

OutbreakShield – Effective and Immediate Protection against Email Virus Outbreaks

Ralf Benzmüller
G DATA Software AG

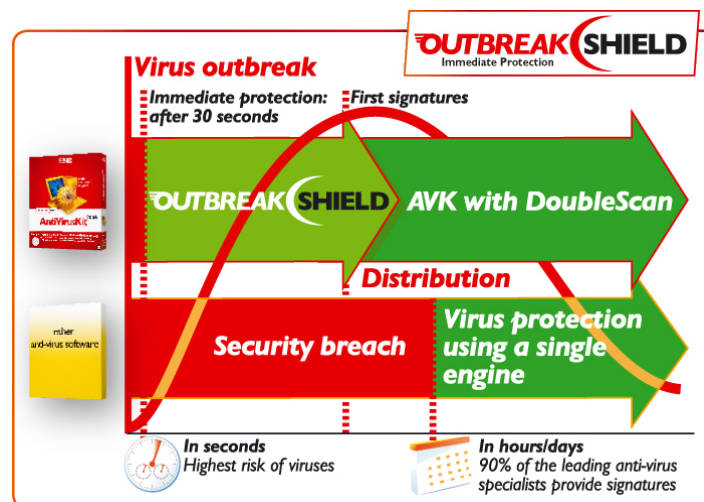
Introduction

The virus protection provided by all current antivirus software products is based on "virus signatures". To create a virus signature, a sample of the worm, etc. must be placed in the virus lab and analysed. Ideally, new virus signatures should be available and installed within 4 hours, but this normally takes 10 hours and, at worst, can take several days! Any home or corporate network computers remain unprotected during this lag time.

Recent trends indicate that increasing numbers of computer viruses target this critical window to launch an attack. G DATA has already reduced the response time by releasing hourly signature updates, but even this improvement in virus signature protection is proving inadequate, so a new procedure has been developed to ensure total protection against current threats. G DATA has set a worldwide precedent with its latest product, AntiVirusKit 2006, by adding the new OutbreakShield to proven DoubleScan technology. This protects the computer against virus outbreaks in seconds, representing one of the most important innovations in G DATA AntiVirusKit 2006.

The Threat or: Why use OutbreakShield?

Despite the efforts of antivirus experts, analysing a new virus and generating an antidote (signature) takes a certain amount of time, known as the "response time"¹. The independent test lab, AV Test GmbH in Magdeburg, Germany (www.av-test.de), reports an average of ten hours². AntiVirusKit's two integrated virus engines (Kaspersky and BitDefender) provide the shortest response time in the test, producing new virus signatures in 2-4 hours. A recent IDC study (www.idc.com) reports that 90% of the leading antivirus software providers release virus signatures 20-30 hours after an outbreak. However, the antivirus program cannot block the new virus until the virus signature is actually present on the computer; meanwhile, there exists a gaping and dangerous vulnerability in the virus protection.

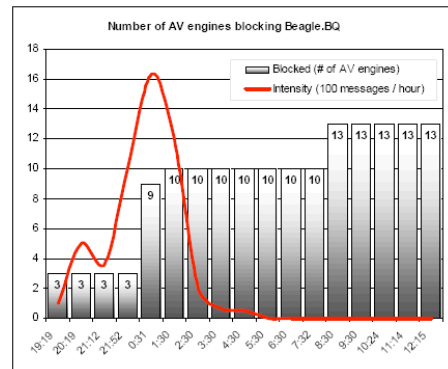


¹ Commtouch (2004a)

² Andreas Marx (2004)

This vulnerability has been increasingly exploited by malware authors. Like spam, many of the latest generation of computer viruses are sent from botnets using zombie computers³. The term "zombie" denotes an infected computer controlled remotely via a backdoor. These zombie computers are grouped together in networks (also called "botnets") of up to 100,000 computers and the number is growing. The zombie report from the company CIPHERTRUST⁴ reported over 172,000 new zombie computers daily in May 2005! The operators then hire out the botnets or use them to carry out distributed Denial of Service attacks on website providers, to send out spam or even to spread malware. The circulation of malware in particular is generally adapted to current conditions:

- Many virus outbreaks are specifically targeted and regional. They are no longer sent out globally and often aim to send out such small volumes of email that they remain undetected by antivirus organisations. Virus outbreaks are frequently directed at certain countries or particular groups of individuals.
- Many outbreaks only last a few hours and, very often, the virus outbreak is already over before all the software providers have the new virus signatures. An example of this is Bagle.bq. *Figure 1* shows how the spread peaked dramatically in several hours and then subsided as quickly and disappeared completely, even though some antivirus software providers had still not released signatures.
- Once the outbreak has died down, the virus authors start developing the next version of the virus. The successors often only vary from their predecessors in a few minor details: just enough to outwit the newly generated virus signatures. When the authors are satisfied that their new version will escape detection, the new wave of attacks commences. An example of this strategy is Mytob, where new variants appear almost daily.
- Compressed Trojan downloaders with an average size of 4 KB are attached to malicious emails instead of the entire worm, which could range in size from 40-120 KB. These downloaders initially impair the infected computer by shutting down all security-related programs and functions and blocking their startup procedure. They then download the actual worm along with a backdoor. The advantage here is that small files can be sent out much more quickly than the whole worm.



Data source: Virus-total reports taken at regular interval between 19:19 GMT, 26/6/2005 and 12:15 GMT, 27/6/2005

Figure 1: Progress of the Bagle.bq outbreak

These tactics were developed purely to target the period when the computer is unprotected before new virus signatures are available.

How serious is this vulnerability? Given the use of botnets, here are some figures.

Let's assume a botnet consists of 1,000 zombies, operating via DSL 1000 on average. If every computer sends out 4 KB files, a minimum of 100 million emails can be sent out in one hour. Bear in mind that's pretty quick if the virus signatures are only available after 2-4 hours. By this time the sender of the damaging email will have reached all his recipients, so he can now stop sending and concentrate on the next version of his malware. It is clear from this that conventional signature-based virus protection is becoming increasingly ineffective and that we need to find alternative methods of protection.

³ Ralf Benzmler (2005)

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

What protection is available?

The available protection mechanisms are divided into proactive and reactive procedures. While reactive processes, e.g. virus signatures, take effect some time after the virus appears, proactive programs can also detect viruses that are as yet unknown.

"Sandbox" technology is considered one of the most significant proactive systems. A sandbox is a simulated computer within a computer. The antivirus system monitors the process as the unidentified file is executed in this isolated environment. Access is denied if the file's behaviour is classified as harmful. However, managing this virtual environment places heavy demands on the computer's performance and system resources; moreover, the effectiveness of the sandbox process has yet to be proved. In a heuristic test carried out by AV Test⁵, an antivirus product with sandbox technology did indeed emerge as the winner. However, the detection rate of 38% was not much higher than the heuristic systems, which came 2nd and 3rd with 30% and 24%.

In some systems, the activities of unknown software are monitored without the protection of the sandbox's "false bottom". Once a file has been executed, its functions and system accesses are rated on a points system. If this scan reveals the software to be malicious, it attempts to stop it from running. However, playing with fire in this way requires in-depth system intervention and an extremely powerful computer.

Another proactive protection system built into many current antivirus products is heuristic detection. The term "heuristics" refers to specific virus signatures which recognise malicious computer programs based on specific characteristics common to all viruses. Unknown viruses can therefore be identified when they attempt to exploit a particular vulnerability or when they activate certain system processes. These heuristics are particularly useful when a virus tries to exploit new security vulnerabilities. They also recognise many behaviour patterns typical of bots, file droppers and backdoors. AVK has used heuristic signatures to block viruses such as the Zotob worm, which used a new vulnerability to cripple networks at CNN, NBC, The New York Times and numerous other organisations in the USA. Tests at AV Test placed AVK's integrated BitDefender engine third with a 24% detection rate, so AntiVirusKit offers one of the best heuristic detection programs available.

In conclusion: neither heuristics nor sandboxes provide adequate protection but AVK, with its DoubleScan technology, provides (multiple) excellent protection against viruses, worms, Trojans and other malware. The AVK DoubleScan engine also leads the field in proactive detection using heuristic virus signatures. The most recent developments in malware circulation target the vulnerable window prior to the release of virus signatures, so this calls for an enhancement to the existing protection. The new threat has one important feature: the vast majority of this malware is circulated via email.

A sandbox is therefore an inappropriate choice of tool for the job, and not only because of the strain it puts on the system. The level of protection achieved by the sandbox is only a marginal improvement on heuristic detection, and a sandbox is also a very generic detection method which does not address the specific problems of email distribution. For this reason, AntiVirusKit 2006 uses a completely new technology: OutbreakShield.

How does OutbreakShield work?

The OutbreakShield program is independent of virus signatures and even independent of email content. The basic premise is that mass mail malware and spam share many common features. The pattern created by the first signs of mass distribution via Internet is very consistent and can be recognised using the same tools that are applied to spam identification.

In Commtouch, G DATA has found a partner which successfully protects 35 million mailboxes worldwide against spam and malware⁶. At the Commtouch Detection Center, Internet data traffic is constantly analysed

⁵ At the end of September 2004, A. Marx (2004) tested 100 different viruses from the period May-September with virus signatures from 1st May, 1st June, 1st August and 1st September. The best detection rate using the oldest signatures was less than 40%. Only 5 out of 23 providers achieved more than a 20% detection rate (BitDefender was in 3rd place with 24%).

⁶ Levitt & Burke (2004)

using the patented Recurrent Pattern Detection (RPD)⁷ system. Recurring patterns based on specific features are extracted from email traffic and saved in a databank. This data includes information such as the sender's IP address, whether the email originates from a botnet, file size, checksums of the information in email headers, etc. An alert is triggered if the number of similar patterns exceeds a certain level over a short period of time. This procedure can classify emails as spam or malware after 30 seconds to 2 minutes and block them. As this data is not based on the analysis of file attachments or the content of the email itself, the classification is independent of language or file formats.

This is how it works in practice: AntiVirusKit checks incoming emails for viruses using its DoubleScan technology with two standalone virus scanners. If no virus is detected, OutbreakShield starts up and generates a checksum, which is analysed in the Commtouch Detection Center (this takes about 300 milliseconds). The response comes back in the form of a rating, which reliably classifies the mails as spam or malware. Current data from the Commtouch databank can be saved on the PC to avoid duplicate requests being transferred via an online connection.

These processes use minimal system resources; OutbreakShield only requires 2.5 MB of memory and hard disk space and uses negligible computing power. This makes it the perfect enhancement to the DoubleScan technology with hourly virus signature updates.

What does OutbreakShield do?

OutbreakShield extends the capability of the AntiVirusKit DoubleScan engine during the early hours of an outbreak. The most significant achievement of OutbreakShield technology is the early detection of mass-mailed email viruses and spam. On average, virus outbreaks are detected after 90 seconds and all further infected emails are blocked. OutbreakShield achieves a detection rate of 95%, even for unknown viruses, which is significantly higher than the proactive procedures' detection rates. Its detection error rate is 0.00004%.

Table 1 lists some recent virus outbreaks. The table shows the times of day when individual viruses were reported to Commtouch and when AVK provided the appropriate protection. The development of the Bagle.bq outbreak is shown above, in Figure 1. AVK was one of the few virus detectors that released a signature before the distribution volume peaked at about 1:00 a.m. However, the worm was still free to cause havoc for over 4½ hours! OutbreakShield eliminates this period of vulnerability.

Virus	Detected at Commtouch	Detected by AVK	Difference
Bagle.be	01.03.2005 01:06 (GMT)	01.03.2005 10:15 (GMT)	9 hours, 9 minutes
Sober.p (the World Cup football worm)	02.05.2005 16:43 (GMT)	02.05.2005 18:25 (GMT)	1 hour, 42 minutes
Mytob.by	29.05.2005 17:49 (GMT)	30.05.2005 01:29 (GMT)	7 hours, 40 minutes
Bagle.bq	26.06.2005 18:05 (GMT)	26.06.2005 22:39 (GMT)	4 hours, 34 minutes
Mytob.bt	09.07.2005 03:29 (GMT)	09.07.2005 05:45 (GMT)	2 hours, 16 minutes

Table 1: Response times for serious outbreaks during the first half of 2005

⁷ Commtouch (2004b)



OutbreakShield provides quick, reliable protection against new email threats using minimal system resources. As it is based on the identification of typical mass mail features, it cannot be foiled easily by crackers and spammers.

Conclusion: OutbreakShield closes a frequently exploited vulnerability and represents a potent addition to the G DATA AntiVirusKit DoubleScan technology. With OutbreakShield, AntiVirusKit is the first antivirus software to provide effective protection during these critical windows.

Bibliography

- Benzm ller, Ralf (2005): Botnets and the Secret Zombie Makers. G DATA Security Whitepaper, Bochum, http://www.antiviruslab.com/whitepapers/WhitePaper.Botnetze+Zombiemacher.G_DATA2005.pdf
- CIPHERTRUST (2005) Zombie Report: <http://www.ciphertrust.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/down/papers/2004-09_vb_2004.zip(262 KB, ZIP)