Bitdefender®

Q4
2020

Fileless Attack Defense

REPORT BY

ASHISH CHAKRABORTTY, TECHNICAL MARKETING ENGINEER

Table of Contents

Fileless Attack Defense

Overview

Fileless malware attacks, unlike the traditional file-based ones, do not download malicious files or write content to disk [2]. Fileless attacks involve leveraging and re-purposing “living-off-the-land” legitimate admin tools like PowerShell and Windows Management Instrumentation (WMI) to run scripts and load malicious code directly into the memory [3].

Bitdefender’s patented machine learning offers an approach that combines security capabilities required to protect against both legacy and modern attacks [2]. HyperDetect, a tunable machine learning technology, extracts meanings and instructions from command line and scripts. Process Inspector operates on a zero-trust basis, monitoring running processes and system events. Behavior analytics coupled with event correlation allows effective remediation action including terminating the process and rolling back changes.

Technical Diagram

As illustrated below, a phishing email containing a malicious link takes the user to an exploit-hosting site. The browser exploit triggers PowerShell running command line (script), then PowerShell follows the instructions to download additional script (typically a larger command line) from a remote site. The larger command line contains fileless malware that is assembled and run directly in memory.

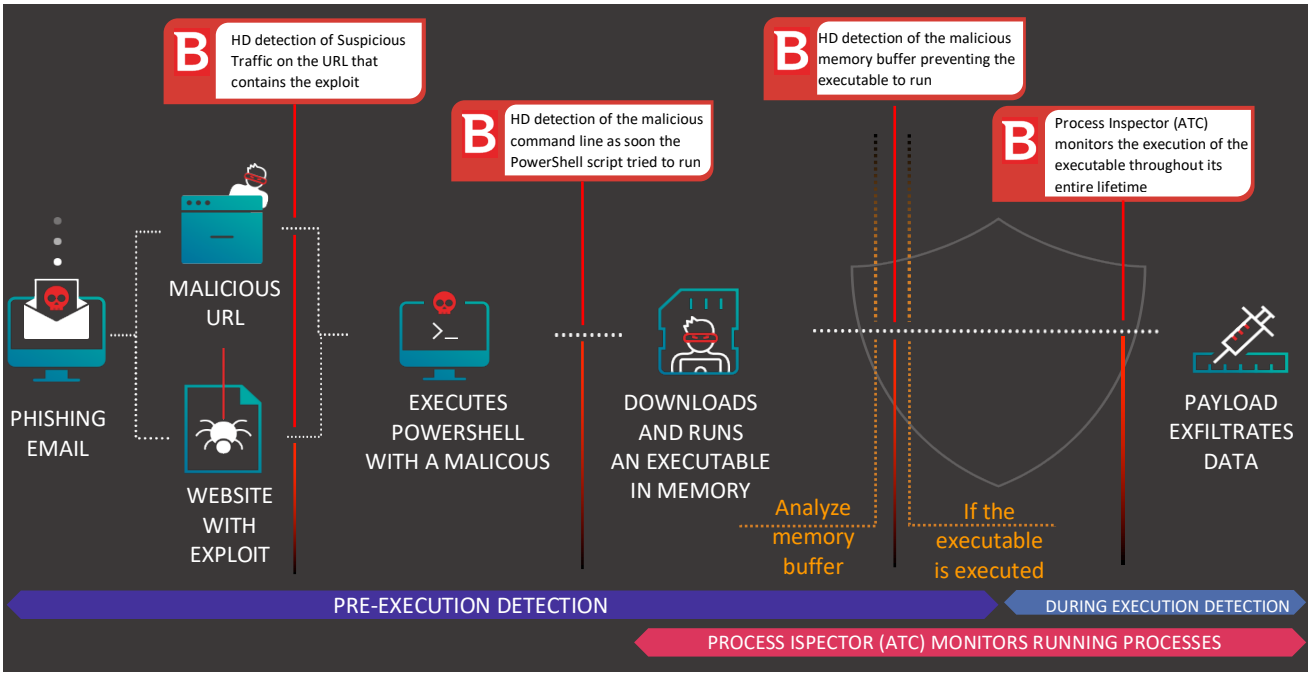

Fig 2. Fileless attack scenario with Bitdefender

Use Case

Behavioral Threat Detection

HyperDetect within GravityZone suite can detect and block fileless attacks at pre-execution. It uses highly tuned machine learning models for spotting new and unknown malware with high accuracy. In a recent APT campaign, a sophisticated attack showed signs of industrial espionage and information exfiltration [4]. Bitdefender’s advanced machine learning was able to successfully detect and block malware during multiple steps in the attack kill-chain by analyzing the behavior at a code level.

Living-off-the-land misuse Detection

Anti-malware technologies like HyperDetect and Process Inspector detect suspicious/malicious process behavior, correlate techniques and provide effective protection to customers at pre-execution. Kingminer, a crypto-jacking malware, used custom payloads disguised as Control Panel Items (.cpl) [5]. Malicious payloads were delivered via a more advanced, fileless execution through PowerShell and Mshta, focusing more on defense evasion. Bitdefender behavioral technologies detected suspicious execution trees launched by the internal tools and blocked them.

Memory Protection

More than 30 machine learning driven security technologies analyze command lines, scrutinize internet connections, monitor process behavior and protect memory space of running process [2]. It intercepts, detects hostile intent and blocks fileless malware at pre-execution including terminating PowerShell running command line, blocking malicious traffic, analyzing memory buffer prior to code injection and blocking code injection process.

Beneficial Outcomes and Consequences

Superior protection against Advanced Threats

Bitdefender performed exceptionally well in third-party independent testing in a simulated real-life threat scenario [1]. In our customer success, Bitdefender replaced Sophos as it had failed to provide any protection from sophisticated attacks like WannaCry [6]. On an international level, Bitdefender's machine learning detected exploits (Cobalt Strike beacons) delivered using spear-phishing campaigns and immediately blocked local PowerShell, Event Viewer and MMC processes from causing damage [7].

Efficient Incident Response for Security Teams

Security teams shoulder the largest cybersecurity burden triaging alerts and incident responses. In MITRE ATT&CK® evaluation tests, Bitdefender shined at actionable detections & alerts across every steps of the entire attack chain [8]. Bitdefender is a perfect solution for resource and skill constrained midsized organizations that are eager to extend their EDR capabilities but are concerned about the complexity of these solutions.

Reduced Performance Impact and False Positives

Bitdefender customers appreciate the low resource utilization when it comes to performance and speed of detection. Bitdefender uses far less memory and provides adaptive, layered endpoint security solution to continuously monitor runtime behavior and help predict, prevent and evade zero-day threats and other cyberattacks [9]. Bitdefender solution is intuitive and self-conjuring which produces low numbers of False Positives than competition [1].

FAQs

How does Bitdefender resolve detection issues with non-traditional malware?
Bitdefender with its patented technologies and zero-trust model, inspect processes and payloads at a behavior level. HyperDetect is designed to detect non-traditional targeted attacks, suspicious files and network traffic, ransomware, grayware and exploits in the pre-execution stage.

How does HyperDetect address issues with False Positives generated by behavioral technologies?
Bitdefender's HyperDetect is a tunable machine learning model which provides ability to configure detection classifiers. It can detect and report at a certain level and block (enforce) at a different level.

Does Process Inspector act on malicious activity early in the attack kill chain?
Process Inspector is a behavior anomaly detection technology that provides post-infection protection against never-before-seen threats in on-execution stage. Behavioral anomaly tracking means active applications and processes are continuously monitored and malicious activity is immediately blocked.

References:

[1] https://businessinsights.bitdefender.com/a-perfect-av-comparatives-detection-score-what-does-it-mean
[2] https://download.bitdefender.com/resources/media/materials/Bitdefender-NGZ-Fileless-SolutionBrief-crea2071-A4-en_En-interactive.pdf
[3] https://securityboulevard.com/2020/01/researchers-find-rdp-abuse-exposes-new-fileless-type-tactic/
[4] https://businessinsights.bitdefender.com/apt-mercenary-groups-pose-real-threat-to-companies-but-detecting-tactics-and-techniques-is-within-reach
[5] https://www.bitdefender.com/files/News/CaseStudies/study/354/Bitdefender-PR-Whitepaper-KingMiner-creat4610-en-EN-GenericUse.pdf
[6] https://download.bitdefender.com/resources/files/News/CaseStudies/study/230/Bitdefender-Business-CaseStudy-expressions-creat4438-210x297-en-EN-GenericUse.pdf
[7] https://www.bitdefender.com/files/News/CaseStudies/study/262/Bitdefender-WhitePaper-An-APT-Blueprint-Gaining-New-Visibility-into-Financial-Threats-interactive.pdf
[8] https://businessinsights.bitdefender.com/mitre-attack-evaluation-results
[9] https://download.bitdefender.com/resources/files/News/CaseStudies/study/166/Bitdefender-CaseStudy-Calcasieu-crea1549-A4-en-EN-GenericUse.pdf