A Honeypot Framework for the Internet of Things

Marco Lucchese and Massimo Merro
Department of Computer Science
University of Verona
A brief history of the Internet of Things

1990
The world’s first Internet-connected toaster

1999
The term Internet of Things was invented by Kevin Ashton

2000
Samsung fridge is the first commercial IoT device. With a whopping price of 20000 USD

2004
Tabloids start mentioning IoT

2016
Mirai infects 600k IoT devices

2020
More than 20 billion of IoT devices
Vulnerabilities of IoT

Kaspersky honeypots find 105 million attacks on IoT devices in first half of 2019

Hacking risk leads to recall of 500,000 pacemakers due to patient death fears

A Hacker Forced 50,000 Printers To Spread PewDiePie Propaganda -- And The Problem Is Much Bigger Than You Know
What is a honeypot?

- VIRTUAL / HARDWARE
- VULNERABLE
- ALLURING
- SAFE
What are honeypots useful for?

- Malware analysis to collect signatures
- Malware analysis to discover zero-days
- Targeted attacks recognition
- Intrusion detection
Honeypots for IoT

- **IoTPOT** > Honeypot that emulates interactions of the Telnet protocol and a variety of IoT devices.

- **IoTCandyJar** > Honeypot that uses machine learning technology to automatically learn behavioural knowledge of IoT devices.

- **SIPHON** > Honeypot that uses physical IoT devices connected to various geographical locations through so-called wormholes.
MieleJar: A framework for IoT honeypots
<table>
<thead>
<tr>
<th>Path</th>
<th>IP</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>GET /setup/bluetooth/status</td>
<td>157.47.21.28</td>
<td>Oct 8, 2020</td>
</tr>
<tr>
<td>GET /setup/scan_results</td>
<td>1557.27.34.156</td>
<td>Oct 8, 2020</td>
</tr>
</tbody>
</table>
Statistics

Google Home (Id. 3)

Attacks

Locations

- 0
- 1 - 10
- 10 - 20
- 20 - 40
- 40 - 75
- > 75

21 Sept 26 Sept 1 Oct 6 Oct
<table>
<thead>
<tr>
<th>File name</th>
<th>Flag</th>
<th>Size</th>
<th>Capture date</th>
</tr>
</thead>
<tbody>
<tr>
<td>325044.bin</td>
<td>Off</td>
<td>147 KB</td>
<td>Oct 8, 2020</td>
</tr>
<tr>
<td>446436.bin</td>
<td>Off</td>
<td>96 KB</td>
<td>Oct 8, 2020</td>
</tr>
</tbody>
</table>
Business logic: Installation protocol

```
curl 0.0.0.60/new_token -d "" -H 'Content-Type: application/json' -u admin:secret

(token)

curl localhost:80/new_honeypot -d '{"token": "a", "lon": "10.784608", "lat": "44.092424", "name": "google"} -H 'Content-Type: application/json' -u admin:secret

{PUB KEY:cyJpZG16im51bWVybyI6InRleHQiOiJwYXlsb2FkIn0=}
```
Business logic: Log protocol

curl 0.0.0.80/new_log -d '{"a": "eyJpZCI6Im51bWVybyIsInRlçHQiOiJwYXIsb2FkIn0="}’ -H "Content-Type: application/json" -u admin secret
Captured Malwares

- **MIRAI** malware for generic IoT devices. Used for botnets
- **HAJIME** variant of Mirai, built on a peer-to-peer network. Used for botnets
- **GAFGYT** malware for BusyBox devices, it connects back to a server. Used for botnets
Attacks in 6 months
Bibliography


• J. D. Guarnizo, A. Tambe, S. S. Bhunia, M. Ochoa, N. O. Tippenhauer, A. Shabtai, Y. Elovici: *SIPHON: Towards Scalable High-Interaction Physical Honeypots* in CPSS@AsiaCCS(2) 2017: 57-68


• B. Lingenfelter, I. Vakilinia, S. Sengupta: *Analyzing Variation Among IoT Botnets Using Medium Interaction Honeypots* in CCWC 2020: 761-767


Mirai: the botnet that disrupted Internet

1. Brute force
2. Report
3. Check status
4. Infect command
5. Malicious binary
6. Attack command
7. Attack