lastline™

TECHNOLOGY BRIEF

Defeating Advanced Malware with Deep Content Inspection

Delivers Total Visibility and Detection Of Advanced Malware

Not all malware detection technology is the same. Lastline's Deep Content Inspection™ goes far beyond the malware detection capabilities found in "next-generation" tools like sandboxes, firewalls, and IPS.

Advanced Malware Defeats Other Detection Systems

Advanced malware is capable of outsmarting the detection capabilities of the wide range of security tools organizations have deployed. More than 75% of the advanced malware detected by Lastline includes sophisticated evasion technologies. And, to make detection even more difficult, the number of evasion methods found in each instance of malware has recently jumped from one or two, to ten or more.

Organizations often deploy multiple security controls to protect against system compromise and data breaches, including: sandboxes, firewalls, NGFW/UTMs, IPS, and web and email gateways. Sandboxing technology in particular has been deployed to detect advanced malware. But today's advanced malware can defeat other sandboxes because of the limited visibility those tools have, their use of obsolete inspection technologies, and operating system dependencies. The malware authors know the limitations of these tools and engineer their malware to evade detection.

Deep Content Inspection Detects Advanced Malware

Lastline Defender™ detects and defeats advanced malware that can easily evade sandboxes and other 'advanced' security controls. These products can only monitor the interaction between an object and the operating system, which significantly limits their visibility into malicious behavior. This means they cannot see what is occurring within the malware itself, nor in other programs, operating system, or kernel functions used by the malware. Lastline's Deep Content Inspection technology imitates a complete operating system and hardware environment. This enables unmatched visibility into the malware, all programs and services it invokes, all operating system functions, and all kernel activity. It analyzes the actions of everything that occurs, including all CPU instructions, memory locations accessed, devices used, and network connections.

The bottom line: Lastline creates an inventory of every malicious behavior engineered into a piece of code. Malware can't execute a behavior without Lastline Defender detecting the behavior. Other security products lack this visibility and will allow malicious objects to penetrate a network and compromise systems.

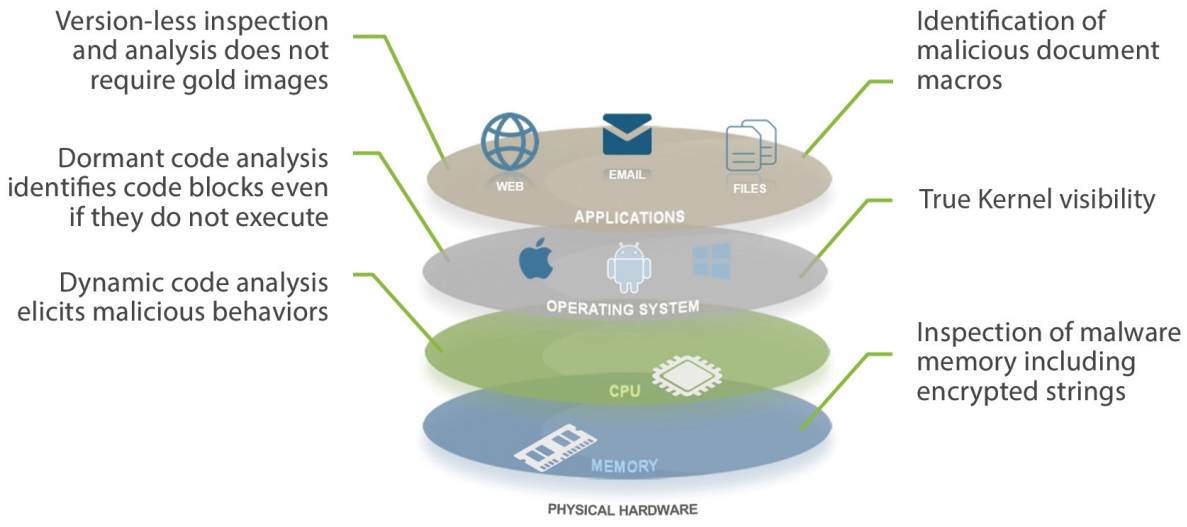

FIGURE 1 TOTAL VISIBILITY OF ADVANCED MALWARE

Comparing Deep Content Inspection to Sandboxes

DEEP CONTENT INSPECTION

- Complete visibility – CPU, O/S, Kernel
- Malware can't execute a behavior that it can't see
- Detects evasion techniques
- Not dependent on signatures
- Not dependent on specific versions of O/S or applications
- Analyzes dormant code as well as active code

SANDBOX

- Limited visibility – O/S level only
- Detectable by advanced malware
- Dependent on specific versions of OS & applications
- Heavy dependency on signatures

Deep Content Inspection Features And Benefits

Deep Content Inspection enables Lastline Defender to deliver a number of critical features and benefits that other technologies cannot:

COMPLETE VISIBILITY OF MALICIOUS BEHAVIOR

It sees everything the malware does, whether performed by the malware's internal code, or by other processes it calls upon, including the O/S, system services, kernel routines, rootkits, or other programs. Every process is visible:

- All CPU instructions executed
- Every memory location accessed
- Each network connection requested
- All files accessed
- Each device accessed

COMPREHENSIVE DETECTION OF EVASION TECHNIQUES, INCLUDING:

- Internal stalling that a sandbox can't observe (timing delays within the malware itself, or waiting for a specific user action)
- Malicious actions performed by the operating system or rootkits that are invisible to a sandbox
- Encryption of communication with C&C infrastructure
- Return Oriented Programming (ROP)
- Fragmentation of malware into different files that only execute when reassembled
- Anomalies in the behavior of the object or system that may indicate an evasion technique

REMAINS HIDDEN FROM MALWARE

Unlike sandbox technologies that rely on virtual machine technology that advanced malware can detect, Deep Content Inspection looks like a complete host. This makes it very difficult for malware to discover.

NOT DEPENDENT ON SIGNATURES

Deep Content Inspection relies on behavior analytics and not signatures. It's effective against zero-day and other unknown variants of older attacks where signatures don't exist.

NO DEPENDENCIES ON SPECIFIC VERSIONS OF O/S OR APPLICATIONS

Many sandbox products require the installation of specific versions of applications to detect malware that could exploit those versions. Deep Content Inspection sees exploit preparation regardless of the version of the application being targeted. It can detect malicious behavior without creating sandbox images of every possible combination of O/S and applications.

DORMANT CODE ANALYSIS

Sandboxes can't detect a malicious block of code in the malware if it doesn't execute during the analysis period. Deep Content Inspection can detect dormant functionality because it statically matches and correlates patterns of code with known malware. This capability enables the detection of functionality that could be executed under certain conditions, but the execution path invoking the behavior is not taken during analysis.

Lastline's Deep Content Inspection is an entirely unique approach to malware analysis. This innovative technology delivers the visibility organizations need to detect evasive malware that other tools miss. With most malware taking advantage of sophisticated evasion technologies, organizations can't rely on outdated detection technologies.

Experience the Lastline Advantage

For more information please visit www.lastline.com

LASTLINE CORPORATE HEADQUARTERS
203 REDWOOD SHORES PARKWAY
SUITE 500
REDWOOD CITY, CA 94065

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