

CLEAR CHOICE TEST

Zero-latency approach gives FaceTime edge

BY BARRY NANCE, NETWORK WORLD LAB ALLIANCE

Ridding a desktop or server of malware is like trying to kill kudzu, an out-of-control vine in the South that can grow 12 inches a day. Rootkit-based spyware is especially tenacious. Using Task Manager doesn't help, because the spyware process inserts Registry entries that cause the spyware to restart automatically. Using the Registry Edit tool to remove autorestart insertions doesn't work, because the instance quickly reinserts the autorestart Registry entries before you can use Task Manager to end the process.

An Internet gateway that prevents malware from reaching clients and servers is a much better approach than installing antispymware tools on each device. To find the best gateway-based system (either software or appliance), we invited several vendors to our lab for testing. We received FaceTime Enterprise Edition (RTG 500 device, IM Auditor software and Greynet Enterprise Manager), eSoft's ThreatWall 200 appliance and Gateway Anti-Spyware SoftPak, Barracuda Networks' Barracuda Web Filter 310, Aladdin Knowledge Systems' eSafe Gateway/Web/Mail V5.2 appliance and Web Security Pack, Trend Micro's InterScan Web Security Appliance 2500 and CP Secure's Content Security Gateway 1500 V2.0 with WebSense's Web Security Suite V6.2 (combination offering). We also downloaded Secure Computing's WebWasher Anti-Virus 5.3

and Secure Anti-Malware product. Three vendors (Sophos, Bluecoat and IronPort) were developing new product versions during our test cycle, and McAfee said it is retooling its antimalware appliances.

All products tested fared well, with FaceTime Enterprise Edition edging out a strong field (three products tied for second with 4.1 scores). FaceTime earns a Clear Choice Award for its zero latency and easy-to-use central console for managing multiple appliances. The table below summarizes the success rates and performance results for each product (see How we did it, last page). See related story on new approaches to malware at www.nwdocfinder.com/5226.

FaceTime Enterprise Edition

This system includes an RTGuardian (RTG)



FaceTime's RTGuardian appliance edged out other antimalware gateways with an innovative TCP Reset feature to create zero latency.

appliance, Greynet Enterprise Manager software and IM Auditor software. Impressively, the RTG 500 caused zero latency as it inspected inbound and outbound Internet traffic for malware and malware references. When it detected unmanaged instant messaging and peer-to-peer protocols (such as Skype) or malware coming over IM or peer-to-peer, the RTG 500 prevented the unwanted computer programs from entering our network by spoofing the source and destination machine addresses to send each session partner a TCP Reset packet. The TCP Reset instructs both sender and receiver to cease the current transfer of data.

FaceTime's use of the TCP Reset packet is extremely clever. The RTG appliance was never a bottleneck, because it doesn't sit inline between the Internet connection and the network. The appliance merely listens to the conversation flow and, when it detects malware, commands the client and the spyware host to halt. In other words, the appliance never has to act as a relay station. While some upstream routers may be programmed to discard the TCP Reset on its way back to the spyware host, you can reconfigure the upstream routers. Most important, the client gets the message to stop requesting the spyware packets.

The RTG 500 thwarted 69 of 70 malware instances with which we attacked our network. The device dealt comprehensively with Web-, Skype- and IM-borne unwanted programs. The 1U device connects to a span port on a switch or any hub port. FaceTime typically distributes malware definition updates twice a week but sends them more when it identifies critical threats.

For each event, the device collects date, time, spyware ID (its name), category (spyware or adware), type of attack (infection, phone home), threat rating, source IP address and number of attempts made. SNMP support for network-management system integration is planned, FaceTime says.

The Greynet Enterprise Manager (GEM) component is a central console that consolidates, in one place, the administration of several remote RTG units. A handy feature of GEM is that it can detect and clean infected desktops without the use of an agent. The IM Auditor component helps the RTG 500 thwart and report on malware carried by IM protocols.

State of the antimalware market

For all the tested products, documentation was comprehensive and clear. Installing each product essentially involved connecting it to our network and assigning an IP address.

All the products worked well in our tests. Because of its excellent accuracy rate and zero latency through the clever use of the TCP Reset command, as well as the central console which improves scalability, FaceTime edged out the formidable competition.

Using one of these gateways can prevent kudzu-like malware from infesting your network. The success rates and quick performance of these appliances led us to conclude that 2006 is the year the antimalware vendors have finally drawn even with the bad guys.

Nance runs Network Testing Labs and is the author of Introduction to Networking, 4th edition, and Client/Server LAN Programming. He can be reached at barryn@erols.com.

How We Did It

Focusing on gateway products, we primarily looked for the ability to identify and block malware (such as keystroke loggers, browser hijackers, adware, rootkits, dialers, data miners and Trojans). We wanted a product to prevent malware from sending data from our network (such as phoning home), identify already infected clients, handle Skype- and instant message-borne malware as well as HTTP-borne malware, scan traffic quickly, receive frequent spyware-definition updates, integrate with a network-management system (such as OpenView) and produce helpful reports on infection attempts and traffic statistics.

We collected a suite of 70 malware samples, and vendors gave us some additional test samples. We moved the collected material to an isolated, quarantined network, which consisted of three subnets. Subnet 1 had 10 client machines with a variety of operating systems, including Windows NT, 98, 2000, ME, XP, Red Hat Linux and Macintosh OS X. Subnet 2 contained three Web servers (Microsoft Internet Information Server, Netscape Enterprise Server and Apache), three e-mail servers (Exchange, Notes and Sendmail), two file servers (Windows 2003 Advanced Server and NetWare) and two database servers

(Oracle 8i and Microsoft SQL Server). Subnet 3, simulating the Internet, had Web, IM and Skype servers and clients containing the malware instances and sporting "bad guy" IP addresses and URLs. Systems on the first two subnets accessed the third subnet as if it were the real Internet.

To measure performance, we used two time-synchronized protocol analyzers on the Internet and local network sides of the gateway device and examined the resulting packet captures to know the time taken by a device to forward or discard each network message.

Each gateway product connected our simulated Internet to the other two subnets. Client and server machines started off in a pristine state for each test.

Our clients and servers attempted to download malware from the simulated Internet. We noted how well the products identified malware traffic and blocked attempts by the malware to send data back to the source. We gauged success or failure by examining each machine for malware after each test. We looked for running malware processes, new program files (EXE, DLL or OCX, possibly marked with the "Hidden" attribute) and directories as well as Registry and Start Menu changes.

Antimalware gateway latency and accuracy

Product	Latency (nonexecutable)	Latency (executable)	Accuracy*
FaceTime Enterprise Edition	0 ms	0 ms	98.5% (69/70)
CSGateway 1500 (CP Secure)	15 ms	45 ms to 80 ms	98.5% (69/70)
InterScan WS 2500 (Trend)	16 ms to 25 ms	150 ms to 190 ms	97.1% (68/70)
eSafe Gateway (Aladdin)	18 ms	70 ms to 150 ms	97.1% (68/70)
ThreatWall 200 (eSoft)	18 ms to 25 ms	110 ms to 190 ms	95.7% (67/70)
WebWasher AV/AM (Secure)	20 ms to 24 ms	170 ms to 250 ms	95.7% (67/70)
Barracuda Web Filter 310	20 ms to 27 ms	180 ms to 230 ms	95.7% (67/70)

* Accuracy defined at time of testing. Because there are no standards for naming spyware instances, we are not naming the instances that got through. A vendor may know our instances as a different name — in addition, there are many variations of spyware instances and a vendor product may or may not handle the specific version of the malware instance we tested with.

Lab Alliance

■ Nance is also a member of the Network World Lab Alliance, a cooperative of the premier testers in the network industry, each bringing to bear years of practical experience on every test. For more Lab Alliance information, including what it takes to become a partner, go to www.networkworld.com/alliance.

NetResults

Product	FaceTime Enterprise Edition
Vendor	FaceTime Communications www.facetime.com
Price	Starts at \$7,000.
Pros	Zero latency, good spyware recognition.
Cons	No SNMP support.
Score	4.55

FaceTime®

FaceTime Communications
1-888-349-3223 (FACE)
+1-650-574-1600
sales@facetime.com
www.facetime.com