# Stacked Security Tools Detect Less Malware Than Predicted: Study

By Robert Lemos | Posted 2013-05-26 Email Print



## Combining two security products can improve detection rates of attacks, but generally less than predicted, research finds.

Security companies tend to use the same threat data to construct their defenses against the latest attacks, a practice that causes different security products to fail to catch specific attacks more often than expected, according to a report released by security information firm NSS Labs.

In tests over the past 18 months, the company evaluated 37 intrusion-prevention systems, antivirus programs and next-generation firewalls and found that none of them stopped every exploit in the company's testing

pool. While 19 out of the 606 combinations of two security products were able to stop all the exploits, combining two products tended to not produce the level of improvement expected, Stefan Frei, research director at NSS Labs, told *eWEEK*.

"Layered security performs well if you do the right combinations," he said. "If you don't do the right combinations, you will not see as much benefit."

The results of the tests suggest that security applications, even those from different vendors, tend to miss the same exploits. For example, in tests conducted against next-generation firewalls in 2013, eight exploits bypassed all nine devices tested, while it took at least 12 different intrusion-prevention systems to block all the exploits in the 2012 tests of those devices.



Overall, the number of attacks that are able to bypass more than one device are significantly higher than predicted by models that do not assume correlation between results, the report concluded.



"The test results show that, regardless of the security products deployed, it remains highly probable that a cyber-criminal will be able to successfully penetrate several layers of security of a targeted organization, or successfully attack a large number of different organizations," the report stated.

NSS Labs combined data from several previous studies in the last 18 months and examined the correlation between the exploits missed by each product. In its tests, the company studied the effectiveness of 16 intrusion-prevention systems and eight next-generation firewalls against 1,486 exploits in 2012.

In 2013, the company performed more tests against the next-generation firewalls, including an additional vendor and tested 13 endpoint-protection systems, more commonly known as antivirus software, against 43 recent exploits. No attacks using zero-day vulnerabilities were used.

The average failure rate for intrusion-prevention systems and next-generation firewalls varied between 4 and 9 percent, depending on the test. The failure rate using two systems in combination was 0.8 percent. The average failure rate for the endpoint-protection products against the 43 recent exploits was 45 percent, while using two products together reduced it to 26 percent.

The vulnerabilities exploited in the tests consisted of 21 percent of the most highly critical vulnerability affecting 208 vendors in the past decade, the company said.

The study found that many products missed a "significant number" of older exploits, and that basic evasion techniques—such as delivering an exploit using secure HTTP instead of simple HTTP—foiled many defenses.

LATEST STACKED SECURITY TOOLS DETECT LESS MALWARE THAN PREDICTED STUDY ARTICLES

- Home Depot Security Breach Affects 56M Credit Card Holders
- Bitcoin Poses Danger to British Economy, Warns Bank of England
- Home Depot Confirms Data Breach but Gives Few Details
- IBM Buys Lighthouse Security Group for Cloud-Based Identity Management
- IBM Acquires Security Software Provider CrossIdeas

Submit a Comment

There are no comments for this article yet.

Manage your Newsletters: Login Register My Newsletters

Enter your E-mail Address

- [x] eWeek Editor's Pick
- [ ] News & Views
- [ ] Cloud Computing
- [ ] Mobile and Wireless Update
- [ ] Best of eWeek
- [ ] eWeek Sunday Brunch
- [ ] eCareers Smart Moves
- [ ] Enterprise Applications Topic Center Update
- [ ] Enterprise IT Advantage
- [ ] eWeek Whitepaper Spotlight
- [ ] eWeek Labs
- [ ] eWeek Enterprise Update
- [ ] eWeek Storage Report
- [ ] Industry Center Update : Finance
- [ ] Industry Center Update : Government
- [ ] Industry Center Update : Health Care
- [ ] Infrastructure Topic Center Update
- [ ] Linux & Open Source Topic Center Update
- [ ] Mid-Market Solutions
- [ ] Securing the Enterprise
- [ ] VoIP Topic Center Update
- [ ] What's Hot Now
- [ ] eWeekend

Safari Power Saver
Click to Start Flash Plug-in



MOST POPULAR

- News and Reviews

- Slideshows

- Home Depot Rushes to Deploy EMV Cards in Wake of Massive Data Theft
- Samsung's New Galaxy Tab S Tablets Available for Preorder by AT&T
- Microsoft Plans Early 2015 Windows Phone 9 Developer Preview
- Apple Sells 10 Million iPhone 6 Devices in First Weekend After Launch

- Topics by Type
- Android
- Apple
- Cloud
- Database
- Developer
- Enterprise Apps
- Innovation
- IT Management
-
- Mobile
- Networking
- PC Hardware
- Security
- Servers
- Small Business
- Storage
- Virtualization
- Articles by Type
- News & Analysis
- Slideshows
- Blogs
- Reviews
- Video
-
- Contact Us
- About eWeek
- Sitemap
- Blogs
- Security Watch

- Upfront
- First Read
- Storage Station
- Careers
- Google Watch

- Special Features
- eWeekChat
- eWeek 30th Anniversary
- Cloud Backup Project Center
- Next Generation Firewall Project Center
- Big Data Analytics Project Center
- Research Center