Bitdefender

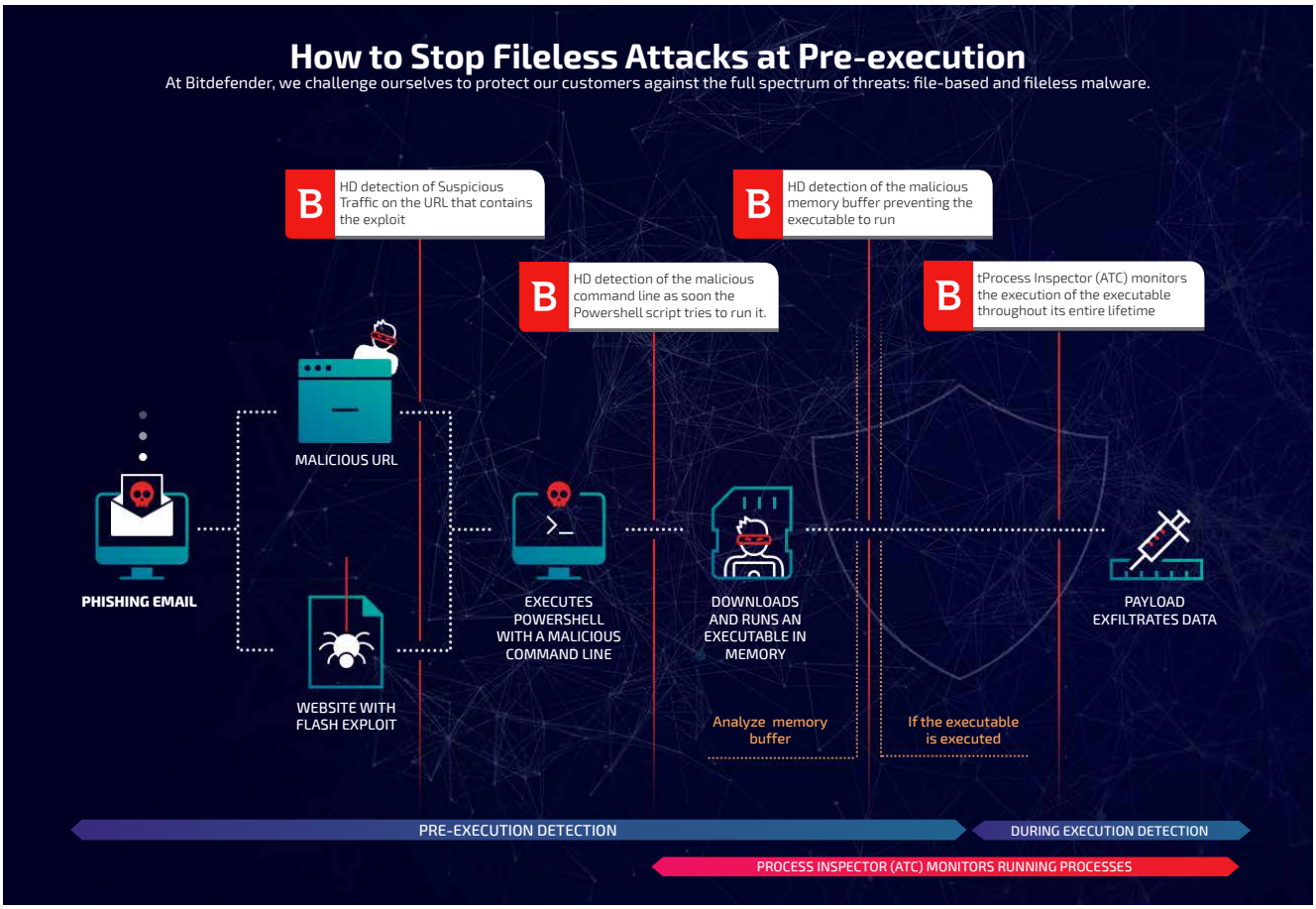
Stop Fileless Attacks at Pre-execution

Threat actors are shifting to fileless attacks. Experts would tell you that these attacks cannot be prevented by endpoint security solutions. At Bitdefender, we challenge ourselves to protect our customers against the full spectrum of threats – file-based and fileless malware.

What is fileless attack?

Fileless malware attacks are also referred to as fileless attacks. They are sometimes also referred to as non-malware attacks, although the term is not technically accurate.

Unlike file-based attacks, fileless malware attacks do not download malicious files or write content to disk. Attackers exploit application vulnerabilities to inject code directly into the memory space of an existing application. They can also leverage trusted office applications or administration tools native to Windows OS, such as PowerShell or Windows Management Instrumentation (WMI), to run scripts and load malicious code directly into memory. Like all attacks, the goal is to gain control of computers to achieve the attacker's goal, such as destruction, distortion (ransomware), data/credential theft, or additional attacks.



As in the example illustrated above, a phishing email containing a 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.

In a second example, a user may receive a phishing email with a .doc attachment containing a macro. If the user enables the macro, essentially a VBA script, it triggers the PowerShell script that downloads additional scripts containing fileless malware code from a remote location. It then injects that malicious code into the memory space of a vulnerable application.

Non-persistent vs persistent

True fileless malware is non-persistent -- all traces of it disappear when the system is rebooted, making forensic investigation difficult. However, we have seen fileless attacks gain persistency by installing themselves in Windows registry keys entries or as rootkits, evading detection because traditional AV tools don't scan these areas. By hiding malicious code in Windows registry entries, attackers can hijack various Windows components and allow the code to re-execute within the memory each time the operating system boots up.

Challenges

Fileless malware already presents a significant problem, and it's gaining further popularity among attackers because it is virtually undetectable by traditional file-based prevention and detection techniques. Endpoint security tools, including so called next-gen AV, don't scrutinize scripts or command line, such as PowerShell scripts, and no file is written on disk. Since traditional AV and so-called next-gen AV focus on static file analysis, fileless attacks can evade these AV tools without triggering alarms because no file is downloaded and saved to the disk.

Blocking file-less attacks at pre-execution requires an integrated approach to detection, prevention and interruption

The Bitdefender GravityZone Elite Suite is the first endpoint security solution that can discover and block fileless attacks at pre-execution automatically.

The GravityZone Elite Suite features layered next-gen endpoint security. It leverages machine learning to analyze command lines, scrutinize internet connections, monitor process behavior and protect the memory space of running process. It detects and block fileless malware at pre-execution, including terminating PowerShell running malicious command line, blocking malicious traffic, analyzing memory buffer prior to code injection and blocking the code injection process.

I. Suspicious traffic and file download – Inspect internet connection and block C&C communication and attempts to download malicious shell code
II. **Process Inspector** – The behavior-based detection technology operates on a zero-trust basis, monitoring running processes and system events (in the OS using filters in user mode and kernel mode). It analyses behavior, connects events, and tags suspicious activities, then takes the necessary remediation actions, including terminating the process and rolling back system changes.
    Examples of actions detected by Process Inspector to stop fileless attacks:
    - Powershell.exe or mshta.exe are launched with several specific arguments
    - Processes like Office Macro or internet browser spawn PowerShell that normally do not perform this action
    - A process injects code in other processes' memory space

III. Command analysis – **HyperDetect** uses machine learning to extract meanings and instructions from command line and scripts including Java scripts, visual basic scripts and PowerShell scripts. As soon as a malicious command is detected, it can terminate Powershell.exe and other script interpreting tools such as wscript.exe, cscript.exe, rundll32.exe; mshta.exe; powershell_ise.exe, regedit.exe, reg.edit, autoit.exe and others.

IV. Code injection protection with memory buffer analysis – Just before the code is injected into another (usually approved but vulnerable) application's memory space, Bitdefender Endpoint HD (part of the Elite Suite) has the unique ability to protect the target application's memory space and analyze the code in memory buffer. If the code is deemed malicious, it will block the process and thwart the fileless attack. The precision of this method, as opposed to bluntly shutting down all code injection processes, reduces false positives.

Unlike other applications that require administrators to manually write rules to bluntly block certain routines, such as code injection or Word Macro spawn cmd.exe, Bitdefender's layered next-gen endpoint solution works out of the box, and provides the flexibility to tune detection sensitivity.

GravityZone Elite Suite is the first endpoint security solution that can detect and block fileless attacks at pre-execution automatically.

To learn more about how Bitdefender's layered next-gen solution can detect and prevent sophisticated attacks such as fileless attacks visit https://www.bitdefender.com/business/elite-security.html

Bitdefender

Bitdefender is a global security technology company that provides cutting edge end-to-end cyber security solutions and advanced threat protection to more than 500 million users in more than 150 countries. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a provider of choice in both hybrid infrastructure security and endpoint protection. Through R&D, alliances and partnerships, Bitdefender is trusted to be ahead and deliver robust security you can rely on. More information is available at http://www.bitdefender.com.

FOR MORE INFORMATION VISIT: bitdefender.com/business

BD-NGZ-Jan 12-2018-TH#
Bitdefender-NGZ-Fileless-SolutionBrief-cnsa2071-A4-en_EN