Global Threats | Issue 3

How to Combat Fileless Attacks

vmware Carbon Black

What Is a Fileless Attack?

A fileless attack (memory-based or living-off-the-land, for example) is one in which an attacker uses existing software, allowed applications and authorized protocols to carry out malicious activities. More and more attackers are moving away from traditional malware—in fact, 60 percent of today's attacks involve fileless techniques. These attacks are capable of gaining control of computers without using traditional executable files as a first level of attack.

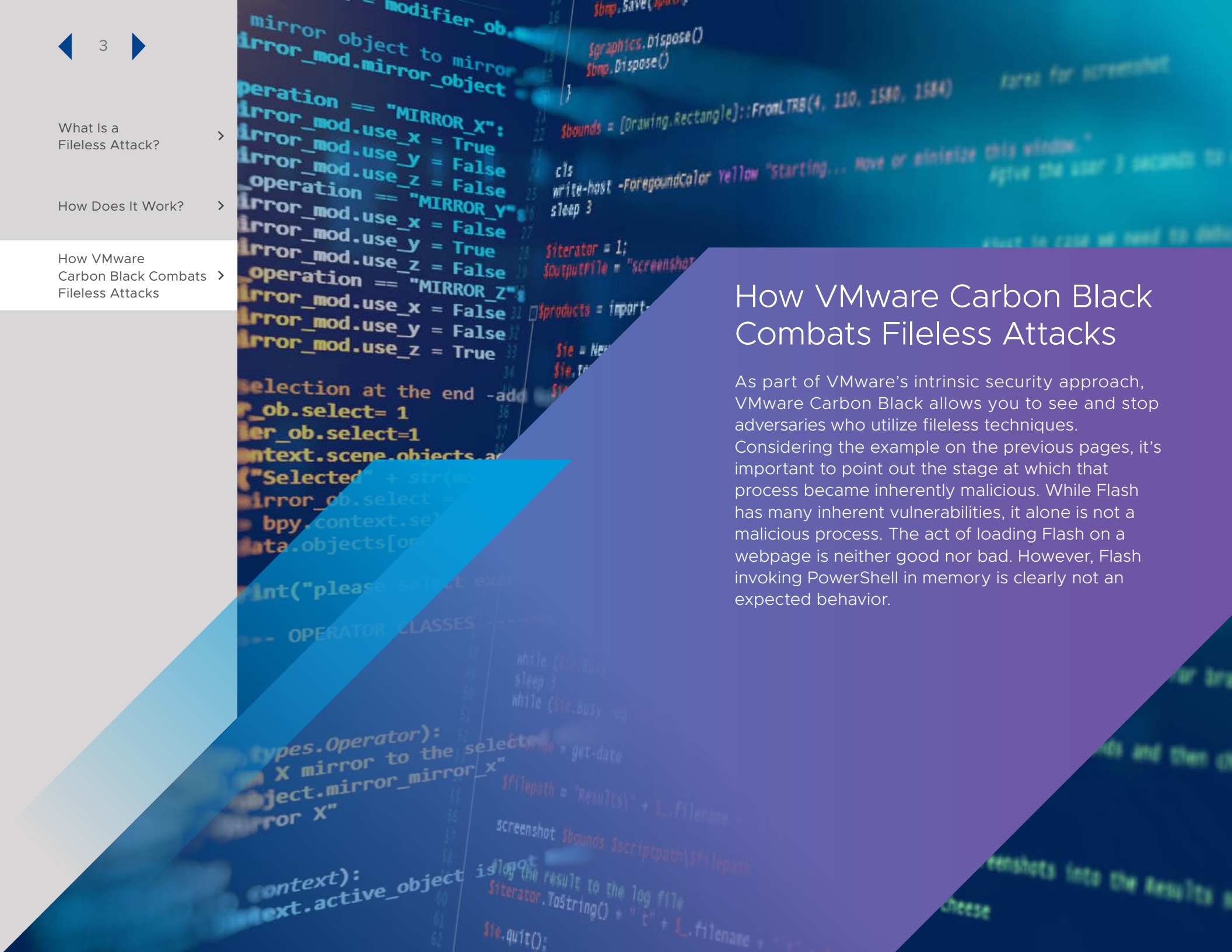
With fileless attacks, an attacker is able to infiltrate, take control and carry out objectives by taking advantage of vulnerable software that a typical end user would leverage on a day-to-day basis (such as web browsers or Office suite applications). Attackers will also use the successful exploit to gain access to native operating system tools (such as PowerShell and Windows Management Instrumentation, or WMI) or other applications that grant the attacker a level of execution freedom. These native tools grant users exceptional access and privileges to carry out the most basic commands across a network that lead to valuable data.

The reason fileless attacks are so prominent is because traditional antivirus (AV) and machine-learning AV can't prevent (or even detect) non-malware attacks, providing attackers with a point of entry that goes completely overlooked. If the goal of an attacker is to gain a foothold or exfiltrate valuable data, then non-malware attacks accomplish this without fear of detection.

How Does It Work?

Fileless attacks leverage a robust suite of tactics and techniques to penetrate systems and steal data without using malware at all. They have grown in prevalence in recent years as attackers have developed ways to launch these attacks at large scale.

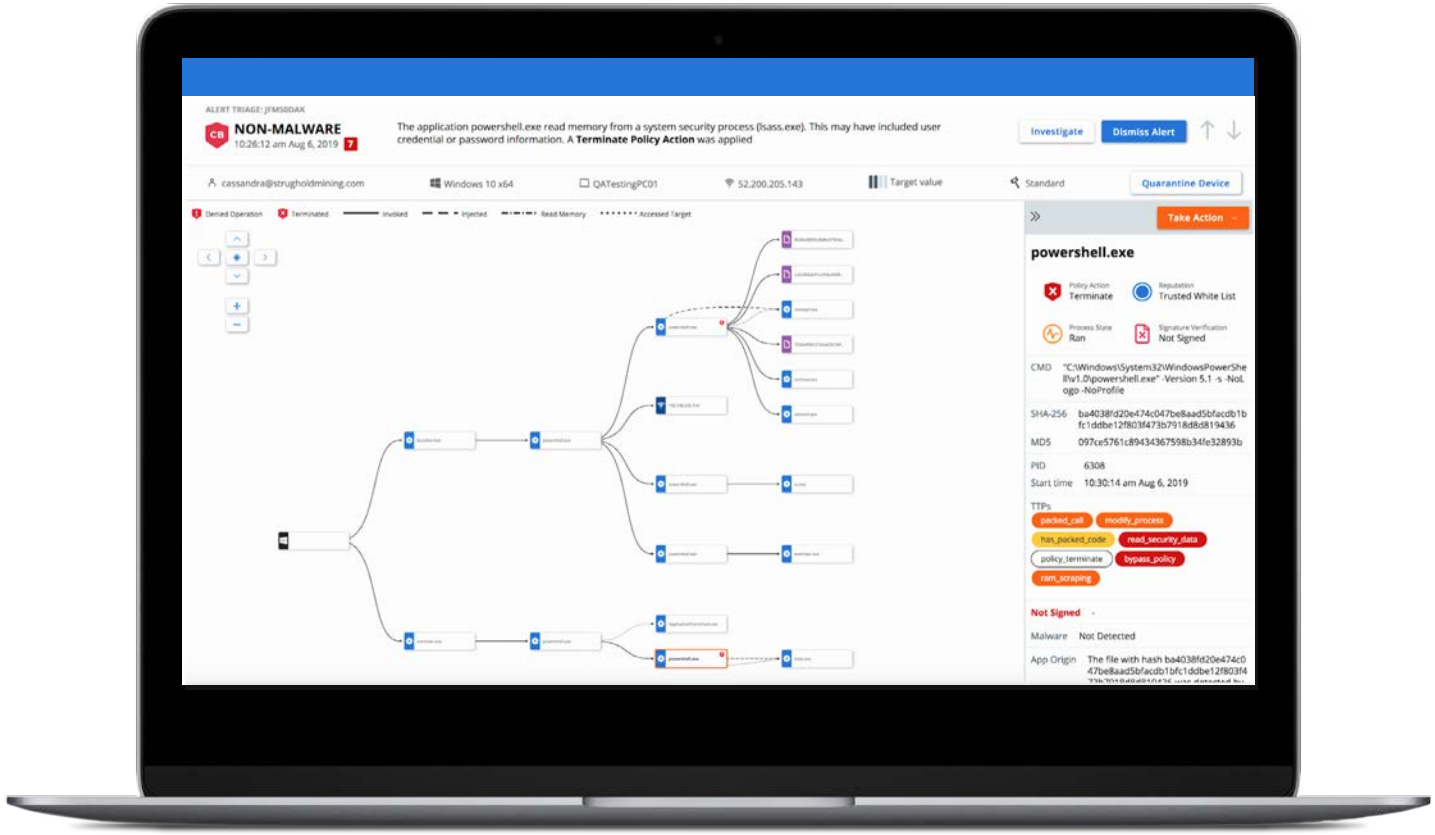
1. A user visits a website using Firefox, perhaps driven there from a cleverly disguised spam message.
2. On this page, Flash is loaded. Flash is a common attack vector due to its seemingly never-ending set of vulnerabilities.
3. Flash invokes PowerShell, an administrator tool available on every Windows machine, and feeds it instructions through the command line—all operating in memory.
4. PowerShell connects to a stealth command and control server, where it downloads a malicious PowerShell script that finds sensitive data and sends it to the attacker. This attack never downloads any malware.



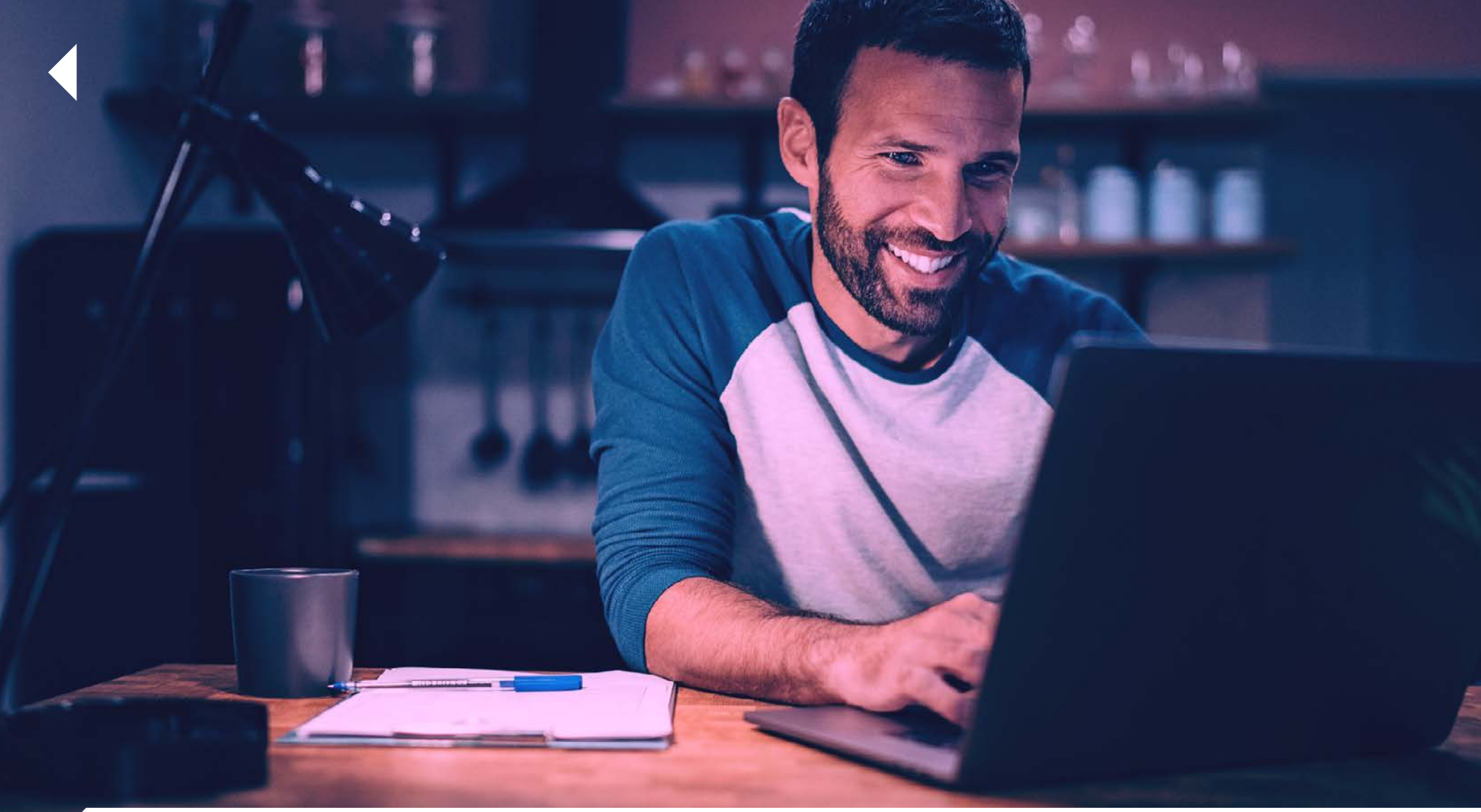
How VMware Carbon Black Combats Fileless Attacks

As part of VMware's intrinsic security approach, VMware Carbon Black allows you to see and stop adversaries who utilize fileless techniques. Considering the example on the previous pages, it's important to point out the stage at which that process became inherently malicious. While Flash has many inherent vulnerabilities, it alone is not a malicious process. The act of loading Flash on a webpage is neither good nor bad. However, Flash invoking PowerShell in memory is clearly not an expected behavior.

VMware Carbon Black's solutions are built on kernel-level visibility, allowing for a holistic view across your entire environment at all times. When our universal agent sees PowerShell begin executing, with a browser as the parent process, it immediately generates alerts and escalates based on the suspicious nature of that action. Let's say that as a next step, PowerShell attempts to harvest user credentials by scraping lsass.exe. This is the point at which VMware Carbon Black steps in and shuts PowerShell down completely. Scraping memory of an executable such as lsass.exe in that sequence of events is a common technique used by attackers in many different attacks, so that specific behavior is seen as inherently malicious and prevented from successfully completing.



vmware Carbon Black



Get Started Today

See how you can combat threats in your environment

Learn More

Join us online:

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com