# Digital Ghost Ships: Abandoned Internet-enabled Devices

Ricardo Yaben and Emmanouil Vasilomanolakis
Section for Cybersecurity Engineering
Department of Applied Mathematics and Computer Science

## INTRODUCTION

- Internet-enabled devices have underlined a critical issue: *the lack of security management*. Abandoning or neglecting the device's security invites attackers to take control.
- We coin the term Digital Ghost Ships (DGSs) to group these devices under a single term.

## CHARACTERIZING DIGITAL GHOST SHIPS

### Technical Characteristics

Internet-enabled:

- Can connect to other devices and networks with Internet access, including wireless.
- Exposed to attacks from the Internet, within wireless range, and pivot attacks.

Abandoned:

- Lack regular security maintenance (e.g. misconfigured or outdated).
- Attackers exploit DGSs using simplistic methods (e.g., brute-force and known vulnerabilities).

### Sociological aspects for Digital Ghost Ships

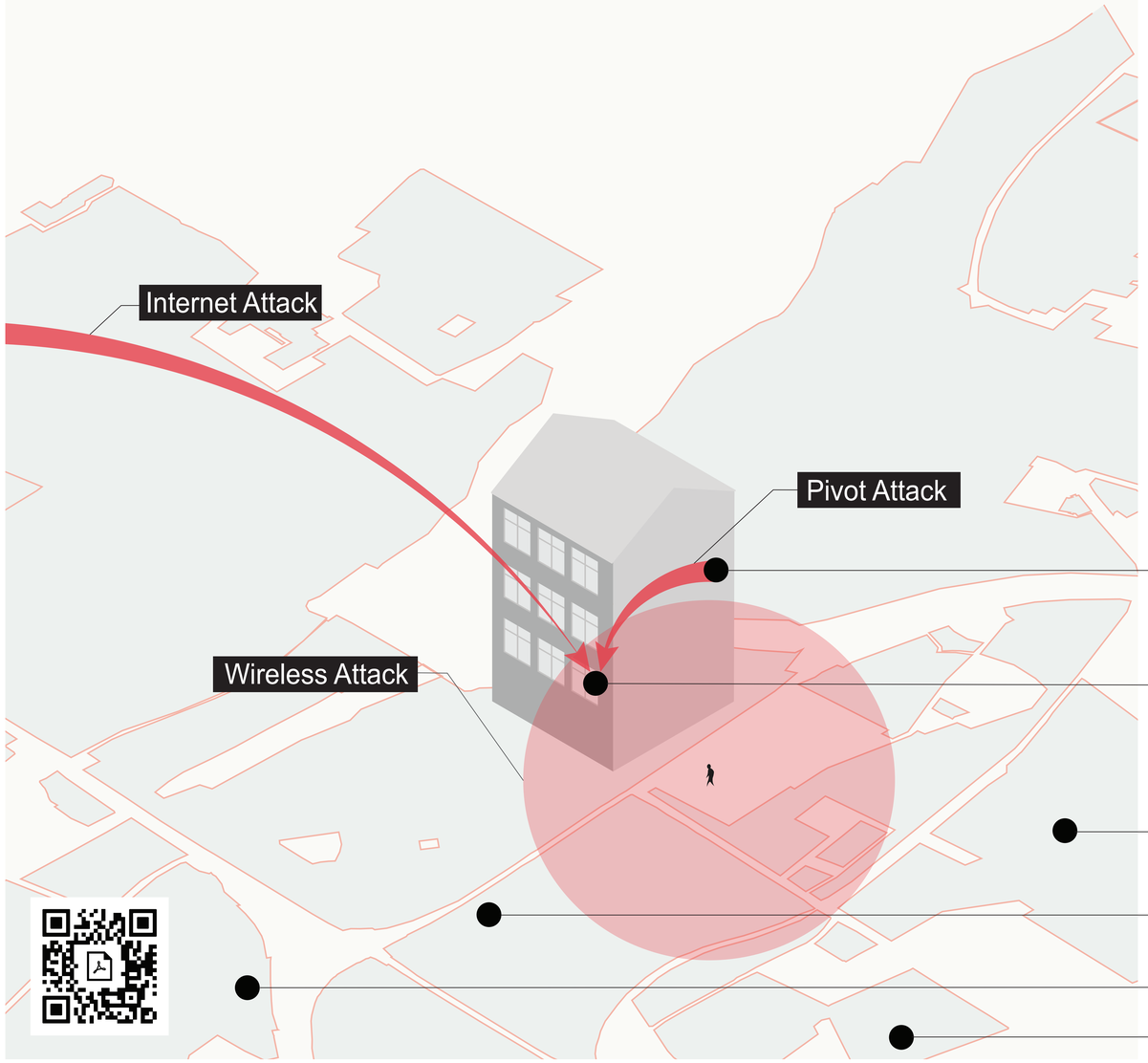
Manufacturer:

- Default configurations are predictable (e.g., hardcoded passwords).
- The vulnerability management process depends on their secuirty attitude.
- Lack of support for retired devices.

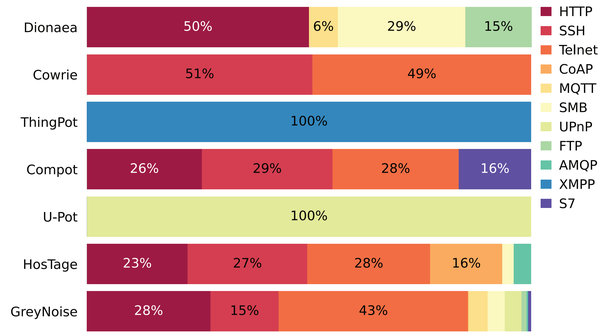
Consumer:

- Continue to overlook cyber-security.
- Entrust their security decisions to external sources (e.g., online tutorials).
- Cultural factors influence their perception of risk (e.g., overconfidence).
- Attackers exploit DGSs using simplistic methods (e.g., brute-force and known vulnerabilities).

# The Internet is flooded with vulnerable devices that suffer from lack of security management.




Attackers target devices that expose services prone to contain known vulnerabilities, such as missing authentication or being misconfigured.




**Distribution of attacks on potential DGS; data collected from GreyNoise (90 days) and from [1] using 6 honeypots**

## STEPS AHEAD

- Scanning the Internet with custom probes aimed at DGSs.
- Fingerprinting devices using unsupervised machine-learning methods.
- Identifying DGSs through anomaly detection.

## REFERENCES

[1] Shreyas Srinivasa, Jens Myrup Pedersen, and Emmanouil Vasilomanolakis. 2021. Open for Hire: Attack Trends and Misconfiguration Pitfalls of IoT Devices. In Proceedings of the 21st ACM Internet Measurement Conference (Virtual Event) (IMC '21). Association for Computing Machinery, New York, NY, USA, 195–215. https://doi.org/10.1145/3487552.3487833

## POOL OF DIGITAL GHOST SHIPS