CROWDSTRIKE

Modern Adversaries and Evasion Techniques: Why Legacy AV Is an Easy Target

CrowdStrike eBook

Table of Contents

Where Legacy AV Went Wrong

If you take away one thing from this eBook, make it this: Legacy antivirus (AV) is no longer capable of stopping adversaries. Modern endpoint security is required to stop breaches — period.

Where did legacy AV go wrong? First, the decades-old technology is too slow. Implementation takes months. And endless scans and updates swamp resources while slowing down endpoints. In other words, as adversaries have sped up, legacy AV has only slowed down.

But the fatal flaw of legacy AV is that it just doesn't work anymore. The technology relies on signatures, which are hard to update and ineffective against fileless attacks. And given that 71% of detections are now malware-free,[1] a technology that relies purely on known threats is going to miss the vast majority of attacks.

These shortcomings aren't for lack of effort. Some legacy AV vendors have added behavioral analysis and machine learning capabilities over the years, but it's become a patchwork of additional agents that are cumbersome to deploy and manage. New agents often lack native integration with existing agents, forcing customers to configure connections across agents. By the time a new agent is deployed, it's already obsolete.

Read on to learn how adversaries are evading legacy AV, hear five cautionary tales of adversaries in action and understand why modern endpoint security is the only way to stop breaches. Let's go.

71%

of detections are now malware-free

=

560,000

new pieces of malware detected every day

How Adversaries Evade Legacy AV

Until recently, malware was the preferred point of entry for adversaries. Not anymore. While malware remains a top threat — with 560,000 new pieces of malware detected every day and more than a billion malware programs available in the wild[2] — CrowdStrike research shows that malware is being used further down the attack chain.

Let's examine seven emerging defense evasion techniques, **according to MITRE**.

[1] CrowdStrike 2023 Global Threat Report

[2] DataProt. A Not-So-Common Cold: Malware Statistics in 2023. March 2023.

7 Defense Evasion Techniques Legacy AV Can't Stop

1. Impairing defenses: Adversaries may modify components of a victim's environment to hinder or disable defense mechanisms. This could involve preventative defenses, such as firewalls and AV, or detection capabilities used to audit activity and identify malicious behavior.

2. Removing indicators: Adversaries can delete or modify artifacts generated within systems to remove evidence of their presence or hinder defenses. Various artifacts may be created by an adversary or could be attributed to an adversary's actions. Examples include file deletion or obfuscation.

3. Subverting trust controls: Undermining security controls that either warn users of untrusted activity or prevent execution of untrusted programs is another way adversaries can bypass legacy AV. Operating systems and security products may contain mechanisms to identify programs or websites as possessing some level of trust. Adversaries may attempt to subvert these trust mechanisms by modifying registries or file and directory permissions. Adversaries may also create or steal code-signing certificates to acquire trust on target systems.

4. Hijacking execution flow: Adversaries may execute their own malicious payloads by hijacking the way operating systems run programs. Hijacking execution flow can be for persistence, since this hijacked execution may recur over time. Adversaries might also use these mechanisms to elevate privileges or evade defenses such as application control.

5. Injecting code into processes: Injecting code into processes can allow adversaries to evade process-based defenses or elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory and/or system/network resources and possibly elevate privileges.

6. Proxying execution with system binaries: Adversaries may bypass process and/or signature-based defenses by proxying execution of malicious content with signed or otherwise trusted binaries. Binaries used in this technique are often Microsoft-signed files, indicating they've been either downloaded from Microsoft or are already native in the operating system.

7. Masquerading: Manipulating features of their artifacts to make them appear legitimate or benign to users and/or security tools is another way adversaries bypass legacy AV. Masquerading occurs when the name or location of an object — legitimate or malicious — is manipulated or abused to evade defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type and giving legitimate task or service names.

According to CrowdStrike research,

86%

of eCrime actors use one or multiple forms of evasion techniques to bypass detection such as legacy AV software.

From Legacy AV to Modern Endpoint Security

Modern endpoint security is a comprehensive security strategy designed to detect evasion techniques and ultimately stop breaches. At a basic level, it includes two components: next-generation AV (NGAV) and endpoint detection and response (EDR).

What Is NGAV?

NGAV is a cybersecurity tool that uses a combination of artificial intelligence (AI), behavioral detection, machine learning algorithms and exploit mitigation to anticipate and prevent both known and unknown threats. Unlike legacy AV solutions, NGAV is cloud-based, which allows it to be deployed more quickly and without over-burdening the endpoint. In addition, it eliminates or significantly reduces the hassle of maintaining software, managing infrastructure and updating signature databases.

What Is EDR?

EDR is a cybersecurity solution that detects and mitigates threats by continuously monitoring endpoint devices and analyzing endpoint data. EDR solutions work by providing continuous and comprehensive real-time visibility into what's happening across all endpoints. Behavioral analysis and actionable intelligence is then applied to endpoint data to prevent an incident from turning into a breach. EDR tools also provide advanced threat detection, investigation and response capabilities, including incident data search and investigation alert triage, suspicious activity validation, threat hunting, and malicious activity detection and containment.

Given the increasing sophistication of adversaries and their constantly evolving tactics, techniques and procedures (TTPs), organizations should use both EDR and NGAV solutions for complete protection against modern attacks.

Next, read five cautionary tales of adversaries that evaded legacy AV and how modern endpoint security would have stopped the breaches.

5 Adversary Evasion Techniques in Action

Adversary:

WANDERING SPIDER

When
Early 2023

What Happened
CrowdStrike Intelligence has tracked WANDERING SPIDER since April 2020. This adversary has conducted ransomware campaigns using Black Basta, DOPPEL SPIDER'S DoppelPaymer, PINCHY SPIDER'S REvil and ProLock, TWISTER SPIDER'S Egregor and Maze, and WIZARD SPIDER'S Conti. In early 2023, CrowdStrike discovered WANDERING SPIDER was using the legitimate binary `fs _ uninstall _ 32.exe` to uninstall an enterprise legacy AV solution.

How Modern Endpoint Security Helps
One way threat actors evade detection is by using legitimate tools to blend in with benign, day-to-day activities. These types of attacks are extremely challenging to detect using signature-based methods. Modern endpoint security excels at discerning between malicious and benign behavior. Tamper-resistant capabilities, for example, block attempts to tamper with the sensor. This setting protects the sensor-related files, folders and registry objects from renaming or deletion. If disabled, the sensor still identifies and alerts on tampering attempts.

Adversary:

MALLARD SPIDER

When
February 2023

What Happened
Industry sources reported an email spam campaign distributing QakBot using Windows Script Files (WSF) masquerading as a file certificate. The WSF file contained an embedded JavaScript that attempted to download and execute the QakBot payload. Following the decline of ISO and OneNote as delivery methods, eCrime threat actors have been experimenting with many alternative delivery methods and masquerading tactics, including previously seen techniques such as HTML smuggling, password-protected ZIP files, Base64 encoding and file size inflation. These techniques are often effective in bypassing legacy AV scanning.

How Modern Endpoint Security Helps
Adversaries continue to experiment with new malware distributions and use tactics like obfuscating characters and Base64 encoding to bypass signature-based detections. Through the use of indicators of compromise, advanced AI and behavioral analysis, modern endpoint security enables early detection of obfuscation techniques and attempted execution of malicious payloads, thereby stopping these attacks.

Adversary:

SCATTERED SPIDER

When
Early 2023

What Happened
CrowdStrike Intelligence detected probable **SCATTERED SPIDER** activity in which the adversary accessed multiple North America-based technology companies that specialize in business process outsourcing. While the initial infection vectors were not confirmed, the adversary deployed either remote management and monitoring (RMM) tools or tested the ability to reach domains relating to such software. Furthermore, SCATTERED SPIDER used numerous living-off-the-land (LOTL) utilities and legitimate tools to conduct elements of their post-exploitation activity. Legacy AV vendors routinely fail to scan RMM and legitimate tools, allowing these types of supply chain attacks to occur.

How Modern Endpoint Security Helps
Modern endpoint security uses advanced behavioral analysis to understand the context of seemingly benign activity. In this case, the adversary navigated to a legitimate but uncommonly used website and proceeded to remotely log into victim systems to run reconnaissance commands such as `mmc.ex` to enumerate Active Directory information or `whoami` to determine the account of the currently logged-in user. A modern endpoint security solution would have detected and stopped this malicious activity.

Adversary:

Raccoon Stealer Customer

When
August 2022

What Happened
CrowdStrike Intelligence identified a new phishing campaign involving a heavily obfuscated .NET-based loader that attempted to download and install a sample of the newly released Raccoon Stealer 2.0. The extremely popular Raccoon Stealer is a tiny malware package that can be easily bundled into larger packages. When users download a large package, legacy AV vendors typically don't scan all components in the package, allowing malware to pass through unnoticed.

How Modern Endpoint Security Helps
This detection was made by observing a known downloader that uses several evasion techniques to bypass host and network-level detections, including multistage fileless payloads, different types of obfuscations, and legitimate tools such as Discord and OneDrive to host next stages. Modern endpoint security that combines behavioral analysis and fileless attack detection capabilities can stop these types of attacks, which typically evade legacy AV tools.

Adversary:

BITWISE SPIDER

When
February 2023

What Happened
In early 2023, CrowdStrike Services responded to a **BITWISE SPIDER** LockBit incident in which the Sender2 exfiltration tool was deployed. The actor gained initial access using valid credentials, then proceeded to perform host and network reconnaissance using living-off-the-land (LotL) tools such as the `net`, `nltest` and `qwinsta` utilities, which are not identified as malicious by legacy AV.

How Modern Endpoint Security Helps
In this instance, modern endpoint security would have applied behavioral analysis to identify uncommon behavior emanating from legitimate tools. A security system that also combines identity threat protection can provide further protection by detecting the presence of threat actors that use compromised accounts or stolen credentials to gain access and move laterally across systems.

Make the Switch: Modern Threats Require Modern Endpoint Security

Adversaries have evolved and devised numerous ways to evade legacy AV. If you want to protect your organization, you need modern endpoint security.

CrowdStrike is the industry leader in modern endpoint security. **CrowdStrike Falcon® Prevent** is the new standard in NGAV, delivering superior protection from malware, exploits, malware-free intrusions and advanced persistent threats. **CrowdStrike Falcon® Insight XDR** endpoint detection and response delivers continuous, comprehensive visibility that spans detection, investigation and response to ensure potential breaches are stopped.

All CrowdStrike solutions are deployed on the CrowdStrike Falcon® platform using a single lightweight agent. This integrated approach spans endpoint, identity, cloud and threat intelligence — allowing you to easily expand your protections as adversary TTPs evolve. One platform for complete protection.

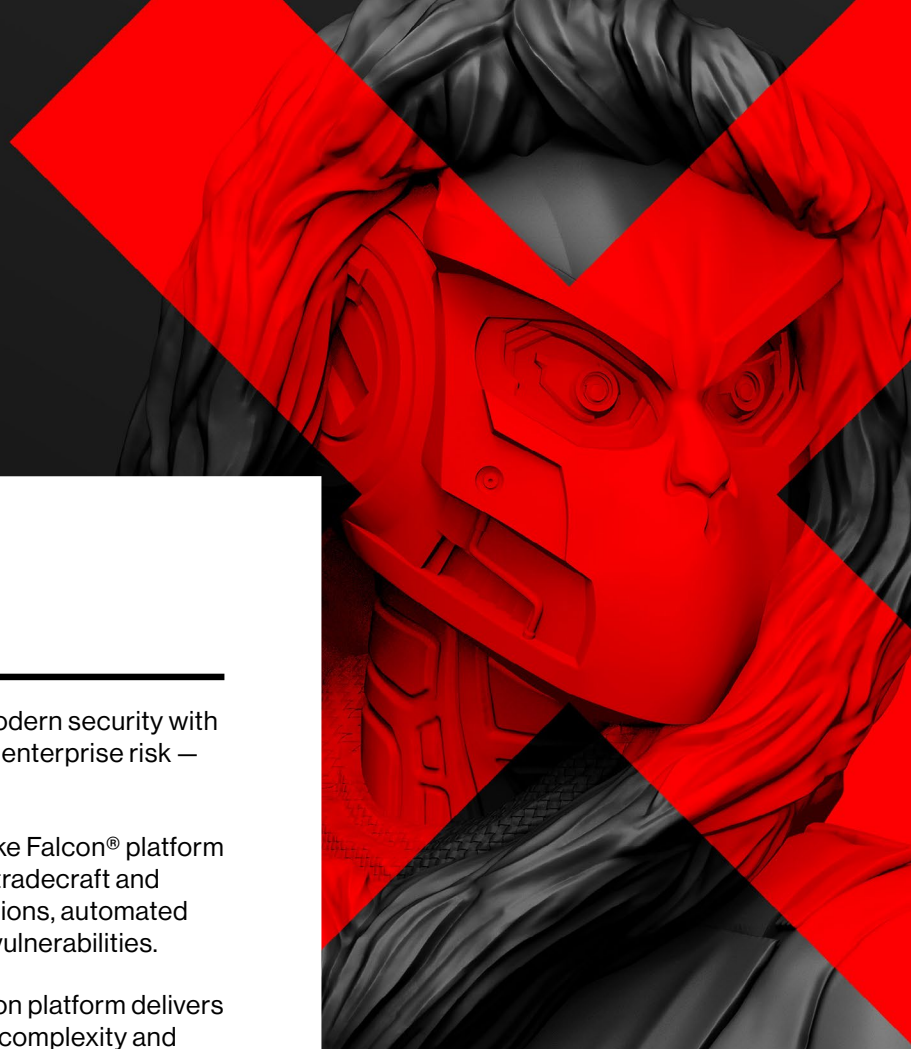
Next Steps

- **Discover** adversaries that are targeting your industry.
- **Access** a modern endpoint security toolkit for additional resources.
- **Try** CrowdStrike Falcon free for 15 days.

"In the old days when we had only AV tools, everything was a thick client with power-hungry agents. Managing that was time-consuming and we had some challenges with resources on workstations — whereas CrowdStrike is cloud-based and has just one agent for all the different solution modules compared to competitor products that need multiple agents."

–CISO of Berkshire Bank

CROWDSTRIKE



About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: **We stop breaches.**

Follow us: **Blog | Twitter | LinkedIn | Facebook | Instagram**