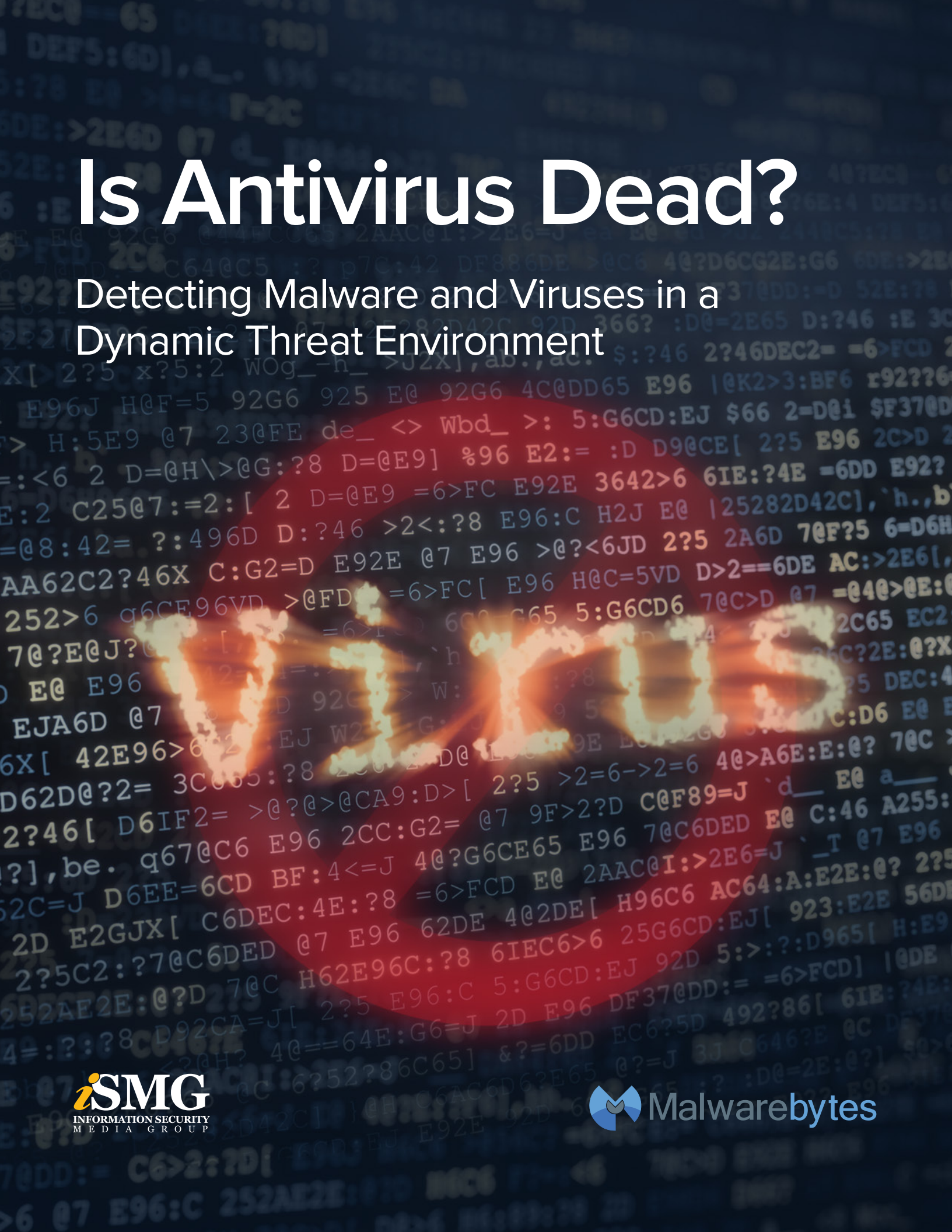
Is Antivirus Dead?

Detecting Malware and Viruses in a Dynamic Threat Environment



ISMG
INFORMATION SECURITY
MEDIA GROUP

Malwarebytes

READER ROI

Despite the presence of advanced antivirus solutions, cyber criminals continue to launch successful attacks using increasingly sophisticated malware. Read this paper to learn:

- Why antivirus software is no longer effective in detecting, let alone stopping, most malware
- Why a layered approach to cybersecurity offers more complete protection than antivirus or other "silver bullet" solutions can on their own
- Why a malware hunting tool is essential to detect any malware that breaches the network

Introduction

In November 2015, Starwood Hotels and Resorts confirmed it had fallen victim to a malware attack that spanned eight months and involved 54 locations. Infiltrating its network via point-of-sale (POS) channels within the chain's restaurants and gift shops, the malware stole payment card information, including card numbers, cardholder names, expiration dates, and security codes.

Less than a week later, Hilton Hotels and Resorts admitted to having suffered an almost identical malware breach in its own POS systems. And both entities are just the latest in a series of high profile breaches that range from well-known corporations such as Target to the U.S. Office of Personnel Management.

No wonder companies are fearful of becoming the next target, says Pedro Bustamente, Vice President of Technology at Malwarebytes. "Their worst fear is to have a situation like a Target or a Home Depot, where they have been breached, don't know about it for a long time, and all of a sudden it comes out. Meanwhile, during the dwell time, the infection gathered customer information or internal information," Bustamente explains.

Out of all this chaos, one thing is clear: Antivirus solutions, at least on their own, are no longer effective in stopping cyber attacks.

Is Antivirus Dead?

John McAfee, the founder and former CEO of McAfee, says it is. AV pioneer Dr. Alan Solomon, who created one of the first antivirus toolkits back in 1988, has written that he hasn't used antivirus in over a decade because he can't see "how it could work in a world where you would need daily updates."

But, at least in the case of enterprises, the answer is: not exactly. Plenty of old-school worms and Trojan horses still roam the online world, waiting to infect PCs with outdated operating systems, unpatched server hardware, and people who can't resist clicking the links in spammy email. Therefore, antivirus still needs to be part of any comprehensive cyber defense plan.

At the same time, however, antivirus software can no longer thwart today's complex

malware, let alone zero-day exploits, of which malware is just one component. Antivirus software uses static signatures to detect malware, and it often takes as long as three months to isolate a given strain and then issue the necessary security patch. According to researchers at McAfee Labs, at least 100,000 new pieces of malware are released in the wild every single day; therefore, this static approach is ineffective (at best) in isolating zero-day exploits, quickly mutating ransomware, or other malware using advanced delivery mechanisms.

In an ideal world, trapping malware requires antivirus and anti-malware working together as part of layered approach to enterprise security. Each solution would still need frequent updates to handle "the proliferation, the pervasiveness, [and] perniciousness of attacks that you have today," says Laura DiDio, Director, Enterprise Research, Systems Research and Consulting at Strategy Analytics. While a high percentage of organizations struggle to keep their software up to date, according to DiDio, that's what is required to stay on top of the threat.

Too Many Endpoints

Today's IT environments differ drastically from those just a decade ago. Not only was malware static and easy to detect, IT departments ruled their data centers in near absolute fashion, DiDio remembers. "During the terminal mainframe days, they could have everything on lockdown," she says.

In contrast, today's IT departments have limited ability to control what's on their networks because networks contain far too many endpoints to manage. Employees access networks using a multitude of mobile devices, each with different versions of varying operating systems. They perform tasks on a variety of client-based and cloud-based applications, exchange files on various cloud services, some of which may be outside the company network (shadow IT), and visit websites containing malware that antivirus software has yet to blacklist. And lockdown as a response to a cyber attack is no longer an option because most IT infrastructures are made up of so many physical, virtual, and cloud-based components that it's impossible to do so.

You Will Be Breached

Antivirus software, along with other perimeter defense solutions, no longer can guarantee protection from the seemingly countless types of malware infiltrating networks. According to Verizon's "2015 Data Breach Investigations Report," malware is part of the event chain in virtually every security incident. Moreover, Verizon's survey points out that between 70 and 90 percent of malware found in breach investigations are unique to the organization that has been compromised.

In addition, 80 percent of malware is delivered via exploit kits, and 80 percent of subsequent malware infections come as a result of application vulnerabilities, Bustamente says, citing recent Malwarebytes threat research. The latter statistic is not surprising. In 2004, Carnegie Mellon University published a definitive study finding that commercial software has, on average, 20–30 errors for every thousand lines of code (LOC). Even if that number were cut in half over the last 10 years, it would still come out to about 10,000 bugs per one million lines of code. And commonly used enterprise suite Microsoft Office 2013 is made up of about 45 million LOC.

"You can design your perimeter framework as best as possible, but the reality is that in today's environment, you will be breached," Bustamente says. "And companies acknowledge that regardless of the technology they invest in, they continue to experience infections."

The Need for a Layered Approach

The first step to improving security is to take a layered approach, one that doesn't place excessive reliance on a single tool or

"A layered cybersecurity plan will only be an effective one if the proper groundwork is laid, and each layer is carefully considered. Otherwise the complexities inherent in trying to integrate multiple solutions will cancel out any potential benefit."

tactic to stop malware from damaging the network. "A robust layered information security framework should include employee education, the deployment of network connection firewalls and sandboxes, endpoint security, and the creation of crisis response teams," Bustamente says. Antivirus software would play a supporting role in this framework, rather than a primary one.

Ideally a layered cyber defense strategy works much like a series of spider webs. For example:

- A firewall sandboxes any malware that antivirus software fails to identify
- Employee education teaches staff not to click on an unfamiliar or unexpected file delivered by email, but instead contact IT immediately.
- A comprehensive backup and disaster recovery solution enables IT staff to quickly restore files to their original state in order to minimize downtime and avoid paying ransoms
- Strong authentication and access control can strip a BYOD smartphone of its credentials the moment it is reported lost or stolen.
- Automating alerts for updates and changes in preset baseline thresholds lets IT staff know when to apply patches or take other measures without having to monitor all the data that passes through their networks on a given day, hour, or even minute.

Because a variety of tools collaborate to preserve secure boundaries, the majority of threat actors will be less able (or inclined) to attempt breaching networks.

Challenges of Implementing Layered Security

At the same time, a layered cybersecurity plan will only be an effective one if the proper groundwork is laid, and each layer is carefully considered. Otherwise the complexities inherent in trying to integrate multiple solutions will cancel out any potential benefit. "These various software packages could be incompatible with one another, duplicate similar processes, or otherwise render other solutions within an IT environment useless," DiDio cautions.

Even when the layers do work together, organizations must commit themselves to maintaining the same level of agility that threat actors continuously demonstrate in their methods of attack. If the various layers are not properly monitored and updated, particularly as new threats emerge, organizations risk finding themselves in a similar predicament to the days when they relied on so-called "silver bullet" solutions such as antivirus suites.

Finally, a layered security strategy still relies on a fortress-style framework designed to keep malware out. It doesn't necessarily address ways to discover and remediate malware that has sneaked past "the moat," as Bustamente puts it.

A New Approach: Hunting for Malware

When effectively integrated into the organization, antivirus and related solutions can repel malware at the gates and can protect organizations from inventive threat actors and sophisticated, rapidly mutating malware. Yet, the tools that make up a layered cybersecurity strategy are not often effective in finding malware, much of which may be hidden or lying dormant in a network waiting to strike.

Therefore, a new proactive approach to cybersecurity is needed, one that acknowledges the inevitability of malware breaching networks and the importance of detecting that breach as quickly as possible. This approach requires tools that can hunt down malware, no matter how it infiltrates a network, and then destroy it before it can irreparably damage the safety and reputation of organizations, their partners, and their customers.

An effective malware hunting tool focuses on heuristics rather than static signatures, locating malware by studying the behavior of applications and files and then comparing those behaviors to those of "normal" applications, as well as those commonly manifested by malware.

Sun Products Corporation cleans up malware

A leading provider of household products adds a layer of protection against malware and exploits with Malwarebytes Endpoint Security.

The Sun Products Corporation makes many of the well-known brands found in the laundry rooms of homes across America, including Wisk, Sunlight, Snuggle, and Surf. Fifteen hundred employees work in 11 locations in the U.S. and Canada.

In spite of a robust, layered approach to enterprise security, malware continued to find its way inside the company. Malicious content arrived through emails or from infected websites. Once in, malware would propagate quickly, bubbling up like soapsuds across the company.

The IT team fought back with a range of tools. If one tool wasn't able to remove the malware, they tried another tool. It typically consumed up to three hours to clean up a machine or completely wipe and re-image it.

The Sun Products IT team selected Malwarebytes Endpoint Security for Business, which includes Malwarebytes Anti-Malware for Business, Malwarebytes Anti-Exploit for Business, and the Management Console. With Malwarebytes' ability to block malicious websites and proactively address malware, the company is no longer in firefighting mode.

"We're very happy with the performance of Malwarebytes," said John Major, IT Operations Manager for Sun Products. "No other product we tried does what Malwarebytes does as well. It's been much quieter since we deployed Malwarebytes Endpoint Security. It's been a breath of fresh air for us."

An effective malware hunting tool performs intrusion assessment in a number of ways, including:

- Leveraging information from the latest threat research on malware behaviors
- Scanning using the constantly updated IOC (Indicators of Compromise) information
- Seeking out seemingly minuscule alterations in files and apps, such as a change in color of a file icon
- Scanning every endpoint, no matter how many exist on the network
- Creating rules that catch zero-day exploits and push those rules out to every endpoint on the network to isolate potential malware

This malware hunter would then isolate and destroy the malware, and forward the results to a sandbox or SIEM for forensics purposes. The SIEM correlates the information and creates fast alerts to report the intrusion to the appropriate people so that, for example, the IT staff could patch the vulnerabilities that enabled penetration, stop secondary infections from taking place, and inform other stakeholders of the situation in order to mitigate any potential damage caused by the breach.

A malware hunting tool is akin to a bounty hunter for an organization's security stack because it works as a back up to other methods of malware detection—and it can destroy malware. Given that no security strategy is 100 percent foolproof and breaches are inevitable, this hunting tool can target any malware that slips past other defenses and hunt it down before the latter can stalk and destroy anything of value to the organization.

Conclusion

Mounting an effective defense against malware involves the integration of antivirus and anti-malware solutions as part of layered approach to security. However, despite the existence of multifaceted approaches to enterprise security, companies cannot assume that their primary line of defense will always win the fight against malware. By embracing proactive detection, which recognizes the ingenuity and technical resources available to cyber criminals, companies can mount a credible and defensible approach to the detection, prevention, and remediation of threats.

About Malwarebytes

Malwarebytes provides anti-malware and anti-exploit software designed to protect users against zero-day threats that consistently escape detection by traditional endpoint security solutions. Malwarebytes Anti-Malware earned an "Outstanding" rating by CNET editors, is a PCMag.com Editor's Choice, and was the only security software to earn a perfect malware remediation score from AV-TEST.org. That's why large Enterprise businesses worldwide, including Disney, Dole, and Samsung, trust Malwarebytes to protect their mission-critical data. For more information, please go to www.malwarebytes.org/business.

About ISMG

Headquartered in Princeton, New Jersey, Information Security Media Group, Corp. (ISMG) is a media company focusing on Information Technology Risk Management for vertical industries. The company provides news, training, education and other related content for risk management professionals in their respective industries.

This information is used by ISMG's subscribers in a variety of ways—researching for a specific information security compliance issue, learning from their peers in the industry, gaining insights into compliance related regulatory guidance and simply keeping up with the Information Technology Risk Management landscape.

Contact

(800) 944-0401

sales@ismgcorp.com

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY CAREERS INFO SECURITY® Data Breach Prevention. Response. Notification. TODAY

ISMG INFORMATION SECURITY MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismgcorp.com