Deceptive Bytes

Active Endpoint Cyber Defense

Prevention by Deception

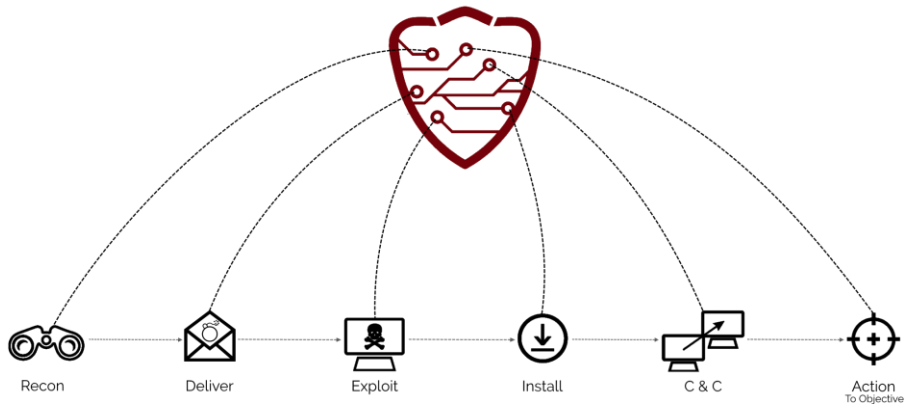
Product Overview

Background (Malware Behavior)

Malware is very clever and evasive, trying to understand where it is, using different methods and techniques in order to evade detection and analysis by security systems and researchers.
A recent research shows that *98% of malware uses at least 1 sandbox evasion technique*, Every time that a malware sees such an environment, it knows it's being detected or investigated which causes it to stop its malicious activities in one way or another. In Lastline's research on malware evasion techniques, it showed that most malware used at least 10 different evasion techniques to evade detection.

Deceptive Bytes - Active Endpoint Deception

Deceptive Bytes provides a fully endpoint-centric deception platform that uses existing IT infrastructure, responds to the evolving nature of advanced threat landscape and interferes with attackers attempts to recon & take hold of enterprise IT, in a preventative solution which covers sophisticated malware techniques & defenses through all the stages of the endpoint kill chain, and in several ways…

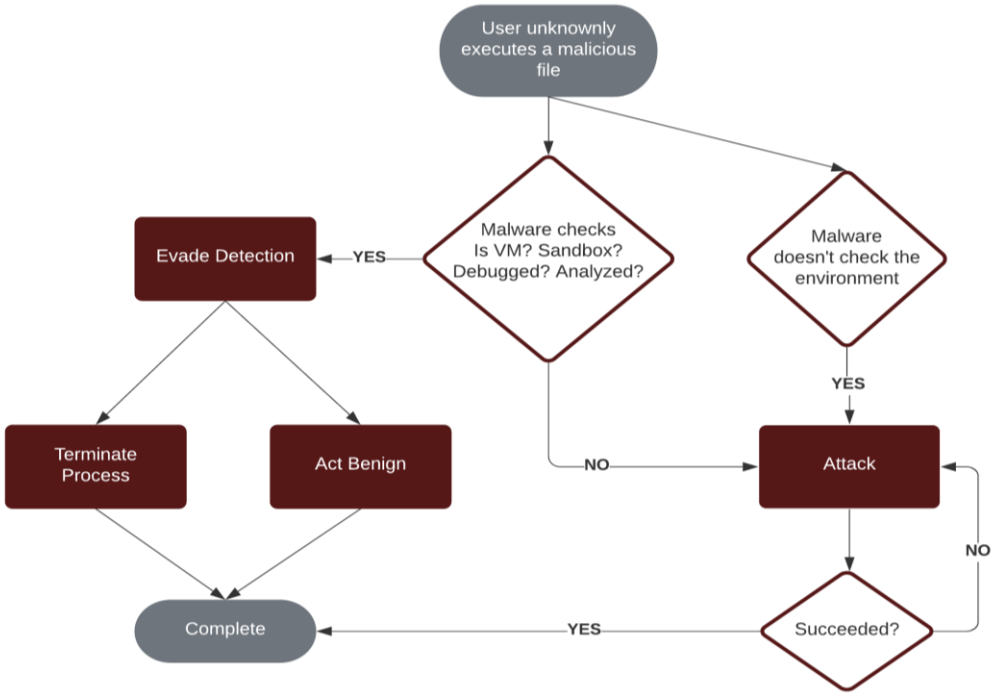


Shaping the Attackers' Decision Making

Preemptive Defense:
Making malware believe it's in an unattractive/hostile environment to attack, reducing its motivation to attack and the chance of infection.
For example, the solution makes malware believe it's in a sandbox or virtual machine (VM) that is used to detect and analyze it.

Proactive Defense:
Dynamically responding to threats as they evolve, based on the current detected stage of compromise, and changing the outcome of the attack.
For example, the solution deceives and stops Ransomware that operates immediately, making it believe it succeeded encrypting the files as the solution safeguard them.

Malware decision making diagram



How a malware evades an environment

- **Anti-Virtualization** - the malware searches for files, folders, registry keys and other artifacts that indicate it is running in a virtual machine environment, like VMWare, VirtualBox & others. It also checks if the system has minimal resources which also indicates it's running in a VM.
- **Anti-Sandboxing** - the malware searches for artifacts of sandbox environments like Cuckoo sandbox or if it's in a VM (used by some sandbox systems).
- **Anti-Debugging** - the malware checks if it's being debugged or any debuggers are installed
- **Anti-Analysis** - the malware checks if there's a malware researcher and tools that are used to investigate it and analyze its behavior.
- **Anti-Antivirus** - the malware goes against existing security systems and bypasses them, including machine learning and AI based products.

	What malware sees		
What malware check?	**In regular devices**	**Our solution**	**Result**
No. of CPUs	> 1	= 1	**Evade!**
Memory size	>= 2GB	< 2GB	
Hard disk size	>= 100GB	< 100GB	
Is debugged	NO (usually)	YES	
VM/Sandbox files, dirs, etc…	NONE	exist	

Agent Prerequisites

- Windows 7/Server 2008 R2 and above
- Microsoft .NET framework (v4.6.1 and above)
- Microsoft Visual C++ 2015/7 redistributables
- The installation must run with administrator rights
- Internet connection (for cloud based management)

System Impact

The product is extremely lightweight and operates in user mode, it has a very small footprint on the endpoint. It takes <0.01% CPU, <20MB of RAM & <1.5MB of disk space.

Key advantages

- Very high prevention rates of unknown & sophisticated threats (in real-time)
- Fast deployment (<30 seconds)
- High-fidelity alerts (low to none F/P rate)
- Reduces operational burden & costs
- Multi-layered approach
- Easy to manage
- No constant updates & No signatures
- Operates in standalone/disconnected/VDI environments
- High stability - operates in user-mode

Key features

- Deception-based endpoint security
- Prevention first approach
- On-premise/cloud deployment
- Multi-tenancy support
- Auto-response to attacks
- Windows Defender & Firewall integrations
- App control and automatic whitelisting
- Behavioral engine
- SIEM/Log integrations
- Threat Intelligence integrations
- Active Directory integration & AD-SSO
- Live device forensics & control

Effective Against

- ✓ APTs
- ✓ Ransomware
- ✓ CryptoMiners
- ✓ Zero-Day attacks
- ✓ Fileless attacks
- ✓ Trojans
- ✓ Evasive malware
- ✓ Malicious links *
- ✓ Malicious documents *
- ✓ Viruses
- ✓ Worms
- ✓ Spyware
- ✓ And more...

* Protects: MS Office, browsers, email clients, etc...

More info

Website LinkedIn Twitter Facebook info@deceptivebytes.com