Medium-Interactivity Operational Technology Honeypots for Threat Intelligence

Jacob Williams[1]

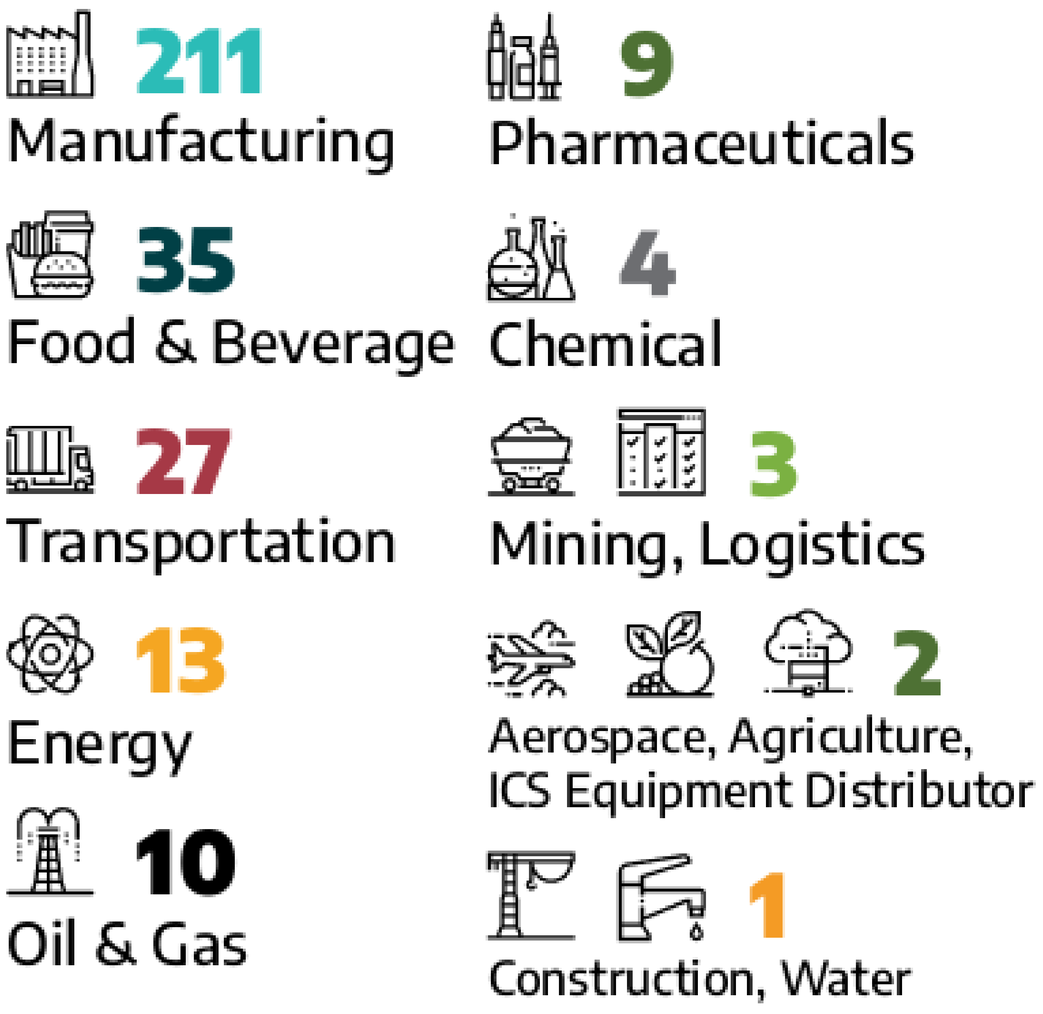
[1]Bristol Cyber Security Group, University of Bristol, UK

University of BRISTOL
Bristol Cyber Security Group

The Problem

Attacks on operational technology systems have only increased in recent years. Both directed at level one systems with uniquely crafted malware payloads and level three systems with the rise of ransomware-as-a-service models.

In 2021, Dragos recorded over 300 cases of ransomware attacks in level three systems, as well as new exploitation tool kits including level 1 payloads [2], and Claroty documented 637 industrial control system vulnerabilities across 76 vendors, 70% of which are classified as high or critical [1].



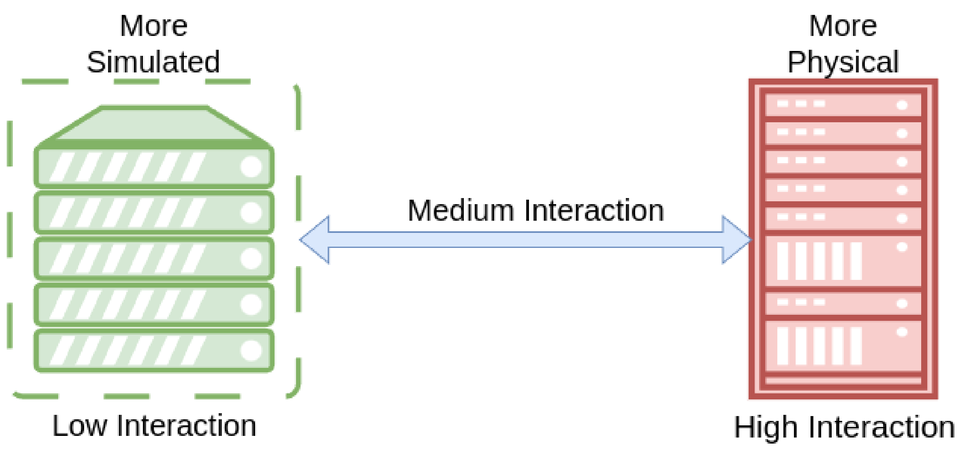
2021 Ransomware Observed By Sector

Honeypots

Traditionally used as a network security method, honeypots have been repurposed for gathering threat intelligence across different environments. However, the concept of operational technology honeypots has been relatively unexplored, which can leave operational technology oriented threat intelligence acting in response rather than being proactive.

OT honeypots are typically implemented as Low-Interactivity(LI), being mostly virtual, or as High-Interactivity(HI), mostly physical. This has lead to a division where LI is under-implemented and not convincing, or where HI is unachievable due to high costs.

A possible solution to this is the middle ground, Medium Interactivity honeypots combining the use of hardware where virtualisation is difficult and unconvincing, virtualisation where hardware is expensive or inaccessible, and simulation where it is effective [5].



During the creation and deployment of the honeypots, it would be prudent to study why certain features may or may not be effective from both a social and a technical standpoint. Is there a certain level of implementation that is capable of deceiving attackers? What do they look for in order to discern a simulated device? Is there a certain level of skeptical attacker that is impossible to deceive?

Threat Intelligence

By running these medium interactivity honeypots exposed to the wider web, we can observe activity that takes place directed at it. Taking this activity and enriching it with other contextual data information gained from any tools or exploits utilised, we can create effective threat intelligence that can be used by network security engineers and security operations centre analysts [3, 4].

Badpackets, a simple yet effective threat intel feed.

We can further analyse this threat intelligence by considering it socio-technically, what was it about the honeypot that attracted the attacker? What avenue did they first explore? Can we gleam their objectives through their actions? Or is this attacker simply an automated service?

Conclusions

By exploring the creation of medium interactivity honeypots and finding the desirable balance of simulation and physicality, we can work towards creating more effective threat intelligence solutions that are accessible to academic and independent researchers.

To do so, we will also explore what makes honeypots effective and why. Interacting with the cyber security community in order to explore both the technical and social rationale behind the features implemented. Then looking at distributing our findings back into the community to contribute towards the improvement of security honeypots.

References

[1] *Claroty Biannual ICS Risk & Vulnerability Report: 1H 2021*. en. URL: https://security.claroty.com/1H-vulnerability-report-2021 (visited on 09/05/2022).

[2] Dragos. *2021 ICS/OT Cybersecurity Year in Review*. en. Tech. rep. 2022. URL: https://hub.dragos.com/report/2021-year-in-review (visited on 05/18/2022).

[3] Vector Guo Li et al. "Reading the Tea leaves: A Comparative Analysis of Threat Intelligence". en. In: 2019, pp. 851–867. ISBN: 978-1-939133-06-9. URL: https://www.usenix.org/conference/usenixsecurity19/presentation/li (visited on 06/13/2022).

[4] Daisuke Mashima, Yuan Li, and Binbin Chen. "Who's Scanning Our Smart Grid? Empirical Study on Honeypot Data". In: *2019 IEEE Global Communications Conference (GLOBECOM)*. ISSN: 2576-6813. Dec. 2019, pp. 1–6. DOI: 10.1109/GLOBECOM38437.2019.9013835.

[5] Georg Wicherski. *Medium Interaction Honeypots*. en. 2006. URL: https://www.semanticscholar.org/paper/Medium-Interaction-Honeypots-Wicherski/9d468fa983b844c76a07b1e3ea63d6f7a9cae294 (visited on 06/27/2022).