RevBits®

PRODUCT BRIEF

Endpoint Security

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

The amount of data, applications and devices traversing the Internet every day is unbelievably vast. The almost uncontainable exposure to malicious malware grows exponentially every day. Like the endless granules of sand at the beach that seem to get into every nook and cranny of our skin, clothes and equipment, malware can permeate rapidly, with widespread consequences. Controlling and limiting malicious software programs that surreptitiously worm their way into corporate endpoint devices requires moving those unwanted programs into a contained sandbox.

Using a sandbox for advanced malware detection provides an additional layer of protection against new security threats, like zero-day malware and other clandestine cyberattacks. By sandboxing programs, IT can quarantine, analyze and remove malicious software within a confined and safe environment.

To eliminate false positives, many endpoint security products lower their scan detections by trusting core applications within the Windows operating system. When normally trusted applications are not sandboxed for analysis before being allowed to run, malware can infiltrate computers and remain undetected. These attacks even get past Microsoft Defender for endpoints, as evidenced in a recent report and testing of over a dozen EDR products. The published results can be found in a report offered through Cornell University entitled, An Empirical Assessment of Endpoint Detection and Response Systems against Advanced Persistent Threats Attack Vectors.

A new and rapidly growing exploit is being used by hackers to bypass EDR hooks with function calls that invoke syscalls directly from user mode to kernel mode.

RevBits transparent file system (sandbox) provides a strong security defense against malicious attacks. When questionable software is effectively sandboxed, it can only access the memory and disk space assigned to it. This prevents malicious software from spreading. The advantages of sandboxing:

- Removes risk to host device operating systems, preventing exposure
- Evaluates software programs for potentially malicious code from untrusted sources
- Confines and removes zero-day threats
- Complements a multi-layered security strategy
- Strengthens an enterprise's overall security posture

RevBits EPS transparent file system protects operating systems

RevBits EPS utilizes a transparent file system to monitor software program activities, automatically redirecting and caching new programs in a separate location. After analysis determines a program is trusted and clean, new changes are automatically applied to the computer's file system, without impacting the user. If malware is detected, all cache activities are deleted and all changes are purged. The actual file system is never impacted or impaired.

Any program that is executed into a system for the first time, that has not been whitelisted or blacklisted, is confined into the transparent file system. There it is monitored from the kernel, and prevented from executing changes to the file system or registry until its approved.

RevBits EPS transparent file system runs in Windows, macOS, IOS, Linux and Android systems; whether on-premises or in the cloud. The analysis looks for malicious programs, like executables, computer memory-based artifacts like fileless malware, and other malicious files that target operating systems. These nefarious programs can come through Word documents, PDFs, web links and emails.

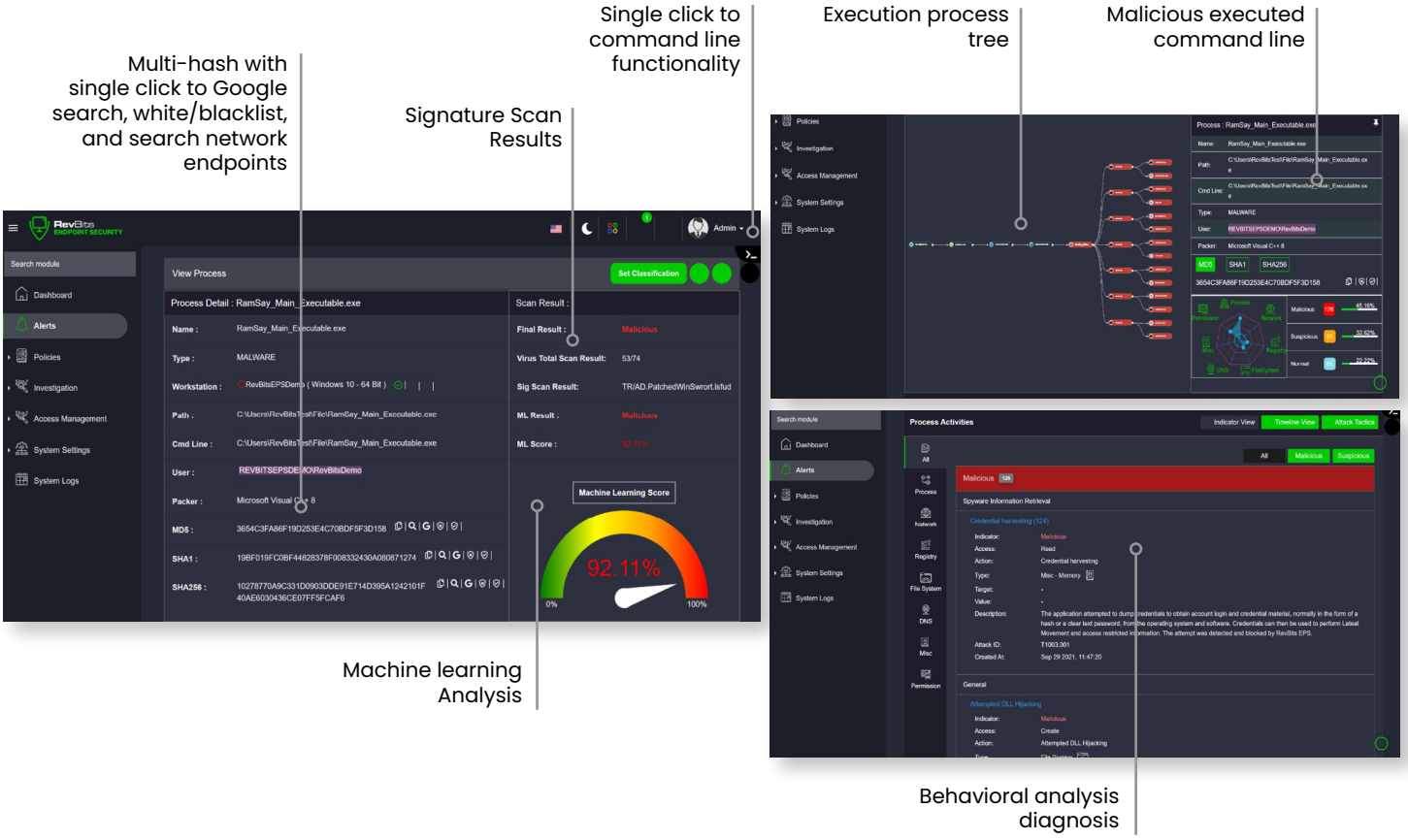
When ransomware is downloaded, it makes file system calls to find a document to encrypt, read the code, and write back encrypted files to the computer. It will do this again and again to as many documents and files as it can. However, when ransomware is within the RevBits transparent file system, the original files remain completely untouched. The ransomware assumes it has accomplished its objective. But it's actually confined, with all of the write to disk API calls sent to a temporary location, cached and documented.

Monitoring and analysis are conducted to understand how the malicious program operates, and what it tried to accomplish, including context and intent, and an extensive report is created. If a program is determined to be malware, RevBits EPS removes it and reports it. However, if it is deemed to be clean, RevBits EPS carefully applies all of the cached data to the computer's file system.

Bad actors outwit traditional sandboxes

Sandboxing is a proactive approach to detecting, analyzing and killing malware code within a safe and isolated environment to observe the code's activity. However, hackers are very familiar with this approach and have many ways to embed code that will detect when the program is inside a sandbox.

Hackers use many anti-sandbox techniques to frustrate attempts at analysis. They code malware to detect VM config files, executables, registry entries and other indicators. If the malware detects it's being run within a sandbox, it will respond accordingly, by simply not running.



RevBits Endpoint Security's (RB-EPS) main alert dashboard for an individual workstation. RB-EPS provides a feature rich robust GUI.

For more information, go to www.revbits.com

RevBits EPS transparent file system is different

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.

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.

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