Detection of critical infrastructure devices on the public Internet

Martin Mladenov m.mladenov@student.tudelft.nl Georgios Smaragdakis (TU Delft) László Erdődi (NTNU)

TU Delft

Motivation

- *Industrial Control Systems* (ICS) and *Supervisory Control and Data Acquisition* (SCADA) systems are often used in **critical infrastructure**, such as the **power grid** [1].
- They are usually **small industrial computers**, which control crucial processes.
- **Cyber attacks** against such devices are common and a successful attack can potentially have a **devastating outcome** [2].
- Researchers have analysed the state of the Internet in the past [3]. However, existing research has not considered the existence of **honeypots**, which mimic real SCADA devices in order to detect intrusion attempts [4].

Contributions

- **Find** ICS/SCADA devices on the public Internet.
- Classify hosts as real or as **honeypots** that mimic real ones.
- Evaluate whether hosts could be part of **critical infrastructure**.
- Observe what **metadata** can be collected from devices.

Methodology and tools

- The **Censys** Universal Internet Dataset is a platform which constantly monitors the public Internet in order to detect what hosts have which ports open and for which service. [8]
- **Honeypot** classification is done using other data related to the host, such as the total **number of open ports** on the host, the **reverse *Domain Name System* (DNS) record** of the IP address of the host, and the ***Autonomous System* (AS)** of the host's network.

Key results and takeaways

- An **unexpectedly large part** of all exposed ICS/SCADA devices are honeypots.
- Previous large-scale Internet studies may have **overestimated the number of exposed devices by up to 45%** by failing to classify and exclude honeypots.
- We made multiple **vulnerability reports** about exposed ICS devices, including to one of the largest Norwegian **power grid companies**. As a result of our reports, devices were taken offline.
- Many honeypots use a **default configuration**, making them trivial to detect.
- There are significant **correlations** between independent honeypot-related indicators.
- Network information is largely **sufficient** to classify hosts as honeypots or as real.

Figure 1: Siemens SIMATIC S7-1500 6ES7517-3AP00-0AB0. [5]

Figure 2: Russian hackers targeting Western critical infrastructure, UK says. *Reuters*. [6]

Figure 3: Hacker could sabotage tens of thousands of solar panels. *RTL Nieuws*. [7]

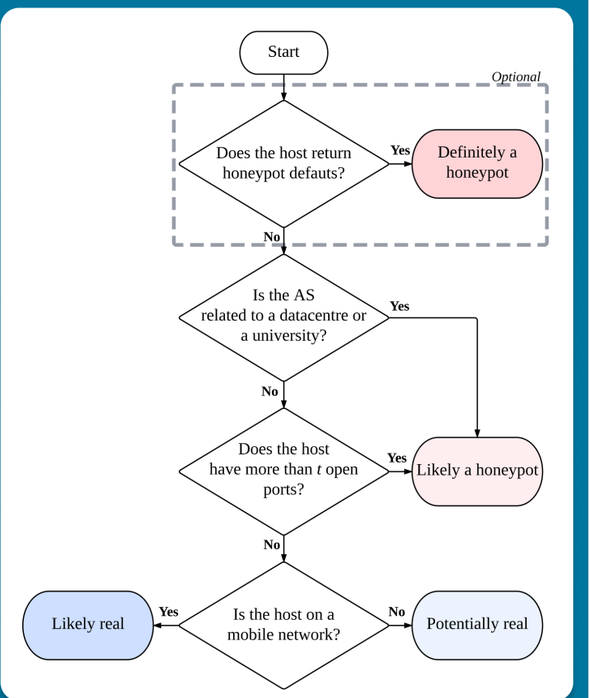

Figure 7: Our honeypot classification algorithm.

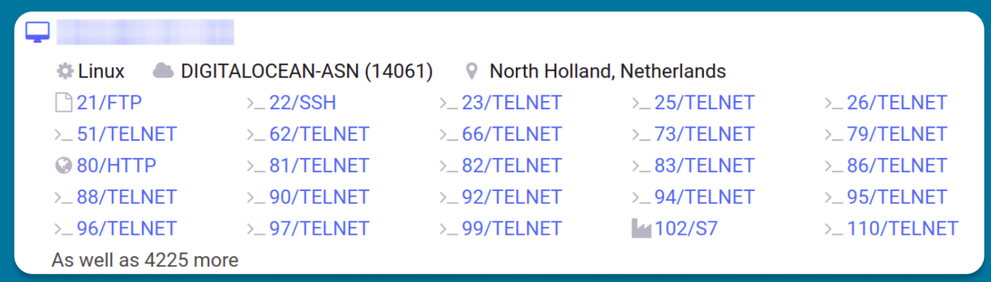

Figure 4: Port scan results of a highly probable honeypot. [8]

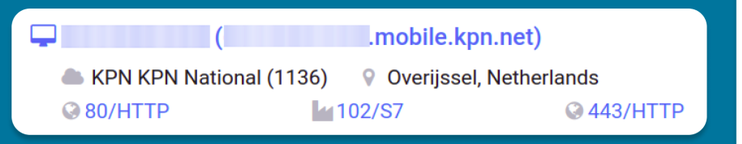

Figure 5: Port scan results of a highly probable real device. [8]

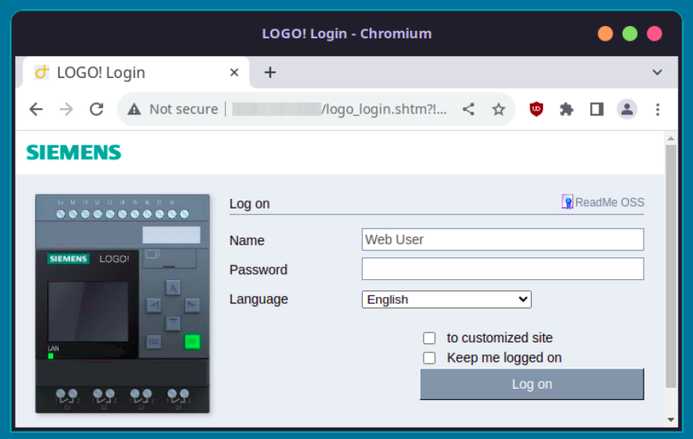

Figure 6: Web interface of an exposed Siemens ICS device.

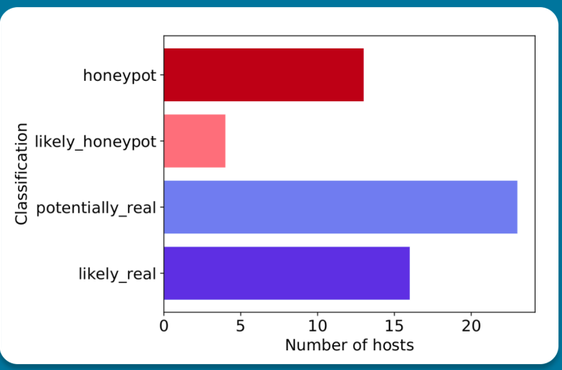

Figure 8: Classification labels of Dutch hosts running the S7 Communication protocol.

References

[1] K. Stouffer, S. Lightman, V. Pillitteri, M. Abrams, and A. Hahn, "Guide to Industrial Control Systems (ICS) Security," NIST special publication, vol. 800, no. 82, pp. 16–16, 2011.
[2] J. M. Ceron, J. J. Chromik, J. Santanna, and A. Pras, "Online discoverability and vulnerabilities of ICS/SCADA devices in the Netherlands," arXiv preprint arXiv:2011.02019, 2020.
[3] General Intelligence and Security Service of the Netherlands. Internationale dreigingen — aivd.nl. https://www.aivd.nl/onderwerpen/jaarverslagen/jaarverslag-2022/internationale-dreigingen, 2022.
[4] A. Jicha, M. Patton, and H. Chen. SCADA honeypots: An in-depth analysis of Conpot. IEEE Xplore, 2016.
[5] Siemens. CPU 1517-3 PN/DP - siemens.com. https://mall.industry.siemens.com/mall/nl/nl/Catalog/Product/6ES7517-3AP00-0AB0. [Accessed 16-May-2023].
[6] J. Pearson, "Russian hackers targeting Western critical infrastructure, UK says," *Reuters*, 18-Apr-2023. https://www.reuters.com/world/europe/russian-hackers-targeting-western-critical-infrastructure-uk-says-2023-04-18/
[7] S. Hulsen, "Hacker kon tienduizenden zonnepanelen saboteren door rondslingerend wachtwoord," *RTL Nieuws*, 24-Jul-2022. https://www.rtlnieuws.nl/tech/artikel/5322854/hacker-kon-tienduizenden-zonnepanelen-saboteren-door-rondslingerend-wachtwoord
[8] Zakir Durumeric, David Adrian, Ariana Mirian, Michael Bailey, and J. Alex Halderman. A search engine backed by Internet-wide scanning. In *22nd ACM Conference on Computer and Communications Security*, October 2015.