lastline™

WHITE PAPER

An Introduction to Advanced Malware and How It Avoids Detection

The growing presence and capabilities of advanced malware is alarming. In spite of millions being spent on security products, organizations are still suffering from data breaches. Organizations interested in safeguarding their data need to understand how evasive malware operates. It's especially critical to recognize how advanced malware is outsmarting many of the most popular malware detection tools in the industry.

What is Advanced Malware?

Most of us are familiar with the concept of *malware*—a broad term applied to many related types of unwanted or harmful objects that can compromise systems, harvest data, and otherwise damage corporate networks. But just what is *advanced malware*, and how is it different from the older viruses, Trojans, bots, and worms that have been around for decades?

The term *advanced malware*, refers to sophisticated malicious software that has been designed with superior evasion and infection capabilities. Advanced malware avoids being detected and can remain hidden for extended periods of time as it conducts complex and damaging cyberattacks. "Advanced malware" does not necessarily refer to a specific *type* of malware (e.g. ransomware). Instead, it describes sophisticated behavior and evasion capabilities.

Who is Behind Advanced Malware?

Advanced malware is created and perpetrated by organized crime rings and state-sponsored factions. This sophisticated malware is usually designed to aggressively target anything and everything that can be monetized. Malware that steals user actions, data, identities, passwords, payment card information, or intellectual property is a lucrative multi-billion dollar enterprise, and major crime organizations are the primary authors.

The cartels behind advanced malware are intelligent, hardworking, and numerous. Their presence permeates every corner of the world. These organizations range in size from small hacker crews to large multinational syndicates.

There are many small groups involved in advanced cybercrime, but the big players in this dark space dominate. It's these larger, controlling organizations that are typically credited with creating the malware tools and malware as-a-service amenities that the smaller or less sophisticated crime rings use.

How Advanced Malware Avoids Detection

The vast majority of organizations today rely on the malware detection capabilities present in their network and email gateways, IPS (intrusion prevention systems), and firewalls to protect them.

Although these security tools may be new, in most cases they depend on an outdated, signature-based approach to malware detection.

Why Signature-Based Malware Detection Is Ineffective

Conventional malware detection products work by examining each object and calculating its digital signature. If that signature appears in a database of known malware, the object is acknowledged as malicious. As long as the malware has been previously identified and its signature exists in the database, this is an effective method of detecting malware. It works well for known malware.

Unfortunately, today's advanced malware can alter its signature to avoid detection. Signatures are created by examining the internal components of an object. Skilled malware authors modify these components while preserving the object's functionality. There are multiple transformation techniques used by malware authors and applying any of the following procedures can alter a signature:

- Code permutation
- Register renaming
- Expanding and shrinking code
- Insertion of garbage code or other constructs

According to Trend Micro, a million new malicious objects are created every day. It can be several days before vendors update their signatures for a new piece of malware (although it's not unusual for two weeks to pass before the provider makes a signature available). Until the new signature arrives, the malware will go undetected by conventional security controls and organizations are vulnerable to breach and data exfiltration during that time.

Perhaps more concerning, vendors may never add signatures to a database of known malware for many of the advanced malware objects. When less-sophisticated malware targets millions of entities, it will likely be reported to malware detection vendors who will create and distribute a signature. But, advanced malware is often designed to be single-use, targeting just one organization or a few people within one organization. This narrow focus greatly reduces the odds that its signature will ever appear in a database of malicious objects.

Advanced Malware Knows When It's in a Sandbox

Given the failures of signature-based technologies to detect advanced malware, a number of security vendors have developed sandboxes to provide additional detection capabilities. A sandbox is an isolated malware testing environment that is completely separate from an organization's real data or computer network. If an object running in a sandbox demonstrates malicious behavior, the sandbox can remove or quarantine the object. This behavior-based method of identifying malware is not dependent on signatures, so it can be very effective in detecting new malware.

However, today's advanced malware is engineered specifically to detect when it is running in a sandbox. When that happens, the malware will avoid taking any malicious actions and evade detection. Subsequently, when the malware has been allowed to enter the network and finds itself in a real machine, it will begin its malicious behavior.

Sandbox technologies typically utilize VM (virtual machine) environments like VMware, Xen, KVM, Parallels/Odin and VDI. This allows a user or an administrator to run one or more "guest" operating systems on top of another "host" operating system. Each guest operating system executes within a virtual environment and allows managed access to both virtual and actual hardware. In theory, the environment provided by the VM is self-contained, isolated, and indistinguishable from a "real" machine.

Unfortunately, VM technologies insert artifacts, which allow advanced malware to discover that it is running in a virtual environment. These artifacts include additional operating system files and processes, supplementary CPU features, and other components necessary for the virtualization to work.

Advanced malware looks for these artifacts to detect the presence of a VM or sandbox. Some of the techniques used by malware to recognize a VMware based environment include:

- Examining registry keys for values that are unique to virtual systems. In VMware, there are over 300 references in the registry to "VMware".
- Looking to see if VM tools are installed. In a VMware Windows Workstation, there are over 50 references in the file system to "VMware" or "VMX".

- Checking for certain processes and services that are specific to VM environments such as VMwareService.exe, VMwareTray.exe, etc.
- Identifying the BIOS serial number or MAC address of the virtual network adapter to reveal the vendor. For example, MAC addresses beginning with 00-05-69, 00-0c-29, 00-1c-14 or 00-50-56 are associated with VMware.
- Analyzing specific structures within system memory, such as the Interrupt Descriptor Table (IDT). This table is located in different areas for VM environments compared to physical machines.
- Examining specific hardware parameters that are unique to either VM or real physical environments. Advanced malware may query various attributes like serial numbers or other values belonging to the motherboard, processor, SCSI controller, etc.

One might think only highly skilled hackers would be capable of implementing this amount of sophistication. But, there are numerous toolkits available that allow even non-technical and novice cybercriminals to create malware that can detect the presence of a VM.

Advanced Evasion Tactics

One of the key characteristics of advanced malware is its level of stealth and ability to evade detection. As covered previously, today's sophisticated malware easily defeats signature-based anti-malware products. Furthermore, it can detect behavior-based anti-malware tools if they are built using conventional VM technologies like sandboxes do. Advanced malware will avoid detection by using a number of evasion tactics. Table 1 lists some of the more common ones.

MALWARE EVASION TACTIC	DESCRIPTION	MALWARE RESPONSE
Stalling Delays	The malware remains idle for an extended period, avoiding all malicious activity.	Ten minutes is usually sufficient for most sandboxes to timeout and assume the object is benign, providing an opportunity for malware to infect a system. Note that most legacy sandboxes can detect if the malware calls the operating system's sleep function, but if the malware performs the delay internally without calling the O/S, a conventional sandbox will not see the evasive behavior.
User Action Required Delays	Some malware avoids doing anything malicious until a user performs a specific action (e.g. a mouse click, pressing a key, opening or closing a file, exiting the program).	Malware avoids malicious activity until it sees user action, thereby avoiding detection by a conventional sandbox.
Intelligent Suspension of Malicious Activity	Unlike simple stalling techniques, this category includes sophisticated evasion techniques that discover the presence of a sandbox and suspend malicious actions to avoid detection	Malware generally avoid these behaviors until it has penetrated an actual host or machine: • The injection or modification of code within other applications • Attempts to establish persistence and download additional code • Decryption of files • Attempts to move laterally across the network • Connections to its command and control servers
Fragmentation	A technology that splits malware into several components that only execute when it is reassembled by the targeted system.	When fragments are evaluated separately, (which is typically the case with conventional sandbox technology) each fragment remains dormant, so that the malware appears harmless.
Return-Oriented Programming (ROP) Evasion	A technique where malware injects functionality into another process without altering the code of that process by modifying the contents of the stack (the set of memory addresses that tells the system which segment of code to execute next).	Malware authors replace the correct return contents of the stack with a specifically-crafted sequence of addresses that changes which code is executed, thus altering the functionality of the program. Malware using ROP evasion avoid discovery by delegating the execution of its malicious code to other programs. Since the malicious activities are not performed directly by the malware program itself, the chances of being detected by a conventional sandbox are greatly reduced.
Rootkits	A Rootkit is an application (or set of applications) that hides malicious code in the lower layers of the operating system.	Because a conventional sandbox can only monitor calls to the operating system and not what the operating system does with those calls, the malicious actions performed by a rootkit will generally go undetected by a sandbox.

Lastline – A Unique Approach to Detecting Advanced Malware

To effectively detect advanced malware, it's critical that the isolation environment remains hidden. Equally important, the technology must be capable of detecting dangerous objects that don't have signatures, and of identifying malicious capabilities—even if the corresponding code hasn't yet executed.

Lastline® developed Deep Content Inspection™ to provide complete visibility into malware behavior that other technologies miss, while remaining hidden from the malware itself. We created a unique isolation and inspection environment that simulates an entire host including the CPU, system memory, and all input/output devices. This environment allows Lastline to observe 100% of all the actions a malicious object might take.

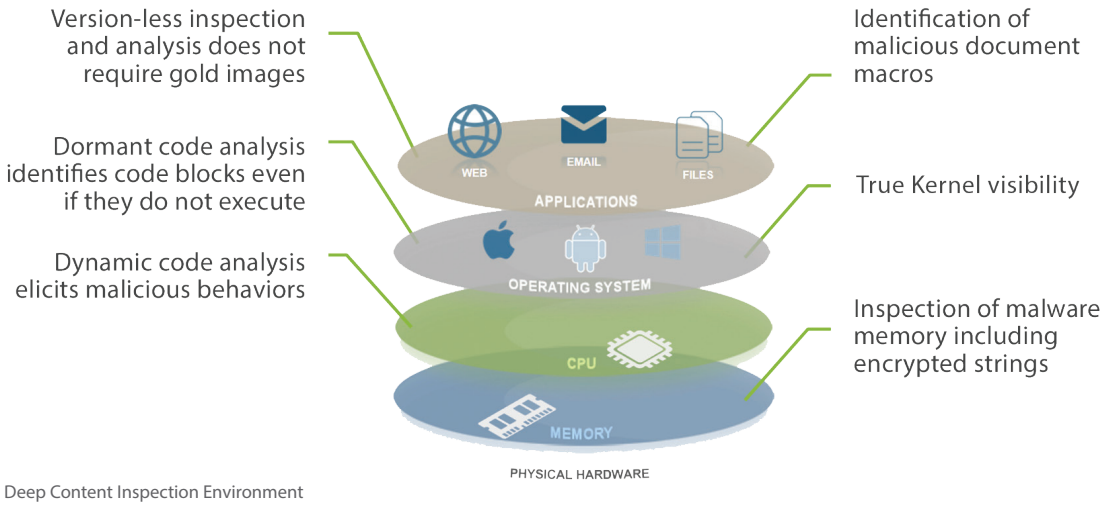

Figure 1 Lastline Deep Content Inspection Environment

Sandboxes only have visibility of the communication that occurs between malware and the operating system. They can't inspect the actual malware's execution, nor interact with it like Lastline Enterprise can. As a result, Sandboxes have significantly lower detection rates and higher false positives than Lastline.

Yesterday's Technology Will Not Detect Today's Advanced Malware

Organizations everywhere are experiencing advanced malware attacks and data breaches at an unprecedented rate, in spite of spending vast amounts of money on security tools that claim to detect such threats.

The only way to defeat this sophisticated type of malware is to implement tools that have been specifically designed to detect all known evasion techniques and easily adapt to new ones. Sadly, today's VM-based sandboxes, network and email gateways, IPS, and firewalls (even next generation firewalls) are not up to that task.

Organizations that rely on these products for detecting malware run a significant risk of succumbing to cyberattacks. Fortunately, Lastline Enterprise is uniquely suited to detect today's advanced malware.

Experience the Lastline Advantage

For more information please visit www.lastline.com

LASTLINE CORPORATE HEADQUARTERS
203 REDWOOD SHORES PARKWAY
SUITE 620
REDWOOD CITY, CA 94065

AMERICAS: +1 (877) 671 3239
EMEA: +44 (0) 207 749 5156
APAC: +65 6829 2207
WWW.LASTLINE.COM