

# THE UNKNOWN 300 TEST REPORT

**ACROSS 4 TESTED  
VENDORS, CHECK POINT  
SECURITY SOLUTIONS  
LED WITH INDUSTRY'S  
BEST CATCH RATE**

## About VirusTotal

VirusTotal is a Google-owned service that analyzes suspicious files and URLs and maintains a malware database that is shared with the security research community.

Organizations today are facing unprecedented growth in the diversity and number of security threats from advanced and sophisticated malware. New attack types combine known and unknown threats to exploit “unknown” vulnerabilities. Attackers are also hiding malware inside documents, websites, hosts and networks. These attacks have many purposes such as financial and ideological motives. They focus on stealing data, sabotaging business continuity, or damaging a company’s reputation.

This document describes Check Point testing methodology for catching malware and compares Check Point products with other competing solutions. The goal of the test is to provide the catch rate performance amongst various market offerings.

The net result, across 4 tested vendors of Check Point, FireEye, Palo Alto Networks and Fortinet, was that Check Point security solutions led with industry’s best catch rate of 100% followed by FireEye at 70%.

## TEST OVERVIEW

Check Point research analysts downloaded a sample set of 300 well-known malicious PDF, DOC and executable files from Google’s “VirusTotal” database. They then used a simple technique to create new and unknown variants (hence the “Unknown 300”) from existing malware. The resulting 300 samples preserved the original malicious functionality but are unknown and unregistered in any hash-based database such as VirusTotal. With this set of unknown malware samples, the analysts tested Check Point and other vendors’ solutions ability to detect new and unknown malware.

## TESTED VENDORS

- Check Point—ThreatCloud™ on 13500 gateway
- FireEye—MVX on NX series 1310
- Palo Alto—WildFire Cloud on PA-5020 gateway
- Fortinet—FortiSandbox Cloud on FG-1500D gateway

To ensure the test validity, platforms were updated and patched with the latest firmware and updates available from each vendor as of mid July 2014. The test configuration also matched the vendor’s best practices. The only objective of the test was to test the catch rate of malicious files. Performance was not tested and did not influence the test results in any way.

## SECURITY FINDINGS

As the Check Point research analysts were conducting the “Unknown 300” test, they came across security findings that are important to consider in the fight against malware.

### File Size

Malware comes in many sizes and a security solution should offer the flexibility to accommodate varying file sizes. Palo Alto Networks has a default size limit of only 500Kb ([max 1Mb](#)) for PDF files that can be scanned by the WildFire emulation cloud. Many PDF files queried by VirusTotal were above 1Mb.

## PALO ALTO NETWORKS LIMITS YOU TO 1MB PDF FILE SIZE FOR THREAT EMULATION

## FIREEYE DOESN'T SCAN INSIDE SSL TRAFFIC

## PALO ALTO NETWORKS AND FORTINET CAN DETECT BUT CANNOT PREVENT UNKNOWN MALWARE

### SSL Traffic

Malware doesn't discriminate whether it arrives at your network encrypted or not. It is critical to scan inside SSL traffic, the same way non-encrypted traffic is examined. FireEye does not support scanning inside SSL traffic, creating a potential vulnerability for your network.

### Detection versus Prevention

Many security solutions tested can detect the unknown malware but cannot prevent it from entering the network. For example, both Palo Alto Networks and Fortinet allow all files into the network while the suspicious files are being uploaded and emulated. There is a delay of 30 minutes for Palo Alto Networks and 60 minutes for Fortinet before updated signature blocks are created to block the unknown malware. This timeframe allows a significant window for malware propagation in the network. Additionally, emulation time in the Fortiguard cloud was the longest, more than 10 minutes a file on average.

### Archived Files

Many organizations use archived files such as rar. A security solution must support the inspection of archived files. The researchers found that Palo Alto Networks could not emulate any archive file except zip.

### Total Cost of Ownership

Many security solutions require separate appliances and do not support multi-protocol scanning on a single appliance. It is optimal for ease of deployment and management to choose a solution that can support multi-protocol scanning. For example, FireEye needs a separate appliance for email protection and for web protection, increasing the total cost of ownership.

### LAB SETUP

A lab was setup to simulate the reality of a user downloading an infected file. Figure 1 shows the configuration consistently used across all the tests. All platforms in the test were activated with the maximum number of threat prevention services (IPS, Anti-Malware, Anti-Bot, Threat Emulation) and with the most up-to-date signatures. The Unknown 300 files were a mix of 40% PDF files, 40% EXE files and 20% DOC files. The files were downloaded to a host behind the security device, simulating the accidental downloading of malware from a malicious Web page by an internal end-user. A different host header was used for each of the files to avoid "blacklisting" of the destination ip.



Figure 1: Lab Test Setup

### Sandboxing Solution Considerations

- Protect against the latest cyber threats: It's important that the solution has multiple layers of protection to deal with the latest cyber threats—both known and unknown.
- Inspect SSL Traffic: A solution that cannot scan for malwares in SSL traffic is blind to an important vector of attacks used by attackers.
- Prevent files from entering your network: Many solutions can only detect malware but not prevent it from infecting the network in the first place. This increases risk and compromises the security posture of the organization.
- Number of appliances required to inspect both web and email: Some solutions require a dedicated appliance for each protocol scanned (i.e. web, email, files) increasing TCO and complicating management.
- Inspect all archive types: Malware that is compressed in an archive file (zip, rar, etc.) cannot be detected by some solutions, making this attack a very common vehicle for hackers.

## CREATING THE UNKNOWN 300

To develop the unknown malware test, the researchers queried VirusTotal for pdf, doc and portable executable files that were detected as malicious by at least 10 antivirus engines. All candidate files were uploaded to VirusTotal after July 2014, had a size of 1MB or less, and demonstrated various malicious behaviors. From this selection, 300 files were randomly chosen (120 PDF, 120 EXE, and 60 DOC).

Using this sample of 300 known malware, Check Point research analysts added a null to the end of each PDF and DOC file (e.g. "echo `0000` >> 1.doc"). In addition, an "unused" header section was modified on each executable file. The analysts then opened and ran each file to validate that the original behavior was kept unchanged. For the executables, a free tool named [LordPE](#) was used to change the checksum as shown in Figure 2.

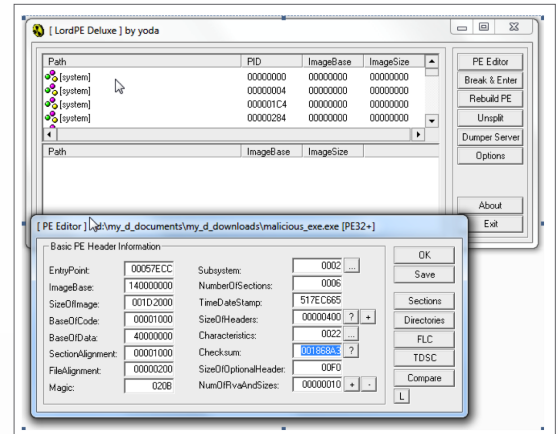


Figure 2: Modifying EXE file checksums

## TEST RESULTS

The catch rate when scanning these varying file types by each vendor is shown in Figures 3 - 6.

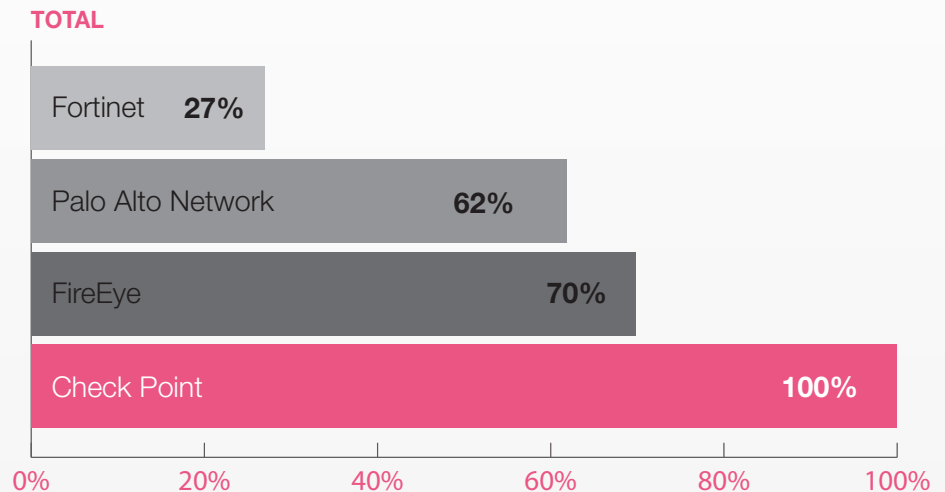


Figure 3

**PDF**

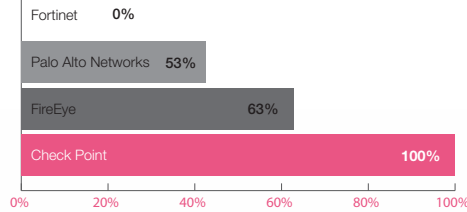


Figure 4

**EXE**

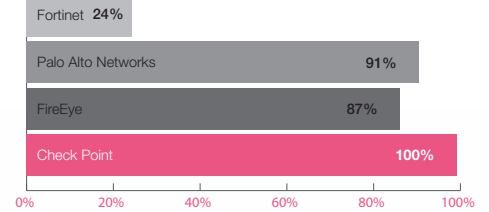


Figure 5

**DOC**

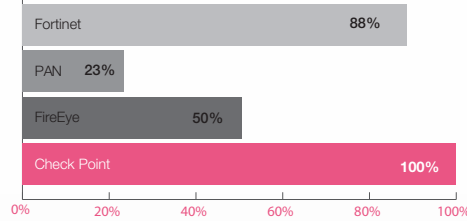


Figure 6

**SUMMARY**

When it comes to protecting your organization, it is optimal to choose security solutions with the best malware catch rate. Your organization's security should not be at risk from the Unknown 300. If you would like to replicate this test, please contact us at [threatprevention@checkpoint.com](mailto:threatprevention@checkpoint.com).

Given the disruption and loss of productivity that both known and unknown malware can cause, taking the time to verify claims by various vendors on their catch rate is a worthwhile effort.

---

For more information, contact us at: [threatprevention@checkpoint.com](mailto:threatprevention@checkpoint.com)

---