

70% of Malware Infections Go Undetected by Antivirus Software, Study Says



MARITZA SANTILLAN ([HTTPS://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/CONTRIBUTORS/MARITZA-SANTILLAN/](https://www.tripwire.com/state-of-security/contributors/maritza-santillan/))

Follow @ritzanti

FEB 13, 2015 | LATEST SECURITY NEWS ([/STATE-OF-SECURITY/TOPICS/LATEST-SECURITY-NEWS/](https://www.tripwire.com/state-of-security/topics/latest-security-news/))

([HTTPS://WWW.TRIPWIRE.COM/STATE-](https://www.tripwire.com/state-)



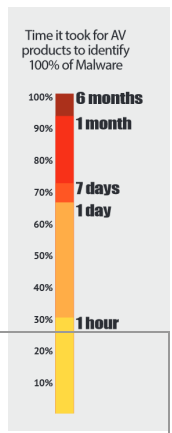
31

According to recent research, the average enterprise receives nearly 17,000 malware alerts per week; however, of these alerts, only 19 percent are considered reliable and a mere 4 percent are further investigated by security engineers.

As IT teams are bombarded with “noise,” and potentially legitimate threats, Damballa’s latest State of Infections report revealed that Antivirus (AV) products overlooked 70 percent of malware infections within the first hour.

After 24 hours, 66 percent of these malicious files were detected, and after one week, a total of 72 percent were successfully identified. It took AV products one month to detect 93 percent of the malicious files analyzed, and more than six months for 100 percent of the malware to be discovered.

“In a real world environment, a file would only be scanned once by AV,” read the report. “If the average security team received 17,000 weekly alerts, or 2,430 daily, AV products would have missed 796 malicious files in day one.”



Source: Damballa State of Infections Report, Q4 2014

“Consider the risk associated with that number of infections potentially dwelling undetected inside the network.”

As Damballa CTO Brian Foster explains, the ‘dwell time’ until hundreds of harmful files are identified and addressed could have serious consequences for any enterprise.

“If it took you six months to get detected, that’s six months when that hacker has had access to one of your systems,” said Foster.

The study analyzed tens of thousands of files submitted by companies for review using the four most commonly deployed AV products, although the names of these specific products were not disclosed.

Daniel Schneersohn, APAC VP at Damballa, acknowledges the challenge that IT security teams deal with in order to identify “the needle in the haystack” from the overwhelming amount of alerts.

“In the case of Target, for more than three months, they had several systems that were warning them of the infection, but it is just part of the hundreds of alerts the same system was sending them; all of the other ones were false positives,” said Schneersohn (<http://www.zdnet.com/article/security-engineers-are-playing-russian-roulette-with-alerts-damballa/>).

With an infinite number of malware code at attackers’ disposal and only a finite number of skilled security staff on deck, it’s critical that security professionals implement a “forward-thinking breach readiness strategy,” concludes the report.

“Enterprises should prevent what they can, and there are millions of known threats that can be identified with AV,” said Foster (<http://www.eweek.com/security/new-malware-too-often-escapes-antivirus-detection.html>). “But the real threat lies in what AV can’t identify.”

◀ 31

0 Comments **The State of Security**

 Login ▾

 Recommend  Share

Sort by Best ▾






Start the discussion...


LOG IN WITH

OR SIGN UP WITH DISQUS 

Name

Be the first to comment.

 Subscribe  Add Disqus to your site [Add DisqusAdd](#)  Privacy



Subscribe!

JOIN 20,000+
SECURITY PROS

Get our top stories delivered
to your inbox every week!

Security Configuration Management ...made easy.

DOWNLOAD EBOOK

([https://www.tripwire.com/solutions/configure-and-harden-your-systems/security-configuration-management-for-dummies-](https://www.tripwire.com/solutions/configure-and-harden-your-systems/security-configuration-management-for-dummies-book-register/?utm_source=sos&utm_medium=sb-bnr&utm_content=pdf&utm_campaign=scm-for-dummies)

[book-register/?utm_source=sos&utm_medium=sb-bnr&utm_content=pdf&utm_campaign=scm-for-dummies](https://www.tripwire.com/solutions/configure-and-harden-your-systems/security-configuration-management-for-dummies-book-register/?utm_source=sos&utm_medium=sb-bnr&utm_content=pdf&utm_campaign=scm-for-dummies))

DRIVING DEVOPS SECURITY

SECURE YOUR NETWORK.
SAVE TIME.
GET THE BOOK.

DOWNLOAD

(<https://www.tripwire.com/solutions/devops/devops-book/?referredby=blogsidebar/>)

TOPICS

- [ICS Security \(/state-of-security/topics/ics-security/\)](/state-of-security/topics/ics-security/)
- [Cloud \(/state-of-security/topics/security-data-protection/cloud/\)](/state-of-security/topics/security-data-protection/cloud/)
- [IT Security and Data Protection \(/state-of-security/topics/security-data-protection/\)](/state-of-security/topics/security-data-protection/)
- [Latest Security News \(/state-of-security/topics/tripwire-news/\)](/state-of-security/topics/tripwire-news/)
- [Regulatory Compliance \(/state-of-security/topics/regulatory-compliance/\)](/state-of-security/topics/regulatory-compliance/)
- [Government \(/state-of-security/topics/government/\)](/state-of-security/topics/government/)
- [Vulnerability Management \(/state-of-security/topics/vulnerability-management/\)](/state-of-security/topics/vulnerability-management/)

ABOUT

- [About \(/state-of-security/about/\)](/state-of-security/about/)
- [Contributors \(/state-of-security/contributors/\)](/state-of-security/contributors/)
- [Write for us \(/state-of-security/about/contact-us/\)](/state-of-security/about/contact-us/)
- [Privacy Policy \(/legal/privacy/\)](/legal/privacy/)
- [Tripwire.com \(/\)](/)

CONTACT US

US Headquarters
101 SW Main St., Ste. 1500
Portland, OR 97204

(<https://www.google.com/maps/place/One+Main+Place,+101+SW+Main+St+%231500,+Portland,+OR+97204/@45.5155036,-122.6775251,17z/data=!3m1!4b1!4m5!3m4!1s0x54950a0fb0d1122.6753364>)

Direct: 503.276.7500 (tel:5032767500)

[International Offices \(/contact/\)](/contact/)

SEARCH

