

OutbreakShield - Effektiver Sofortschutz bei Outbreaks von E-Mail-Viren

Ralf Benzmüller
G DATA Software AG

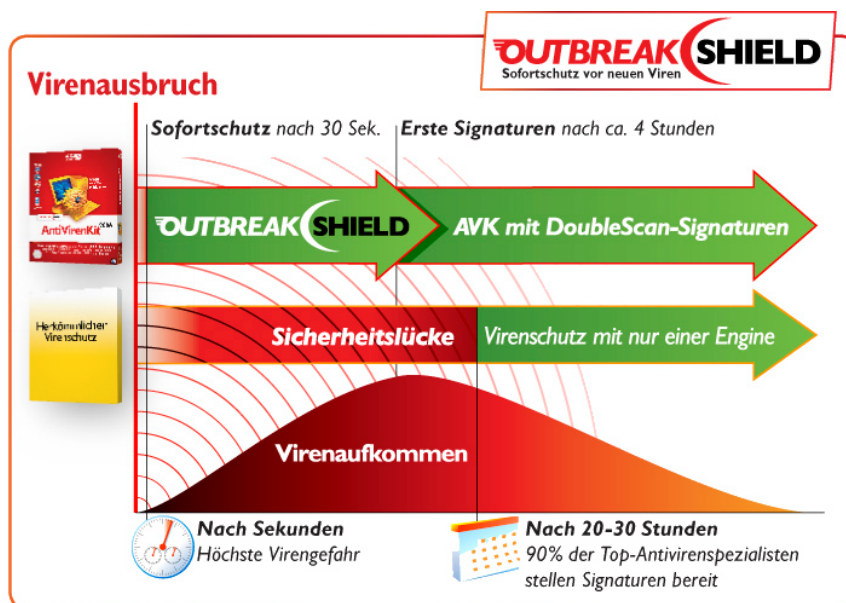
Einleitung

Virenschutz, wie er in allen gängigen Antiviren-Produkten praktiziert wird, basiert auf so genannten Virensignaturen. Um eine solche Signatur zu erstellen, muss ein Exemplar des Schädlings im Virenlabor vorliegen und analysiert werden. Bis die neuen Virensignaturen auf den bedrohten Rechnern verfügbar sind, vergehen im Idealfall vier Stunden, im Standardfall zehn Stunden und im schlimmsten Fall mehrere Tage. In dieser Zeit sind die Rechner zuhause und im Firmennetzwerk ungeschützt.

In letzter Zeit greifen immer mehr Computerschädlinge gezielt in diesem Zeitfenster an. G DATA verkürzte bereits die Reaktionszeit durch die Bereitstellung stündlicher Signatur-Updates. Aber auch diese Verbesserung des Schutzes durch Virensignaturen reicht noch nicht aus. Er wird nun um ein Verfahren ergänzt, das umgehend vor aktuellen Bedrohungen schützt. Als erstes Unternehmen weltweit hat G DATA im AntiVirenKit 2006 die bewährte DoubleScan-Technologie durch das neue OutbreakShield ergänzt. Es schützt den Rechner bei Viren-Outbreaks bereits nach wenigen Sekunden und ist damit eine der wichtigsten Neuerungen von G DATA AntiVirenKit 2006.

Die Bedrohungslage oder: Warum braucht man OutbreakShield?

Die Analyse eines neuen Virus und die Herstellung eines Gegenmittels (Signatur) benötigt trotz aller Anstrengungen der Antivirenspezialisten eine gewisse Zeit, die so genannte Response-Zeit¹. Das unabhängige Testlabor AV-Test GmbH in Magdeburg (www.av-test.de) misst hierfür eine durchschnittliche Zeitdauer von zehn Stunden². Die beiden Viren-Engines, die im AntiVirenKit eingesetzt werden (Kaspersky und BitDefender), sind mit zwei bis vier Stunden bis zur Bereitstellung der Virensignaturen die schnellsten Hersteller im Test. Eine aktuelle IDC Studie (www.idc.com) stellt fest, dass erst 20 bis 30 Stunden nach einem Outbreak bei 90 Prozent der marktführenden Antiviren-Softwarehersteller Virensignaturen zur Verfügung stehen. Aber erst, wenn eine Virensignatur auf dem Rechner vorliegt, kann das Antiviren-Programm die neuesten Schädlinge blockieren. In der Zwischenzeit klafft eine gefährliche Lücke im Virenschutz.

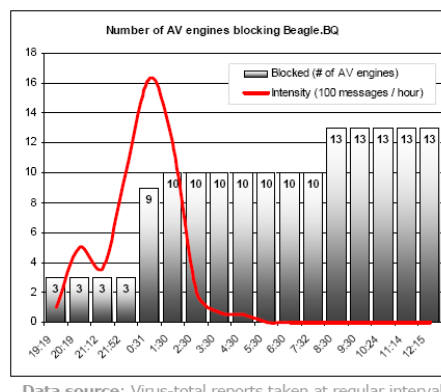


¹ Commtouch (2004a)

² Andreas Marx (2004)

Diese Lücke wird in letzter Zeit immer häufiger von Malware-Autoren ausgenutzt. Viele Computerschädlinge der neuesten Generation werden - ähnlich wie Spam - über Zombie-Rechner von Botnetzen versendet³. Als Zombie bezeichnet man einen infizierten Rechner, der über eine Backdoor von außen fernsteuerbar ist. Diese Zombie-Rechner werden von Kriminellen zu Netzwerken (auch "Botnetze" genannt) mit bis zu 100.000 Rechnern zusammengeschlossen. Und ihre Zahl nimmt zu. Der Zombie-Report der Firma CIPHERTRUST⁴ belegt für den Mai 2005 täglich mehr als 172.000 neue Zombie-Rechner. Die Botnetze werden dann von Ihren Betreibern vermietet oder selbst genutzt, um verteilte Denial-of-Service Angriffe auf Webseitenbetreiber auszuführen, Spam zu versenden oder eben Malware zu verbreiten. Gerade beim Versand von Malware wurde die Vorgehensweise u.a. in folgenden Punkten an die aktuellen Bedingungen angepasst:

- Viele Viren-Outbreaks sind zielgerichtet und regional begrenzt. Sie sind nicht mehr global ausgerichtet und oft wird versucht, die Anzahl der versendeten E-Mails so gering zu halten, dass sie von AV-Unternehmen nicht bemerkt werden. Häufig sind Viren-Outbreaks auf bestimmte Länder oder Personengruppen ausgerichtet.
- Viele Outbreaks dauern nur wenige Stunden und in etlichen Fällen ist der Viren-Outbreak schon beendet, bevor bei allen Anbietern neue Virensignaturen vorliegen. Ein Beispiel ist Bagle.BQ. *Grafik 1* zeigt, wie innerhalb weniger Stunden die Verbreitung massiv ansteigt, um dann genau so plötzlich abzubauen und zu verklingen. Bis zu diesem Zeitpunkt hatten noch nicht alle AV-Hersteller Signaturen veröffentlicht.
- Wenn der Viren-Outbreak vorüber ist, beginnen die Virenautoren mit der Entwicklung der nächsten Version des Schädlings. Der Nachfolger wird oft nur in wenigen Punkten verändert - gerade so viel, dass die nun vorliegenden neuen Virensignaturen ihn nicht entdecken. Wenn sicher gestellt ist, dass die neue Kreation nicht erkannt wird, startet die nächste Angriffswelle. Ein Beispiel für diese Vorgehensweise ist MytoB. Fast täglich gibt es neue Varianten.
- Anstelle eines vollständigen Wurms, der zwischen 40 KB und 120 KB groß ist, werden an die schädlichen E-Mails kompakte Trojan-Downloader mit einer durchschnittlichen Größe von 4 KB angehängt. Diese Downloader schwächen zunächst den infizierten Rechner, indem sie sicherheitsrelevante Prozesse und Programme beenden und deren Start blockieren. Dann laden sie den eigentlichen Wurm und eine Backdoor nach. Der Vorteil dieser Vorgehensweise ist, dass die kleinen Dateien viel schneller verschickt werden können, als der vollständige Wurm.



Grafik 1: Verlauf des Outbreaks von Bagle.bq

Diese Anpassungen zielen einzig und allein darauf ab, die Zeit zu nutzen, in der ein Rechner wegen noch nicht vorhandener Virensignatur ungeschützt ist.

Wie groß - angesichts des Einsatzes von Botnetzen - die o.g. Lücke ist, verdeutlichen die folgenden Zahlen: Angenommen ein Botnetz besteht aus 1.000 Zombies, die durchschnittlich über DSL 1000 verfügen. Wenn jeder dieser Rechner 4 KB große Dateien versendet, dann können in einer Stunde leicht 100 Millionen E-Mails versendet werden. Noch mal zur Erinnerung: Wenn die Virensignaturen nach zwei bis vier Stunden zur Verfügung stehen, ist das schnell. Bis dahin hat der Autor der schädlichen Post wahrscheinlich alle seine Adressaten erreicht. Er kann den Versand einstellen und sich der nächsten Version seiner Malware zuwenden. Somit ist klar, dass ein herkömmlicher signaturbasierter Virenschutz hier nicht mehr ausreicht und ein alternativer Schutz gefunden werden muss.

Welche Schutzmechanismen gibt es?

Bei den verfügbaren Schutzmechanismen unterscheidet man zwischen proaktiven und reaktiven Verfahren. Während reaktive Verfahren wie z.B. Virensignaturen erst greifen, wenn ein Schädling schon aufgetreten ist, erkennen proaktive Verfahren auch Schädlinge, die zu diesem Zeitpunkt noch unbekannt sind. Als eines der wichtigsten proaktiven Verfahren wird die Sandbox-Technologie angesehen. Eine Sandbox ist ein virtueller Rechner im Rechner. In dieser abgeschotteten Umgebung wird die unbekannte Datei ausgeführt und der Virenschutz beobachtet, was passiert. Wenn die Aktionen als schädlich eingestuft werden, wird der Zugriff verweigert. Die Verwaltung einer virtuellen Umgebung stellt allerdings hohe Anforderungen an die Rechenleistung und Systemressourcen. Das Sandbox-Verfahren muss außerdem auch seine Leistungsfähigkeit noch unter Beweis

³ Ralf Benz Müller (2005)

⁴ CIPHERTRUST (2005), <http://www.ciphertrust.com/resources/statistics/zombie.php>

stellen. In einem Heuristik-Test von AV-Test⁵ war zwar ein Antiviren-Produkt mit Sandbox-Technologie der Gewinner. Die Erkennungsrate lag allerdings mit 38 Prozent nicht bedeutend über den Heuristiken, die mit 30 und 24 Prozent die Plätze zwei und drei belegten.

In einigen Systemen erfolgt die Überwachung der Aktivitäten von unbekannter Software ohne die Absicherung durch den "doppelten Boden" einer Sandbox. Nachdem eine Datei ausgeführt wurde, werden deren Prozesse und Systemzugriffe durch ein Punktesystem bewertet. Wenn diese Prüfung ergibt, dass die Software schädlich ist, wird versucht deren Ausführung zu verhindern. Dieses Spiel mit dem Feuer erfordert tiefe Eingriffe in das System und einen leistungsfähigen Rechner.

Ein weiterer proaktiver Schutz, der auch in vielen aktuellen Antiviren-Produkten eingesetzt wird, ist die Heuristik. Als Heuristiken bezeichnet man spezielle Virensignaturen, die Computerschädlinge anhand bestimmter virenübergreifender Eigenschaften erkennen. So können auch unbekannte Viren erkannt werden, wenn sie versuchen, eine bestimmte Sicherheitslücke auszunutzen oder wenn sie bestimmte Systemprozesse aufrufen. Solche Heuristiken sind besonders nützlich wenn ein Schädling versucht neue Sicherheitslücken zu nutzen. Sie erkennen auch viele Standardverhaltensweisen von Bots, Dateidroppern und Backdoors. So hat AVK mit heuristischen Signaturen z.B. auch den Zotob-Wurm blockiert, der eine neue Sicherheitslücke nutzte und bei CNN, NBC, der New York Times und vielen weiteren Organisationen in den USA die Netzwerke lahm legte. In den Tests der Firma AV-Test erreichte die im AVK verwendete BitDefender-Engine mit 24 Prozent Erkennungsrate den dritten Rang. Somit bietet AntiVirenKit eine der besten verfügbaren Heuristiken.

Die Schlussfolgerung daraus: Weder Heuristiken noch Sandboxes bieten einen ausreichenden Schutz. Aber AVK bietet mit der DoubleScan-Technologie bereits einen (vielfach) ausgezeichneten Schutz gegen Viren, Würmer, Trojanische Pferde und andere Malware. Auch für den Bereich der proaktiven Erkennung mit heuristischen Signaturen liegt die DoubleScan-Engine des AVK im Spitzenfeld. Die neuesten Entwicklungen beim Versand von Malware zielen auf eine zeitliche Lücke im Virenschutz und das erfordert eine Ergänzung des bestehenden Schutzes. Die neue Bedrohung hat aber eine wichtige Eigenschaft: Die überwiegende Mehrheit dieser Malware wird per E-Mail versendet.

Eine Sandbox ist daher nicht nur wegen der hohen Systembelastung nicht das richtige Mittel der Wahl. Der Schutz, der durch eine Sandbox erreicht wird, ist nicht viel besser als der von Heuristiken und eine Sandbox ist eine sehr allgemeine Maßnahme, die nicht auf die spezielle Situation des E-Mail-Versands eingeht. Deshalb wurde das AntiVirenKit 2006 um eine völlig neue Technologie erweitert - das OutbreakShield.

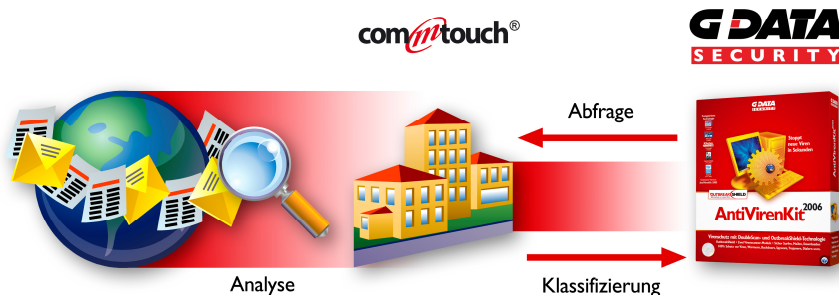
Wie funktioniert OutbreakShield?

Der Ansatz, der beim OutbreakShield verfolgt wird, ist völlig unabhängig von Virensignaturen und sogar unabhängig vom Inhalt der E-Mail. Ausgangspunkt der Überlegungen ist, dass Massenmail-Malware und Spam viele gemeinsame Eigenschaften teilen. Das Muster, das sich aus den Spuren der massenhaften Verbreitung im Internet ergibt, ist sehr typisch und kann mit den gleichen Mitteln erkannt werden, die auch zur Erkennung von Spam verwendet werden. Mit Commtouch hat G DATA einen Partner gefunden, der weltweit 35 Millionen Postfächer erfolgreich vor Spam und Malware schützt⁶. Im Commtouch Detection Center wird mit der patentierten Recurrent Pattern Detection (RPD)⁷ ständig der Datenverkehr im Internet analysiert. Aus dem E-Mail-Verkehr werden anhand bestimmter Eigenschaften wiederkehrende Muster extrahiert und in einer Datenbank gespeichert. Diese Eigenschaften umfassen Informationen wie IP-Adresse des Senders, Herkunft aus einem Botnetz, Dateigröße, Prüfsummen der Informationen im Header einer E-Mail etc. Übersteigt die Anzahl gleicher Patterns in kurzer Zeit einen Schwellwert, wird Alarm ausgelöst. E-Mails können so nach 0,5 bis 2 Minuten als Spam bzw. als Malware klassifiziert und blockiert werden. Da diese Eigenschaften nicht auf dem Inhalt der Mail oder auf einer Analyse des Dateianhangs basieren, ist die Klassifizierung unabhängig von Sprachen und Dateiformaten.

⁵ A. Marx (2004) hat Ende September .2004 100 verschiedene Viren aus dem Zeitraum von Mai bis September mit den Virensignaturen vom 1.Mai, 1.Juni, 1.August und 1.September getestet. Die beste Erkennungsrate mit den ältesten Signaturen lag bei weniger als 40%. Nur 5 von 23 Anbietern erreichten mehr als 20% Erkennung (darunter auch BitDefender mit 24% auf Platz 3).

⁶ Levitt & Burke (2004)

⁷ Commtouch (2004b)



In der Praxis sieht dies wie folgt aus: AntiVirenKit überprüft eingehende E-Mails anhand der DoubleScan-Technologie mit zwei unabhängigen Virenschannern auf Viren. Wird kein Schädling gefunden, startet OutbreakShield und errechnet eine Prüfsumme, die im Commtouch Detection Center verglichen wird (das dauert ca. 300 Millisekunden). Als Antwort kommt dann eine Klassifikation, die die Mail zuverlässig als Spam oder als Malware klassifiziert. Damit nicht immer die gleichen Anfragen über eine Online-Verbindung übertragen werden müssen, können aktuelle Informationen aus der Commtouch-Datenbank auf dem Rechner gespeichert werden.

Der Vorteil dieser Methode besteht in der geringen Belastung der Systemressourcen. OutbreakShield braucht nur 2,5 MB Speicher- und Festplattenplatz und kommt mit sehr wenig Rechenleistung aus. Damit ist es die ideale Ergänzung zur DoubleScan-Technologie mit stündlichen Updates der Virensignaturen.

Was leistet OutbreakShield?

Das OutbreakShield ergänzt die DoubleScan-Engine des AntiVirenKits in den ersten Stunden eines Outbreaks. Die wichtigste Leistung der OutbreakShield-Technologie ist die frühzeitige Erkennung von E-Mail-Schädlingen (und Spam), die massenhaft versendet werden. Im Durchschnitt wird ein Viren-Outbreak nach 90 Sekunden erkannt und alle weiteren E-Mails werden blockiert. Dabei erreicht OutbreakShield eine Erkennungsrate von 95 Prozent auch bei unbekanntem Viren. Das liegt weit über der Erkennungsrate von proaktiven Verfahren. Der Anteil an Fehlerkennungen liegt bei 0,00004 Prozent.

In *Tabelle 1* sind einige Viren-Outbreaks der letzten Zeit aufgelistet. Für die einzelnen Viren sind die Uhrzeiten angegeben, wann sie bei Commtouch gemeldet wurden und wann ein Schutz durch das AVK bestand. Der Verlauf des Outbreaks von Bagle.bq ist oben in *Grafik 1* dargestellt. AVK gehört zu den wenigen Virenerkennern, die noch vor dem Höhepunkt der Verbreitung gegen 1:00 h eine Signatur bereit stellen. Dennoch konnte der Wurm mehr als viereinhalb Stunden ungestört sein Unwesen treiben. OutbreakShield schließt diese Lücke.

Virus	Erkannt bei Commtouch	Erkannt durch AVK	Differenz
Bagle.be	01.03.2005 01:06 (GMT)	01.03.2005 10:15 (GMT)	9:07 h
Sober.p (der Fußball-WM-Wurm)	02.05.2005 16:43 (GMT)	02.05.2005 18:25 (GMT)	1:48 h
Mytob.by	29.05.2005 17:49 (GMT)	30.05.2005 01:29 (GMT)	7:40 h
Bagle.bq	26.06.2005 18:05 (GMT)	26.06.2005 22:39 (GMT)	4:34 h
Mytob.bt	09.07.2005 03:29 (GMT)	09.07.2005 05:45 (GMT)	2:16 h

Tabelle 1: Erkennungszeiten für größere Outbreaks im 1. Halbjahr 2005

OutbreakShield schützt schnell und zuverlässig vor neuen E-Mail-Bedrohungen und das bei geringer Systembelastung. Da es auf typischen Eigenschaften für Massenmails basiert, lässt es sich von Crackern und Spammern nur schwer umgehen.

Fazit: OutbreakShield schließt eine häufig genutzte Sicherheitslücke und ist eine effektive Ergänzung der DoubleScan-Technologie des G DATA AntiVirenKit. AntiVirenKit ist die erste Antivirensoftware, die dank OutbreakShield einen wirksamen Schutz für diese kritische Sicherheitslücke bietet.

Bibliografie

- Benzmüller, Ralf (2005): Botnetze und die (un-)heimlichen Zombiemacher. G DATA Security Whitepaper, Bochum, http://www.antiviruslab.com/whitepapers/WhitePaper.Botnetze+Zombiemacher.G_DATA2005.pdf
- Ciphitrust (2005) Zombie-Report: <http://www.ciphitrust.com/resources/statistics/zombie.php>
- Commtouch (2004a): Preemptive Malware Protection through Outbreak Detection. Commtouch Whitepaper, Netanya, <http://www.commtouch.com/downloads/Preemptive%20Malware%20Protection%20-%20White%20Paper.pdf>
- Commtouch (2004b): Recurrent-Pattern Detection (RPD) Technology. Commtouch, Whitepaper, Netanya, <http://www.commtouch.com/downloads/RPD%20Technology%20-%20White%20Paper.pdf>
- Levitt, Mark & Brian E. Burke (2004): Choosing the Best Technology to Fight Spam. IDC-Whitepaper, Framingham, http://www.commtouch.com/downloads/Choosing%20the%20Best%20technology%20to%20fight%20spam%20-%204094_IDC.pdf
- Marx, Andreas (2004): Antivirus outbreak response testing and impact. Proc. Virus Bulletin Conference, Chicago, http://www.av-test.org/download/papers/2004-09_vb_2004.zip (262 KB, ZIP)