Memory Protection
Technical Brief

Multi-Stage Detection Techniques: **1.** Machine Learning **2.** Hyper Detect **3.** Sandbox Analyzer **4. Memory Protection** **5.** Process Inspector

Overview

In the current cybersecurity landscape, threat actors are always probing and constantly switching tactics, making companies susceptible to malware incidents and outbreaks, business disruption and data breaches. Bitdefender GravityZone Endpoint Security Platform defends your endpoints from the full range of sophisticated cyber-attacks with high efficacy, low end user impact and low administrative overhead. It consists of multiple layers of defenses to ensure that the bad guys keep stumbling over various impediments that these layers put in their way. Each layer is designed to stop specific types of threats, tools, or techniques, covering multiple stages of the attacks. The Bitdefender Memory Protection layer is part of the GravityZone Endpoint Security platform. It provides protection against known and unknown exploits targeting browser and application vulnerabilities in on-execution stage.

Detection Stage	Technology Type	Threat Coverage
On-Execution	Exploits	Phishing Attacks, Malvertizing, Drive-by Downloads, Fileless attacks, Social Engineering attacks, OS and Application vulnerabilities, privilege escalation, process injection

Understanding the importance of Memory Protection

An exploit is an attack that takes advantage of a vulnerability to compromise computers and infect them with malware. Many malware outbreaks, including ransomware attacks, are caused by exploits. Threat actors often use an exploit kit readily available on the black market to launch attacks and find new victims. An exploit kit is a toolkit that automates the exploitation of client-side vulnerabilities that exist in commonly used end user applications such as browsers, Microsoft Office applications and Adobe Reader. When a potential victim's browser connects with a website hosting an exploit kit, the kit probes the end user's system and extracts information such as OS version and browser type, to find vulnerabilities to exploit. Once the threat actor identifies a vulnerability, a malicious payload is delivered on the system and the attack is launched.

Although numerous old and new vulnerabilities continue to exist in applications, threat actors still use a relatively small number of exploitation techniques. Bitdefender's memory protection technology defends against these exploitation techniques to prevent known and unknown attacks.

Features

- Protects commonly used end user applications including:Browser, Browser components, PDF readers, Microsoft applications
- Contains several different advanced mechanisms for exploit detection to protect against operating system security bypass and memory corruption: Caller check, Stack pivot, Execute recently allocated memory, Executable stack, Return to stack, Thread to recently allocated memory, Shellcode action, Flash function pointer overwrite

Benefits

- Detect advanced attacks early and prevent breaches, reduce incident response costs and efforts.
- Reduce threat-hunting burden.
- Memory Protection greatly increases detection rate of zero-day threats including Phishing Attacks, Malvertizing, Drive-by Downloads, Fileless attacks, Social Engineering attacks, privilege escalation, and process injection.
- It forms part of a single, integrated endpoint security agent and central management platform, greatly reducing administrative burden. Customers don't need to deploy a mixture of endpoint security solutions.

Bitdefender is a global security technology company that provides cutting edge end-to-end cyber security solutions and advanced threat protection to more than 500 million users in more than 150 countries. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a provider of choice in both hybrid infrastructure security and endpoint protection. Through R&D, alliances and partnerships, Bitdefender is trusted to be ahead and deliver robust security you can rely on. More information is available at http://www.bitdefender.com.

FOR MORE INFORMATION VISIT: bitdefender.com/business

BD-NGZ-Dec.05.2017-Tk#:
Bitdefender-2017-TechnicalBrief-MemoryProtection-crea2103-A4-en_EN-2