DECEPTIVE BYTES

Cyberdis

DISTRIBUTED BY CYBERDIS · DECEPTION SURFACE

ENDPOINT DECEPTION · ACTIVE ENDPOINT DECEPTION · RANSOMWARE PREVENTION · PREEMPTIVE DEFENSE · EDR-FRIENDLY

Active Endpoint Deception that turns malware's own evasion tactics against it - ransomware aborts before it ever runs.

ABOUT DECEPTIVE BYTES

Deceptive Bytes is an Active Endpoint Deception platform that prevents ransomware and other evasive malware by turning the attacker's own evasion techniques against it. Rather than detecting attacks after they execute, it makes the endpoint look hostile and unworthy to malware: it generates the signals of an analysis environment that malicious code checks for before detonating, so the attack aborts itself before execution.

The agent runs in user mode with a footprint under 1.5 megabytes, needs no reboots and no signature database, and covers Windows and Linux. The company reports a prevention rate above 99.9 percent with up to 90 percent fewer alerts sent to SIEM.

Malware's greatest strength is also its weakness: before it runs, it carefully checks whether the environment is real, unmonitored and worth attacking. Deceptive Bytes answers those checks with the wrong answers - prevention that needs no prior knowledge of the threat and runs alongside the endpoint stack a customer already owns.

THE PROBLEM

Modern malware checks for sandboxes and security tools before it detonates - evading detection is its core skill, and detection-based tools see it too late.

HOW DECEPTIVE BYTES SOLVES IT

Deceptive Bytes turns that evasion against the attacker: the endpoint looks hostile and unworthy to malware, so it aborts before it ever executes.

CAPABILITIES

Preemptive deception
Creates the artifacts of a hostile analysis environment on every endpoint. Malware performing reconnaissance concludes it is being watched - and terminates itself before executing.

Evasion-technique coverage
Built around the 1,000+ techniques malware uses to fingerprint its target before detonating - the checks that make threats evasive become the tripwire that stops them.

High-fidelity alerts, less noise
Threats reveal themselves during reconnaissance, so alerts carry intent, not noise - the company reports up to 90 percent fewer alerts reaching SIEM and downstream systems.

Featherweight, stack-friendly agent
User mode, under 1.5MB on disk, no reboots, no threat database to update. Deploys alongside EDR, EPP and XDR platforms without conflicts - on Windows and Linux (Ubuntu, Debian, RHEL, SLES).

QUICK FACTS

FOUNDED: 2016, Holon, Israel LEADERSHIP: Sagi Lamay (CEO), Avi Lamay (CTO), Hen Lamay (COO)

RECOGNITION: Gartner Cool Vendor 2019 - Security Operations & Threat Intelligence

FOOTPRINT: User-mode agent, <1.5MB disk, no reboots - Windows & Linux

WHO BUYS IT CISOs, SOC managers, IT & security leads

See Deceptive Bytes *on your own terms.*

Deceptive Bytes is distributed by Cyberdis: a demo tailored to your environment, or a full proof of concept - run by a Cyberdis engineer, sold through channel partners.

cyberdis.io/vendors/deceptive-bytes/

info@cyberdis.io