TECHNICAL SOLUTION BRIEF

Bitdefender

Security

Anti-Exploit for Windows

www.bitdefender.com

Preventing Exploits on Windows Systems

A core aspect of Cloud Workload Security is that cloud workloads run on servers in an on-premises datacenter or an external datacenter, such as public cloud infrastructure-as-a-service or other hosted services. Unlike end-user systems, cloud workloads often have direct access to sensitive data, and have a one-to-many footprint. Many users – internal, external, employees and customers – leverage the solutions these workloads power. The breach of a cloud workload, whether data exfiltration, file-less attack, or ransomware, impacts an organization significantly. Securing servers and the workloads they host is a critical part of a comprehensive Cloud Workload Security strategy.

Vulnerabilities, Exploits and Attacks

Vulnerabilities are faults in the software stack – operating system or applications – that give an attacker the chance to access a system. An exploit is a method of taking advantage of a vulnerability to gain access to a system. An attack is the use of an exploit against vulnerable systems to achieve a desired outcome, such as exfiltrating data or encrypting valuable information to hold for ransom.

An oft-cited example is EternalBlue and WannaCry. EternalBlue is an exploit kit developed to take advantage of a Windows SMB vulnerability that was not previously exposed – a zero-day. The EternalBlue exploit kit was allegedly developed by an American intelligence agency and leaked by a foreign attacker. While patches for the vulnerability were developed quickly, attackers leveraged the exploit kit to spread malware such as the WannaCry ransomware payload faster than organizations patched their systems.

Tools that prevent the exploit of vulnerabilities in a generic fashion are extremely important. Even after a zero-day becomes yesterday's exploit, organizations often struggle to deploy patches on their most critical assets before attackers take advantage.

What to look for

- A complete prevention stack managed from a single console
- Applicability across multi-, hybrid-cloud, end-user and server
- Kernel- and user-mode protection, including Virtual Desktop Infrastructure (full-session, terminal services hosts, Remote Desktop Protocol)
- Kernel memory protection to stop privilege escalation and LSASS leaks
- User memory protection to address the most common sources of risk, such as web browsers and plug-ins, productivity tools and utilities, and other commonly exploited applications

Bitdefender Windows Anti-Exploit

Bitdefender Windows anti-exploit capabilities focus on prevention. We recognize that the malware payload (if any) is the symptom of a breach, not the cause. Stopping an attack before a foothold is achieved is ideal. Whether or not an attack succeeds, investigators require straightforward information and in-depth tools to navigate the attack chain to determine the root cause.

Various security techniques, such as Address Space Layout Randomization and application/process whitelisting bring value, but don't cover the risk spectrum. Vulnerabilities in Windows operating systems – servers and end-user - and the applications they run pose a serious risk. To put it simply, sometimes a trusted application goes bad.

Bitdefender anti-exploit techniques use a wide variety of detection and mitigation capabilities. Following is a list – always evolving based on our leading threat intelligence – that offers insight into Bitdefender's prevention and detection controls:.

Note that individual detections can be configured to be enabled, disabled, or report-only, providing flexibility when deploying Bitdefender anti-exploit.

Server Platform Coverage

Bitdefender Windows Server anti-exploit technology is available to all GravityZone customers hosting cloud workloads on the following operating systems:

- Windows Server 2019
- Windows Server 2019 Core
- Windows Server 2016
- Windows Server 2016 Core
- Windows Server 2012 R2
- Windows Server 2012
- Windows Small Business Server (SBS) 2011
- Windows Server 2008 R2

Examples of Proactively Blocked Exploits

- CVE-2015-2419 – JScript 9 in Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code used in “Double Free” exploit kits
- CVE-2016-4117 – 0-day Flash exploit used in targeted attacks
- CVE-2018-8174 – 0-day VBScript used in targeted attacks (dubbed “Double Kill”)
- CVE-2021-1732 – 0-day Win32k Elevation of Privilege, exploited by BITTER APT in targeted attacks

User-mode detection

- Making executable the memory pages for data
- Hijacking the code flow using the ROP technique, by validating call targets
- Hijacking the code flow using the ROP technique, by validating stack location
- Corrupting the stack using the ROP technique, by validating the stack address alignment
- Executing code directly on stack using the ROP technique, by validating return address range
- Corrupting the stack using the ROP technique, by validating the stack page protection
- Flash Player exploitation attempts
- Executing malicious code into Flash Player, by scanning Flash objects in memory
- VBScript exploitation attempts
- Creating new processes or download files, using shellcode
- Executing code via network paths, using shellcode
- Bypassing security checks for creating new processes
- Accessing sensitive system functions from DLL exports
- Injecting malicious code by validating newlycreated threads
- Creating a reverse shell, by scanning executable memory pages
- Creating new processes using obsolete techniques
- Hijacking the code flow using the ROP technique, by validating executions inside Equation Editor
- Code execution through remotely bound monikers via office macros
- Attempts of malicious code to access sensitive system functions from DLL imports
- Executing sensitive system functions by abusing object virtual tables

User-mode mitigation

- Enforce Data Execution Prevention (DEP) to block the running of code from data pages

Kernel-mode detection

- Prevent processes from gaining unauthorized privileges and access to resources

Kernel-mode mitigation

- Prevent processes from reading the memory of the lsass.exe process and obtaining credentials to use for lateral movement / migration to other systems within the organization.

Supported Across

Conclusions

In modern workload stacks, from the underlying hardware to containers, vulnerabilities are inevitable. That can leave people and organizations feeling as though the attackers are in control. However, the security mechanisms in place to prevent the exploitation of vulnerabilities are in your control. When looking for anti-exploit security, ask your vendor if their anti-exploit controls are built for servers and end-user systems, and delve into the how and why. Your cloud workloads, on-premises or hosted, are the most critical assets in your environment. They deserve comprehensive protection. Bitdefender has created anti-exploit solutions to protect your workloads wherever they run, to thwart attacks and give your teams insight and control.

About Bitdefender

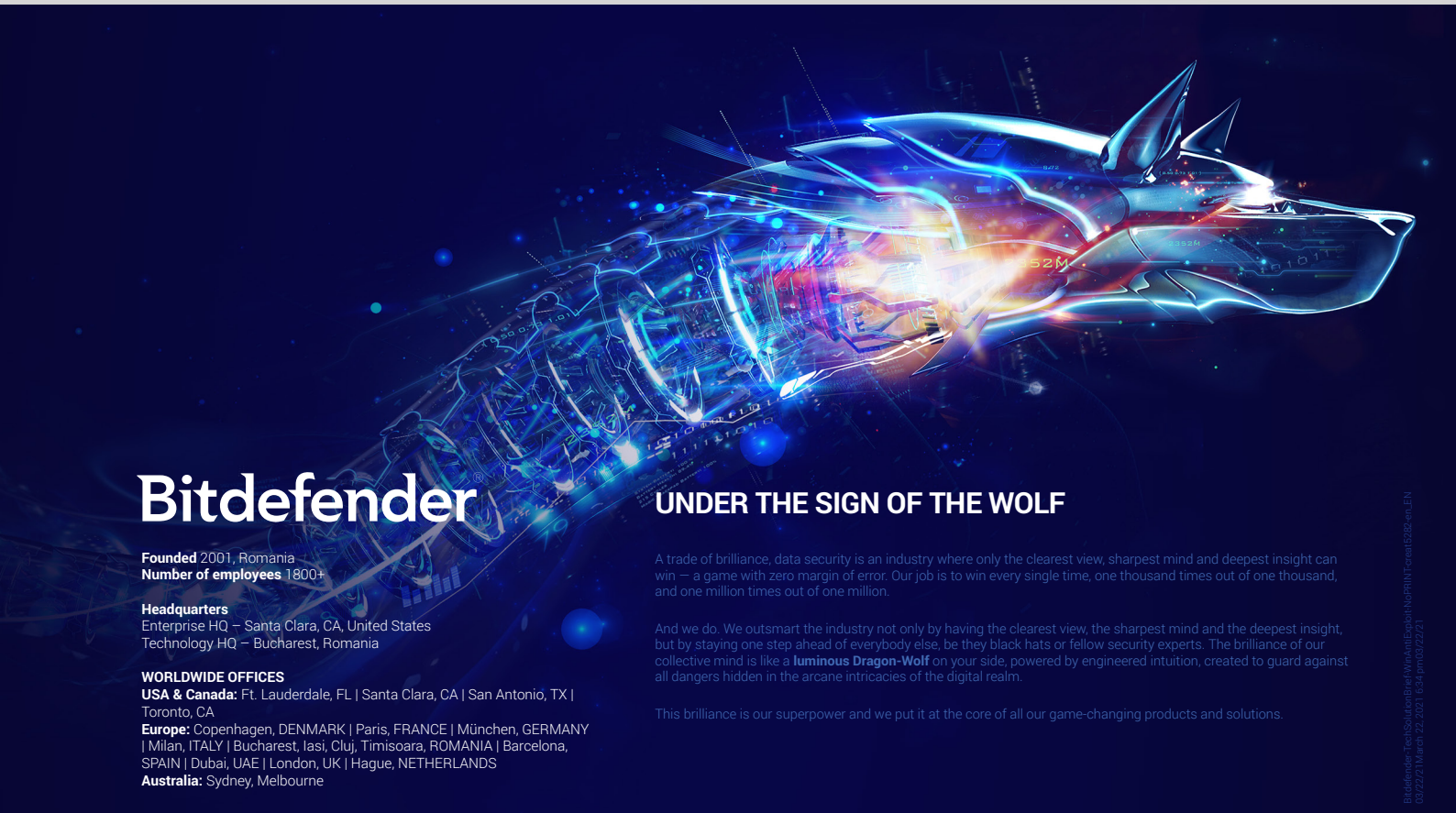
Bitdefender is a cybersecurity leader delivering best-in-class threat prevention, detection, and response solutions worldwide. Guardian over millions of consumer, business, and government environments, Bitdefender is the industry's trusted expert* for eliminating threats, protecting privacy and data, and enabling cyber resiliency. With deep investments in research and development, Bitdefender Labs discovers 400 new threats each minute and validates 30 billion threat queries daily. The company has pioneered breakthrough innovations in antimalware, IoT security, behavioral analytics, and artificial intelligence and its technology is licensed by more than 150 of the world's most recognized technology brands. Founded in 2001, Bitdefender has customers in 170 countries with offices around the world.

For more information, visit https://www.bitdefender.com.

RECOGNIZED BY LEADING ANALYSTS AND INDEPENDENT TESTING ORGANIZATIONS

TECHNOLOGY ALLIANCES

*Bitdefender has ranked #1 in 54% of all tests by AV-Comparatives 2018-2021 for real-world protection, performance, malware protection & advanced threat protection.



Bitdefender

Founded 2001, Romania
Number of employees 1800+

Headquarters
Enterprise HQ – Santa Clara, CA, United States
Technology HQ – Bucharest, Romania

WORLDWIDE OFFICES
USA & Canada: Ft. Lauderdale, FL | Santa Clara, CA | San Antonio, TX | Toronto, CA
Europe: Copenhagen, DENMARK | Paris, FRANCE | München, GERMANY | Milan, ITALY | Bucharest, Iasi, Cluj, Timisoara, ROMANIA | Barcelona, SPAIN | Dubai, UAE | London, UK | Hague, NETHERLANDS
Australia: Sydney, Melbourne

UNDER THE SIGN OF THE WOLF

A trade of brilliance, data security is an industry where only the clearest view, sharpest mind and deepest insight can win — a game with zero margin of error. Our job is to win every single time, one thousand times out of one thousand, and one million times out of one million.

And we do. We outsmart the industry not only by having the clearest view, the sharpest mind and the deepest insight, but by staying one step ahead of everybody else, be they black hats or fellow security experts. The brilliance of our collective mind is like a **luminous Dragon-Wolf** on your side, powered by engineered intuition, created to guard against all dangers hidden in the arcane intricacies of the digital realm.

This brilliance is our superpower and we put it at the core of all our game-changing products and solutions.

Bitdefender-TechSolutionBrief-WinAntiExploit-NoPRINT-creat5282-en-EN
03/22/21March 22, 2021 6:44 pm03/22/21