Heuristic Scanners Hit the Spot

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

One of the problem any columnist faces when interviewing people in specific companies or highlighting particular products is that the public relations professionals working for other companies begin swarming like piranhas around a fallen capybara (or should that be a Kabaypara?). The number of pleading letters I’ve been receiving begging me to feature this or that product in my column is growing faster than the junk mail being blocked by various filters on my e-mail system.

Every now and then, though, someone manages to catch my eye with some interesting tidbits, so today I will share some information sent to me by a lady with the fascinating name of Angelica Micallef Trigona. She works for GFI Software Ltd (<http://www.gfi.com>), a company based in the beautiful island of Malta that makes “GFI FAXmaker fax connector for Exchange and fax server for networks; GFI MailSecurity email content/exploit checking and anti-virus software; GFI MailEssentials server-based anti-spam software; GFI LANguard Network Security Scanner (N.S.S.) security scanning and patch management software; GFI Network Server Monitor that automatically sends alerts, and corrects network and server issues; and GFI LANguard Security Event Log Monitor (S.E.L.M.) that performs event log based intrusion detection and network-wide event log management.”

[Disclaimer: This article is not an endorsement of any product. I have no financial involvement whatever with GFI Software and have not tested their software.]

Ms Trigona wrote, “Novarg (also known as Mydoom and Mimail.R), the latest email virus to threaten the security of networks worldwide, highlights yet again that it is not enough to rely on anti-virus protection alone. The time it takes for anti-virus vendors to discover a virus and issue an update against a new virus is too long and allows ample room for infection and distribution. GFI's Trojan and Executable Scanner, on the other hand, catches Novarg and other new viruses immediately - before their signatures are issued.” The press release she sent me states that “GFI MailSecurity's Trojan and Executable Scanner takes a different approach: Rather than relying on signatures, it uses built-in intelligence to rate an executable's risk level. It does this by disassembling the executable, detecting in real time what it might do, and comparing its actions to a database of malicious actions. This way, GFI MailSecurity can detect unknown viruses and Trojans before they enter the network -- and before anti-virus engine vendors have issued signatures against them.”

David Vella, GFI MailSecurity Product Manager, said, "Organizations need to take a proactive approach to protecting themselves and should install gateway-level protection against one-off and unknown email threats and Trojans, as well as standard virus scanning software. . . . Novarg.A is reported to be infecting a vast number of computers. This worm is an executable that travels in the form of an email attachment, and it requires users to run the executable to be activated. The worm spoofs the email sender and the executable is usually compressed inside a ZIP file. It also launches a denial-of-service attack on www.sco.com and opens a back door on the infected computers. The GFI Trojan and Executable Scanner feature is able to catch
Novarg.A because this infringes the scanner's 'CheckUPX' rule; the worm is compressed using a UPX packer, which indicates that such an executable might be malicious. Further information is available at <http://www.gfi.com/news/en/novarg.htm>.

* * *

In conclusion, everyone should check their current antivirus software to ensure that it automatically downloads signature file updates and that its heuristic scanning engines are enabled so that it can catch malicious software (malware) that hasn’t yet made it into the signature files. All inbound e-mail attachments should be scanned automatically for malware. Although some outbound e-mail scanners can cause timeouts on SMTP servers, if tests show no such interference, then outbound e-mail scanning should also be enabled to help reduce the spread of e-mail enabled worms.

* * *


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2004 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.