DIGITAL FORENSICS WRITEUP

Author: Nikhil Birla

Date: 28 December 2025

Lab: Advent of The Relics 1 - A Call from the Museum (Part 1)

Difficulty Level: Easy

Evidence: network: Email (.eml) and PDF stating the scenario

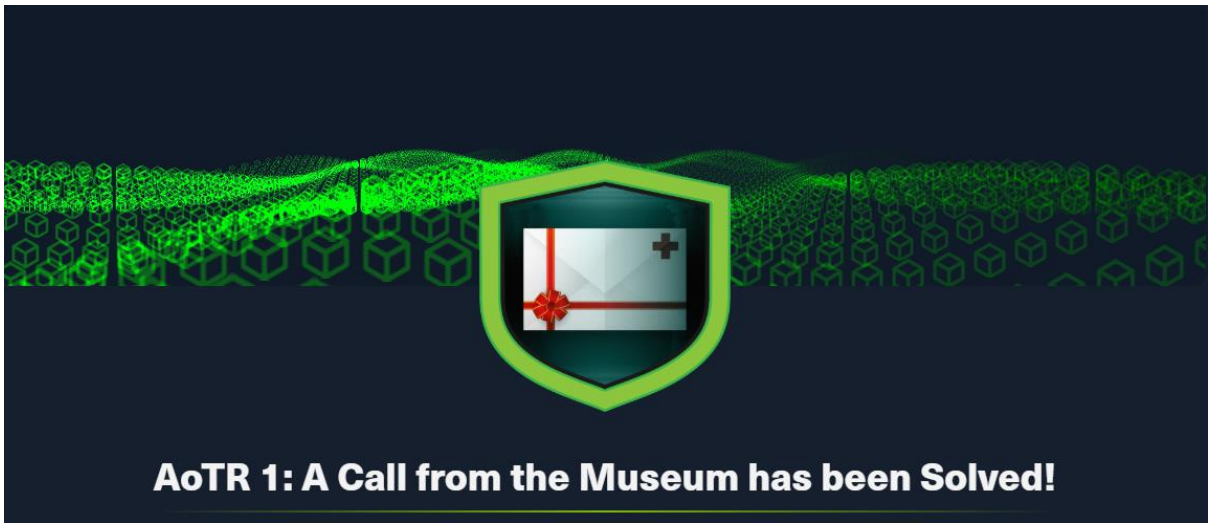

Table of Contents

1. Executive Summary

A phishing email sent to a CALE Corporation employee delivered a malicious ZIP archive containing a PDF and a LNK file. The LNK executed obfuscated PowerShell that beaconed to a C2 server, exfiltrated system identifiers, and retrieved a second-stage payload from a threat-actor forum. This report details the technical analysis of the initial compromise chain.

---

2. Email Analysis

2.1 Suspicious Sender

- **From Address:** eu-health@ca1e-corp.org
- **Method:** Email headers inspected with **PhishTool**.
- **Finding:** SPF/DKIM mismatch; sender was spoofed.

2.2 Legitimate Origin Server

- **Server:** BG1P293CU004.outbound.protection.outlook.com
- **Method:** Traced Received: headers in the email.
- **Finding:** Email originated from Microsoft 365 infrastructure before spoofing.

---

3. Attachment & Payload Examination

3.1 Malicious Attachment

- **Filename:** Health_Clearance-December_Archive.zip
- **Method:** Extracted via PhishTool's attachment viewer.
- **Contents:**

- Health_Clearance_Guidelines.pdf
- EU_Health_Compliance_Portal.lnk

3.2 Document Code

- **Code:** EU-HMU-24X
- **Method:** Used pdftotext to extract PDF content.
- **Finding:** Document code embedded in the header of the PDF.

---

4. Malware Behavior & C2 Communication

4.1 Initial Beacon

- **URL:** https://health-status-rs.com/api/v1/checkin
- **Method:** POST
- **Source:** PowerShell command observed in **Hybrid Analysis** sandbox.
- **Exfiltrated Data:**
  1. Username ($env:USERNAME)
  2. Domain ($env:USERDOMAIN)
  3. MachineGuid from registry key HKLM\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\MACHINEGUID

4.2 Second-Stage Payload Retrieval

- **Domain:** advent-of-the-relics-forum.htb.blue
- **Path:** /api/v1/implant/

- **Authentication:** Basic Auth header Authorization: Basic c3ZjX3RlbXA6U25vd0JsYWNrT3V0XzIwMjYh

4.3 Credential Recovery

- **Decoded Credentials:** svc_temp:SnowBlackOut_2026!
- **Method:** Base64-decoded the Authorization header from the PowerShell script.
- **Verification:** Successful login to the forum using these credentials.

---

5. Indicators of Compromise (IOCs)

Type	Indicator
Sender Email	eu-health@ca1e-corp.org
Attachment	Health_Clearance-December_Archive.zip
Document Code	EU-HMU-24X
C2 URL (POST)	https://health-status-rs.com/api/v1/checkin
C2 URL (GET)	https://advent-of-the-relics-forum.htb.blue/api/v1/implant/
Credentials	svc_temp:SnowBlackOut_2026!

Type	Indicator
Registry Key	HKLM\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\MACHINE

---

6. MITRE ATT&CK Mapping

- **T1566.001** – Phishing: Spearphishing Attachment
- **T1204.002** – User Execution: Malicious File
- **T1059.001** – Command and Scripting Interpreter: PowerShell
- **T1573** – Encrypted Channel
- **T1552.001** – Unsecured Credentials: Credentials in Files
- **T1583.001** – Acquire Infrastructure: Domains

---

7. Recommendations

1. **Block IOCs** at email gateway and network perimeter.
2. **Monitor registry access** to HKLM\SOFTWARE\Microsoft\Cryptography.
3. **Detect PowerShell** with unusual arguments (-EncodedCommand, -eXeC bYPaSs).
4. **User training** on identifying spoofed senders and suspicious attachments.
5. **Hunt for beaconing** to health-status-rs.com and forum domain.

---

8. Appendix – Tools Used

- **PhishTool** – Email header analysis
- **Hybrid Analysis** – Sandbox execution
- **pdftotext** – PDF text extraction
- **CyberChef** – Base64 decoding
- **Windows Command Line** – Registry key verification