

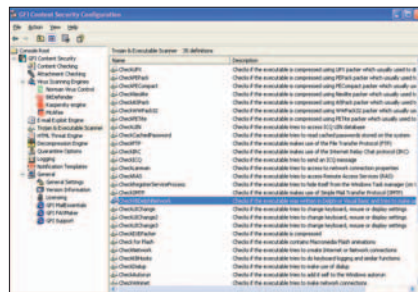
Several server-based gateway antivirus products also use heuristic analysis. A server, shared by many users on a network, can perform much more analytical work on code without slowing down individual PCs. We tested GFI MailSecurity, which has extensive heuristic capabilities. Both MessageLabs and GFI first test messages with conventional antivirus signature-based scanners, because of their speed, and then apply the more time-consuming scrutinies of heuristics to the files that pass the first tests.

Then there are products that use *sandboxing*, which lets programs not known to be trustworthy run on a virtual machine, so nothing they do can affect your computer. The vendors of sandbox products don't view them as a full security solution; rather, they are a safety net to catch the attacks that slip through your main antivirus program and other protection.

To test these products, we had to isolate the infected e-mail on a system and run the attachments—in other words, attempt to infect ourselves.

HOW WE TESTED

We always have two basic concerns about AV products: false negatives,



A SERIES OF HEURISTIC OPTIONS gives administrators extensive control over what mail is blocked.

when a product misses actual malicious code, and false positives, when software misidentifies innocent code as malicious. Unlike in signature-based scanning, where a program knows exactly what it's looking for, in heuristic detection and sandboxing there is a trade-off between false positives and false negatives, as a function of the given product's aggressiveness.

Unlike with antispam products, many of which use heuristic techniques to identify spam, we require perfection from antivirus products, and with good reason. It's unacceptable for a nonviral program to be blocked, even worse to let a virus through undetected. False positives are quite rare with conventional antivirus software, although such programs will often flag payloads that cannot infect a system, such as bounce messages (more on them below) and

damaged versions of true viruses.

To test scanners' ability to detect "unknown" viruses, we had to be sneaky. We installed the programs, updated them, and set them not to update their virus signatures, forcing them to rely on other methods for detecting new viruses or variants.

We shut the test systems down and waited for about two weeks. For comparison, we also set up systems with Norton AntiVirus 2004 and McAfee VirusScan 2004 in the same way; these claim to use heuristics as well as signatures. We had to relax some default restrictions in Outlook Express 6 that would have blocked many of the attacks, such as the default setting that strips executable attachments. It's harder to get yourself infected on purpose than you might think.

In the meantime, we took the e-mail sent to a popular *PC Magazine* address and forwarded it to some test accounts. During the two-week period, many new viruses came out, as they always do, including a few that made their way to these accounts. At the end of the test period we shut off the flow of mail and loaded the messages into the nonupdated products.

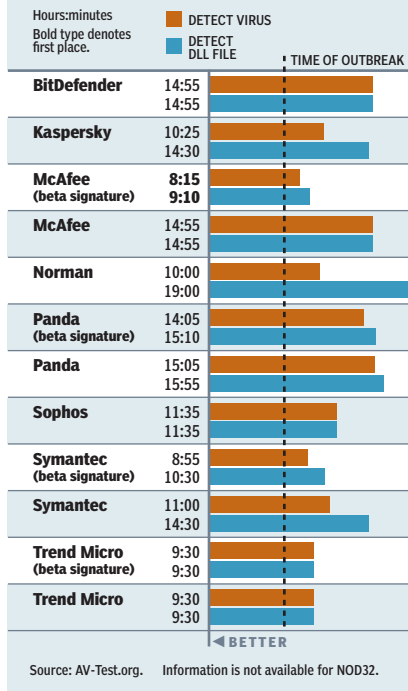
Unfortunately, we were unable to test MessageLabs, because controlling test conditions in this way would be impossible with such a service. Also, VirusScan crashed when we tried to load the messages, and we couldn't update it to fix the bug without potentially updating its signatures and invalidating the results. So we had to pull it from the test as well.

Our testing methodology was a bit more speculative than usual for an antivirus story; we didn't know exactly what viruses we would get. In all, we found 69 infected messages in our mailbox, including several infected with three virus strains that first appeared during the freeze period. If we had tested about a month before, we would have been fortunate enough to experience the birth of several generations of new viruses, including the prolific Bagle and Netsky families. We missed this viral gold rush, but we did see two new versions of Bagle and one of Netsky that were not yet out when we froze our test products. These are sufficient to give you a good idea of the state of unknown-virus detection.

There was another monkey wrench thrown in: Most of the infected messages were in fact *bounce messages*. Someone's infected system sent a virus to a third party using our e-mail address as the From: address. In each case, the recipient's mail server rejected the message, bouncing it back to the apparent sender—us. (Such bounce

Major-Vendor Response Times: MyDoom.A

The MyDoom virus has two detectable components: the distributed virus itself and a DLL file that it drops. The chart indicates how much time passed, after MessageLabs' first sightings of the virus, before each vendor released signature files to detect the virus and the DLL file. About 6.5 hours elapsed between the first sightings and the full-scale outbreak.



messages were once useful, but now they only clog network pipes and cause unwarranted hysteria.)

When the infected message is preceded by the rejecting server's message header, e-mail clients generally prevent the user from accessing the infected payload. Even so, conventional antivirus products, including Norton AntiVirus and Trend Micro's PC-cillin Internet Security 2004 (which we used as an independent standard of comparison), scan such messages, recognize the viruses in them, and flag them.



NOD32's detection window makes a rare appearance. NOD32 missed this virus when it was attached to an e-mail.

CONCLUSIONS

Conspiracy theorists will suggest that the antivirus-industrial complex is suppressing heuristics to protect the subscription-based business model, and it's true that the real money in the antivirus business is in the subscriptions. But our testing—and all other evidence—shows that today's heuristics cannot be an effective tool on a single-user PC.

Of our admittedly small number of new viruses, Norton AntiVirus found none using heuristic methods, and NOD32 found only one out of three. GFI MailSecurity showed that heuristics can be helpful on a powerful server, and MessageLabs illustrated what can be done when you throw serious iron at the problem. But as we noted, even these tools still rely primarily on signature-based scanning.

We can't recommend even supplementing your protection with either of the sandbox products, in view of their deficiencies. OS Security's OSSurance did block all the attacks, but its crashes were frustrating.

Administrators looking to protect an entire network would do well with GFI MailSecurity, but they should carefully fine-tune the program's rules to find a point at which they and their users are comfortable. A large organization might do well to outsource its mail to MessageLabs and benefit from the company's worldwide facilities. With service-based protection, however, you still need your own server antivirus program to stop threats that originate from within or pass among users in your organization.

For now, although a signature-based antivirus product is still an absolute must for known viruses, every PC user's best tool for detecting *unknown* viruses is the old noggin: You can learn to recognize the traits of virus-bearing e-mail, such as attachments, often with intriguing filenames, on nonsensical messages that seem to come from people you know. Most people just aren't inclined to think like computer security analysts, but if we don't start, a lot more of us are going to be asking, "Why me?"

HEURISTIC PROGRAMS

GFI MailSecurity for Exchange/SMTP 8.0

25 users, \$315 direct. GFI Software Ltd., www.gfi.com. ●●●○○

Unlike the other products here, GFI MailSecurity is server-based; it protects all users on a server. The program integrates directly into Microsoft Exchange Server 2000 or 2003, but we

PERFORMANCE TESTS

False Positives

To test for false positives, AV-Test.org ran a total of 2 terabytes of uninfected files (more than 3,700,000 files) through the signature/heuristic products and noted how many files each product erroneously flagged as infected. For sandbox testing, AV-Test.org attempted to launch 1,200 distinct, uninfected executables and noted how many each product blocked.

SIGNATURE/HEURISTIC PRODUCTS	False positives
GFI using BitDefender	19
GFI using Kaspersky	7
GFI using McAfee	1
GFI using Norman	0
GFI's Trojan & Executable Scanner	28,677**
NOD32 Antivirus System	30
McAfee Antivirus*	1
Norton AntiVirus 2004*	1
SANDBOX PRODUCTS	
OSSurance Desktop	37
SurfinGuard Pro	1,200***

Source: AV-Test.org * Reported for comparison.
 ** GFI flagged these files as "suspicious."
 *** Finjan blocks every executable file except those on a whitelist.

tested it as a separate mail gateway for a conventional SMTP server.

GFI MailSecurity has more configuration options than are worth counting. This can be overwhelming, but it confers a great deal of control. Out of the box, though, it comes configured in paranoid secret-police mode, blocking large numbers of nonviral messages. But many of the rules that caused this performance were designed to block typical spam, not viruses, so it's not necessarily fair to call the harmless blocked messages "false positives" in an antivirus context (although some of them undoubtedly were). Moreover, the program blocked every virus we threw at it, right out of the box.

GFI MailSecurity comes with fully licensed versions of conventional antiviral engines from BitDefender and Norman Virus Control. It also supports Kaspersky Labs and McAfee Security, but you have to purchase those licenses separately. For our tests we updated the two included engines and GFI MailSecurity's rules, and then we froze updates, just as with the other products.

The product also includes engines for checking the characteristics of attachments, as well as a series of true heuristic engines. The e-mail exploit engine checks messages against 27 specific exploit rules, including rules for some very recent and specific exploits, such as the Outlook 2002 mailto: exploit, as well as some more generic ones. The Trojan and Executable Scanner checks 35 rules

about executables, such as whether they attempt to send an ICQ message, use SMTP, dial, or set themselves to launch at Windows start-up.

The HTML threat engine checks HTML mail for the presence of scripts and removes either most or all of them (removing most is the default). Finally, the decompression engine sets rules for how archive files (like ZIP files) are handled. It lets you set rules for password-protected files, corrupted files, and recursively compressed files. You can also set size limits.

The large number of e-mail messages that GFI MailSecurity's default configuration blocks might scare some people, but we are more impressed with the product's configurability and ability to block actual viruses. It's a shame—though not surprising—that power like this requires a dedicated server.

NOD32 Antivirus System

\$39 list. Eset s.r.o., www.nod32.com.

●●●○○

We chose to review NOD32 Antivirus System because it claims to have a "state-of-the-art virus/worm/Trojan detection engine" for advanced heuristics. We tested the version for Windows NT; other versions support Windows 2000 and XP. Not only did we see little evidence of heuristic virus detection on our tests, NOD32 barely showed up at all.

NOD32 found only 2 of the 69 infected messages. This number is not as bad as it seems, but it's still bad: NOD32 missed all of the bounce messages, as well as most of the Bagle variants and Dumaru.Z.

We manually extracted attachments with samples of each virus and scanned them with NOD32's heuristics feature turned on. The program still missed several viruses, but it did detect a Bagle variant that came out after the test began. Interestingly, NOD32 was able to detect Dumaru.Z once we had separated it as an e-mail attachment.

You could make a case that the bounce messages NOD32 missed were not threats at all and that it behaved reasonably in skipping them. We don't think much of this argument; the bar has been set higher by other products, such as Norton AntiVirus and PC-cillin, which found those viruses. The bottom line is that NOD32's failure to detect any of the new viruses in the e-mail stream speaks badly of its capabilities.

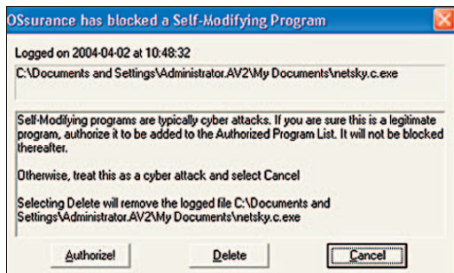
SANDBOXES

Finjan SurfinGuard Pro 5.7

\$30 direct. Finjan Software Ltd., www.finjan.com.

●●●○○

Finjan Software offers nearly identical personal and corporate antivirus packages; we



OSsurance blocked every virus we attempted to run on the system—then it crashed.

tested the personal version, Finjan SurfingGuard Pro 5.7. These products are neither virus scanners nor cleanup tools, and the company recommends that users also run such software.

At the default security level—Medium—SurfingGuard monitors all active content; it asks you whether to monitor, run, or kill certain file types. Any application violating a policy is automatically killed. At the High setting, the program blocks all active content. Set to Low, it allows everything, although the user is often consulted first.

In general, it's good that SurfingGuard monitors only files that come in directly through one of the monitored applications; otherwise the program would be an unreasonable burden on system performance. This does create one big problem: Many worms these days are distributed in ZIP files, but SurfingGuard monitors the ZIP extraction program, not the extracted content. Finjan says the

next version will monitor programs contained within compressed archives.

SurfingGuard did block all of the non-ZIP attacks on our tests. The Run Safe feature confirmed that the tool would have blocked the attacks within the ZIPs if it had been monitoring those files, but that isn't very reassuring.

OSsurance also monitors scripts run directly in a browser or HTML e-mail. And using the panic mode, you can quickly kill all active content and prevent anything else from starting, although by that time it's probably too late.

OSsurance Desktop 3.0 Personal Edition

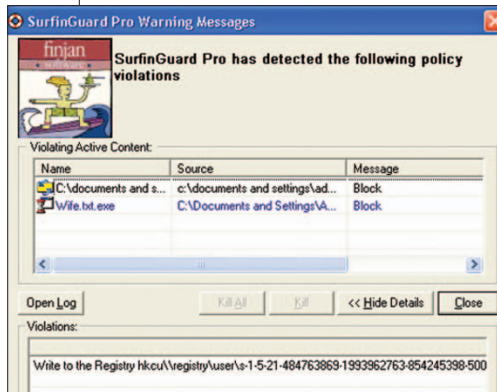
\$100 direct. OS Security Inc., www.ossecurity.ca. ●●●○○

During installation, OSsurance Desktop 3.0 Personal Edition scans your system to create an Authorized Program List (APL) of applications already on your system. This means that if the computer is already infected, the virus itself will be considered safe. We advise you to scan your PC first with a conventional antivirus scanner—and to keep that scanner active and current.

Since none of our viruses were on the APL, we tested them by simply running them. In every case, OSsurance popped up to block the infected program. (Interestingly,

it flagged all the viral programs as “self-modifying,” because all of them are compressed and uncompress themselves at load time. If this weren't the case, OSsurance would have blocked some other behavior of the programs.)

A few minutes later, the OS Monitor program crashed. This is not the actual protection process in OSsurance, which runs as part of the Windows kernel; it's the part that can interact with the user, for example by displaying dialog boxes explaining that a program was blocked and why. If we had kept testing viruses at this point, OSsurance would have blocked them, but we would have gotten no feedback. We could have simply rerun the OS Monitor, but we shouldn't have to do that. The company was



SURFINGGUARD monitors content that comes in from the outside, looking for disapproved behaviors.

familiar with the problem and emphasized that the protection was still present.

OSsurance does seem to be aware of the difference between viruses (which unpack themselves) and installation programs (which unpack their contents from an install file). When we ran an installation program, OSsurance gave us a different alert, which said the installation program was a “probable cyber attack,” adding that if we knew it was a legitimate program we could add it to the APL.

OSsurance's approach to sandboxing seems more straightforward than SurfingGuard's: Either a program is on the APL or it isn't. These days, we'd prefer to give up some system performance as the price of extra monitoring if it would increase the chances of malicious code being monitored as well. If only the OS Monitor program didn't keep crashing.

PERFORMANCE TESTS

Virus Detection

We shut down all of our antivirus products on March 11, 2004. Over the following two weeks, three brand-new viruses appeared in our mailbox: HTML_BAGLE.Q-1, PE_BAGLE.N-O, and WORM_NETSKY.P. We restored the AV programs but did not let them update their signatures, forcing them to use their ability to detect unknown viruses to stop these new threats. We could not test OSsurance and SurfingGuard with HTML_BAGLE.Q-1, because patches to Internet Explorer stopped it first. Here's how the others fared.

PROGRAM	TECHNIQUES USED	RESULTS
GFI MailSecurity	Content filtering, heuristics	Stopped all three viruses, apparently because of heuristic rules.
NOD32 Antivirus System	Heuristics	Detected only PE_BAGLE.N-O (as “probably unknown NewHeur_PE virus”).
OSsurance Desktop	Sandboxing	Caught PE_BAGLE.N-O and WORM_NETSKY.P.
SurfingGuard Pro	Sandboxing	Missed PE_BAGLE.N-O. Caught WORM_NETSKY.P.
Norton AntiVirus 2004*	Heuristics	Missed all three viruses.

* Reported for comparison.

Reprinted from PC Magazine, June 8, 2004 with permission from Ziff Davis Media Inc.

©2004 Ziff Davis Publishing Holdings Inc. All rights reserved.



GFI
 15300 Weston Parkway, Suite 104
 Cary, NC 27513 USA
 Tel: +1 (888) 243-4329, +1 (919) 379-3397
 Fax: +1 (919) 388-5621
 sales@gfi.com • www.gfi.com