ALIEN VAULT

# Five Endpoint Attacks Your Antivirus Won't Catch

## A GUIDE TO ENDPOINT DETECTION AND RESPONSE

www.alienvault.com

# For cyber attackers, the endpoint is **THE** point.

Endpoints are the point of entry into your environment, your data, your credentials, and potentially your entire business. A compromised endpoint provides everything an attacker needs to gain a foothold on your network, steal data, and potentially hold it for ransom. Unless you secure your critical endpoints (including servers, laptops, and desktops), you may be leaving the front door wide open for attackers.

Attackers have figured out how to bypass traditional antivirus software with fileless attacks designed to hide within sanctioned applications and even within the OS itself. According to the Ponemon Institute, fileless endpoints attacks made up 77 percent of all reported endpoint compromises in 2017.

So, even if you're vigilant about installing patches and pushing out antivirus updates, your organization is likely still at risk. Keep reading to understand how attackers have adapted their tactics to evade traditional antivirus, how these increasingly common attacks work and how to quickly evolve your threat detection strategy.

# FIVE ATTACKS
## Your Traditional Antivirus Won't Detect

### 01 CRYPTOMINING MALWARE

Cryptomining tools convert computing power into revenue. While the cryptocurrency market is growing rapidly, it turns out that the CPU required to mine for cryptocurrencies happens to be very costly[2]. So, attackers create malware and other attacks to quietly siphon computing resources from victims for cryptomining. Methods include exploiting exposed AWS resources or AWS account credentials to steal cloud computing resources, often referred to as "cryptojacking"; browser-based attacks that work while a visitor is browsing a legitimate, yet compromised website; and cryptomining malware, often delivered through phishing campaigns, that consumes CPU on your endpoints. Any flavor of cryptomining attacks can have disastrous effects for your business. Attackers can turn compromised endpoints and clouds into silent zombie armies of cryptocurrency miners (all without a single antivirus alert). Without advanced threat detection tools that span your endpoints and public clouds, your only indication that your computing resources may have been hijacked could be an application or network performance hit or a skyrocketing AWS invoice.

[2] According to Check Point, cryptominers can use as much as 65% of an endpoint's CPU. https://blog.checkpoint.com/2017/10/23/crypto-miners-the-silent-cpu-killer-of-2017/

# FIVE ATTACKS
## Your Traditional Antivirus Won't Detect

## 02 REVERSE POWERSHELL ATTACKS

Even in spy novels, everyone knows that the best way to avoid detection is to act like you belong. Attackers follow this approach, as they increasingly use PowerShell and other sanctioned services to evade traditional antivirus software. By gaining access to admin credentials and executing authorized administration actions, cyber attackers can reduce their reliance on malware and exploit kits and more easily evade detection, making for a stealthier data theft operation.

## 03 RDP SESSION JACKING

The Remote Desktop Protocol (RDP) enables you to remotely connect to a Windows system, usually requiring you to provide the user password before you can gain session access. However, a known exploit to bypass this is to run tscon.exe (the RDP client process) as SYSTEM user, which does not prompt you for a password. And, no antivirus alarms go off. **Pro-tip:** Publicly available RDP services on your endpoints serve as an open invitation to attackers, so make sure your gateway firewall policy blocks these connections by default (or only allows connections from authorized IP addresses).

[2] According to Check Point, cryptominers can use as much as 65% of an endpoint's CPU. https://blog.checkpoint.com/2017/10/23/crypto-miners-the-silent-cpu-killer-of-2017/

# FIVE ATTACKS
## Your Traditional Antivirus Won't Detect

### 04 APTS/ROOTKITS

Advanced Persistent Threats (APTs) involve a series of steps, each of which can easily evade traditional methods of detection (we address each of these steps in detail in the next section). These blended threats often start with a phishing email to capture credentials and then move on to installing malware such as rootkits, which embed themselves deep into the endpoint's OS. Once you've got root access at a kernel level, all bets are off and the system is fully pwned.

### 05 RANSOMWARE

Attackers know how to innovate. Recent ransomware innovations include offering ransomware-as-a-service, as well as targeting widely-used corporate cloud apps. One example that easily evades antivirus is the ShurL0ckr ransomware, which targets cloud-based enterprise file sharing platforms. Ransomware-as-a-service enables attackers to pay its author a percentage of the ransom once the payload that encrypts the files on the disk is generated and distributed.

[2] According to Check Point, cryptominers can use as much as 65% of an endpoint's CPU. https://blog.checkpoint.com/2017/10/23/crypto-miners-the-silent-cpu-killer-of-2017/

# How These **Attacks Evade Detection** by Antivirus:

While these attacks may have their differences, they share some specific characteristics that help them avoid detection by traditional antivirus tools. These four critical steps show how it's done.

# Four Critical Steps
# **To Avoid Detection**

## 01 DELIVERY

Signature-based antivirus tools try to catch and quarantine malicious files as they are downloaded or executed on endpoints. The problem is that modern attacks operate without downloading or executing malicious files on the hard drive. Instead, they leverage social engineering (phishing), exploit OS vulnerabilities, and package malicious code within normal-looking files to evade detection in the delivery process.

For example, the widespread banking trojan, Emotet, employs email phishing to deliver malicious code as a Microsoft Office macro. Recent, headline-grabbing ransomware attacks, including WannaCry and NotPetya, exploited the EternalBlue SMB vulnerability in Windows for remote code execution.

Once an attacker has a foothold on the victim's endpoint, they can use PowerShell to download the payload and propagate. And, because traditional antivirus is built to look for unusual files, PowerShell and other native processes run easily under their radar.

# Four Critical Steps
# **To Avoid Detection**

## 02 EVASION

The best offense is to use the native components of a system against itself. By using what's already on an endpoint (e.g. tscon.exe, PowerShell, etc.), cyber attackers execute attacks much faster while also evading antivirus detection.

## 03 LATERAL MOVEMENT

Endpoints provide attackers a necessary foothold into a victim's network. Once an endpoint is compromised - any endpoint will do - the next step is to move laterally through the network to find desired assets and targets (domain admin credentials, file servers, etc.). Once an attacker has domain admin credentials, they can move literally anywhere within that domain, stealing and exfiltrating data without antivirus software triggering a single alert.

## 04 COVER TRACKS

After doing their dirty work, a smart attacker will cover their tracks. With domain admin credentials, attackers easily delete log files on each endpoint they used within that domain to avoid leaving critical forensic evidence behind for investigators. With one PowerShell script, all digital breadcrumbs of the theft disappear, and not a single antivirus tool is built to notice this.

# Detecting Advanced Endpoint Threat **WITH EDR**

**Here are three key strategies for effective, scalable, and responsive endpoint defense:**

## 01 PREVENTION IS NECESSARY, BUT NOT SUFFICIENT.

Layer Endpoint Detection and Response (EDR) with your antivirus. Detecting endpoint threats at each of the four stages (outlined above) requires looking at activities more holistically, as a chain of events rather than distinct ones that slip under your radar. One example is the “cover your tracks” scenario. As long as you’re collecting and archiving endpoint event logs (off of the endpoint), you’ll be able to capture key forensic data required for data breach investigations.

## 02 MONITOR EVERYWHERE (NOT JUST THE ENDPOINT).

Security monitoring is at its most valuable when it’s comprehensive. In addition to monitoring endpoints, you’ll also need to monitor the cloud apps they’re connecting to, the authentication systems that gave them access, the firewalls that allowed the connections, and the local domain controllers in your office (just to name a few).

## 03 MAKE IT MANAGEABLE AND SCALABLE.

In order to keep pace with emerging risks, simplifying your toolset and automating where possible will serve you well. By unifying your network, host, and cloud security monitoring capabilities into a single platform, you can respond faster to incidents and you’ll have the full picture. Additionally, security automation and orchestration capabilities enable you to stop some attacks when they’re detected.

# How AlienVault Can Help

AlienVault Unified Security Management® (USM) delivers endpoint detection and response (EDR) as part of a unified platform for threat detection, incident response, and compliance. AlienVault's cloud-based solution, USM Anywhere™, centralizes and automates threat hunting everywhere modern threats appear, including cloud and on-premises environments, so you can detect threats earlier and respond faster. And with continuous threat intelligence from AlienVault Labs, your defenses stay current as threats evolve.

Unlike point security solutions, USM Anywhere combines multiple security capabilities into a unified cloud platform, including EDR, SIEM, IDS, vulnerability assessment, and more, giving you the essential security capabilities you need in a single pane of glass, drastically reducing cost and complexity.

**Learn More:**

› Explore USM Anywhere in our hands-on online demo

› Start detecting threats in your environment today with a free trial, and link here

› Watch a 2-minute overview video