White Paper

Secure Beyond the Signature

A multilayered strategy for advanced malware security in today's post-signature threatscape

Table of Contents

Why Advanced Malware Is Challenging Signature-Based Inspection

IT security is an arms race with no commercial breaks, half-time intermission, seventh inning stretch, or finish line. Nonstop innovation by well-organized cybercriminals keeps the frontlines moving and periodically bypasses defensive strategies that once marked the conflict's cutting edge. Such is the case with signature-based security and today's advanced malware.

For years, signature-based security alone provided fast, reliable protection from most known attacks, so the more capable hackers inevitably learned to avoid easily identified attacks. Their tactics became stealthy, evasive, defense-aware, and intelligently adaptive. Zero-day attacks and other targeted, advanced malware now frequently challenge the defenses of signature-based IPS systems, despite fully up-to-date signature sets. Although signature-based detection provides an important foundation for intrusion inspection, clearly, something more must be done to combat these next-generation malware attacks.

The recent attacks on the retail chains bring to light the devastation a malware attack can have on an organization's operations and reputation. A layered signature-less detection architecture greatly enhances signature-based detection and reduces the risk of these kinds of attacks.

In a survey conducted at the 2013 Black Hat USA conference, 81% of respondents cited advanced malware as a major concern for their organizations, and 35% claimed to spend 10 or more hours each week combatting malware penetrations. In light of those sentiments, it is surprising that 67% of security professionals have no technology deployed specifically to fight advanced malware, according to a McAfee report published in December 2013.

The New Worst-Case Scenario: Target and BlackPOS

This may change as the impacts of the massive malware-enabled data breaches at Target and other retailers sink in. The Target incursion alone appears to have exposed 40 million payment card numbers and compromised the personal data of 70 million customers. The FBI has signaled that further breach revelations can be expected, and investigations are under way at the US Department of Justice, the Secret Service, and in both houses of Congress.

Much remains to be learned about these break-ins, including how the BlackPOS malware made its way onto the retailers' point-of-sale (POS) systems and how it evaded detection while exfiltrating more than 12 gigabytes of data. But a great deal can be learned about the requirements of advanced malware security by examining a common, well-understood example: a PDF file with malicious embedded JavaScript.

How Signatures Miss Serious Attacks: The Predatory PDF

PDFs have become indispensable tools for platform-independent distribution of rich, interactive content. Email attachments and web downloads carry thousands of PDF files across enterprise firewalls every day, bearing everything from business proposals to software manuals, legal documents, and presentations. To automate various aspects of presentation and interactivity, the format supports dynamic elements, such as dynamic action triggers, remote data retrieval, and embedded scripts. Scripts have a wide range of useful applications, such as enforcing conditional formatting in a user-populated form so that an email address or phone number can only be entered in the correct format for the designated data type.

At the same time, scripts are an increasingly popular vector for infection, offering an almost unlimited number of malicious possibilities. A script might download and install a keylogger, rootkit, or bot. Unfortunately, while some intrusion prevention systems (IPS) can recognize an embedded script, they cannot parse its code or predict its runtime behavior. Unless the IPS scan matches a known threat signature, the file is allowed to pass. When opened on the destination host, the malicious script automatically extracts or downloads a malware payload and installs it on the host. The attack creates new application processes that may capture user credentials and other valuables, export stolen data to a command and control server, or propagate the infection to other endpoints on the network.

Stopping Threats Known and Unknown

How can such attacks be stopped? Signature-based security can only catch attacks that have been previously identified and analyzed, not a new variant making its first appearance. We could simply block all files with embedded scripts, but that would eliminate a popular and useful communication tool. We could send all files with embedded scripts to an offline sandbox for dynamic analysis, but this would delay content delivery and add a large workload to a computationally intensive resource. What we need is a more sophisticated approach capable of efficiently determining the safety of an unknown executable in the absence of signature-based certainty.

A proper signature-less security solution uses signatures on top of multiple signature-less technologies. This in-depth approach covers both known exploits and unknown malicious behavior with superior protection, accuracy, and efficiency.

To succeed, such an advanced approach must discover new threats through pattern analysis and behavioral prediction, without resorting to historical records of known exploits and incidents. Since no other detection method is likely to match the reliability of a known signature, an advanced approach should apply multiple detection methods in a multilayered stack. It must also limit the false positives generated by intelligently extracting faint threat signals from the normal noise of network activity.

Three Keys: Code Behavior, Traffic Behavior, Reputation

McAfee believes that unknown malware attacks can be identified and stopped with high levels of accuracy and reliability by layering three types of analytical techniques over a conventional signature-based defense.

- Code behavior analysis that uses lightweight emulation, sandboxing, and advanced static analysis to assess and predict the behavior of files and executables through direct examination or execution of the code.
- Traffic behavior analysis that identifies malware attacks within the network through behavioral anomalies in the traffic flows they create. These techniques correlate large volumes of network and endpoint events to extract faint threat signals from the background noise of normal network activity.
- Global reputation analysis that adds external context and intelligence to local inspection and assessment.

These detection analytics are applied to unknown threats in a sequence of increasing computational intensity through the appliances that deliver the McAfee® network intrusion prevention system (IPS) solution. These include:

- *McAfee Network Security Platform*—An integrated IPS appliance that discovers and blocks sophisticated threats in the network, including advanced malware, zero-day threats, denial-of-service attacks, and botnets. Its advanced architecture provides deep inspection of network traffic while maintaining line speeds of up to 40 Gbps on a single appliance.
- *McAfee Advanced Threat Defense*—An advanced malware prevention solution that employs a series of detection engines, including dynamic analysis (sandboxing) and static code analysis, arranged in a down-select sequence to optimize performance. The appliance deploys easily in the network as a central malware inspection point for McAfee IPS and other Security Connected devices.
- *McAfee Endpoint Intelligence Agent*—A small-footprint, plug-and-play software module deployed on the McAfee endpoint agent. It provides real-time, per-connection traffic intelligence that positively associates every session with the originating host system, user, and application.
- *McAfee Network Threat Behavior Analysis*—A threat correlation appliance that baselines network operations using behavior-based algorithms to swiftly correlate anomalies that indicate risks and threats. As an optional component of McAfee Network Security Platform, it extends that product's traffic inspection capabilities by mapping the activities of endpoint executables to network connections and traffic flows.
- *McAfee Network Security Manager*—An intuitive, web-based platform that provides centralized, policy-based control of McAfee Network Security Platform, McAfee Network Threat Behavior Analysis, and McAfee Advanced Threat Defense. McAfee Network Security Manager helps administrators reduce the time spent investigating alerts with advanced correlation workflows that organize multiple alerts into single events.

The Signature-Less Approach from McAfee

Let's examine each of the analytical components that comprise McAfee advanced security and role of each appliance in delivering the overall solution.

Code behavior analysis

These signature-less inspection engines leverage emulation and sandboxing technologies to examine files or executables and predict or observe their behavior at runtime (Figure 1). Some are resource-thrifty and operate in near real time; others are more computationally intensive and impose a small increment of latency. Combining them in a sequence of escalating resource intensity provides a cost-effective optimization of performance and effectiveness.

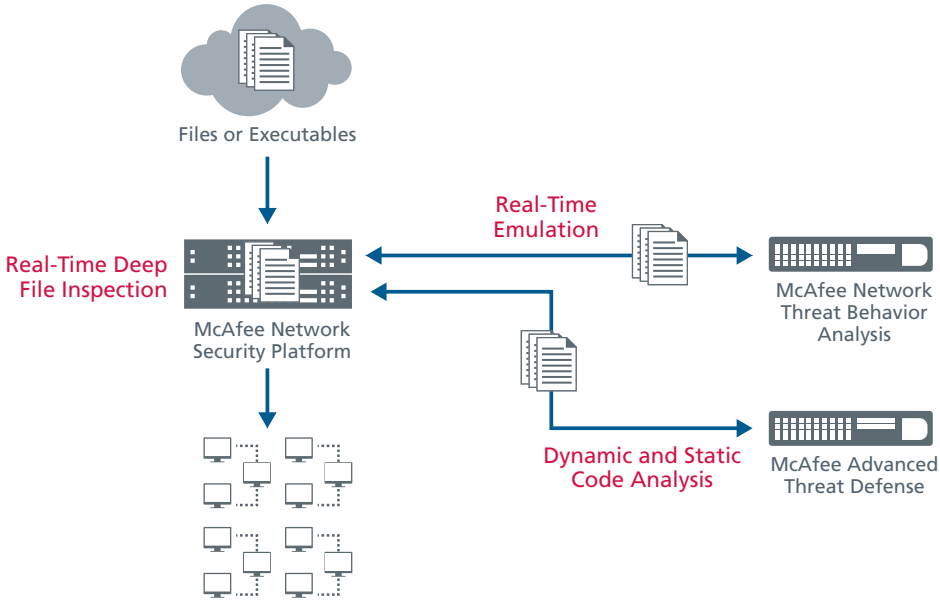

Figure 1. Technologies used in code behavior analysis.

Real-time deep file inspection

This is the first line of defense in a multitier array of non-signature malware analytics from McAfee. This feature of McAfee Network Security Platform finds and stops the threats concealed in embedded scripts, as in the PDF example described above. Deep file analysis uses a streamlined JavaScript environment to emulate script execution and predict runtime behavior. Files containing scripts that are observed to be malicious are blocked immediately and at all further appearances. McAfee Network Security Platform is the only IPS solution that provides intelligent script emulation directly on the IPS sensor. It provides a zero-latency alternative to all-or-nothing script blocking and is far more cost effective than routing all unknown files to a sandbox. In our malicious PDF example, deep file analysis allows McAfee Network Security Platform to identify and block the attack in real time—before the file reaches and infects its target host.

Real-time emulation

Real-time emulation is a feature of McAfee Advanced Threat Detection that emulates a working environment to study the behavior of entire files (not just the scripts embedded within). Multiple lightweight execution environments are available for a wide range of browsers, file types, and scripting languages, offering a stripped down subset of CPU, memory, and operating system application programming interface (API) resources. These emulators simulate code execution, provide hooks for malicious processes, and predict the resulting behaviors. In addition, heuristic analytics applies rules and pattern analysis to identify similarities between a suspect file and related groups of known threats.

Real-time emulation quickly identifies rootkits, zero-day threats, advanced persistent threats, and other advanced malware at a fraction of the computational cost of true dynamic or static code analysis.

Dynamic code analysis

The next step when emulation reveals no threats in an unknown file is dynamic code analysis. It is a feature of the McAfee Advanced Threat Defense appliance, which provides full code execution in a secure virtual machine sandbox. This analysis differs from emulation in that it instantiates a fully operational runtime environment that is isolated to allow safe execution of potentially malicious code. All observed behaviors are logged or classified, including changes to the operating system (OS), files, and registry entries.

McAfee code behavior analysis technologies provide the best of both worlds. Emulation environments provide the advantage of real-time protection from zero-day attacks, while sandboxing provides the ultimate in-depth analysis and protection for the most advanced malware attacks.

Unlike sandbox solutions that use a single generic virtual machine (VM) for all analyses (and miss many behaviors that only appear in specific VM configurations), or that test all samples in multiple virtual environments (more thorough but resource-intensive), McAfee Advanced Threat Defense runs each suspicious executable in a virtual environment that exactly matches the system for which the file is targeted.

Unique among currently available sandbox technologies, McAfee Advanced Threat Defense leverages endpoint information acquired by McAfee® ePolicy Orchestrator® (McAfee ePO™) software to identify the target host's specific operating environment, launching a matching VM on the fly. This greatly increases the probability that a file's full range of potential behaviors are elicited and observed and an accurate assessment is made of its intent. McAfee Advanced Threat Defense also emulates appropriate responses to sample behaviors and resource requests (for example, network connections) and offers a fully interactive mode for manual offline analysis.

Static code analysis

Static code analysis is the indispensable flip side of dynamic analysis. Sandboxing identifies malware with a high degree of confidence based on direct observation of its behavior. It will reliably identify hidden threats in complex executables but can be easily defeated by various strategies. For example, a file may simply outwait the observation period, delaying the start of any revealing behavior for a predetermined interval that may be longer than an economically viable sandbox inspection. Or a file may be programmed to recognize a secure environment by the absence (or presence) of certain resources and execute only a limited set of deceptively innocuous operations.

For these reasons, dynamic analysis should always be paired with true static code analysis. Static inspection provides a window into the nature of latent (non-executing) code for which dynamic analysis is entirely blind. True static analysis identifies structural similarities between latent code and known malware samples, quantifying the percentage of code that executes during a sandbox evaluation, and mapping all of the logical execution paths of a complex file.

On the McAfee Advance Threat Defense appliance, true static code analysis launches concurrently with dynamic analysis and incorporates some of its outputs when available. Unlike many available static malware analysis technologies, this inspection fully unpacks and reverse engineers obfuscated code to recover intact versions of dissembly code. These are then parsed and subjected to statistical analysis, providing:

- An assessment of similarity with known malware families.
- A measurement of the latent code that did not execute during dynamic analysis.
- A logical map of the file's complete execution path(s).

These findings are then incorporated with the observations from dynamic analysis to provide an overall threat score indicating the degree of certainty that the sample file or executable is malicious.

Traffic behavior analysis

These signature-less inspection methods look at behavioral patterns in traffic flows to find anomalous signals hidden in the background noise of normal activity, no matter how faint (Figure 2).

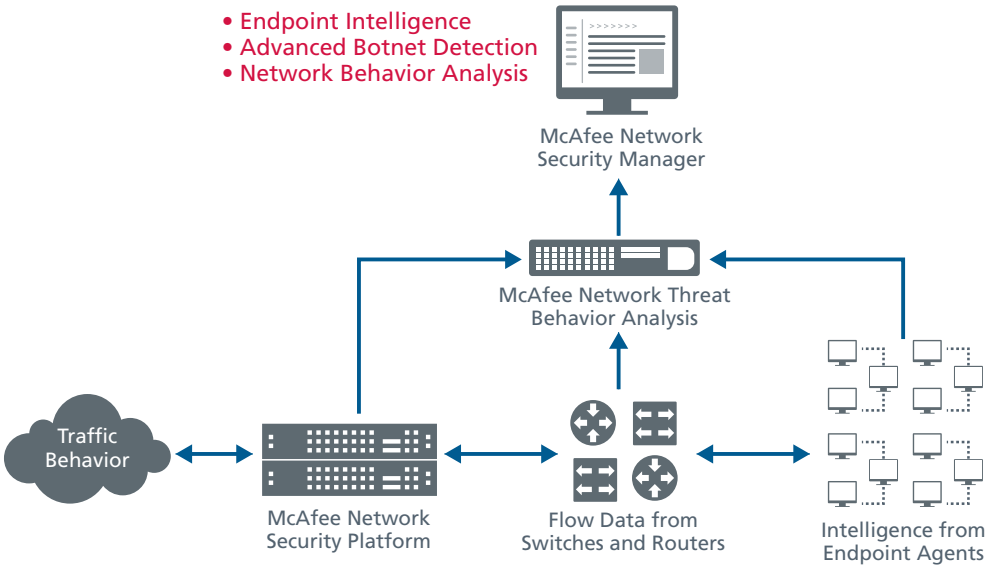

Figure 2. Technologies used in traffic behavior analysis.

McAfee Endpoint Intelligence Agent

This agent provides real-time, per-flow endpoint traffic correlation by positively associating every network session with the originating host system, user, and application process. This solution leverages intelligence in the network and on every Microsoft Windows host to reveal relationships between endpoint executables and network traffic flows, making it possible to:

- Identify malicious network connections and executables in near real time.
- See detailed process context for every attack.
- Block malicious communications and prevent the spread of advanced malware.
- Quarantine and remediate compromised host systems.

With innovative signature-less technologies, like endpoint integration and intelligent correlation, malicious anomalies within your network are isolated from the background noise, no matter how faint they are.

McAfee Endpoint Intelligence Agent acquires its host system insight from a small-footprint, plug-and-play software module deployed from the McAfee endpoint system. When installed and configured, the agent inventories all application processes on the host and monitors their communication activities. Each time a process requests a network connection, the agent first sends a tiny packet of metadata to network security services (usually McAfee Network Threat Behavior Analysis). This packet includes information about the connection (message protocol, source, and destination address and port), the user (name and security identifiers—but no secure personal information), and the endpoint application process (application name and hash).

Security services in the network combine this endpoint and session data with reputation intelligence on the source and destination endpoints, allowing a high-confidence threat assessment of the pending communication and the internal endpoint's security state. Communication attempts by compromised hosts can then be quarantined so that malicious traffic within your network can be controlled. By quarantining the infected host and blacklisting the identified malware, exfiltration of valuable data is prevented and impact on the network is limited.

Advanced botnet detection

This is a layer of traffic and network event correlation specifically dedicated to botnet security, one that far exceeds the signature-based identification and detection algorithms capabilities of other vendors. McAfee Network Security Platform correlates multiple individual network alerts or anomalies and applies heuristics to reveal the true fingerprints of botnet infections. This multi-activity correlation provides threat identification with a far higher degree of confidence than individual, single-activity signatures can provide.

For instance, advanced botnet analysis might correlate an apparently unrelated DNS website query with a PDF download and a sudden traffic surge between an internal endpoint and a high-risk web domain. Individually, none of these events might be sufficient to convict the internal endpoint, but, considered in aggregate, the evidence could justify action to isolate, investigate, and remediate. Advanced botnet protection sequences, correlates, and weighs a wide range of events and activities to pinpoint bot infestations that are invisible to other defenses.

Network threat behavior analysis

McAfee Network Threat Behavior Analysis is an in-network correlation engine that applies behavior-based algorithms to network traffic data. It brings together netflow data from switches, routers, and other network devices from Cisco, Juniper, and Extreme Networks, combining them with layer 7 application traffic data from McAfee Network Security Platform and reputation intelligence from McAfee Global Threat Intelligence (McAfee GTI). From these sources, it automatically creates models of normal bandwidth consumption, by each application, of host-to-host traffic volume and encryption utilization and then applies the models to identify and bring forward the subtle anomalies that reveal successful penetrations. McAfee Network Threat Behavior Analysis drills down into complex, multivector attacks and blended threats. It holistically evaluates network-level threats, identifies the overall behavior of each network element, and instantly abstracts apparent anomalies to identify distributed denial of service (DDoS) attacks, zero-day threats, botnets, worms, and reconnaissance attacks—in real time and entirely without signatures.

Global reputation analysis

These services provide critical context for network threat identification: reputation assessments of external domains, hosts, and message payloads (Figure 3).

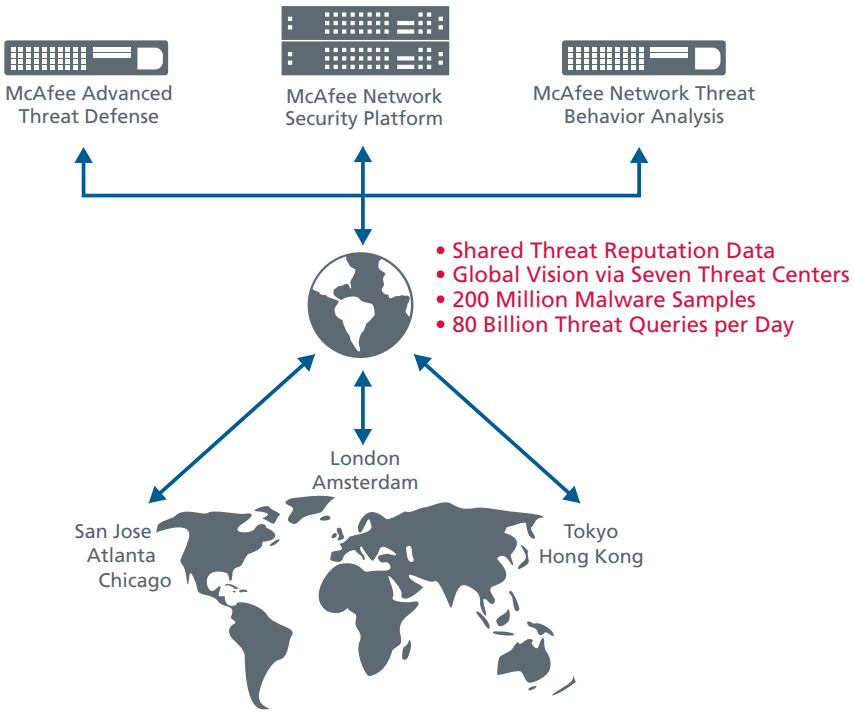

Figure 3: McAfee Global Threat Intelligence.

McAfee GTI

McAfee GTI is a comprehensive set of cloud-based threat intelligence services that protects your network across all attack vectors with real-time reputation insight on files, websites, messages, and network connections. The service collects and correlates threat data from more than 100 million product nodes and from billions of IP addresses. It calculates a reputation score reflecting the likelihood that a network connection poses a threat and processes more than 80 billion threat reputation requests a day. It also provides an endpoint geolocation service, bringing another level of context to IP address reputation.

Using McAfee GTI can significantly improve an organization's protection posture. This global service reduces lead time to protection by an average of four days. In addition, a 12% improvement has been seen on file detection.

—McAfee Labs

McAfee GTI allows you to:

- Protect endpoints from distributed denial-of-service (DDoS) attacks, botnets, command and control activity, advanced persistent threats, and risky web connections.
- Decrease the downtime and remediation costs associated with network-based attacks.
- Reduce system and network burden by blocking threats at the network edge.

In the case of the malicious PDF attack described earlier, reputation intelligence from McAfee GTI would provide multiple opportunities to block or prevent the attack. File reputation intelligence delivered to McAfee Network Security Platform allows the download to be blocked before delivery. Reputation intelligence on a malicious endpoint process allows McAfee Endpoint Intelligence Agent to block the outbound connection request and identify the compromised host. Because McAfee GTI informs every level of anti-malware defense, it enables many overlapping opportunities to catch and contain attacks, all without recourse to signature-based detection.

The Industry's Most Complete Post-Signature Malware Security Solution

The malware threat landscape is always changing, and network security practices evolve on its heels. Signature-based defenses remain essential as the most efficient way to stop the millions of known attacks, but signatures alone cannot stop today's advanced, evasive malware. Effective security now requires signature-less malware detection that leverages multiple detection strategies and deployed in multiple overlapping tiers. No potential security partner offers as complete a portfolio of advanced, post-signature detection technologies or combines them as effectively with traditional signature-based security as McAfee. For more information, contact your McAfee sales representative, or visit us online at mcafee.com.

About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ: INTC), empowers businesses, the public sector, and home users to safely experience the benefits of the Internet. The company delivers proactive and proven security solutions and services for systems, networks, and mobile devices around the world. With its visionary Security Connected strategy, innovative approach to hardware-enhanced security, and unique global threat intelligence network, McAfee is relentlessly focused on keeping its customers safe. http://www.mcafee.com.

McAfee
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

60999wp_beyond-sig_0314_fnl_ETMG