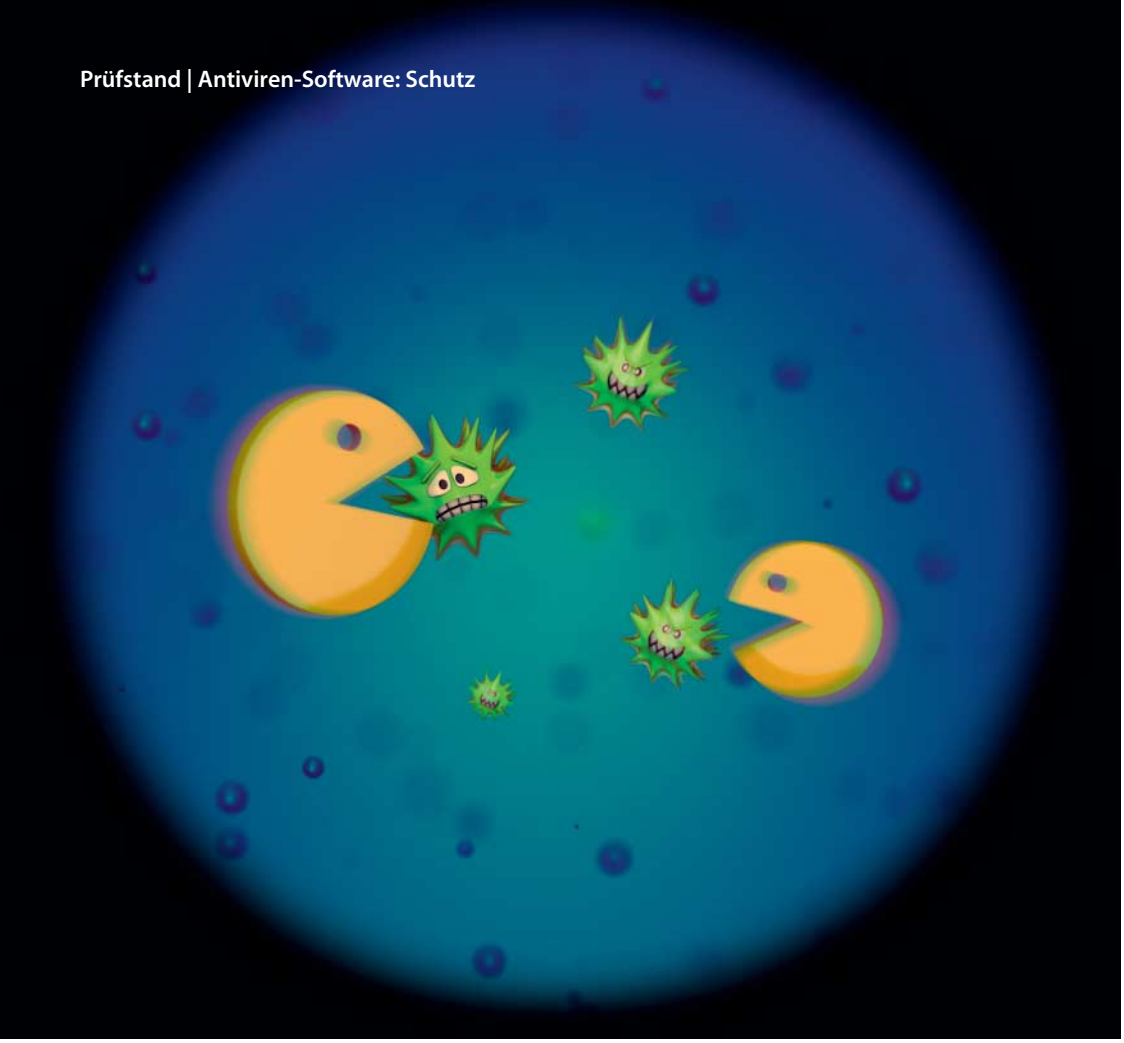


Jürgen Schmidt

Der Trojaner-Test

So gut schützen Virenwächter

In unserem Trojaner-Test dürfen 20 Antiviren-Programme beweisen, dass sie tatsächlich bei einem versehentlichen Klick auf einen Trojaner schützen. Manchen gelang das deutlich besser als anderen.

Antiviren-Programme müssen gerade dann schützen, wenn der Anwender eine Dummheit macht. Also wenn er etwa auf eine Trojaner-Mail hereingefallen ist und selbst eine bösartige Datei startet, die seinen Rechner mit Schadprogrammen infizieren will. Denn das Problem ist in den letzten Jahren eher schlimmer geworden als besser. Rechnungen, Lieferbenachrichtigungen oder Sicherheitsnachfragen – immer mehr Kommunikation läuft über E-Mail ab. Und immer bessere Imitate lassen sich kaum noch von den richtigen und dann auch tatsächlich wichtigen Nachrichten unterscheiden.

„Guten Tag Herr Schmidt, mit dieser E-Mail erhalten Sie Ihre aktuelle Mobilfunk-Rechnung" – ob das jetzt wirklich von der Telekom, von Vodafone oder Arcor stammt oder doch ein gut gemachter Versuch ist, mich zum Öffnen des Anhangs oder des Links zu verleiten, kann ich an Äußerlichkeiten nicht mehr erkennen. Der Name stimmt, Ansprache und Rechtschreibung auch. Ich persönlich würde wohl misstrauisch werden, wenn an der Mail statt einer PDF-Datei ein ZIP-Archiv dranhinge. Aber bei meiner Mutter bin ich mir schon nicht mehr sicher, ob sie nicht doch das ZIP-Archiv und die dort enthaltene Datei „Rechnung_2014_09_1123539708687.pdf.exe" öffnen würde. Selbst wenn das „.exe" am Ende des Dateinamens ihr Misstrauen wecken würde – Windows versteckt diese informative Dateiendung standardmäßig.

Test-Aufbau

Genau diesen Fall stellt der Trojaner-Test nach. Wir haben über zwei Wochen hinweg aus allen auf dem Heise-Server ankommenden E-Mails alle ausführbaren Dateien herausgefiltert. Diese wurden dann direkt zu einem Testlabor geschickt. Das Ganze reicherten wir mit den ausführbaren Inhalten an, die sich in den Spam-Traps des nix-Spam-Projekts der iX-Kollegen verfingen.

Interessant dabei: Es waren zwar ein paar kaputte Dateien dabei – aber keine einzige wirklich harmlose Datei, über deren Nicht-Zustellung jemand erbost gewesen wäre. Es ist somit ernsthaft zu überlegen, ob man nicht von vornherein alle Mails mit ausführbaren Inhalten komplett sperrt.

Insgesamt fast 900 Schädlinge sammelten wir auf diesem Weg ein. Die wurden dann möglichst bald nach dem Eintreffen auf 20 Rechnern gestartet, auf denen jeweils eine Antiviren-Software mit aktuellen Updates installiert war. Das System hatte dabei eine funktionierende Internet-Verbindung – die Trojaner konnten also Unrat aus dem Netz nachladen. Genauso konnten aber auch die Wächter zusätzliche Informationen aus der Cloud einholen. Nach etwa 5 Minuten brach der Test ab und das System wurde gründlich auf Anzeichen einer Infektion untersucht. Danach wurde es für den nächsten Test wieder in einen sauberen Zustand versetzt. Die Basis war übrigens Windows 7 mit einer kleinen Auswahl zusätzlicher Software, die auf vielen PCs so anzutreffen ist.

Bei diesem Test werden die Schädlinge also tatsächlich ausgeführt und nicht wie etwa bei einem Scan mit Virustotal nur die verdächtigen Dateien analysiert. Das bedeutet, dass den Wächtern viel mehr Informationen zur Verfügung stehen als bei einem rein statischen Test. Sie können unter anderem das Verhalten des Schädlings beobachten und bei ausreichend vielen verdächtigen Aktivitäten einschreiten. Allerdings sind solche dynamischen Tests in Echtzeit sehr aufwendig. Besonders schwierig gestaltet sich die Auswertung der Ergebnisse. Wir arbeiteten dazu wie beim letzten Trojaner-Test mit dem in Österreich beheimateten Testlabor AV-Comparatives zusammen.

Sippenhaft

Deren Virenexperten sortierten die Schädlinge bei einer nachträglichen Analyse in 82 Malware-Familien ein. Darunter fanden sich unter anderem rund 80 ZBot-Variationen. Diese gehören zum Online-Banking-Schädling Zeus, der im Untergrund als Baukasten-Trojaner gehandelt wird. Viele ambitionierte Kriminelle kaufen sich einen Zeus-Bausatz und erstellen dann über das grafische User-Interface ihre jeweils maßgeschneiderte ZBot-Version,

die sie dann in Wellen über Bot-Netze in die Mailboxen ihrer anvisierten Opfer spülen.

Besonderes interessant auch, dass sich rund 70 Exemplare des Papras-Trojaners in den E-Mails fanden. Der enthält spezielle Rootkit-Funktionen, um sich tief in Windows zu verstecken, und hat es dann vor allem auf Passwörter und andere Zugangsdaten abgesehen. Darüber hinaus gab es unzählige unspezifische Downloader und Injector-Schädlinge, die das eigentliche Schadprogramm erst übers Netz nachladen. Teilweise geschieht dies erst, nachdem die Schutzfunktion von Antiviren-Software ausgehebelt wurde.

Damit etwa die Erkennung einer häufig auftretenden ZBot-Variante die Testergebnisse nicht allein durch ihre Masse dominiert, haben wir jede Malware-Familie nur einmal gewertet. Eine positive Bewertung gab es nur, wenn wirklich alle Varianten erkannt und blockiert wurden.

Ergebnisse

Wer die im Kasten rechts grafisch aufbereiteten Ergebnisse betrachtet, wundert sich vielleicht, dass dort keineswegs 20, sondern nur 13 Antiviren-Programme aufgeführt sind. Das kommt daher, dass wir bei mehreren Herstellern zwei Versionen parallel getestet haben. So interessierte uns, ob die Microsoft Security Essentials auf Windows 7 anders schützen als der in Windows 8.1 eingebaute Virenschutz namens Windows Defender.

Ebenso wollten wir wissen, ob die kostenlosen Versionen von Avast, AVG, Avira und Panda weniger Schutz bieten als die kostenpflichtigen. Und wir wollten klären, ob – wie vom Hersteller immer wieder betont – Kasperskys Internet Security Suite besser schützt als das reine Antiviren-Programm.

Um es kurz zu machen: Zumindest in diesem Test-Szenario konnten wir keinerlei Unterschiede ausmachen. Die Ergebnisse der Geschwister waren in allen Fällen identisch. Wenn das kostenpflichtige Avira einen Trojaner neutralisierte, gelang dies der kostenlosen Version ebenso. Und MSE schützt genauso gut beziehungsweise eher schlecht wie der Windows Defender. Deshalb gibt es bei den Ergebnissen pro Hersteller nur eine Spalte. Bei Avast testeten wir übrigens noch die Version 2014, nachdem uns der Hersteller versichert hatte, dass das Update auf die kurze Zeit später erscheinende Version 2015 keine gravierenden Änderungen an der AV-Engine mit sich bringen würde.

Die Besten

Anders als beim letzten Trojaner-Test vor knapp zwei Jahren gab es dieses Mal mehrere Programme, die eine exzellente Schutzwirkung entfalteten. Esets NOD32, F-Secure, Kaspersky, Symantec und – für uns überraschend – Trend Micro konnten in über 90 Prozent der getesteten Fälle ihr System sauber halten. Avast verpasste diese Marke nur ganz knapp. Damit verfehlte der beste der auch kostenlos erhältlichen Testkandidaten nur hauchdünn eine Spitzenwertung; der von Avast gebotene Schutz lag aber durchaus auf Augenhöhe etwa mit dem kostenpflichtigen Norton Security.

G Data hätte sich eigentlich ebenfalls ganz oben eingereiht. Allerdings war sich der G-Data-Wächter sehr viel öfter als die anderen nicht so ganz sicher und fragte beim Anwender nach, wie er denn mit dieser Datei verfahren wolle. Dafür stehen die vielen gelben Felder in der Ergebnis-Präsentation. Der Anwender musste in rund einem Drittel der Fälle selbst entscheiden, ob er das Programm ausführen oder es blockieren und in die Quarantäne verschieben möchte. Dies werteten wir lediglich als teilweise geschützt, was zu einer Abwertung in der Gesamtnote von G Data führte.

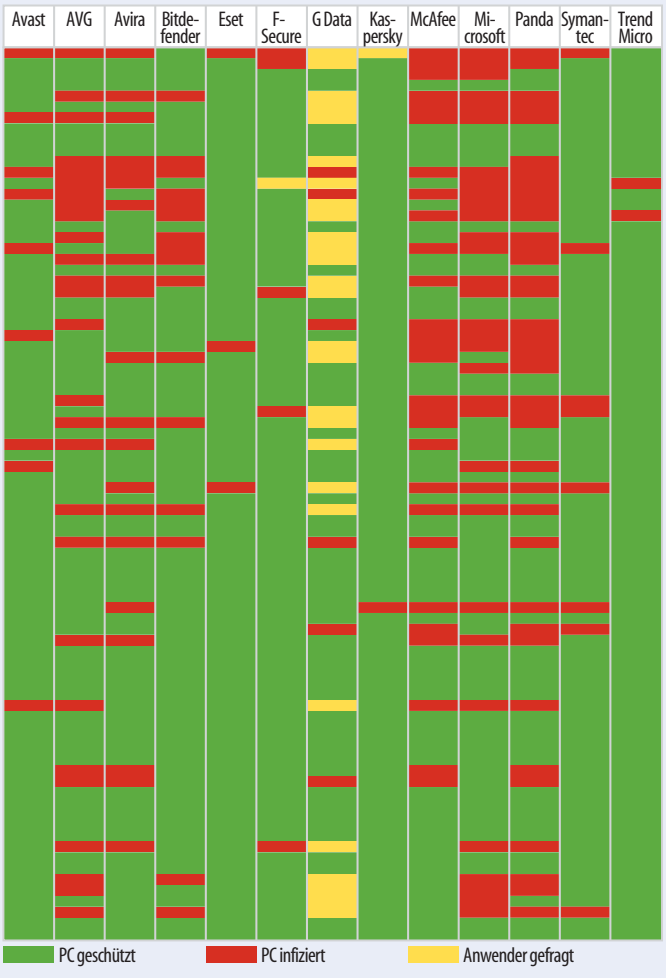
Dass der Trojaner-Test kein harmloser Dummy ist, den jeder schafft, beweisen die schlechten Ergebnisse einiger Kandidaten. Microsofts Basisschutz versagte bei rund 40 Prozent aller Trojaner. Das wurde nur noch von der Ausfallquote von Panda

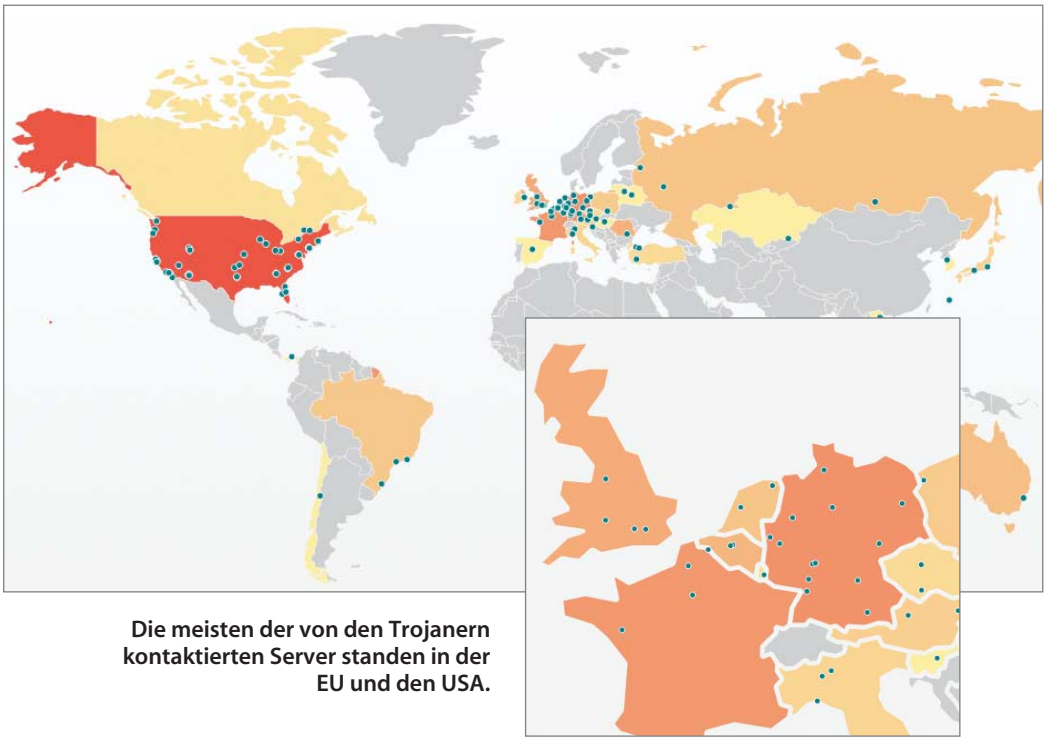
G Data überließ in vielen Fällen dem Anwender die Entscheidung, was zu tun ist.

Trojaner-Testergebnisse

Jeder Balken steht für eine Schädlingsfamilie, deren Angriffe entweder abgewehrt wurden (grün) oder zu einer Infektion des PC führten (rot). Bei gelb musste der Anwender entscheiden, was zu tun ist. Die guten Wächter haben also überwiegend grüne Spalten; bei denen mit viel Rot rutschten viele Trojaner durch.

Die Ergebnisse sind übrigens nach der Zeitspanne zwischen Eintreffen der Mail und dem tatsächlichen Start auf dem Testsystem sortiert. Man kann deutlich erkennen, dass bei den kürzeren Delays mehr Rot auftritt, während unten die komplett grünen Bereiche dominieren. Die Chancen, einen Trojaner abzuwehren, steigen also, wenn man eine Mail erst einen Tag später öffnet.





Die meisten der von den Trojanern kontaktierten Server standen in der EU und den USA.

unterboten, dessen hauptsächlich Cloud-basierte Virenwächter kaum mehr als eine Fifty-fifty-Chance auf Schutz boten. Darauf sollte man sich genauso wenig verlassen, wie auf Intels McAfee und AVG, die bei rund einem Drittel aller Schädlinge passen mussten.

Vor der abschließenden Bewertung noch ein paar erklärende Worte zur Bedeutung dieses Tests – und zu dem, was er nicht leisten kann. Das Testszenario ist darauf angelegt, den Schutz vor massenhaft verbreiteter Schad-Software etwa für den Online-Banking-Betrug, der Erpressung mit verschlüsselten Daten und Ähnlichem auf die Probe zu stellen. Gezielten Attacken etwa im Bereich der Industrie-Spionage, wo maßgeschneiderte Malware-Unikate zum Einsatz kommen, hat Antiviren-Software bekanntermaßen wenig entgegenzusetzen.

Wir haben mit diesem Trojaner-Test auch nur genau einen Infektionspfad getestet: Trojaner, die den Anwender via E-Mail erreichen. Das ist nach unserer Erfahrung ein sehr wichtiges Problem, denn viele der von uns untersuchten Rechner sind tatsächlich auf diesem Weg infiziert worden. Aber es ist nicht der einzige. Das zweite wichtige Einfallstor sind bösartige Webseiten, die gezielt Sicherheitslücken in veralteter Software ausnutzen, um das System zu infizieren.

Wir fanden jedoch keinen Weg, den Schutz vor solch bösartigen Webseiten sinnvoll, also herstellerunabhängig und zeitnah zu testen. Unser Eindruck ist jedoch, dass sich die Ergebnisse nicht grundsätzlich von denen des Trojaner-Tests unterscheiden würden. Denn häufig ist das nur ein alternativer „Vertriebsweg" für den gleichen Unrat.

Außerdem ist die Zusammensetzung der Schädlinge natürlich durch deren Ziel – also die Heise-Mail-Adressen und die Spam-Traps von nixSpam geprägt. Man muss davon ausgehen, dass die Ergebnisse insbesondere in anderen Regionen der Welt anders ausfallen würden. Überhaupt sollte man die exakten Prozentzahlen in den Testergebnissen nicht überstrapazieren. Allein durch eine etwas andere Gruppierung nach Familien schwanken diese um einige Prozent hin und her. Die Tendenz der Ergebnisse bleibt dabei jedoch erhalten und kann somit als aussagekräftig betrachtet werden.

Allerdings haben wir hier nicht getestet, wie viele Fehlalarme die Programme produzieren. Immerhin ist es eigentlich ganz simpel, einen Virenwächter mit hundertprozentiger Erkennungsrate zu bauen: Der verbietet dann einfach alles. Mehr dazu, wie die besseren der Virenwächter mit potenziell verdächtigen Dateien umspringen, verrät der auf Seite 126 folgende Praxistest.

Fazit

Der Test war schwierig zu bestehen; keiner der Wächter konnte alle Schädlinge abfangen. Wirklich erstklassigen Schutz demonstrierten denn auch nur die Virenwächter von Eset, Kaspersky und Trend Micro, denen nur vereinzelte Trojaner durchrutschten.

Das breite Mittelfeld bilden F-Secure, G Data, Symantec, Avast bis hin zu Bitdefender und so gerade noch Avira. Diese Programme kann man durchaus guten Gewissens einsetzen – insbesondere, wenn man die Ergebnisse aus dem Anwendungstest ab Seite 126 mit einbezieht.

„Besser als gar nichts" ist wohl das beste, was man über den Schutz der Virenwächter von AVG, McAfee, Microsoft und Panda sagen kann; verlassen sollte man sich darauf jedoch nicht. Wer Wert auf mehr als rudimentären Basisschutz legt, sollte sich lieber die anderen Kandidaten noch mal genauer ansehen.

Die kostenlosen Programme schnitten ohne Ausnahme genauso gut oder schlecht ab wie die käuflich zu erwerbenden Geschwister. So richtig überzeugen konnte aber nur der Schutz von Avast; Avira geht so grade noch. Microsofts Virenschutz kann da nicht mal ansatzweise mithalten und AVG AntiVirus Free 2015 und Pandas Free Antivirus sind keine Alternativen, die den Umstieg vom eingebauten Windows Defender lohnend erscheinen lassen. (ju)

Zusammenfassung der Testergebnisse

Hersteller	Avast	AVG	Avira	Bitdefender	Eset	F-Secure	G Data	Kaspersky	McAfee	Microsoft	Panda	Symantec	Trend Micro
Produkt(e)	avast! Free Antivirus 2014 / avast! Pro Antivirus 2014	AVG AntiVirus 2015 / AVG AntiVirus Free 2015	Avira Antivirus Pro / Avira Free Antivirus	Bitdefender Antivirus Plus 2015	Eset NOD32 Antivirus 8	F-Secure Anti-Virus	G Data Antivirus / G Data Internet Security	Kaspersky Anti-Virus 2015 / Kaspersky Internet Security 2015	McAfee LiveSafe 2015	Microsoft Security Essentials / Microsoft Windows Defender[2]	Panda Antivirus Pro 2015 / Panda Free Antivirus	Norton Security	Trend Micro Antivirus+ Security
blockiert	73	55	61	66	79	76	49	80	54	50	44	74	80
nachgefragt	0	0	0	0	0	1	27	1	0	0	0	0	0
infiziert	9	27	21	16	3	5	6	1	28	32	38	8	2
Schutz in %	89	67	74	80	96	93	76	98	66	61	54	90	98
Note	⊕	⊖	○	⊕	⊕⊕	⊕⊕	○[1]	⊕⊕	⊖	⊖	⊖⊖	⊕⊕	⊕⊕

[1] deutlich besser, wenn man die Nachfragen als vollwertigen Schutz interpretiert [2] integriert in Windows 8.1

⊕⊕ sehr gut ⊕ gut ○ zufriedenstellend ⊖ schlecht ⊖⊖ sehr schlecht