

Mapping traditional AV detection failures

October 2017

TABLE OF CONTENTS

[Introduction](#) 01

[Methodology](#) 02

[Findings](#) 03

 AV failures common malware 03

 Multiple AV failures 04

 Four leading AVs failures 05

[Conclusion](#) 07

[About Malwarebytes](#) 08

Introduction

Comparative efficacy testing of antivirus (AV) has become increasingly popular as a multitude of solutions, based on the same core technologies, have flooded the market. Those that perform well under these parameters tout the results as a stamp of approval. However, the true value of these tests is yet to be determined, as malware in the wild behaves in a manner significantly different from laboratory samples—even recently captured samples apprehended in security honeypots.

It is little consolation to a business locked down from ransomware that the AV they have installed recently demonstrated positive results and high scores in the latest test (conducted with known malware in a controlled environment).

One way to truly gauge the effectiveness of today's traditional AV solutions is by analyzing real-world data. In the real world, user behavior, malware characteristics and evasion tactics, divergent endpoint and system components, and the proactivity of information technology personnel introduce significant variables that tax market traditional AV solutions—sometimes well beyond their limit.

Malwarebytes captures in-the-wild data while cleaning up the mess that other traditional AV platforms leave behind

Malwarebytes has been the secret weapon of IT professionals for nearly a decade. Often carried by IT staff on a USB thumb-drive, Malwarebytes can be plugged into a troublesome, suspect endpoint to scan and remediate malware and virus infections with the world's most powerful malware removal tools.

Methodology

The following data comes from real-world scans performed by Malwarebytes in the wild for six months, January through June 2017. During a scan, Malwarebytes inspects system components and software for legitimacy and indications of compromise. Legitimate software is recognized and stays on the system. Malware is identified and removed.

Malwarebytes gathered the following information from scans of approximately 10 million endpoints, the vast majority of which had one or more traditional AV tool registered on the Windows® Security Center Service. Our data looks at instances where Malwarebytes was used solely for remediation and excluded data where Malwarebytes proactively blocked threats. The results of these scans clearly indicate the weaknesses of traditional AV solutions and provide a real-time look at how often traditional AV solutions fail outside of the controlled laboratory test bed.

1. In real-world deployments, traditional AV solutions fail to protect against even the most common forms of malware encountered in the wild.

Top five ransomware types compromising an endpoint with traditional AV installed (percentage of all endpoints with ransomware compromises seen):

- HiddenTear 41.65 percent
- Cerber 18.2 percent
- DMALocker 5.17 percent
- Locky 3.75 percent
- FileCryptor 3.12 percent

Top five botnets detected on a compromised computer with traditional AV installed (percentage of all endpoints with botnet infections seen):

- IRCBot 61.56 percent
- Kelihos 26.95 percent
- Qbot 7.13 percent
- Gamarue 3.68 percent
- Upbot 1.43 percent

Top three Trojans compromising an endpoint with at least one traditional AV solution installed (percentage of all endpoints with botnet infections seen):

- Fileless 17.76 percent
- DNSChanger 17.51 percent
- BHO 5.29 percent

2. Endpoints with multiple traditional AV solutions installed performed only marginally better than those with a single traditional AV installed, displaying consistent weaknesses against the most common forms of cyberattacks.

39.21 percent of all malware attacks in the wild among endpoints with AVs installed occurred on endpoints that had two or more traditional AV solutions installed. All endpoints were then remediated by Malwarebytes.

Traditional AV is poor against most common ransomware:

- Percentage of Hidden Tear events on endpoints that had an AV installed that got past multiple traditional AV solutions: 51.75 percent
- 36.17 percent of Cerber events on endpoints that had an AV installed evaded multiple traditional AV solutions

Your traditional AV is vulnerable to most common botnets

- 29.06 percent of the Kelihos compromises remediated by Malwarebytes were on endpoints that had multiple traditional AVs installed on the endpoint
- 22.13 percent of the IRCBot compromises remediated by Malwarebytes were on endpoints that had multiple traditional AVs installed on the endpoint

Traditional AV is susceptible to most common Trojans

- 46.04 percent of the DNSChanger infections remediated by Malwarebytes were on endpoints that had multiple traditional AVs registered on the endpoint
- 40.5 percent of the fileless malware infections remediated by Malwarebytes were on endpoints that had multiple traditional AVs registered on the endpoint

3. Even the four leading traditional AV solutions perform poorly in the real world, with consistent weaknesses against common ransomware, botnets, and Trojans.

A total of 95 traditional AV solutions were detected as registered software on the approximately ten million endpoints Malwarebytes scanned in this data set.

For comparative purposes, Malwarebytes tracked the failure rate of the four leading traditional AV solutions recommended in a recent, high-profile industry analysis used by many enterprises to inform their purchasing decisions. Thus, we could ascertain differences in laboratory performance from real-world protection and detection.

Examining our data, 10.01 percent of the endpoints with an AV installed included in our sample period had one of the four leading traditional AV solutions registered.

When comparing only endpoints with premium traditional AV registered (paid or corporation-deployed) by eliminating the compromised endpoints running free, bundled traditional AV from OS manufacturers from the data set, we can rank the effectiveness of all paid traditional AV solutions to threats encountered in the wild.

Completing this calculation, we were surprised to learn that one of the four leading traditional AV solutions was deployed on 39.16 percent of the millions of compromised endpoints we inspected and remediated.

Today's common threats are not always stopped by the four leading traditional AV brands

If a compromised endpoint had a premium traditional AV (paid or corporation-deployed) registered, at least one of the four leading traditional AV brands was installed on:

- 48.59 percent of total Hidden Tear compromises detected and removed by Malwarebytes
- 26.78 percent of Cerber infections
- 59.09 percent of IRCBot compromises
- 29.94 percent of endpoints commandeered by fileless malware

A total of 95 traditional AV solutions and other security products were documented on endpoints. Among compromised endpoints with premium traditional AV installed, the percent of the top four leading traditional AV brands represented the following:

- Brand A was registered on 12.90 percent of compromised computers
- Brand B was registered on 11.75 percent of hijacked endpoints
- Brand C was registered on 9.23 percent of hacked computers
- Brand D was registered on 5.28 percent of the compromised endpoints

Compared to their overall rate of compromise, the top four leading traditional AVs demonstrated significant variability and weaknesses when we examined how they fared against prolific forms of malware:

Weak against common ransomware

- Brand A had 84.16 percent more endpoints compromised by Hidden Tear than they should have, given their overall failure rate.

Weak against normal botnets

- Brand C experienced a ratio of Kelihos botnet compromise 14.6 percent more than they should have, given their overall failure rate.
- Brand D demonstrated vulnerability to Kelihos as well, with 9.3 percent more infected endpoints than their average failure rate.
- Brand C showed a weakness against IRCBot, with 343 percent more compromises than their overall failure rate.

Weak against everyday trojans

- Brand A also didn't fare well against the DNSChanger trojan, with 150 percent more compromises above their average failure rate.

Weak against emerging fileless attacks

- Brand C experienced 23.4 percent more security compromises against fileless attacks than their failure rate.

Conclusion

With their extensive roster of known malware samples, comparative AV testing labs cannot accurately replicate the results of actual global deployments and the actions and evasive behavior of malware rampant in the wild.

Malwarebytes' analysis using nearly ten million endpoints scanned shows that "new and improved" AV appear to be the technology of the past, dressed in new packaging. Even the top-rated, highly-lauded, "recommended buy" AV solutions continue to struggle in real-world applications. These brightly packaged solutions miss threats targeted at end users and their computers.

Our business and personal lives depend on computing. Malware and cyberthreats can have devastating consequences at work and at home. Trusting traditional AV alone is a losing proposition for individuals and businesses seeking a malware-free existence.


ABOUT MALWAREBYTES


Malwarebytes is the next-gen cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against dangerous threats such as malware, ransomware, and exploits that escape detection by traditional antivirus solutions. The company's flagship product combines advanced heuristic threat detection with signature-less technologies to detect and stop a cyberattack before damage occurs. More than 10,000 businesses worldwide use, trust, and recommend Malwarebytes. Founded in 2008, the company is headquartered in California, with offices in Europe and Asia, and a global team of threat researchers and security experts.

Copyright © 2017, Malwarebytes. All rights reserved. Malwarebytes and the Malwarebytes logo are trademarks of Malwarebytes. Other marks and brands may be claimed as the property of others. All descriptions and specifications herein are subject to change without notice and are provided without warranty of any kind.

 Santa Clara, CA

 malwarebytes.com

 corporate-sales@malwarebytes.com

 1.800.520.2796