BlackBerry | CYLANCE

BUSINESS BRIEF

BLACKBERRY CYLANCE VS. FILELESS MALWARE

How do fileless attacks work?

Fileless attacks operate in volatile memory and may hijack legitimate system resources to attack host systems. This allows them to threaten organizations worldwide by effectively avoiding traditional file-based detection. The number of fileless attacks doubled in 2018[1] and show no signs of slowing. This means every organization not explicitly protected from filelesss attacks is increasingly at risk of being compromised.

WHAT IT IS

Fileless attacks originally described threats existing and operating exclusively in volatile memory. This tactic avoids triggering traditional antivirus file-scanning, leaves no evidence on-disk for examination, and requires experts to capture system memory for analysis. Fileless threats commonly inject themselves into legitimate system processes, further frustrating efforts at detection.

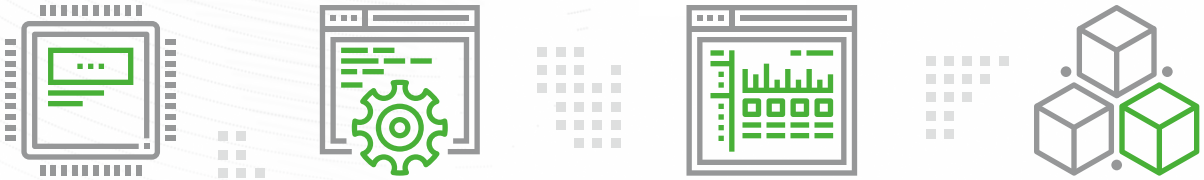
Fileless threats which leverage other system resources are often called living-off-the-land (aka LOL) attacks. These threats can elevate privileges, achieve persistence, and spread across the network by using tools like PowerShell and WMI. Threats like PowerSniff, which temporarily save a malicious DLL to the filesystem, have also been described as fileless. This expands the term fileless to include threats ranging from strictly memory-resident agents to malware which avoids storing malicious executables on-disk.

OUR APPROACH TO COMBATING FILELESS ATTACKS

Blackberry® Cylance® cybersecurity tools prevent, detect, and enable you to respond in real time to the critical components of fileless attacks.

- **CylancePROTECT®** includes a feature called Fileless Memory Protection, which scans and monitors running processes. It prevents fileless malware from executing from within memory space or exploiting processes for malicious purposes. Memory Protection also detects and stops stack pivot attack techniques. CylancePROTECT script control provides robust protection by preventing malicious scripts from running in conjunction with PowerShell, Visual Basic, JavaScript, and macros.
- **CylanceOPTICS™** detects each atomic event that occurs on an endpoint in real time. Each event is evaluated using the Machine Learning Threat Detection Modules to instantly determine if there is malicious intent. For instance, when a process is launched, CylanceOPTICS analyzes the event and compares it with normal process-launching behavior. A user invoking a PowerShell process on a script in a normal directory may not trigger an alert. An automated one-line command invoking PoweShell on a script in a temporary directory may. A range of automated responses (or entire playbooks) can then be triggered, up to and including terminating all related processes in memory.

These kinds of attacks can be recognized by the following traits:



Memory Resident
Malware is memory resident instead of residing on disk

Script Based
Script-intensive malware uses Jscript/JAVAScript to launch initial infection and to assist with attacks

Exploits Resources
Malware exploits resources like PowerShell, WMI, and other legitimate Windows admin tools to conduct activities

System Registry
Malware achieves persistence through modification of the system registry

About BlackBerry Cylance

BlackBerry Cylance develops artificial intelligence to deliver prevention-first, predictive security products and smart, simple, secure solutions that change how organizations approach endpoint security. BlackBerry Cylance provides full-spectrum predictive threat prevention and visibility across the enterprise to combat the most notorious and advanced cybersecurity attacks, fortifying endpoints to promote security hygiene in the security operations center, throughout global networks, and even on employees' home networks. With AI-based malware prevention, threat hunting, automated detection and response, and expert security services, BlackBerry Cylance protects the endpoint without increasing staff workload or costs.

THE BENEFITS OF BLACKBERRY CYLANCE CYBERSECURITY

Blackberry Cylance uses advanced artificial intelligence to combat known, unknown, and zero-day threats, whether file-based or fileless. Our utilization of AI, automated threat response, and detailed forensic analysis offers several benefits including:

- Continuous malware prevention, device and script control, application control, and memory exploitation protection at the endpoint
- Elimination of hidden threats through machine-learning-assisted threat detection and on-demand, enterprise-wide, threat hunting
- Predictive advantage over cyber threats[2]
- Compliance with privacy legislation like GDPR[3]
- Reduced costs of system remediation and fewer system re-images[4]
- Improvement in overall IT and security employee productivity[4]

GET AI-DRIVEN PROTECTION FROM FILELESS ATTACKS TODAY

Protect your organization from the threat of fileless attacks by contacting Blackberry Cylance for a demo or consultation today. Our security experts will help to evaluate your current cybersecurity posture while demonstrating the value our advanced solutions provide. Learn more at www.cylance.com/fileless

[1] https://threatpost.com/2019-malware-trends-to-watch/140344/
[2] https://threatvector.cylance.com/en_us/home/cylance-vs-future-threats-the-predictive-advantage.html
[3] https://threatvector.cylance.com/en_us/home/cylance-gdpr-assessments-offer-sustainable-approach-to-data-privacy.html
[4] https://adapture.com/blog/cylance-forrester-report/

+1-844-CYLANCE
sales@cylance.com
www.cylance.com

BlackBerry | CYLANCE

20190618-0359