RevBits®

PRODUCT BRIEF

Endpoint Security

While EDRs Have Gained a Strong Market Footing, Many Are Too Easy for Hackers to Circumvent

Major EDR products have a critical flaw that allow hackers to bypass them. Spoiler alert, it happens all the time.

Back in 2013, Gartner first classified endpoint detection and response as emerging tools on the market. Since that time, EDR, as it is now called, has replaced traditional antivirus with more advanced malware detection capabilities.

According to Gartner, the worldwide EDR market is expected to reach $18.3 billion by 2031, with an anticipated compound annual growth rate of 25.15% from 2021 to 2031. And as you might expect, dozens of EDR vendors have entered the market.

EDRs conduct analysis using various techniques to hunt for and take action to eliminate malware. While every product approach is somewhat different, the three most widely deployed forms of analysis include signature scanning, machine learning, and behavioral analysis. Because they can find so many potentially malicious events, the challenge is to minimize false positive alerts that can be overwhelming to security teams.

EDRs conduct analysis using various techniques to hunt for and take action to eliminate malware.

The EDR basics

Both malicious and benign applications use code libraries, known as dynamic link libraries (DLLs), to interact with the OS kernel. All applications use DLLs to reuse code and achieve more efficient use of memory and disk space by making calls to the kernel.

To determine if apps are malicious or not, EDRs intercept calls by overwriting libraries with additional code, putting "hooks" into the call execution flow. Rather than the DLL calling the kernel, it calls the EDR, that collects app information and its behavior. The EDR searches the software, and if the code is suspicious, the EDR will put it into a secure sandbox for analysis, before allowing it to access the operating system kernel. EDRs monitor code behavior in real-time running within computer devices and networks and kill ransomware attacks in progress.

Malware evasion techniques

There are three primary obfuscation methods hackers use against EDRs to gain access to an operating systems kernel. These fairly simple evasion techniques are well-documented, allowing hackers to circumvent EDR hooks and avoid detection with minimal effort. The first is when malware unhooks the EDR by overwriting the ntdll.dll with a clean version. The second evasion technique is when the malware conducts direct kernel system calls. In the third evasion technique, malware conducts indirect system calls using code fragments in kernel DLL's without calling the DLL hooked functions.

With all the success EDRs have achieved, multiple research studies have shown many of the major EDR vendors have vulnerabilities that allow hackers to bypass them, putting organizations at risk. In lab tests conducted by Security Research Labs, researchers packed two commonly used malwares. They also used two commercial remote access tools, Cobalt Strike and Silver Toolkit. These execute targeted attacks and emulate post-exploitation actions of advanced threat actors inside.exe and .dll files using bypass techniques. One of the tested EDRs failed to detect any of the samples. The other two EDRs failed to detect samples that came from the .dll file when they used either technique.

Research studies confirm bypass vulnerabilities in major EDR products

One research study, conducted by Security Research Labs, details three obfuscation methods used against three major EDR vendors, including Microsoft Defender for Endpoints, Symantec EDR, and Sentinel One. Researcher, Karsten Nohl, noted that "EDR makers should focus on detecting malicious behavior more generically rather than triggering only on specific behavior of the most popular hacking tools, such as Cobalt Strike. This overfocus on specific behavior makes EDR evasion too easy for hackers using more bespoke tooling." Nohl went on to say, "complementary to better EDRs on endpoints, we still see potential in dynamic analysis within sandboxes. These can run in the cloud or attached to email gateways or web proxies and filter out malware before it even reaches the endpoint."

Another research study by the University of Piraeus in Athens, Greece, recently conducted testing on 18 different EDR products from leading vendors. The testing of attacks against EDR software included Bitdefender, Carbon Black, Check Point, Cisco, Comodo, CrowdStrike, Elastic, ESET, F-Secure, Fortinet, Kaspersky, McAfee, Microsoft, Panda Security, Sentinel One, Sophos, Symantec, and Trend Micro.

Test results were published in a report offered through Cornell University entitled, An Empirical Assessment of Endpoint Detection and Response Systems against Advanced Persistent Threats Attack Vectors. And like the research study conducted by Security Research Labs, the results showed almost all the EDR products lacked the ability to prevent and log the attacks.

The tests simulated common advanced persistent attack (APT) kill chains, and hosted four common attack files, including a Windows control panel shortcut file (CPL), a Microsoft Teams installer that loaded the malicious DLL, an unsigned portable executable file (EXE), and an HTML application file (HTA). When executed, the malicious files exploited legitimate functions to load and run Cobalt Strike Beacon backdoor.

RevBits EPS automatically extends detection across multi-stage attacks

RevBits EPS is built upon a unique architecture, with detection mechanisms that go far beyond other EDRs. RevBits' custom handlers, or proprietary application loading detection capabilities, find multi-stage malicious activities attempting to impersonate Windows applications, signing processes and trusted processes. RevBits EPS also has an accurate detection engine that prevents false positives and a distinctive architectural design for application whitelisting, sandboxing, spawning, and parent/child process analysis.

RevBits EPS accurately scans DLLs with our machine learning model to detect unknown malware. Installing Shell extensions is another way hackers load malicious DLLs and avoid detection. RevBits prevents this by requiring admin approval before allowing Shell extensions, the same way we require driver approvals.

When a new executable is asked to run on a device, if it isn't already whitelisted, RevBits EPS automatically puts it into a sandbox for analysis. Regardless of what may have been added to obfuscate the malware, RevBits EPS evaluates the entire process, including executables, leaving no ability for malware to hide within legitimate programs and applications. RevBits' ability to analyze Microsoft applications and processes is fundamental in preventing malicious code from entering and launching these types of attacks.

To detect and block malware direct syscalls, RevBits EPS debugging engine scans every system call made by the process being monitored. The entire chain of the call stack is traced and analyzed to determine the identity of the caller.

By analyzing the syscall events and checking to make sure they come from the original OS code, RevBits can catch the calls coming from suspicious modules, or memory that doesn't belong to any modules. In such cases we know it is a direct call, and that malware tried to bypass the EDR.

RevBits is the only EDR vendor that can detect and block this devastating exploit. By leveraging an undocumented Microsoft capability, RevBits processes every syscall, and identifies the functions that go to the kernel, to determine if the call is coming from an authentic source, or from somewhere else.

RevBits EPS transparent file system is a better mouse trap

The RevBits EPS transparent file system is unlike a traditional sandbox that runs in a virtual machine or a dedicated device. RevBits EPS is a security layer on top of the endpoint device's operating system that runs and is executed within the actual computer. The transparent file system intercepts and intelligently redirects API calls, file system access and activity within a separate and confined cached location. It returns the encrypted files back to the malware, convincing the program into thinking it has executed successfully.

RevBits EPS acts as a buffer between malware and the computer's operating system. All new program activity comes into the RevBits process, where a determination is made to let it go through, send it to cache, or send it to trash. Custom handlers, or proprietary application loading detection capabilities, are designed to find multi-stage malicious activities attempting to impersonate Windows applications, signing processes and trusted processes. RevBits EPS has a detection engine that prevents false positives and has a distinctive architectural design for application whitelisting, sandboxing, spawning, and parent/child process analysis.

RevBits EPS prevents the installation of hacker-created Shell extensions that can load malicious DLLs and avoid detection. Admin approval is required before allowing new Shell extensions or drivers. RevBits EPS also accurately scans DLLs with a unique machine learning model that detects unknown malware.

When new programs and executables attempt to infiltrate an endpoint device, RevBits EPS automatically puts them into its transparent file sandbox for evaluation. Regardless of what may have been added to obfuscate the malware, the entire process is monitored and analyzed. This makes it impossible for malware to hide within legitimate programs and applications.

Evasion Technique	Evasion Example	RevBits EPS Protection
Evade Static Analysis	Encrypted Payload	RevBits EPS notes the encryption as suspicious and increases threat rating of the .exe and monitors additional actions and blocks when malicious activity detected.
Detectable Sandbox	Sleep Timer, etc.	RevBits EPS transparent file system is unlike a traditional sandbox that runs in a virtual machine or a dedicated device. RevBits EPS is a security layer on top of the endpoint device's operating system that runs and is executed within the actual computer.
Unhook the EDR	Malware Overwrites EDR hooks	RevBits EPS blocks malware from accessing its hooks and monitors changes that to the solutions state regarding hooks in the OS, if any change is detect the solution kills the process.
Direct Syscalls	Malware Circumvents hooks to .dll	To detect and block malware from making direct syscalls, RevBits EPS debugging engine scans every system call made by the process being monitored. The entire chain of the call stack is traced and analyzed to determine the identity of the caller.
Indirect Syscalls	Malware uses code fragments in kernel .dll	Similar to our method to prevent direct syscall obfuscation, RevBits EPS transparent file system sandbox in conjunction with EPS debugging engine can detect and block indirect syscalls.

RevBits protects organizations against all direct and indirect syscalls and all attempts to bypass EDR hooks.

Third-party test results conducted by ICSA give RevBits EPS a top rating

RevBits EPS was recently tested by ICSA Labs, an independent division of Verizon certification testing. Testing was performed under the Advanced Threat Detection protocol, which focuses on evaluating endpoint security products for protection against new and little-known threats across all malware types.

The process included over 1,203 test runs containing 627 malicious samples and 576 innocuous applications, executed over twenty-seven consecutive days. RevBits EPS had a detection rating of 100% and zero false positives.

RevBits EPS was tested against threats missed by traditional security products, and not a single ransomware was able to cripple computers secured by RevBits Endpoint Security. For the detailed certification report, go to the Advanced Threat Test Report.

To learn more about how RevBits protects organizations against all direct and indirect syscalls and all attempts to bypass EDR hooks, download the following product briefs.

RevBits EPS Detects and Blocks User Mode Direct Syscalls to Kernel

RevBits Rids Malware that Doesn't Play Nice in the Sandbox

EDR Testing Found Leading Cybersecurity Solutions Missed the Mark

RevBits EPS System Hardening Detects and Prevents Zero-Day Exploits

Keep Your Enterprise Protected. Get a Demo or Free Evaluation.
To learn more, visit www.revbits.com

34 Willis Avenue • Mineola, NY 11501 • 844-4REVBIT (844-473-8248) • www.revbits.com