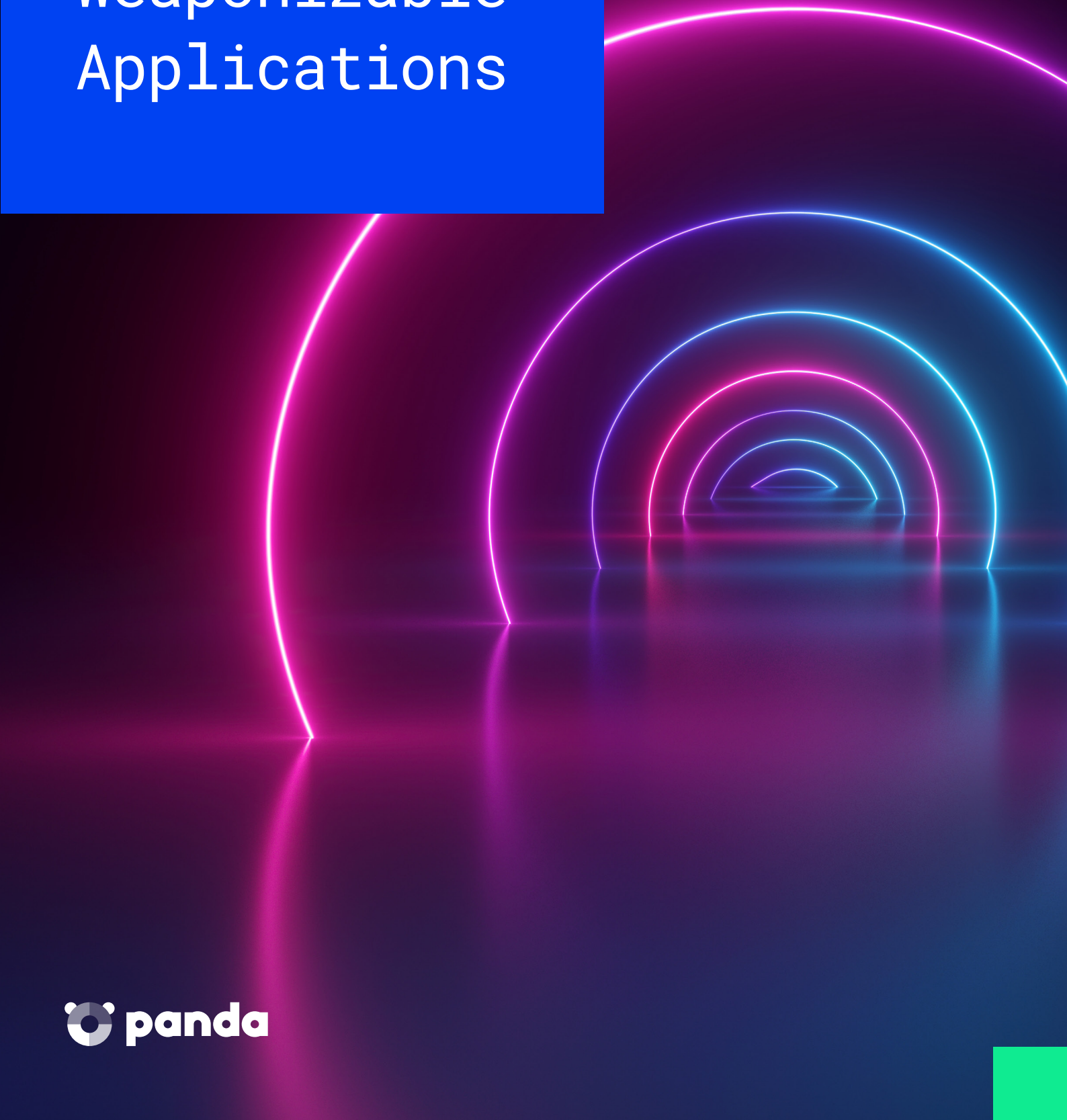
pandasecurity.com/business/

Danger Hiding In Plain Sight:

Controlling Weaponizable Applications



panda

Table of Contents:

Introduccion

When most tech companies talk about threats from within, more often than not they are referring to a company' s most common network gateway: its employees.

But there are far more internal threats than just the human ones, frequently used applications being at the top of that list. In fact, in 2018, fileless attacks were up 94% – 3 times more frequent than ransomware attacks to endpoints. Fileless Malware takes advantage of vulnerabilities in legitimate applications (Lotl*) installed by default and used daily by the workforce, like Microsoft Office, WMI and Adobe, among others. Foregoing use of these applications isn' t an option, so how can you ensure that hackers won' t turn them against you?

In this eBook, we will cover how to identify that a non-malicious application has been weaponized, the most common methods (like PowerShell), used to carry out attacks and methods to ensure your network stays protected against these kinds of threats.

Fileless Malware takes advantage of vulnerabilities in legitimate applications

94%

fileless attacks were up in 2018

* Living-off-the-land (Lotl): LotL techniques are used by attackers to leverage pre-existing and legitimate administrative applications with dual use, in devices and servers, and abusing them, inadvertently to the administrator.

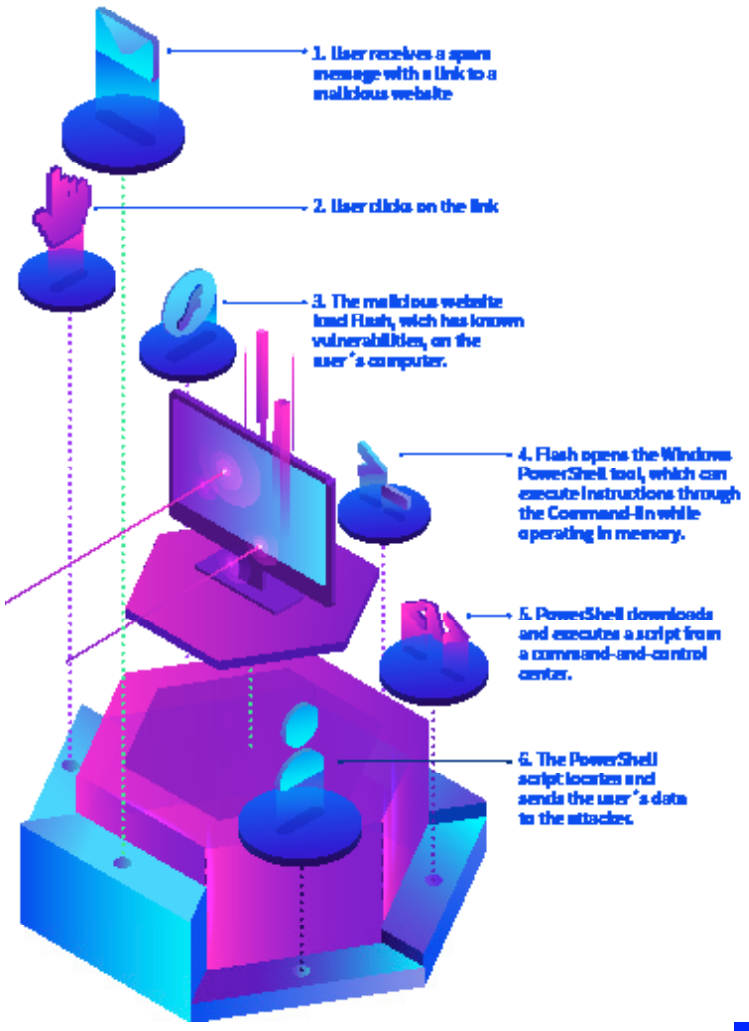
|Fileless Malware Defined

It' s been a trend for years now: hackers looking for new, creative ways to circumvent cybersecurity solutions and get on to a company' s network.

One of the most successful new strategies for cybercriminals has been fileless attacks. These attacks can take many forms, including the use of macros, scripting engines, and in-memory executables. Although the nature of these attacks varies, they are all specifically designed not to write onto the hard drive, and instead work from a computer' s memory (RAM). The lack of known malicious or potentially dan gerous files on a computer' s hard drive makes it impossible for traditional protection systems to detect the threat.

Although there are different variations of fileless attacks, there are several key characteristics that they share. First and foremost, they are notoriously difficult to detect due to a lack of identifiable code that antivirus software can look for and hunt. In addition to the lack of identifiable code, they bypass traditional security solutions by leveraging native applications and processes to carry out the attack, making it nearly impossible to flag irregular behavior.

Fileless Malware attack process



panda

In addition to these fundamental similarities, fileless attacks often share points of entry. Some of the most common ways for these attacks to breach systems include[1]:

- {Scripting Applications}
- {Remote access applications}
- {Admin tools}
- {System tools}
- {Internal operating systems components}

Out of all these entry points, there is one application that is by far the most common vessel for fileless attacks: **PowerShell.**

1 https://blog.eccu.edu/most-common-malware-attacks-fileless-malware-part-2/

|PowerShell: Fileless Malware's Greatest Attack Vector

Fileless malware can be carried out via a variety of vessels, but one of the most common and effective vehicles for this type of attack is the Windows system console, PowerShell.

This console is used to allow system administrators to fully automate tasks on servers and computers. Its broad and powerful feature set means that if compromised, PowerShell can be used to cause major damage to a network. If hackers manage to take control of it, they can gain a variety of permissions across a company' s systems, allowing them to easily introduce more malware. And it' s not just the Windows operating system itself companies need to worry about PowerShell also allows users to control Microsoft Exchange, SQL Server, IIS and others.

With all these capabilities, fileless malware usually leverages PowerShell to introduce its payload, lodging itself in the RAM. Once the code has been executed in PowerShell, it can carry out lateral movements on corporate networks, meaning it propagates centrally rather than relying on external inputs. These attacks typically thrive because they leave no traceable code on the hard drive of the first compromised computer, meaning Windows Defender and other traditional cybersecurity solutions fail to detect the attack. The good news is there are ways you can minimize the risks associated with PowerShell. The most effective way, if possible for your organization, is to completely disable the console. This may be an option if your company' s admin is using a different tool to automate tasks. In other words, if you don' t absolutely have to use PowerShell, don' t!

In cases where disabling PowerShell is simply not an option, there are some proactive actions you can take to protect your company. For example, make sure your organization' s endpoints are always running the latest version of the console; PowerShell 5 packed additional security measures for Windows. Another step you can take is to enable only the specific set of features of PowerShell that your administrator needs using Constrained Language mode. Doing this won' t stop all attacks, but it can stop potentially dangerous actions such as arbitrary calls to Windows APIs or deactivation of certain macros.

In addition to proactive measures, Microsoft has introduced more advanced features in PowerShell logging; that is, the automatic transcription of commands, especially for actions that are potential symptoms of a cyberattack. Enabling these transcription features can help companies discover a fileless malware attack and carry out forensic tasks to diagnose the issue.

|Indicators that a hacker has weaponized applications on the network

As the PowerShell example illustrates, it can be difficult to know when your applications have been weaponized by a cybercriminal.

Many of these attacks have been specifically created to fly under the radar of traditional security solutions. That being said, there are some red flags you can look for if you suspect you have been the victim of a breach.

To combat the elusive nature of fileless attacks, antimalware vendors are adding behavior-based monitoring and reporting capabilities to their products. For example, if Word executes at the same time as a PowerShell connection, that could indicate an attack is in progress.[2] Once flagged, a company' s IT security team can decide whether to quarantine the process or stop it completely. Another behavior that should be a red flag is unusual CPU activity, specifically, major increases in usage. This could imply that a computer has been compromised by a fileless attack and is using CPU to mine Bitcoin or other cryptocurrencies while attempting to fly under the radar.

The biggest challenge in identifying these types of attacks is catching them before they trigger an alert. The potential indicators discussed above are helpful investigative tools, but ultimately only appear after a hacker has carried out an attack and accessed the machine. The only way to proactively protect your organization from fileless malware is to adopt an advanced security solution.

The biggest challenge is catching these types of attacks before they trigger an alert

2 https://www.csoonline.com/article/3227046/what-is-a-fileless-attack-how-hackers-invade-systems-without-installing-software.html

|Advanced Threats Call For Advanced Technology

It' s clear that attackers are continuously advancing their efforts to gain access to corporate information.

By hijacking essential applications and using them to plant malware or access sensitive data, cybercriminals have essentially created an invisible breach that is impossible for traditional security solutions to detect.

While there are ways to proactively defend your organization from these attacks, the only way to guarantee an organization' s safety is with advanced cybersecurity technology with big data, machine learning, and IoA.

Panda Adaptive Defense 360 is an innovative cyber-security solution, which combines the widest range of protection technologies (EPP) with automated Endpoint Detection and Response capabilities. It automates the prevention, detection, containment and response against advanced attacks, zero-day malware, ransomware, phishing, memory exploits and fileless attacks, inside and outside the corporate network.

Cybercriminals have created an invisible breach that is impossible for traditional security solutions to detect

Panda Adaptive Defense 360 also provides greater control through the Program Blocking feature. While this feature helps enhance IT security, it also reduces bandwidth consumption and encourages productivity by blocking software execution by hash (MD5) or process name.

In addition, Panda' s Advanced Reporting Tool includes dashboards that offer full visibility and control over all running applications, enabling you to pinpoint attacks and unusual application and user activity in your network. With the Advanced Reporting Tool, those red flags that are hard to spot with a traditional security product become a lot more visible.

With Panda Adaptive Defense, you can also create custom queries to easily test attack hypothesis after you notice something abnormal on your network.

As business, and the world in general, becomes more interconnected and digital, preventing cybercrime will continue to be a major part of day-to-day operations at organizations across the globe. With an advanced cybersecurity solution like Panda Adaptive Defense 360 in place, you can feel confident knowing your IT assets are safe from even the most sophisticated cyberattacks.

Preventing cybercrime will continue to be a major part of day to day operations at organizations across the globe.

Two high value managed services are included as features of the solution:

The 100% Classification of processes service

The 100% Classification service monitors and prevents the execution of malicious applications and processes on endpoints. For each execution, it issues a real-time classification, malicious or legitimate, with no uncertainty.

Threat Hunting and Investigation service

The managed Threat Hunting and Investigation service is operated by the Threat Hunters team, with profiling, analysis and event correlation tools, in real-time and retrospectively, to proactively discover new hacking and evasion techniques.

* Living-off-the-land (Lotl): LotL techniques are used by attackers to leverage pre-existing and legitimate administrative applications with dual use, in devices and servers, and abusing them, inadvertently to the administrator.

Live demo

Let’s talk*

Toni Jeršin, Ado Hasanović
panda@anni.si