, situazione finanziaria
- Dati di ricerca e sviluppo

... perché la perdita della vostra società è il guadagno di un altro

- Concorrenti, valore di mercato
- Organizzazioni politiche/terroristiche

... perché avete risorse informatiche che possono essere riutilizzati per

- distribuire contenuti illegali
- attaccare i sistemi a tre parti creando il impressione che sia stato tu
- vendere la larghezza di banda della propria connessione Internet per l'utilizzo di botnet (DDoS, cryptominer, ecc.).

... perché è facile e automatizzabile

- ad esempio ransomware, liste di spam, ...

La necessità di **controlli**

Sicurezza stradale

Controlli tecnici

- Controlli di sicurezza attivi
  - ABS, ASR, ESP, ecc.
- Controlli di sicurezza passivi
  - Airbag, cinture di sicurezza, seggiolini, specchietti retrovisori, ecc.

SICUREZZA DELLE INFORMAZIONI

Controlli tecnici

Controlli di sicurezza attivi

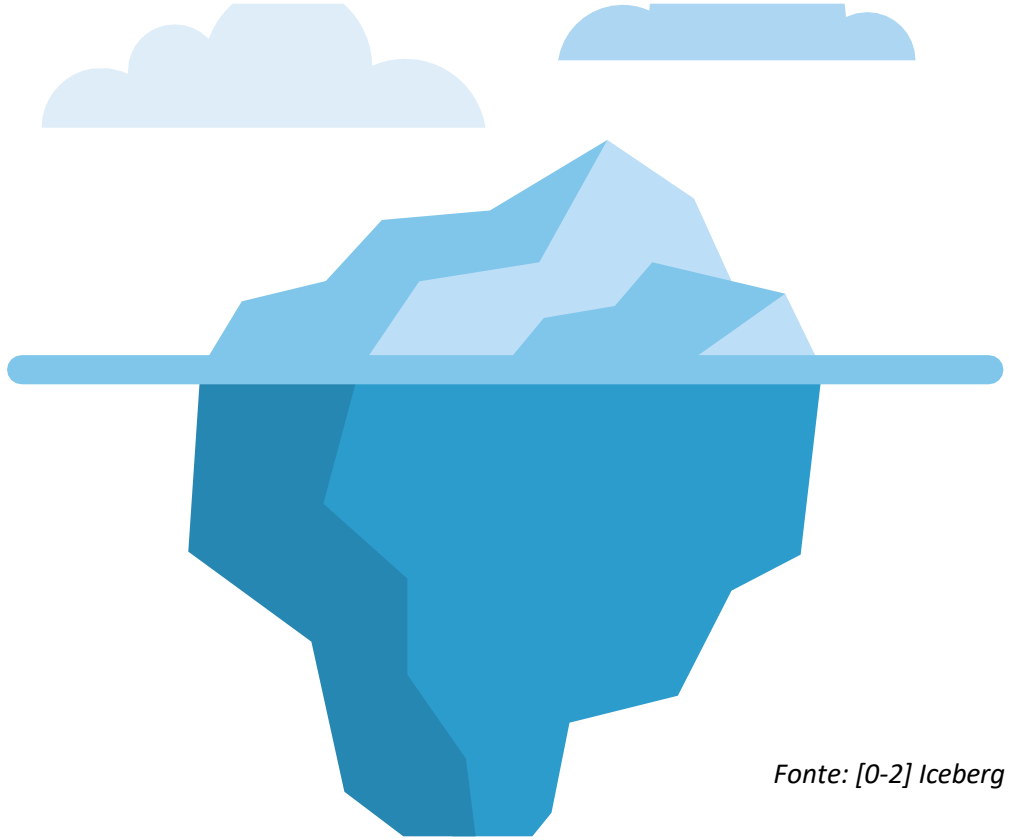
Sistemi di controllo degli accessi, firewall, antivirus, protezione antispam, IPS, ecc.

Controlli di sicurezza passivi

Sistemi di gestione dell'identità, controlli di sicurezza, file di log, ridondanza, IDS, ecc.

Accessibilità delle informazioni

- Web **chiaro**
  - Indicizzati dai motori di ricerca
- **Deep** Web
  - Non indicizzato dai motori di ricerca
- **Dark** Web/Net
  - Indirizzo .onion della rete TOR
  - Processo di invito/verifica



Fonte: [0-2] Iceberg

L'attuale **panorama della** sicurezza informatica

La visione centralizzata della protezione perimetrale è obsoleta

Rilevamento e risposta degli endpoint

Le perdite di dati, le intrusioni e le violazioni della privacy salgono alle stelle

La maggior parte delle intrusioni non viene rilevata tempestivamente.

Solo alcuni esempi quelli che conosciamo...

Prossima diapositiva Fonte:
[1] InformationIsBeautiful.net


Plan, Inc.
Gas & Electric
D&B, Altegrity
Evernote
Agency
Twitter
Ubuntu
"Apple"
Blizzard
California Department of Child Support Services
China Software Developer Network
Dropbox
Emory Healthcare
Formspring
Gamigo
Global Payments
Greek government
Last.fm
KT Corp.
LinkedIn, eHarmony, Last.fm
Militarysingles.com
Medicaid
Memorial Healthcare System
New York State Electric & Gas
Office of the Texas Attorney General
South Carolina Government
South Carolina State Dept. of Revenue
Three Iranian banks
Yahoo Voices
Zappos
Sega
Spartanburg Regional Healthcare System
Nexon Korea Corp
Oregon Department of Motor Vehicles
Sony Online Entertainment
Southern California Medical-Legal Consultants
Stratfor
Massachusetts Government
Nemours Foundation
NHS
Seacoast Radiology, PA
South Shore Hospital, Massachusetts
State of Texas
Sutter Medical Foundation
University of Wisconsin - Milwaukee
Washington Post
Writerspace.com
Yale University
Morgan Stanley Smith Barney
New York City Health & Hospitals Corp.
Restaurant Depot
San Francisco Public Utilities Commission
Sony PSN
Sony Pictures
Steam
Tricare
US Law Enforcement
2011
Ankle & foot Center of Tampa Bay, Inc.
Bethesda Game Studios
Accendo Insurance Co.
Betfair
Chinese gaming sites
Citigroup
Eisenhower Medical Center
Epsilon
Health Net - IBM
Honda Canada
2010
AT&T
Blue Cross Blue Shield of Tennessee
AvMed, Inc.
Classified Iraq War documents
Colorado government
Embassy Cables
Educational Credit Management Corp
Emergency Healthcare Physicians, Ltd.
Gawker.com
Lincoln Medical & Mental Health Center
Ohio State University
Puerto Rico Department of Health
Triple-S Salud, Inc.
US Federal Reserve Bank of Cleveland
US Military
2009
CheckFree Corporation
Health Net
Heartland 130,000,000
Network Solutions
RockYou!
University of California Berkeley
US Military
Virginia Dept. Of Health
US National Guard
Virginia Prescription Monitoring Program

Attori della minaccia

Attori delle minacce, attribuzione e offuscamento

Attori della minaccia:	Motivazione:
Stati-Nazione	Geopolitico Profitto
Criminali informatici	Ideologico
Hacktivisti Gruppi terroristici Cercatori di emozioni	Ideologico, compresa la violenza
	Soddisfazione
Minacce insider	Scontento Egotismo
Script Kiddies	

Attori di minaccia **dello Stato nazionale**

L'attore di minacce più capace grazie alle risorse disponibili

A seconda del contesto organizzativo - stima del caso peggiore per quanto riguarda le capacità e la motivazione della minaccia

Attualmente, i paesi che dispongono di maggiori risorse, capacità offensive e attivi impegni

- Stati Uniti d'America
- Russia
- Cina
- Corea del Nord

Attori di minaccia per la sicurezza informatica a livello nazionale 2019 - **Stati Uniti**

Stati Uniti d'America

- Come dimostrato negli ultimi anni da Edward Snowden e da varie altre fughe di notizie sulle capacità di minaccia informatica degli Stati Uniti, le risorse e le capacità degli Stati Uniti sono enormi.
- Lo ha dimostrato di recente 'attacco informatico degli Stati Uniti alle infrastrutture estere che ha fatto seguito agli attacchi alle petroliere statunitensi.

Gli attori della minaccia alla sicurezza informatica degli Stati nazionali nel 2019 - **Russia**

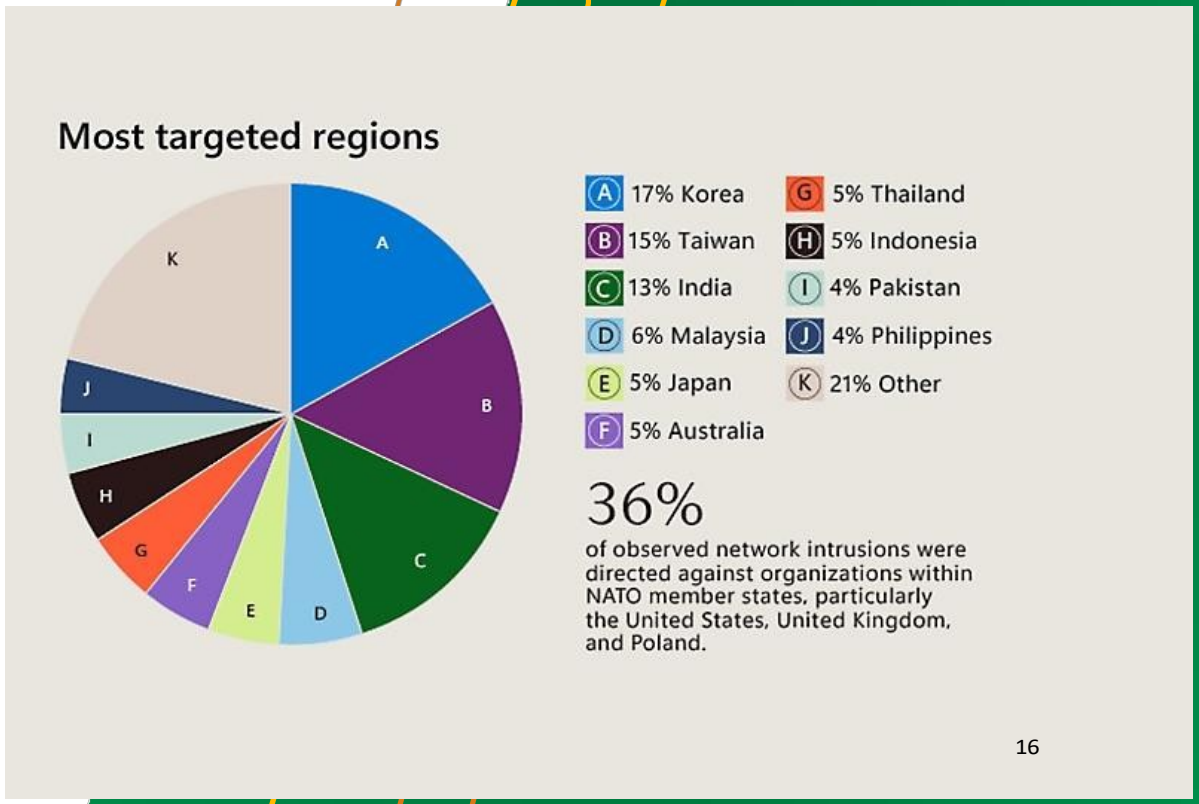
Russia

- La Russia utilizza il cyberspazio come uno dei tanti metodi per ottenere il know-how e la tecnologia necessari per crescere e modernizzare la propria economia, soprattutto in
  - industria della difesa,
  - energia,
  - assistenza sanitaria e
  - settori tecnologici
- Altri esempi di rilievo sono l'attacco caber alla rete idrica ucraina e i test di guerra elettronica in Siria.

Gli attori della cybersicurezza degli Stati nazionali nel 2023 - **Russia**

Russia

- Gli attori delle minacce sponsorizzati dallo Stato russo hanno impiegato varie tattiche, tra cui campagne di phishing ed exploit zero-day.
- Il loro obiettivo era ottenere l'accesso iniziale ai dispositivi e alle reti delle industrie degli Stati membri della NATO.
- Inoltre, gli attori dell'influenza maligna hanno preso di mira la diaspora ucraina per intimidirla e incitare i movimenti di protesta in tutta Europa.



Minacce dello Stato nazionale (MDDR) Ch3| Microsoft Security Insider

Gli attori delle minacce alla sicurezza informatica degli Stati nazionali nel 2019 - **Cina**

Cina

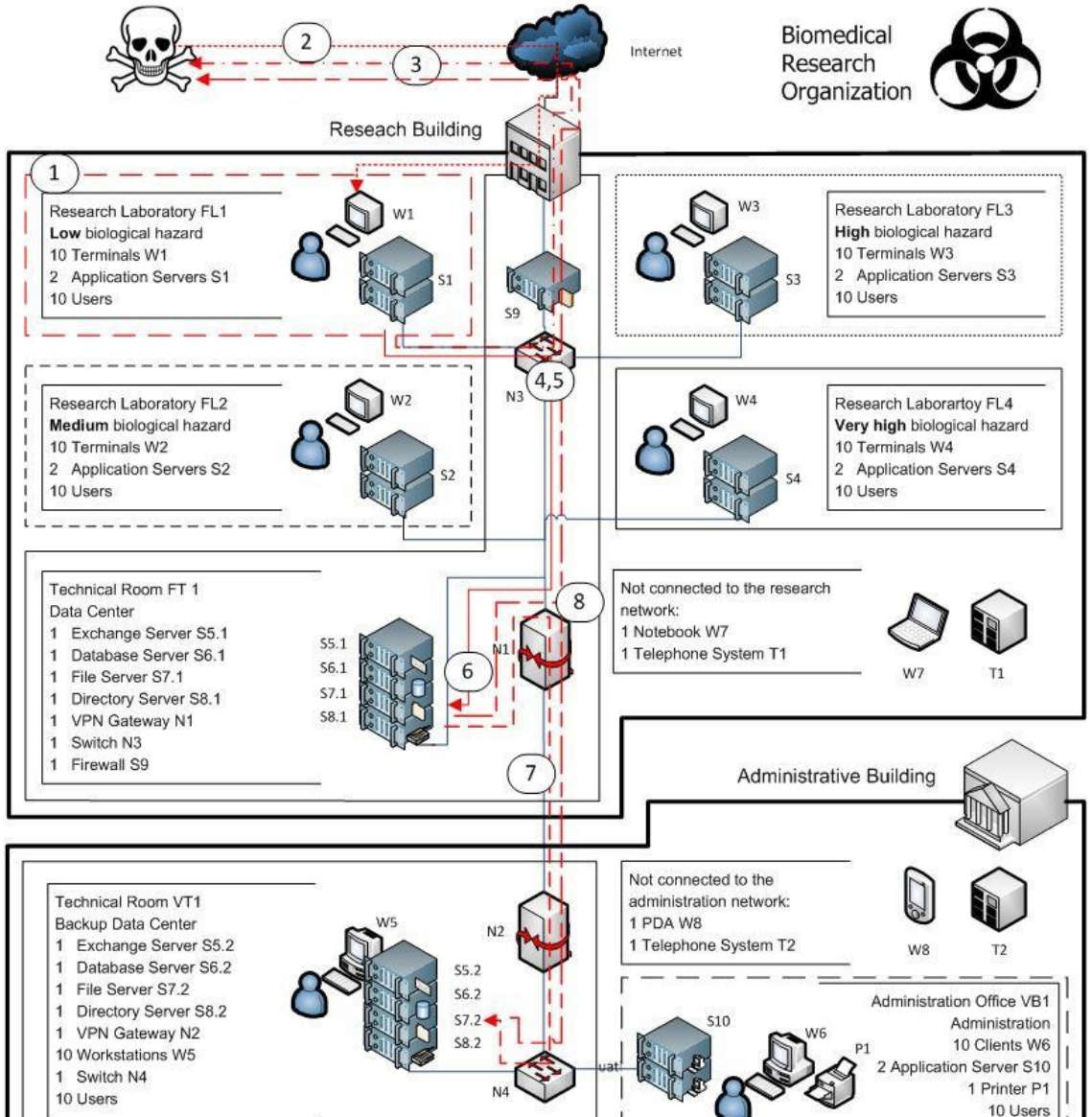
- La Cina continua a utilizzare lo spionaggio informatico per sostenere i suoi obiettivi di sviluppo strategico
  - il progresso della scienza e della tecnologia,
  - modernizzazione militare e
  - obiettivi di politica economica
- I ricercatori di cybersicurezza hanno anche recentemente trovato collegamenti tra i cyber-attori cinesi e una backdoor di una popolare applicazione (CCleaner) che ha permesso agli attori di prendere di mira aziende come Google, Microsoft, Intel e Vmware.
- APT1

Gli attori della cybersicurezza degli Stati nazionali nel 2019 - **Corea del Nord**

Corea del Nord

- Cyberattacco alla centrale idroelettrica e nucleare della Corea del Sud nel dicembre 2014
- Alla fine del 2016, gli hacker nordcoreani sono riusciti a ottenere l'accesso a una rete di computer militari *sicuri* della Corea del Sud.
  - I dati estratti includevano piani di emergenza per un attacco contro la leader del Nord in caso di guerra di confine
- Nel corso del 2019, un gran numero di attacchi alle criptovalute e di infezioni ransomware sono stati attribuiti agli hacker sponsorizzati dallo Stato nordcoreano.

Ciclo di vita tipico di un attacco



1: **Ricognizione iniziale** - ottenere informazioni sull'obiettivo 2: **Compromissione iniziale** - mail di spear phishing all'utente, l'exploit del client si connette al server C&C dell'avversario 3: **Stabilire un punto d'appoggio -** adattamento al sistema, installazione di backdoor standard

4: **Escalation dei privilegi** - nomi utente, combinazioni di password raccolte

5: **Recon interno** - autenticazione e rete

struttura raccolta

6: **Spostamento laterale**: l'avversario si infiltra nel centro dati locale e in quello di backup.

7: **Mantenere la presenza** - tutte le tracce sono coperte, l'avversario rimane in silenzio.

8: **Missione completata** - tutte le informazioni sull'obiettivo vengono raccolte, esportate tramite canali segreti, le tracce vengono cancellate.

Parole d'ordine delle minacce informatiche


Adware e dispositivo a ultrasuoni riconoscimento


Backdoor


Bot e reti bot


Iniezione di codice


Cripto mining


(D) Attacchi DoS e di amplificazione

Sfruttamenti drive-by / watering hole


Sfruttamenti e kit di offuscamento


Man-in-the-Middle Password


cracking


Farmaceutica


Phishing, Spoofing, Spear-Phishing, Whaling, Smishing


Ransomware


Rootkit Spyware


Dirottamento SSL


Tipi di piazza


Malware - Virus, worm, payload, trojan


Intercettazioni WiFi e hacking

Giorni Zero

Altre importanti attività **di R&S**

Falsi profondi

- immagine/video/voce
  - https://www.zdnet.com/article/forget-email- truffatori-usano-ceo-voce-falsi-per-confutare-i-lavoratori- into-wiring-cash/

Comandi della luce

- https://lightcommands.com/

Armamento dell'IA

- Capacità autonome dei droni
- Università di Berkley - Slaughterbots
  - https://www.youtube.com/watch?v=HipTO_7mUOw

Iniziativa DARPA per la rinascita dell'elettronica

- https://www.darpa.mil/work-with-us/electronics-resurgence-initiative

La politica tecnologica estera della Cina

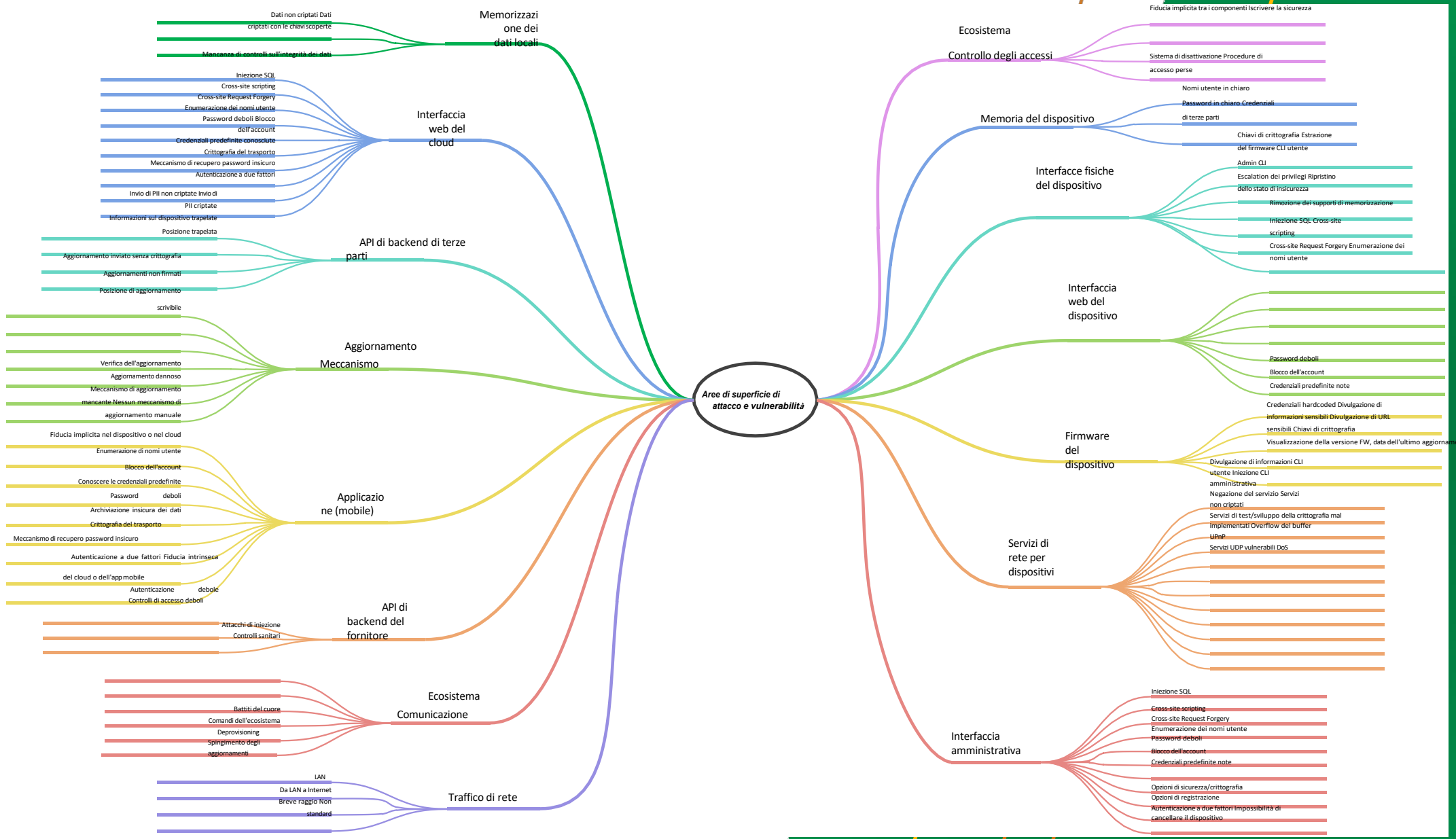
- https://www.cnbc.com/2019/12/09/china- reportedly-orders-state-offices-to-remove- foreign-tech.html

Requisiti dell'app MFA bancaria a causa degli incidenti di SIM-Swapping

- Direttiva UE sui servizi di pagamento

Primo atto ufficiale di guerra informatica (USA -> IRAN)

- https://www.bbc.com/news/world-us- canada-48735097


Aree di superficie di attacco e vulnerabilità
Memorizzazione dei dati locali
Dati non criptati Dati criptati con le chiavi scoperte
Mancanza di controlli sull'integrità dei dati
Interfaccia web del cloud
Iniezione SQL
Cross-site scripting
Cross-site Request Forgery
Enumerazione dei nomi utente
Password deboli Blocco dell'account
Credenziali predefinite conosciute
Crittografia del trasporto
Meccanismo di recupero password insicuro
Autenticazione a due fattori
Invio di PII non criptate Invio di PII criptate
Informazioni sul dispositivo trapelate
API di backend di terze parti
Posizione trapelata
Aggiornamento inviato senza crittografia
Aggiornamenti non firmati
Posizione di aggiornamento
Aggiornamento Meccanismo
scrivibile
Verifica dell'aggiornamento
Aggiornamento dannoso
Meccanismo di aggiornamento mancante Nessun meccanismo di aggiornamento manuale
Applicazione (mobile)
Fiducia implicita nel dispositivo o nel cloud
Enumerazione di nomi utente
Blocco dell'account
Conoscere le credenziali predefinite
Password deboli
Archiviazione insicura dei dati
Crittografia del trasporto
Meccanismo di recupero password insicuro
Autenticazione a due fattori Fiducia intrinseca del cloud o dell'app mobile
Autenticazione debole
Controlli di accesso deboli
API di backend del fornitore
Attacchi di iniezione
Controlli sanitari
Ecosistema Comunicazione
Battiti del cuore
Comandi dell'ecosistema
Deprovisioning
Spingimento degli aggiornamenti
Traffico di rete
LAN
Da LAN a Internet
Breve raggio Non standard
Ecosistema Controllo degli accessi
Fiducia implicita tra i componenti Iscrivere la sicurezza
Sistema di disattivazione Procedure di accesso perse
Memoria del dispositivo
Nomi utente in chiaro
Password in chiaro Credenziali di terze parti
Chiavi di crittografia Estrazione del firmware CLI utente
Interfacce fisiche del dispositivo
Admin CLI
Escalation dei privilegi Ripristino dello stato di insicurezza
Rimozione dei supporti di memorizzazione
Iniezione SQL Cross-site scripting
Cross-site Request Forgery Enumerazione dei nomi utente
Interfaccia web del dispositivo
Password deboli
Blocco dell'account
Credenziali predefinite note
Firmware del dispositivo
Credenziali hardcoded Divulgazione di informazioni sensibili Divulgazione di URL sensibili Chiavi di crittografia
Visualizzazione della versione FW, data dell'ultimo aggiornamento
Divulgazione di informazioni CLI utente Iniezione CLI amministrativa
Servizi di rete per dispositivi
Negazione del servizio Servizi non criptati
Servizi di test/sviluppo della crittografia mal implementati Overflow del buffer
UPnP
Servizi UDP vulnerabili DoS
Interfaccia amministrativa
Iniezione SQL
Cross-site scripting
Cross-site Request Forgery
Enumerazione dei nomi utente
Password deboli
Blocco dell'account
Credenziali predefinite note
Opzioni di sicurezza/crittografia
Opzioni di registrazione
Autenticazione a due fattori Impossibilità di cancellare il dispositivo

La **matrice** MITRE **ATT&CK** per le imprese

MITRE | ATT&CK

Matrices | Tactics | Techniques | Mitigations | Groups | Software | Resources | Blog | Contribute | Search site

MATRICES

- PRE-ATT&CK
- Enterprise
  - All Platforms
  - Windows
  - macOS
  - Linux
  - Cloud
- Mobile

Home > Matrices > Enterprise

Launch the ATT&CK™ Navigator

Enterprise Matrix

Below are the tactics and technique representing the MITRE ATT&CK Matrix™ for Enterprise. The Matrix contains information for the following platforms: Windows, macOS, Linux, AWS, GCP, Azure, Azure AD, Office 365, SaaS.

Last Modified: 2019-10-09 18:48:31.906000

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Application Access Token	Bash History	Application Window Discovery	Application Access Token	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Application Deployment Software	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	BITS Jobs	Cloud Instance Metadata API	Cloud Service Dashboard	Component Object Model and Distributed COM	Data from Cloud Storage Object	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Bypass User Account Control	Credential Dumping	Cloud Service Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	Clear Command History	Credentials from Web Browsers	Domain Trust Discovery	Internal Spearphishing	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe

Fonte: [2] attack.mitre.org

Esercizio: Catena di morte informatica

Esercizio: Catena di morte informatica

- Tutti modellano uno scenario di attacco fittizio (cyber kill chain) basato sulle fasi del ciclo di vita dell'attacco della matrice MITRE Att&ck
  - leggete e scegliete le vostre tattiche preferite e
  - creare una breve presentazione in PowerPoint di uno scenario di attacco (plausibile) - descrivere
    - un'azienda fittizia e ciò che fa
    - il tipo di informazioni sotto attacco / la motivazione dell'attaccante,
    - come hanno coperto tutte o la maggior parte delle fasi del ciclo di vita (accesso iniziale, esecuzione, ecc.)

Modelli di intrusione - in generale

Inoltre, una base di conoscenze dettagliate su metodi di attacco, tattiche, tecniche e difese.

- Tattica
  - https://attack.mitre.org/tactics
- Matrice di attacco
  - https://attack.mitre.org/matrices
- Strategie di mitigazione
  - https://attack.mitre.org/mitigations

Connettersi con CyberSecPro: come registrarsi e altre informazioni pratiche

1. Sito web: _www.cybersecpro-project.eu
2. X (Twitter): https://twitter.com/CyberSecPro_eu
3. LinkedIn: https://www.linkedin.com/company/cybersecpro-euproject/

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.

Project Agreement no. 101083594

Grazie

Si prega di inviare tutte le domande a:
Stefan SchauerStefan.Schauer@ait.ac.at
Abdelkader Shaaban,
abdelkader.Shaaban@ait.ac.at