Bitdefender
BUILT FOR RESILIENCE

Exploit Defense

Security Challenges

Attackers look for the highest probability of success and the path of least resistance, when attempting to compromise a system. They design attacks to take advantage of common human behavior, such as opening an email attachment or clicking on a URL. These simple actions can compromise business security, as attackers target vulnerabilities in applications installed on almost every computer in the world – browsers, document readers, and productivity applications— they use the vulnerabilities as back doors to disrupt systems, exfiltrate data, ransom files, and more.

Security vulnerabilities can often be mitigated through patching affected software, however, keeping every application updated in a modern business of any size is a daunting task for many reasons:

- New application versions are constantly being released
- Administrators don't always have full visibility into installed applications
- Avoiding application downtime is a continuous challenge
- Complex bring-your-own-device ecosystems have become the norm
- Users often access company data on their own personal device

In addition, applications— such as Microsoft Office, Adobe Reader, web browsers, and more— are increasingly becoming more complex, making it harder than ever to secure them, since frequent updates often introduce new flaws to be exploited. Supply-chain attacks are also becoming increasingly more prevalent, as attackers are targeting the software manufactures themselves and planting their malicious code in genuine software updates released by the manufacturers as signed code.

Attackers develop tools designed to take advantage of errors in software code called exploit techniques. These tools can detect the version of the software installed, and then use a variety of tactics that specifically target known security holes in that software version. The techniques that attackers use continually evolve, meaning that traditional detection methods are useless against this enormous variety of malware.

Detection Overview

Early in the history of exploits, techniques like stack overflows allowed attackers to hijack code execution. As a result, various mitigation techniques were implemented at the operating system level like DEP (Data Execution Prevention), ASLR (Address Space Layout Randomization) and SEHOP (Structured Exception Handling Overwrite Protection), amongst others. This helped to reduce exploitation risk, but malicious actors developed ways to work around such operating system-level defense. An example of an evolved exploit technique is Return Object Programming. Using this technique, an attacker hijacks the order in which information is used in software code by

At-a-Glance

Bitdefender Exploit Defense is an advanced anti-exploit capabilitiy which protects businesses from attacks designed to exploit software vulnerabilities in common applications running on Windows systems and prevents common exploits targeting Linux environments.

This capability actively monitors runtime processes and exploit techniques using heuristics, rather than only monitoring for specific attacks using traditional signature-based detection. It identifies and protects against zero-day attacks and other emerging threats.

Key Capabilities

- **Protects popular applications** – prevents exploit techniques from successfully compromising commonly-used applications like Office Suites, PDF readers, web browsers and more.
- **Monitors memory and operating system kernel for suspicious activity** – thwarts exploit attacks that target the Windows application memory space and Linux kernel.
- **Protects against zero-day and emerging threats** – focuses on exploit technique and not specific attacks.
- **Provides security teams with insights into compromised applications** – allows security teams more time to patch software vulnerabilities

"GravityZone generates reports in minutes compared to an hour or more so we can identify root causes and resolve issues more easily. With these time savings, we've limited our headcount increases in IT, even as Tyler has made multiple acquisitions and added staff"

Dan Leming, IT Manager, End User Services, Tyler Technologies

manipulating the structure that stores the informaton in memory. The attacker is able to bypass the operating system defenses in most scenarios except for executables with very strict restrictions for running. By compromising legitimate applications, these types of attacks typically go undetected by standard antivirus solutions

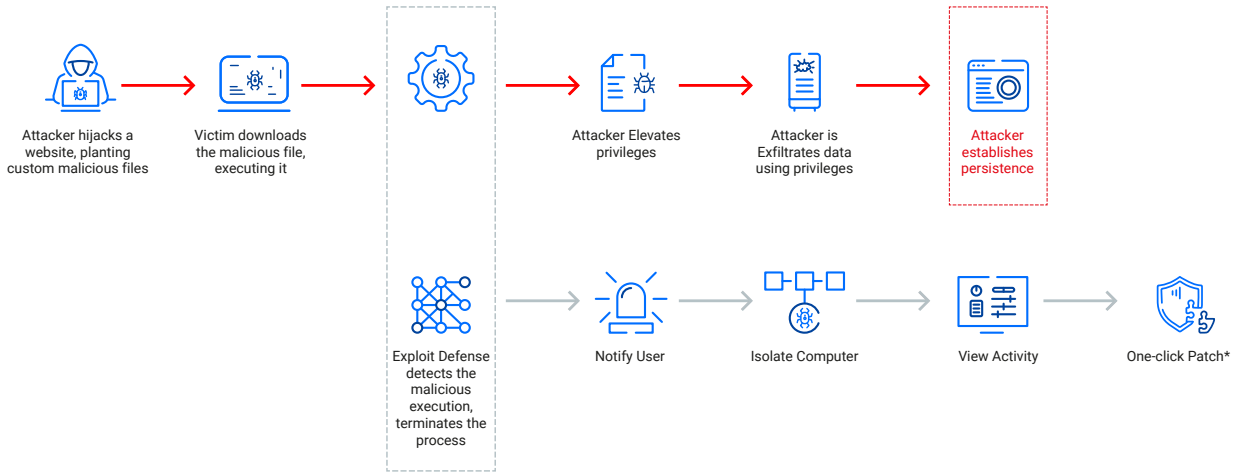

Figure 1.1: A zero-day exploit is used to target a specific, unpatched version of Microsoft® Word, which allows an attacker to access the system and steal valuable data from the victim. With Bitdefender Exploit Defense, the malicious script execution is detected and the process terminated, preventing the exploit from succeeding.

Response Overview

GravityZone Exploit Defense monitors for exploitation attempts using a heuristic model. Instead of relying on signature detection, our model inspects for rules and algorithms associated with exploit techniques. This allows us to detect specific exploits that have been seen in the past, and unknown, or zero-day attacks --newly developed exploits without prescedent. The capability uses real-time threat intelligence from Bitdefender Labs, which is sourced from hundreds of millions of sensors globally and continuously identifies emerging exploit techniques and updates our heuristic detections.

Exploit Defense can block calls to API functions that allow malicious code to run with elevated privileges. Our advanced anti-exploit technology can obstruct Visual Basic scripts and can scan Flash objects in memory for exploits. It can detect and block the creation of child processes from Microsoft Word and other productivity applications. Exploit Defense can detect applications trying to read the memory from the Windows Local Security Authority Server Service (LSASS) that stores passwords, pins, access tokens, and other credential information.

Bitdefender also protects against kernel-mode, post-exploitation attempts in Linux environments that can allow an unprivileged local user to gain write access to read-only memory spaces, giving the attacker elevated access to the system. These are just a few examples of the exploit techniques Bitdefender is capable of detecting to prevent new or zero-day attacks

Exploit Prevention

When Bitdefender detects behavior associated with an exploit, the offending process can be terminated to protect the vulnerable application or the activity can be reported as an incident for investigation.

With Bitdefender Endpoint Detection and Response (EDR) -- included with GravityZone Business Security Enterprise and also available as a standalone solution -- an incident record is generated when an exploit attempt is detected. Security teams can then review the results of our automated root cause analysis to understand the user and system behavior that led to the detected exploit.

Using Bitdefender EDR, IT and security teams can perform actions such as isolating the affected machine while they perform their investigation and, when combined with Bitdefender's Patch Management, can patch the vulnerable application with a simple click of a button.

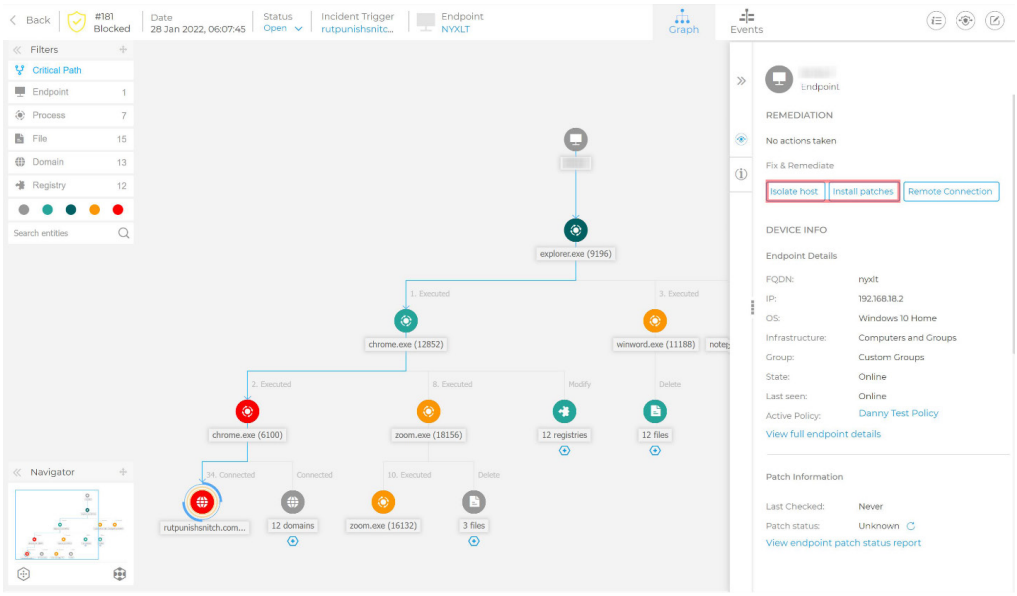

Figure 2.1: Bitdefender EDR enables security teams to review the critical path of an exploit attack, providing full visibility into compromised software. Teams can then isolate the host until the investigation is complete and also patch the vulnerable software with a simple press of a button

Memory Space Protection

Exploit Defense continuously monitors process memory space by running structural analysis during key execution points. Structural analysis allows us to understand the overall functionality of the system and how its designed to behave. By doing this, Exploit Defense thwarts malicious actors from pulling credentials by dumping the LSASS from memory to disk. Elevated privileges are required to access the LSASS data in memory. By moving the LSASS process to disk, this prevents the attacker from gaining the privileged access necessary to acquire this data. If an attempt is made to access this data from LSASS, Exploit Defense can report on the activity and immediately kill the process responsible for the behavior

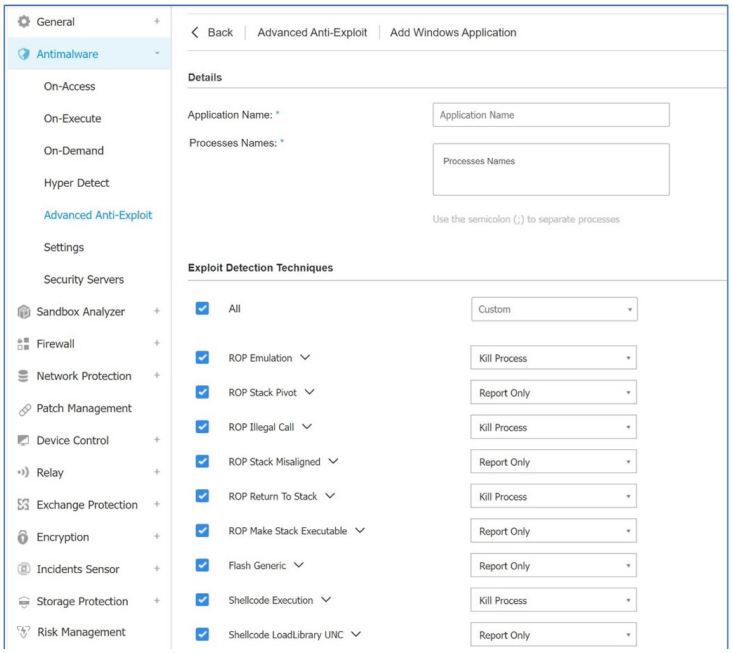

Figure 2.2: Using simple-to-use policies, additional applications can be added to the Bitdefender Advanced Anti-Exploit monitoring pool

Reduced Attack Surface

Bitdefender Exploit Defense provides modular controls that harden security and prevent a hostile takeover by threat actors. New zero-day vulnerabilities as well as published CVEs – a catalog of publicly disclosed cybersecurity vulnerabilities – can be mitigated by setting aggressive controls against techniques like return-oriented programming (ROP) or Shellcode Execution.

In addition to safeguarding popular applications, an administrator can add other software for Bitdefender Gravityzone to monitor through easy-to-use policies, thus, extending Exploit Defense to address customer-specific needs.

Emerging Threats Protection

Exploit Defense uses Deep Process Introspection (DPI) technology to detect memory exploits, memory injections, and privilege escalation techniques for all running processes. DPI is an operating system and architecture agnostic technology that can identify an ever-expanding list of exploit techniques for several pre-configured applications – such as widely-used browsers and office suites – as well as custom applications added by the security team through the GravityZone policies. The Deep Process Inspection technology carefully curates the techniques to identify those capable of exploiting a process, while ignoring those that can lead to false-positive alerts. The technology helps security teams become more efficient by allowing them to focus their resources on addressing actual threats.

Complete Protection Against Vulnerabilites

Bitdefender Exploit Defense paired with Bitdefender Risk Management helps provide protection against and comprehensive visibility into software vulnerabilities. With the addition of Bitdefender Patch Management, critical software patches can be deployed with an easy-to-use, intuitive tool -- all managed from the same console.

Bitdefender
BUILT FOR RESILIENCE

3945 Freedom Circle
Ste 500, Santa Clara
California, 95054, USA

Bitdefender BSG ExploitDefense TechnicalBrief DEX4889-en_EN
CD-FB/17/2022 MD-49/05/2022