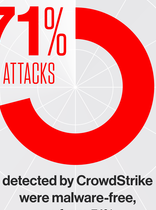
CROWDSTRIKE

MEMORY MANIPULATION

Why Fileless Attacks Hide in Memory and How to Detect Them

Malware-free attacks are on the rise.



71% OF ATTACKS

detected by CrowdStrike were malware-free, up from 51%

84 MINUTES

is the average time before an attack spreads laterally

* Statistics are from July 2021 to June 2022 — for more insights, see the CrowdStrike 2022 Falcon OverWatch Threat Hunting Report.

Fileless attacks like ransomware, advanced persistent threats (APTs) and dual-use tooling are especially difficult to combat since many use legitimate, built-in OS tools. On top of that, **threat actors can orchestrate these attacks entirely in memory.**

THE IMPACT OF FILELESS ATTACKS

SLOWED INFRASTRUCTURE AND OPERATIONS

Legacy memory scanning approaches use resource-intensive scans that bring business-critical systems to a crawl.

INCREASED RISK

Delayed prevention caused by narrow detection types and arbitrary scan schedules allows threats to potentially advance farther down the kill chain.

SILENT FAILURE

Missed detections can enable a threat actor to move unseen, accessing sensitive data and other high-value assets.

THE REASON THEY ARE DIFFICULT TO DETECT

NOT TIED TO INDICATORS OF COMPROMISE

as they leave little to no trace in memory, and can disappear periodically.

EVADE TRADITIONAL ANTIVIRUS

because they can't be detected by static signatures and file scanning.

AVOID DETONATION

by not using Portable Executable (PE) files and instead hijacking legitimate processes to go unnoticed.

EXPLOIT ALLOWLISTING

by using legitimate allowlisted applications and OS executables in an attempt to evade detection and prevention.

THE SOLUTION

CROWDSTRIKE GOES BEYOND WITH ADVANCED MEMORY SCANNING THAT DETECTS FILELESS ATTACKS BY

EMPLOYING AUTOMATION

to initiate real-time surgical scans through behavior-based triggers, not tied to arbitrary time intervals.

IMPROVING PERFORMANCE

through advanced memory scanning capabilities, developed in partnership with Intel Corp., eliminating the slog of legacy memory scanning approaches.

ENABLING HIGH-FIDELITY DETECTION

and protection across fileless attack types, going beyond just ransomware and cryptominers.

USING CROWDSTRIKE'S INDICATOR OF ATTACK

technology and rapid response team to deliver real-time detection updates enterprise-wide, without the need for sensor updates.

FOR MORE ON ADVANCED MEMORY SCANNING DETECTION

Register for our CrowdCast

Visit the CrowdStrike Falcon® Insight XDR webpage.

Follow us: