

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

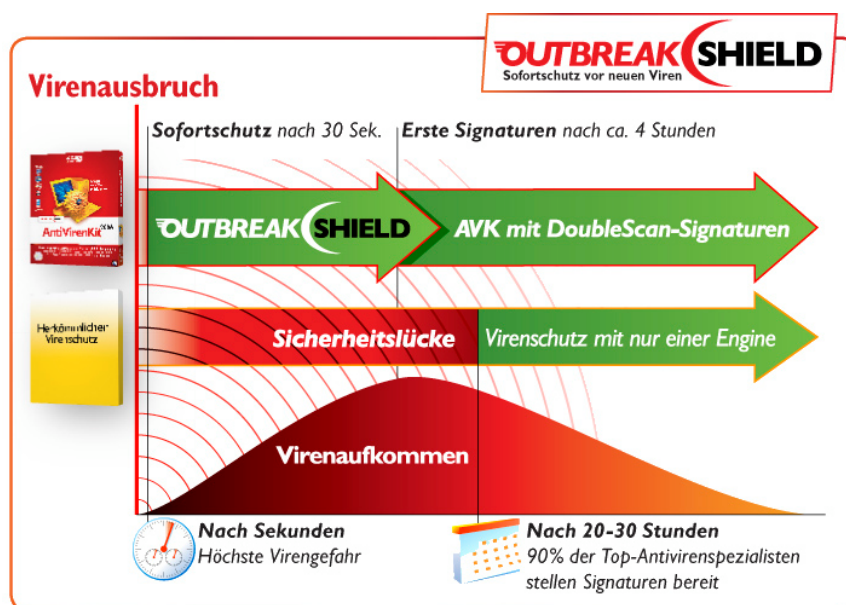
Ralf Benzmüller
G DATA Software AG

Einleitung

Virenschutz wie er in allen gängigen Antiviren-Produkten praktiziert wird, basiert auf sogenannten 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 10 Stunden und im schlimmsten Fall mehrere Tage. In dieser Zeit sind die Rechner zuhause und im Firmennetzwerk ungeschützt. Immer mehr Computerschädlinge greifen gezielt in dieser Zeitlücke an. G DATA reagierte darauf durch stündliche Virensignatur-Updates. Aber der Schutz durch Virensignaturen ist nicht mehr ausreichend. Deshalb ist eine der wichtigsten Neuerungen von G DATA AntiVirenKit 2006 das OutbreakShield, mit dem Rechner schon nach wenigen Sekunden vor neuen E-Mail-Viren geschützt sind.

Die Bedrohungslage oder Warum braucht man OutbreakShield?

Naturgemäß benötigt die Analyse eines neuen Virus und die Herstellung eines Gegenmittels (Signatur) ein gewisses Zeitfenster (die sog. Response-Zeit). Die AV-Test GmbH in Magdeburg (www.av-test.de) misst hierfür eine durchschnittliche Zeitdauer von 10 Stunden¹. Die beiden Virenengines, 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 nach 20 bis 30 Stunden nach einem Outbreak bei 90% der marktführenden Antiviren-Softwareherstellern Virensignaturen zur Verfügung stehen. Aber erst wenn eine Virensignatur auf dem Rechner eintrifft, kann der Virenschutz die neuesten Schädlinge blockieren. In der Zwischenzeit besteht eine Lücke im Virenschutz.



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 versendet. Als Zombie bezeichnet man einen infizierten Rechner, der über eine Backdoor von außen fernsteuerbar ist. Diese Zombie-Rechner werden von Kriminellen zu Netzwerken mit bis zu 100.000 Rechnern zusammengeschlossen. Und ihre Zahl nimmt zu. Der Zombie-Report der Firma Cipherttrust² belegt für den Mai 2005 täglich mehr als 172.000 neue

¹ Andreas Marx (2004) Antivirus outbreak response testing and impact. Proc. Virus Bulletin Conference Chicago, http://www.av-test.org/down/papers/2004-09_vb_2004.zip (262 KB, ZIP)

² <http://www.cipherttrust.com/resources/statistics/zombie.php>

Zombie-Rechner. Diese sog. 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. Auch hier hat sich die Vorgehensweise angepasst. Anstelle eines vollständigen Wurms, der zwischen 50 KB und 120 KB groß ist, werden an die schädlichen E-Mails sog. Trojan-Downloader mit einer durchschnittlichen Größe von 4 KB angehängt. Diese Downloader schwächen zunächst den infizierten Rechner und laden dann den eigentlichen Wurm und eine Backdoor nach. Der Vorteil dieser Vorgehensweise ist, dass die kleinen Dateien viel schneller verschickt werden können, als die vollständige Wurm.

Wie groß - angesichts des Einsatzes von Botnetzen - die o.g. Lücke ist verdeutlichen die Zahlen des folgenden Beispiels. Angenommen ein Botnetz besteht aus 1.000 Zombies, die durchschnittlich über DSL 1000 verfügen. Wenn jeder dieser Rechner 4 KB große E-Mails versendet, dann können in einer Stunde leicht 100 Millionen versendet werden. Nochmal 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 und kann den Versand beenden und sich der nächsten Version seiner Malware zuwenden. Es ist klar, dass ein herkömmlicher signaturbasierter Virenschutz hier nicht mehr ausreicht.

Welche Schutzmechanismen gibt es?

Völlig schutzlos sind auch herkömmliche Antiviren-Programme nicht. Sie enthalten nämlich meist auch sog. Heuristiken. Das sind spezielle Virensignaturen, die Computerschädlinge anhand bestimmter virenübergreifender Eigenschaften erkennen. Allerdings haben die Test der Firma AV-Test ergeben, dass heuristische Signaturen im besten Fall knapp 30% der Malware erkennen³. Mit 24% erkannter Viren lag die im AVK verwendete BitDefender Engine im Spitzenfeld und somit bietet auch AntiVirenKit eine der besten verfügbaren Heuristiken.

Als Wunderwaffe in der Erkennung von Malware werden sog. Sandboxes angesehen. Eine Sandbox ist sozusagen ein abgeschotteter Rechner im Rechner. In dieser virtuellen Umgebung wird die unbekannte Datei ausgeführt und der Virenschutz beobachtet, was passiert. Wenn die Aktionen als schädlich eingestuft werden, wird der Zugriff verweigert. Bislang muss dieses Verfahren allerdings seine Leistungsfähigkeit noch unter Beweis stellen. Der Gewinner des "Heuristik-Tests" von Andreas Marx war ein Antiviren-Produkt mit Sandbox-Technologie. Die Erkennung lag allerdings mit 38% nicht bedeutend über den Heuristiken. Zudem erhöht die Ausführung der Sandbox die notwendige Rechenleistung.

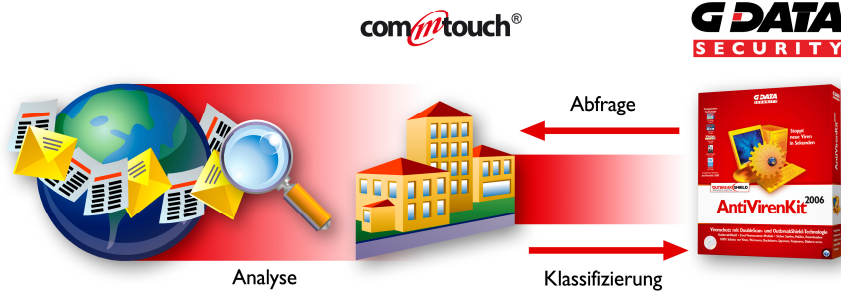
Die Schlussfolgerung daraus: Weder Heuristiken noch Sandboxes bieten einen ausreichenden Schutz. Deshalb wurde das AntiVirenKit 2006 um eine völlig neue Technologie erweitert - das OutbreakShield.

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 ausschlaggebend. Mit Commtouch hat G DATA einen Partner gefunden, der weltweit 35 Millionen Postfächer vor Spam und Malware schützt. Im Commtouch Detection Center wird mit der patentierten Recurrent Pattern Detection (RPD) der Traffic im Internet analysiert. Aus dem E-Mail-Verkehr werden wiederkehrende Muster gesammelt und in einer Datenbank gespeichert. Aufgrund bestimmter Eigenschaften (Herkunft aus einem Botnetz, Anzahl der gleichen Patterns in kurzer Zeit etc.) können E-Mails nach 0,5 bis 2 Minuten als Spam bzw. als Malware erkannt 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.

Wenn nun die E-Mail eines AVK-Kunden geprüft werden soll, wird eine Prüfsumme errechnet, die mit den Daten im Commtouch Detection Center verglichen wird (das dauert ca. 300 ms). 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 Datenbank auf dem Rechner gespeichert werden.

³ A. Marx (2004) a.a.O. 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).



Der Vorteil dieser Methode ist, dass sie sehr wenig Systemressourcen benötigt. 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?

Die wichtigste Leistung der OutbreakShields ist die frühzeitige Erkennung von E-Mail-Schädlingen (und Spam), die massenhaft versendet werden. Im Durchschnitt wird ein Outbreak nach 90 Sekunden erkannt. Dabei erreicht OutbreakShield eine Erkennungsrate von 95% auch bei unbekanntem Viren. Der Anteil an Fehlerkennungen liegt bei 0,00004%. 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.