Poster: HoneyOrg: Towards Attracting Targeted ICS Attacks with Standalone Honeypots

Matthew Rodda[*], Chris Hicks[†], Vasilios Mavroudis[†]
[*]Defence Science and Technology Group [†]The Alan Turing Institute

***Abstract*—Honeypots are invaluable for analyzing adversary behavior and enhancing proactive cybersecurity measures. While IT honeypots are well-established, their methodologies often fail to translate to industrial control systems (ICSs), which face heightened threats due to their role in critical infrastructure. Despite this urgency, ICS honeypots remain scarce and struggle to capture advanced, targeted attacks effectively. To address this gap, we present *HoneyOrg*, a novel ICS honeypot that incorporates realistic IT and supervisory infrastructure to enhance authenticity. Designed to reflect the historically targeted nature of ICS attacks, HoneyOrg simulates a manufacturer within the defence supply chain, providing a credible and enticing attack surface aimed at attracting sophisticated adversaries.**

I. Introduction

Industrial control systems (ICSs) form the backbone of critical infrastructure, representing a small but vital subset of networked systems. Often, ICSs lack basic security measures, such as authentication and encryption, and instead rely upon the integrity of their surrounding IT infrastructure. This reliance, in addition to potentially devastating impact following compromise, makes ICSs attractive targets for adversaries.

To address these risks, researchers have developed ICS honeypots—sandboxed environments designed to mimic real systems and attract cyberattacks. Honeypots serve as valuable tools for collecting threat intelligence, enabling the development of attack signatures and mitigation strategies to strengthen defences. To maximize authenticity and engagement, recent efforts have introduced detailed simulations of ICS hardware, protocols, and physical processes [1], [2].

However, *standalone* ICS honeypots often fail to attract advanced attacks [1]–[4]. In contrast, honeypots deployed within actual ICS environments have successfully captured complex attacks, including zero-day exploits [5]. This disparity can be attributed to the highly targeted nature of ICS attacks, where adversaries often focus on analysing or disrupting specific organizations or field devices [6]. While standalone honeypots offer scalability, they typically lack the organisational context and surrounding infrastructure that lend credibility to their deception. In-situ honeypots, embedded within real operational networks, address these shortcomings but present significant challenges in scaling and widespread adoption. Deploying such systems requires substantial organisational approval, precise tailoring to the existing environment, and modifications to legacy infrastructure, which can risk disruption.

This paper explores how standalone ICS honeypots can be enhanced to better emulate authentic environments, aiming to bridge the gap between scalability and targeted attack capture.

II. Contributions & Approach

We propose *HoneyOrg*, the first ICS honeypot associated with a fictitious organisation. HoneyOrg is designed to bridge the gap between the scalability of standalone honeypots and the authenticity of in-situ deployments.

HoneyOrg Design. HoneyOrg, posing as a manufacturer within the Defence supply chain, creates a realistic facade by simulating organisational infrastructure. This includes a public webpage, email inbox, phone number, and an employee workforce with a social media presence. This setup facilitates open-source intelligence gathering by adversaries. Access to the honeypot is restricted through a Remote Access Portal, ostensibly supporting employee virtual private network (VPN) connections to the on-premises ICS, as shown in Figure 1.

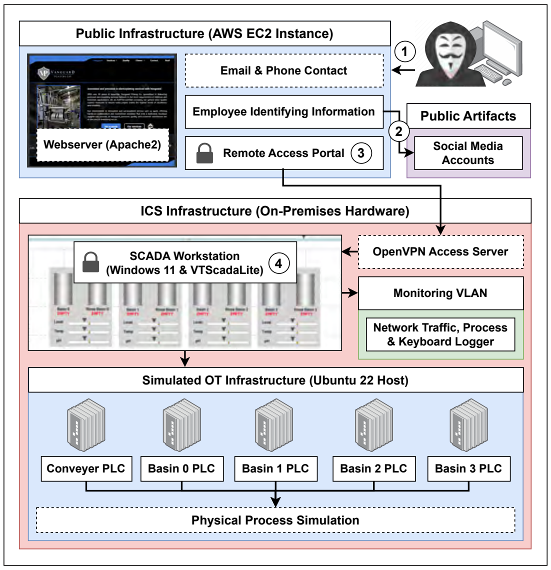

Public Infrastructure (AWS EC2 Instance)
Webserver (Apache2)
Email & Phone Contact
Employee Identifying Information
Remote Access Portal
1
2
3
Public Artifacts
Social Media Accounts
ICS Infrastructure (On-Premises Hardware)
SCADA Workstation (Windows 11 & VTScadaLite)
4
OpenVPN Access Server
Monitoring VLAN
Network Traffic, Process & Keyboard Logger
Simulated OT Infrastructure (Ubuntu 22 Host)
Conveyer PLC
Basin 0 PLC
Basin 1 PLC
Basin 2 PLC
Basin 3 PLC
Physical Process Simulation

Fig. 1. HoneyOrg architecture, illustrating the intended attack path. Dashed borders indicate local logging, and padlock icons denote authentication barriers.

Attack Simulation. Adversaries can exploit the Remote Access Portal by leveraging employee credentials obtained through an intentionally SQL-injectable webform, dictionary attacks using public employee information, or default credentials in an exposed `.env` file. Successful authentication provides a VPN profile, granting access to a SCADA workstation. From this point, attackers can stage further actions within a simulated ICS environment comprising five Modbuscompatible programmable logic controllers (PLCs), performing a commercial rack-electroplating process.

Addressing Key Limitations. HoneyOrg overcomes two significant shortcomings in existing standalone honeypots:

1) *Lack of Segmentation*: Many standalone honeypots expose ICS devices directly to the public, which contradicts established best-practices for network segmentation and may appear suspicious to experienced adversaries [7]. HoneyOrg addresses this by incorporating IT and supervisory infrastructure to mirror real-world network segmentation and access control.
2) *Absence of Organizational Context*: Existing honeypots often lack identifying information that could tie the device to an organization. This reduces attractiveness to actors typically attributed to ICS attacks, such as advanced persistent threat groups, known to target specific organizations [6]. By embedding the honeypot within a public business context, HoneyOrg increases its attractiveness to such actors.

III. Preliminary Results

We conducted a month-long pilot study in which the honeypot was made publicly accessible. During this period, the webpage received 58 395 requests from 3 434 unique IP addresses, with the majority of interactions consisting of directory enumeration and scanning for known vulnerabilities. While most of the traffic appeared automated, the server logs revealed 52 browser visits that loaded assets in ensemble, such as images and style sheets. This activity, although potentially automated, suggests manual inspection by adversaries.

Notably, no visitors arrived via Google or Bing search engines, implying that browser visits likely originated from adversaries rather than benign users. As shown in Figure 2, the highest ratio of browser visits to total requests occurred soon after the honeypot's initial discovery by automated web crawlers.

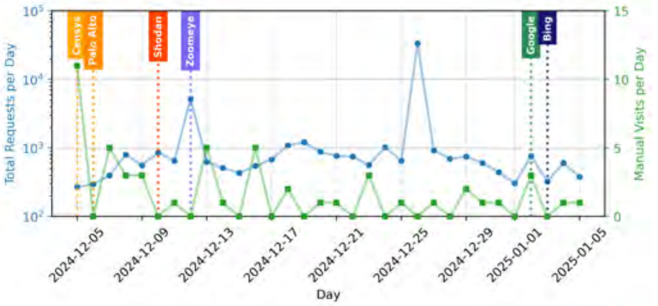


Fig. 2. Webpage requests and browser visits per day. Indexation dates by common search engines and web scrapers are annotated with dashed lines.

Following indexation by Shodan and Zoomeye, two widely used internet vulnerability scanners, the request volume increased significantly and became more exploitative. The webpage received numerous crafted requests targeting vulnerabilities in the deployed Apache2 version and persistent directory enumeration, including two thorough scans, shown in Figure 2.

Distinct patterns emerged between IP addresses performing malicious scanning and those accessing the webpage via a browser. The latter group exhibited reluctance to interact with inbuilt functionality, indicating that most attackers were opportunistic, aiming to exploit known vulnerabilities without deeper manual probing. Approximately one-quarter of the IP addresses revisited the webpage over multiple days, demonstrating some level of engagement following initial discovery. Despite this, no adversaries successfully authenticated themselves via the Remote Access Portal, and the ICS environment remained uncompromised during the study. These findings suggest that while the honeypot attracted significant reconnaissance activity, additional mechanisms may be needed to entice more advanced adversaries to fully engage.

IV. Conclusion and Future Work

In this work, we introduced HoneyOrg, a novel ICS honeypot designed to attract targeted attacks by incorporating realistic organisational infrastructure. Through the pilot study, HoneyOrg demonstrated its potential to engage adversaries and provide insights into reconnaissance and initial access techniques. However, no adversaries successfully completed the authentication process required to access the ICS environment during the study, suggesting that standalone honeypots require further enhancements to capture advanced ICS attacks.

Future work will focus on improving the attractiveness and authenticity of the honeypot to better engage sophisticated adversaries. This includes extending deployment and introducing scannable methods for initial access to the OT environment, such as deliberate vulnerabilities, to increase the likelihood of interaction. Additionally, hosting the honeypot with a local Internet Service Provider, rather than a cloud provider, will align the infrastructure with the honeypot's facade and improve appeal to adversaries targeting specific geographic locations.

Finally, we will enhance the credibility of the honeypot's organisational guise by employing repurposed domains, consistent SSL certificates, and realistic WHOIS records. These improvements aim to increase attacker trust and facilitate more targeted and sophisticated engagements, enabling deeper insights into adversarial methodologies in ICS environments.

References

[1] M. Conti, F. Trolese, and F. Turrin, "ICSpot: A high-interaction honeypot for industrial control systems," in *2022 International Symposium on Networks, Computers and Communications (ISNCC)*. IEEE, 2022.

[2] E. López-Morales, C. Rubio-Medrano, A. Doupé, Y. Shoshitaishvili, R. Wang, T. Bao, and G.-J. Ahn, "HoneyPLC: A next-generation honeypot for industrial control systems," in *ACM SIGSAC CCS*, 2020.

[3] S. M. Wade, "SCADA honeynets: The attractiveness of honeypots as critical infrastructure security tools for the detection and analysis of advanced threats," Ph.D. dissertation, Iowa State University, 2011.

[4] S. Srinivasa, J. M. Pedersen, and E. Vasilomanolakis, "RIoTPot: a modular hybrid-interaction IoT/OT honeypot," in *26th European Symposium on Research in Computer Security (ESORICS)*, 2021.

[5] M. Dodson, A. R. Beresford, and M. Vingaard, "Using global honeypot networks to detect targeted ICS attacks," in *2020 12th International Conference on Cyber Conflict (CyCon)*, vol. 1300, 2020.

[6] M. Graham, C. Ahlers, and K. O'Meara, "Impact of FrostyGoop ICS Malware on Connected OT Systems," Dragos Inc., Tech. Rep., July 2024.

[7] T. Williams, "The purdue enterprise reference architecture," *IFAC Proceedings Volumes*, vol. 26, no. 2, p. 559–564, Jul. 1993.

HoneyOrg: Towards Attracting Targeted ICS Attacks with Standalone Honeypots

Matthew Rodda[1], Vasilios Mavroudis[2], Chris Hicks[2]

[1]Defence Science and Technology Group, [2]The Alan Turing Institute

Introduction and Research Gaps

- Industrial control systems are attractive targets for cyberattack due to tie to critical infrastructure and lack of intrinsic security.
- Researchers deploy ICS honeypots to gather intelligence about such attackers, enabling the development of mitigations.
- Standalone honeypots often fail to capture advanced ICS attacks, despite implementing high-interaction simulations.
- **In situ ICS honeypots attract novel attacks, but require organizational approval and risk disrupting production.**

How can experienced attackers be attracted to compromise standalone ICS honeypots?

Limitations of Existing Standalone ICS Honeypots

1. Technical Realism in Deployment:

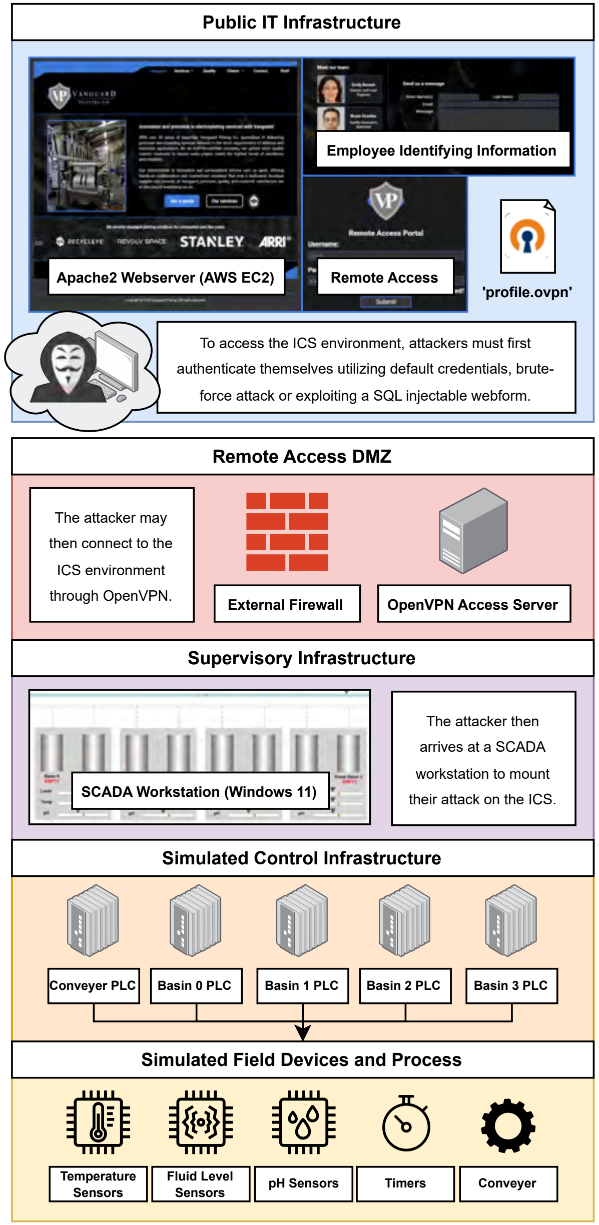
An attractive honeypot must appear authentic to attackers. While previous works have made ICS honeypots highly available through standalone deployment, this opposes recommended practices for network segmentation and would appear suspicious to potential adversaries.

2. Attracting Sophisticated Attackers:

ICS attacks are historically targeted in nature, with threat actors compromising specific organizations or field devices to incur a physical effect (such as Stuxnet, Triton and FrostyGoop). Existing ICS honeypots lack identifying information tying them to an organization, disallowing targeting by APT groups.

HoneyOrg Contributions

1. **Organizational Guise:** Propose the first ICS honeypot tied to a fake organization, increasing authenticity and enabling targeted attacks.
2. **Segmented ICS Environment:** Implemented private ICS environment with SCADA workstation networked to simulated PLCs & sensors.
3. **Realistic Attack Path:** Implemented VPN access to the ICS environment, provided a realistic attack path to deceive adversaries.
4. **Associated Online Presence:** Included a compelling public presence, including an employee workforce, email inbox and phone number.



To access the ICS environment, attackers must first authenticate themselves utilizing default credentials, brute-force attack or exploiting a SQL injectable webform.

The attacker may then connect to the ICS environment through OpenVPN.

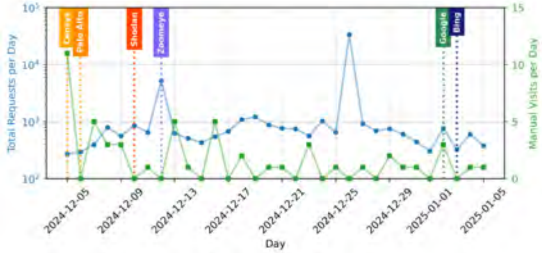
The attacker then arrives at a SCADA workstation to mount their attack on the ICS.

Visit the Honeypot

https://vanguard-plating.co.uk

Preliminary Results

As part of a pilot-study, the honeypot was deployed publicly for one month. During this time, the honeypot received 58,395 requests from 3,434 unique IP addresses, primarily performing directory enumeration and scanning. Following indexation by Shodan and Zoomeye, the request volume surged with more exploitative and targeted activities, including attempts to exploit Apache2 remote-code execution vulnerabilities.



Total requests and manual visits per day throughout honeypot deployment.

The webpage attracted 52 browser visits, suggesting possible manual probing by adversaries as they did not originate from benign search engines. Despite 22 visitors to the Remote Access Portal, no successful authentications occurred. As such the ICS environment was not compromised.

Future Work

- Reduce interaction required for initial access.
- Implement internet-facing services using vulnerable versions.
- Respond to common scanning tools to engage attackers.
- Host with local ISP, utilizing a repurposed domain name.
- Deploy honeypots long-term, allowing time for targeting.

Australian Government
Department of Defence

The Alan Turing Institute