**Threat Hunting Report**

# Incident Snapshot – Solvi Systems

Laura Salguero[a]

[a]*Simulated Enterprise Environment*

Compiled on February 19, 2026

**Abstract—**Solvi Systems, a key software provider for South Africa's energy sector, was the target of a coordinated cyberattack involving reconnaissance, phishing, malware deployment, lateral movement, data theft, and attempted privilege escalation. The incident began with suspicious web traffic and multiple failed XSS attempts against the company's public website. The attacker used several IP addresses and performed extensive reconnaissance before launching the intrusion.

Phishing emails impersonating energy-industry news outlets were sent to multiple Solvi employees, containing malicious links to weaponized .docx files hosted on fake news domains. One employee, Carla Wharton, clicked a link leading to the execution of ecobug.exe, a malware sample that established persistent outbound connections to an attacker-controlled IP. The malware spread to 38 distinct employee machines, generating hundreds of connection attempts.

The adversary attempted to create a new local administrator account and executed discovery commands on compromised hosts. On Alexei Petrov's machine, the attacker accessed internal network shares, copied sensitive software development documents, compressed them, and exfiltrated the data to an external server via HTTPS. The threat actor also accessed internal development portals and sent social-engineering emails seeking additional documentation. The campaign shows a clear interest in Solvi's software lifecycle, likely aiming to understand or manipulate the DOCKS ICS software used across the region's power infrastructure.

## EXECUTIVE SUMMARY

### Incident Overview

**Trigger:** WAF alert detecting XSS attempt + anomalous browsing patterns.
**Impact:** Malware execution, lateral movement, data exfiltration.
**Scope:** 38 hosts communicating with C2 + 2 compromised users.
**Severity:** Critical.

## ATTACK FLOW

### Attack Phases Identified

Reconnaissance
↓
Initial Access (phishing + malicious DOCX)
↓
Execution (ecobug.exe)
↓
Persistence (daily C2 connections)
↓
Privilege Escalation (creation of gu@rd!an)
↓
Discovery (net use, internal portal access)
↓
Lateral Movement (to Alexei's machine)
↓
Collection (copying software lifecycle docs)
↓
Exfiltration (curl upload to attacker domain)

## MITRE ATT&CK MAPPING

| Tactic | Technique ID |
|---|---|
| Reconnaissance | TA0043 |
| Initial Access | T1566.002 (Spearphishing Link) |
| Execution | T1204.002 (User Execution – Malicious File) |
| Persistence | T1053 (Scheduled/Recurring C2) |
| Privilege Escalation | T1136.001 (Create Local Account) |
| Discovery | T1087, T1135 (Account & Network Share Discovery) |
| Lateral Movement | T1021.002 (SMB/Network Shares) |
| Collection | T1005 (Data from Local System) |
| Exfiltration | T1041 (Exfiltration over C2 Channel) |
| Command & Control | T1071 (Application Layer Protocol) |

## RECOMMENDATIONS

### Detection Improvements

- Block malicious domains and IPs
- Remove unauthorized user gu@rd!an
- Reset credentials for affected users
- Deploy EDR scanning for ecobug.exe hash
- Harden email filtering
- Restrict access to internal dev portal
- Monitor outbound HTTPS uploads
- Review permissions on network shares
- Conduct phishing awareness training

## INDICATORS OF COMPROMISE

### IOCs Identified

| Category | IOC |
|---|---|
| Malicious JS | `alert('xss')` |
| Attacker IPs | `98.117.26.236`, `13.201.46.208`, `105.78.23.64`, `56.6.30.190` |
| Malicious domains | `energy-trends4u.net`, `news-on-industry.com`, `eco-awareness-update.net` |
| Malware | `ecobug.exe` fcc075087c36825a5a8a6fefbc9a90e6c6ee53e7 |
| C2 | `98.117.26.236:1337` |
| Unauthorized user | `gu@rd!an` |
| Exfiltration URL | `hxxps://api.eco-awareness-update.net/upload` |