RevBits®

PRODUCT BRIEF

Endpoint Security

RevBits EPS Detects and Blocks User Mode Direct Syscalls to Kernel

Hooking functions are one of the many ways advanced Endpoint Detection and Response (EDR) solutions determine if applications are malicious. Endpoint security solutions embed hooks into operating systems, like Windows, Linux and Mac. These hooks read and analyze sensors and data to see who is writing to files, deleting files, encrypting files, and launching processes. By analyzing this data, they make decisions to block or allow activity, and notify admins.

However, 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. BluStealer Loader is just one example of malware that uses direct syscalls to evade detection.

There are two types of EDR hooks. Ring0 (kernel mode) are low-level hooks that are placed deep into the kernel OS, monitoring activities like file system access and process creation. Ring3 (user mode) are higher-level hooks that monitor user actions like resizing a window, DLL injections, and executing process hollowing that enables hackers to remove legitimate code in an executable file and replace it with malicious code. To detect if an EDR has implemented hooks, hackers look at function call instructions, and use that information to bypass the EDR.

EDRs are vulnerable to direct syscall exploits

Two US Patents for a unique technological advancement All applications, whether legitimate or malware, begin their activity at the user mode, and then load drivers into the kernel. In user mode, user actions and EDR actions have equal privilege. When an EDR places hooks into a user application process to find out what it's calling, if that process is malicious it may attempt to "unhook" the EDR. However, the EDR will detect such action and terminate the process.

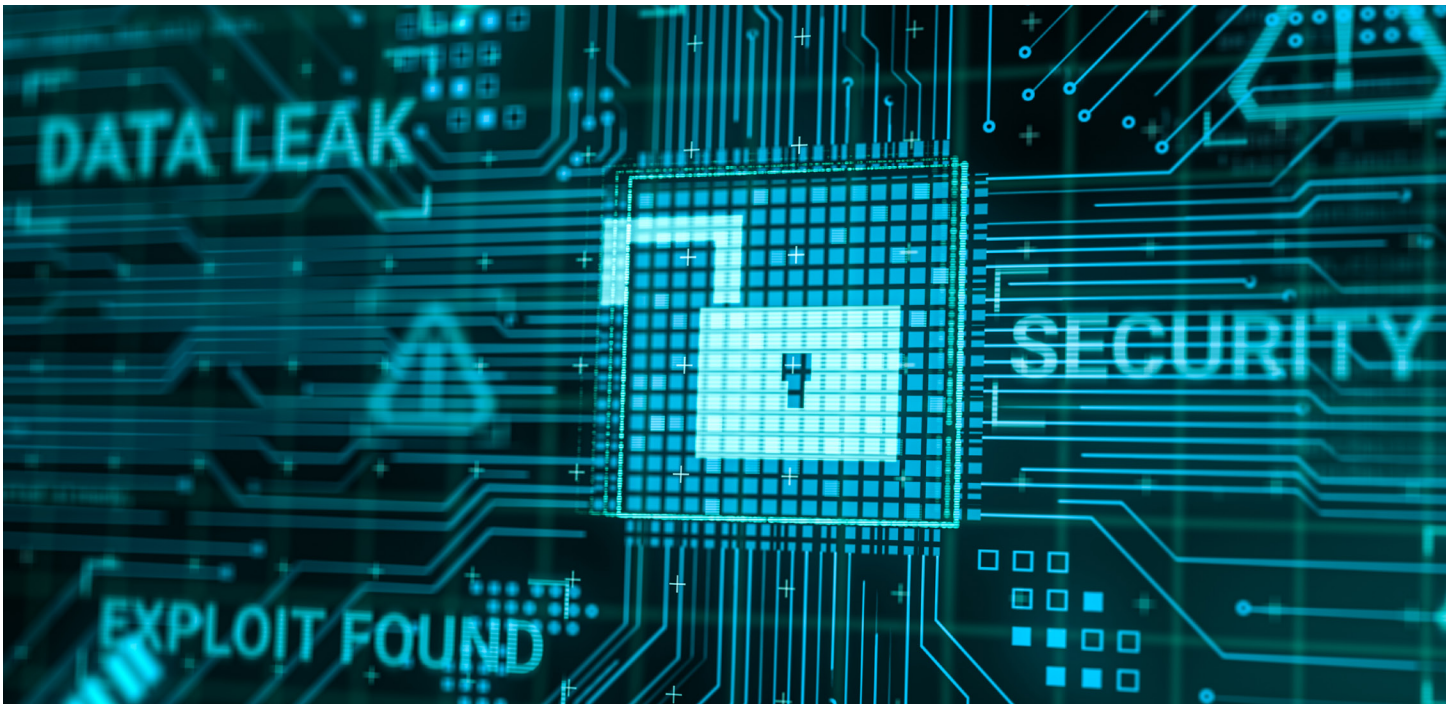
Advanced malware may use a method called "direct syscall" to bypass the EDR hooks. This technique avoids calling ordinary OS APIs (which are hooked by the EDRs), and instead, the malware determines the locations of syscalls in the OS memory and calls those directly using specially crafted memory structures. This lets the malware get straight into the kernel.

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.

Using a single function call, a hacker can bypass EDR hooks, escape detection, and inject their malware into the system. While in the past, this required a very sophisticated hacker today this capability is accessible to anyone who is inclined. Detecting and blocking direct syscall attacks is problematic with almost every EDR. They habitually become bogged down processing data, to the point where performance suffers at an unacceptable level.

RevBits EPS prohibits direct syscall bypass attempts

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 calls coming from suspicious modules, or memory that don't belong to any modules. In such case we know it is a direct call, and that malware tried to bypass the EDR. Protecting against malware using direct syscalls to evade EDR hooks is a difficult and growing cybersecurity problem. EDR vendors avoid this topic, even though they understand the devastation this malware exploit causes. Their solutions are inherently vulnerable, and hackers have the capabilities, tools and know-how to bypass them. For EDR customers, this is equivalent to leaving the hen house door open while the chickens are roosting, and a hungry fox is waiting for their opportune moment.

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.

Cybersecurity is all about layered, multi-functional capabilities, from data, applications, endpoints and network security; to email, perimeter and privileged access management and even human security. These, and more, represent the layers of security that organizations need to ensure a strong security posture.

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