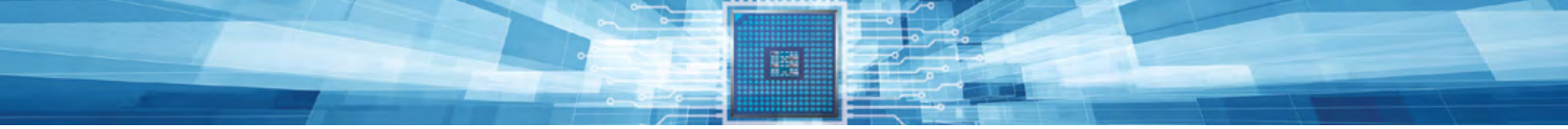
Deterministic Protection Against Fileless Memory-Based Cyber Attacks

White Paper



Introduction

Sophisticated cyber hacking is increasingly leveraging fileless, memory-based exploits. Unlike amateur "script kiddie" attacks, these attacks require a higher level of technical sophistication, and used to be regarded as arcane and rare. However, the recent wave of high profile attacks, such as WannyCry, Petya and Industroyer all took advantage of advanced tools developed by the NSA, and publicly leaked by the Shadow Brokers. Techniques that used to be limited to well-funded nation-state actors, have now been "democratized", dramatically raising the stakes for global cyber security.

This should be of tremendous concern to enterprises, given the near indefensible nature of memory-corruption and memory-based attacks. This paper examines this class of attacks and the limitations of current approaches in thwarting them. Also covered are the unique capabilities of the Virsec platform and its patented Trusted Execution™ technology, providing organizations with an effective defense mechanism against these insidious and growing threats.

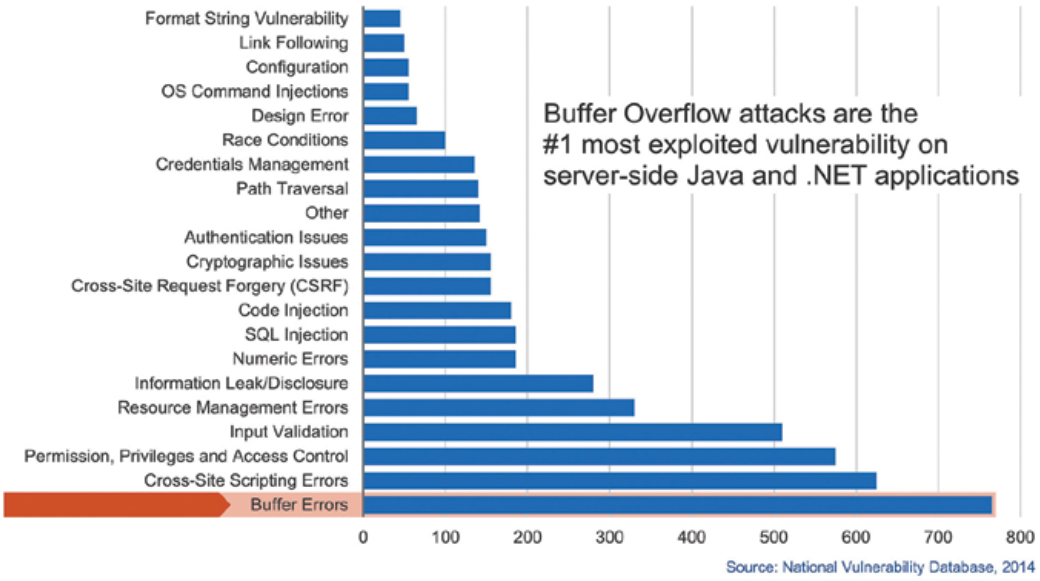
Memory Corruption Attacks are Pervasive

Memory corruption attacks were defined in 2010, covering techniques that allow attackers to alter the execution flow of a program by submitting crafted input to an application. This definition is adequate for past memory corruption attacks such as return-to-libc attacks.

However, since then, more sophisticated return-oriented programming (ROP) chain attacks have emerged as a leading malicious exploit on Windows-based servers. ROP chains are more insidious and have been proven to circumvent many of the OS mitigations introduced for prior memory-corruption attacks such as Address Space Layout Randomization (ASLR) Data Execution Prevention (DEP). ROP chains can manipulate an application's legitimate instruction sequences, known as gadgets, to execute malicious code when chained in a specific and unexpected ways. While memory corruption attacks may seem arcane and require patience to understand, a typical enterprise computing infrastructure provides plenty of vulnerabilities and opportunities to exploit them. According to the National Vulnerability Database (managed by NIST and US-CERT), buffer errors consistently rank as the most frequent vulnerabilities found in applications.

This is a significant problem as well-crafted buffer overrun exploits can be the starting point for attacks such as remote code execution that can give an external hacker direct access to an internal network.

In summary, memory-based attacks comprise the most insidious threats to critical applications, exploit the most common vulnerability in applications (buffer overflows), and represent the most frequently used advanced exploit over the past two years. Given that no new mitigations have been introduced in the past several years to deal with these attacks, it is no wonder that many IT professionals regard memory attacks as "indefensible" by today's security products.



Graphic A: *NVD Categories Covered*

The Challenge of Stopping Memory-Based Cyber Attacks

Almost every week we see new examples of well-funded enterprises, such as Home Depot, Target, Sony, and even the NSA, becoming victims of the latest security breach. These attacks are circumventing staple security products such as next-gen firewalls, IDS/IPS systems, web and endpoint security defenses, web application firewalls and database monitoring solutions. Breaches continue to happen at an increasing rate, and with more severe consequences.

While substantial sums have been spent on network and endpoint-based security, these breaches reflect a general lack of investment in adequate application security. This has continued despite repeated surveys pointing to applications and OS vulnerabilities as the largest areas of enterprise security exposure.

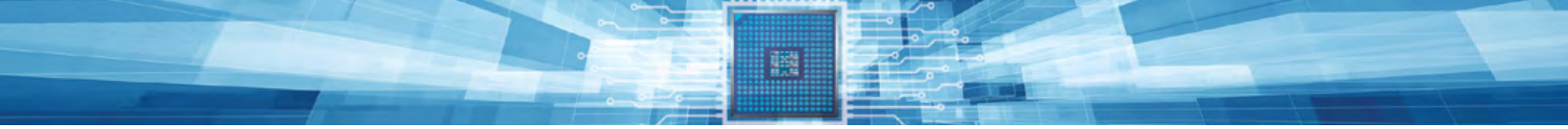
Below are five key reasons why memory-based attacks evade existing security solutions today:

1. Memory-based attacks cannot be identified via signature

Buffer errors, return-to-libc attacks, and many other memory corruption exploits, attack the call stack or memory registers of an application in non-repeating ways. This presents problems for traditional security solutions because most approaches are based on pattern matching, using signatures of past malware or malicious actions. While some endpoint vendors promote defenses against "memory exploit techniques", they are still based on signatures and pattern matching of pieces of existing executable code. Today's advanced attackers are innovative and resourceful and easily avoid repetitive behavior that can be detected by pattern matching.

2. Most security defenses focus on network protection and authorization, while memory-based attacks happen in the guts of applications

Today's advanced attacks are aimed at high value targets, take place in the memory of an application, and manipulate the application's execution path. By the time a successful memory-based attack makes a network transmission, it is doing so over normal channels and will evade detection. Most enterprise



security strategy is built on an authentication/authorization model, network checkpoints and sandboxes that sample or inspect moving packets across the network. However, memory-based attacks typically use phished or insider credentials with escalated privileges or they use remote OS commands to execute such as PowerShell. These techniques make memory threats, such as ROP chain attacks invisible at the packet level.

3. Endpoint security is pervasive in enterprises but lacks the ability to stop fileless exploits

Focusing on the endpoint has become a popular model as traditional perimeter security is disappearing. But most endpoint technologies focus on end user devices, and less on core, high-value servers. Other technologies such as host-based IPS (HIPS), app control, file whitelisting, and server endpoint suites, also have significant limitations against memory-based attacks, and are known for producing large quantities of false positives. File whitelisting is growing in use, but misses most memory-based attacks which use legitimate applications that are allowed to run in a file whitelist environment.

4. "Application Security" solutions focus on eliminating code vulnerabilities, not securing applications at run-time

While most memory-based attacks target enterprise applications, the majority of application security solutions focus only on identifying and remediating vulnerabilities in developer code. Relying on developers to find and eliminate all weaknesses is not adequate. Most developers prefer to focus on application features over security, and have limited experience in risk management, and enterprise security automation across large numbers of applications and 3rd-party components. Additionally, these solutions tend to be imprecise in identifying advanced attacks and generate larger numbers of false positives.

5. Most companies fail at systematically patching vital applications and host OS binaries

A study by Trustwave found that 58% of companies did not have a mature patch management strategy in place and 12% did not have one at all. Keeping up with patching is a significant challenge for many organizations that have a wide range of heterogenous servers, many of which may no longer receive updates. Advanced hackers have become adept at scanning networks to identify unpatched systems and target vulnerable applications with zero-day exploits. Verizon's Annual Data Breach Report confirms that most breaches occur using vulnerabilities for which CVE (common event vulnerability) or patch has existed for several years, but not been deployed consistently.

Trusted Execution™

The Virsec platform enables enterprises to protect their most valuable applications and data from fileless, memory-based attacks. Virsec's patented Trusted Execution™ technology delivers a radically new approach to threat detection that is specifically designed to protect against application-based exploits involved in data breaches or more complex, long chain cyberattacks. Trusted Execution enables applications to defend themselves at runtime in a deterministic and highly precise manner.

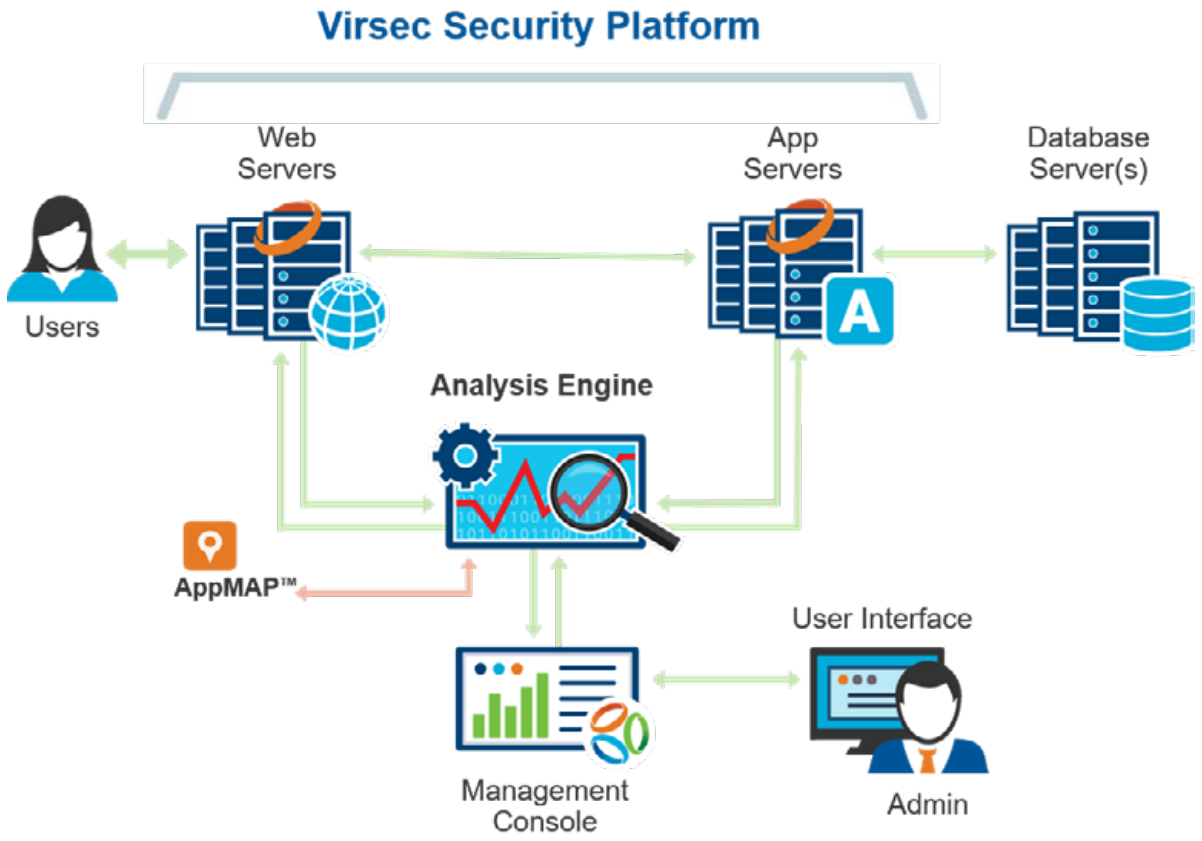
This approach differs from legacy security detection and monitoring solutions, by focusing on execution integrity. Rather than relying on pattern matching of past malicious events or malware, Virsec monitors application processes down to the memory level and ensures that they stay on their legitimate control flow paths. By ensuring applications execute in the manner intended by their original coding, the protection extends to all threats, including zero-day exploits on unknown vulnerabilities.

Because Trusted Execution focuses on the known, acceptable behavior of an application, it can detect and protect against never-before-seen, unknown attacks on vulnerable code. Virsec effectively closes the window of exposure organizations face with zero-day vulnerabilities and the attacks that exploit them.

Virsec also provides precise, contextual granularity. By working deep in the guts of an application process, the solution continuously monitors and protects the CPU execution of all processes of the application in memory. In this way, Trusted Execution uniquely detects and helps prevent breaches from fileless exploits that can only be detected in memory, through intimate knowledge of the application process being attacked. All application binaries are profiled during load time to produce an AppMAP™, which is used to ensure an application's execution integrity.

Because of the deterministic nature and absence of any "guessing" for indicators of compromise or attack, Virsec produces no false positives in protecting an application from memory corruption events and attacks on compiled binaries.

Protected application binaries are instrumented with a lightweight probe, which communicate with a remote Analysis Engine for security detection. The Virsec Management Server acts as the central coordination point for the solution for various administrative and system functions.



Graphic B: Deployment Overview

Key Design Capabilities

Low Performance Impact – Performance testing has shown that Virsec adds less than 5% CPU performance impact on protected applications. This low impact is achieved by separating collection of inspection events from analysis processing, which takes place remotely from the application being protected.

Ease of Deployment – Applications are instrumented dynamically as they load into memory, providing simple deployment for any Windows or Linux applications. The solution supports both 64-bit systems and older 32-bit servers, without requiring any modifications, or updates to source code.

Microsecond Detection – Trusted Execution enables real-time detection of memory-based attacks on protected application processes and reacts within microseconds. Security analysts can be notified as soon as suspicious events occur to enable proactive action to thwart attacks before serious harm is done. In addition, the Virsec Protection Engine can immediately block suspicious access, or connect to other network security devices via an API. Virsec eliminates the large windows of threat dwell time (weeks, months) that have become characteristic of advanced persistent threats on breached organizations.

Full-Stack Application Protection

With the growing use of web applications, memory-based attacks are increasingly used in conjunction with traditional attacks on interpreted, server-side languages such as Java and PHP. Well-documented web application attacks such as path traversal, privilege escalation and file upload attacks can provide the starting point for execution of malicious code that ultimately takes advantage of vulnerabilities enabling memory-based attacks.

Virsec also enables protection of web applications against the OWASP Top Ten and similar web attacks. With a single platform, the solution delivers memory-level protection and real-time detection of web application attacks such as SQL injection and XSS (cross-site scripting). This delivers comprehensive, full-stack defense against hacking attacks that may lead to data breaches.

Conclusion

Virsec and its Trusted Execution technology represents a powerful new approach for organizations to protect their critical applications against the growing use of memory-based attacks from advanced hackers. Unlike existing security approaches or OS mitigations, the approach is deterministic and highly accurate, eliminating exposure from data breaches through this previously indefensible vector of attack.

More information is available at www.virsec.com.

Virsec®

Headquarters:
226 Airport Parkway, Suite 350 • San Jose, CA 95110

Email: info@virsec.com • Phone: (877) 213-3558 • Web: www.virsec.com • Twitter: virsecsystems