TLP: WHITE

ESET DEEP BEHAVIORAL INSPECTION

Authors:
Ondrej Kubovič, ESET Security Awareness Specialist

with contributions from

Előd Kironský, ESET Head of Core Technology Development
Mateusz Wójcik, ESET Senior Specialized Software Engineer
Peter Košinár, ESET Technical Fellow

CONTENTS

Authors:
Ondrej Kubovič, ESET Security Awareness Specialist

with contributions from

Előd Kironský, ESET Head of Core Technology Development
Mateusz Wójcik, ESET Senior Specialized Software Engineer
Peter Košinár, ESET Technical Fellow

January 2020

INTRODUCTION

Today's cybercriminals will go to great lengths to achieve their ultimate goal – stealing information, computing resources or money. Apart from social engineering techniques such as lying, extorting and manipulating victims, they employ technical tricks designed to help their code avoid detection by built-in as well as third-party security solutions.

However, no amount of updating, repacking, obfuscating or modifying can change the essence of what the malware does in the end, namely: act maliciously on the targeted system. This is one of the things that allows ESET solutions to use some of their multiple layers to identify and block known as well as emerging threats.

In this document we will describe the inner workings of one such layer – designed specifically to perform advanced behavioral analysis and detection – named **ESET Host-based Intrusion Prevention System (HIPS)**.

We will also look at some of its components and provide a more detailed look into **Deep Behavioral Inspection**, a recent addition to the HIPS layer. Deep Behavioral Inspection, released early in 2019 with version 12.1 of ESET consumer solutions, includes new detection heuristics and enables an even deeper monitoring of unknown, suspicious processes.

DEEP BEHAVIORAL MONITOR

Microsoft has invested a lot of effort into making its operating systems more and more secure. While every new protective feature has made new versions of the system more stable, they also have made it quite difficult for security solutions to monitor some malware-related activity.

To uncover such activity nowadays, a deeper and more granular user-mode monitoring of API calls is necessary. To meet this requirement, ESET added the Deep Behavioral Inspection (DBI) component with its new detection heuristics, to the existing HIPS layer in its endpoint products.

DBI creates hooks within unknown, potentially harmful processes, monitoring their activity and requests to the operating system. If malicious behavior is detected, DBI mitigates the activity and informs the user.

If the process is suspicious, but does not show clear signs of malicious behavior, HIPS can use the data gathered by DBI and run further analysis via its other components. If necessary, HIPS can also request additional examination via technologies outside HIPS that are part of the broader ESET scanning engine.

Based on all these outputs, the process is then identified as clean, or potentially unwanted, or malicious.

It is true that modifications of the malicious process – performed by DBI – can trigger anti-sandboxing mechanisms built into the malware. However, this is of benefit to the user, since often such malicious code will not run its course when a virtual, emulated or otherwise monitored environment is suspected, and will thus inflict no harm.

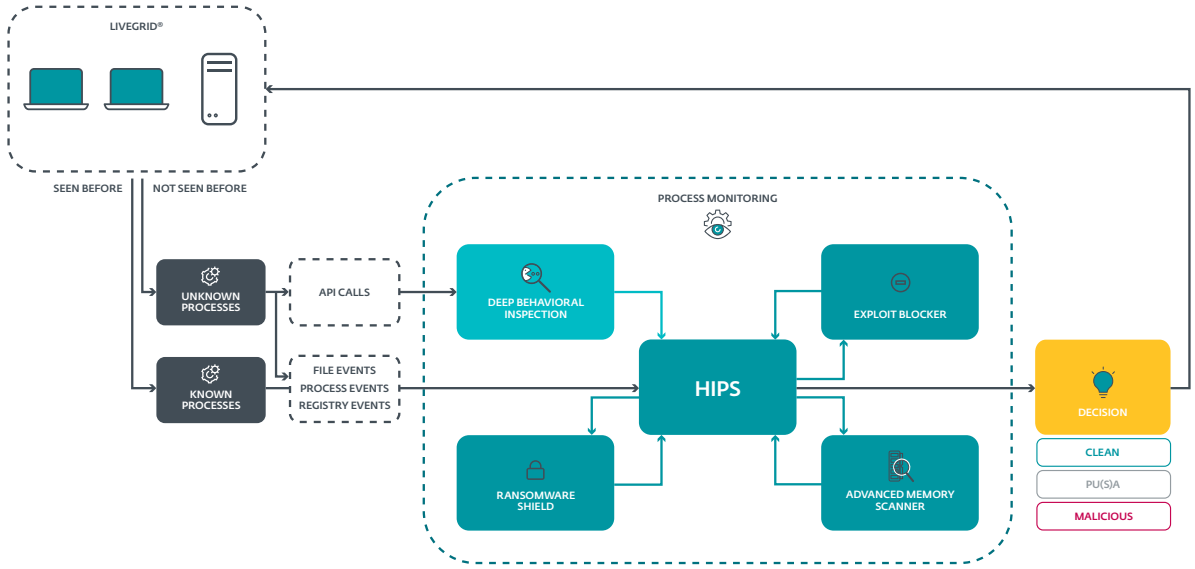

Figure 1 // Schematic indication of how DBI fits into the existing HIPS process-monitoring layer.

Why is Deep Behavioral Inspection important?

Malware writers know that they need to design their code in a way that will not attract the attention of built-in security features or third-party security solutions. To make their "products" as stealthy as possible, they employ various techniques including obfuscation, encryption, and process injection.

By adding the DBI module, ESET solutions can perform deeper and more granular monitoring, offering useful insight into process behavior. In turn, this allows for the creation of new types of detection, which can serve as an effective antidote for evasion techniques.

For advanced users:
Modifying an unknown or suspicious process for the sake of monitoring it can cause instability or even crash the process. Thus, users can manually whitelist legitimate processes from Deep Behavioral Inspection if necessary, to avoid issues while maintaining the overall increased level of security DBI provides.

In order to understand DBI and its role properly, we must first understand the background – namely how the ESET HIPS works.

How does ESET HIPS work?

ESET Host-based Intrusion Prevention System is a detection technology that was specifically created to monitor and scan behavioral events from running processes, files and registry keys, looking for suspicious activity.

HIPS decisions are based on **built-in rules and internal heuristics**, designed by ESET engineers, considering security intelligence collected over the past three decades. Optionally, **users/system administrators can define their own custom sets of rules** which can be used on top of the default set; however, creation of effective rules requires advanced knowledge of applications, operating systems and malware.

If suspicious activity is found, HIPS reports the offending process or – if a more detailed analysis is necessary – performs further inspection via its internal components. These focus on a variety of malicious behaviors used either to wreak havoc on a victim's device or to avoid detection by security solutions. The list of HIPS modules includes:

- **Advanced Memory Scanner (AMS)**
  - Malware authors today tend to use obfuscation and encryption, or let their code operate "in-memory only" to avoid detection as well as further analysis. These malware-protection tactics cause problems for more traditional detection approaches, which employ unpacking techniques such as emulation or sandboxing. To tackle these issues, AMS constantly scans the memory to catch malware when it reveals its true nature.
- **Exploit Blocker (EB)**
  - Exploit Blocker is designed to detect anomalies in the execution environment of certain processes that might suggest an exploitation attempt. When triggered, EB may block the threat immediately and subsequently may provide the gathered metadata to the ESET LiveGrid® cloud system for further analysis. EB monitors typically exploited applications such as browsers, document readers, email clients, Flash, Java, and others.
- **Ransomware Shield (RS)**
  - ESET Ransomware Shield is an additional layer protecting users from the class of threats known as ransomware. This protective technology monitors and evaluates all executed applications using behavioral and reputation-based heuristics. Whenever a behavior that resembles ransomware is identified or potential malware tries to make typically unwanted modifications to existing files (i.e., to encrypt them), RS notifies the user, who can then choose to block the activity.
- **Deep Behavioral Inspection (DBI)**
  - DBI is one of the new HIPS features, released in 2019. It enables HIPS to perform deeper user-mode monitoring of unknown and suspicious processes.

Threat intelligence gathered by HIPS is valuable to other layers in the ESET detection engine as well and may thus be submitted outside of HIPS, for additional analysis.

CONCLUSION

One of the goals of cybercriminals is to design their code to avoid detection. Defenders have to adapt and constantly upgrade and innovate their solutions to take evasion techniques – such as obfuscation, encryption and process injection – into account.

Deep Behavioral Inspection – the latest addition to the ESET HIPS layer, introduced in early 2019 – addresses such techniques by thoroughly inspecting API calls made by suspicious or unknown processes. This, together with other HIPS modules and ESET's multi-layered detection engine, provides ESET customers with superior protection to their data and devices.

ABOUT ESET

For more than 30 years, *ESET®* has been developing industry-leading IT security software and services for businesses and consumers worldwide. With solutions ranging from endpoint and mobile security to encryption and two-factor authentication, ESET's high-performing, easy-to-use products give consumers and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defenses in real time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company. Backed by R&D centers worldwide, ESET is still the only IT security company to earn *100 Virus Bulletin VB100* awards, identifying every single "in-the-wild" malware without interruption since 2003. For more information, visit www.eset.com or follow us on *LinkedIn*, *Facebook* and *Twitter*.

ENJOY SAFER TECHNOLOGY™