Product Focus: Behavior-Blocking Stops Unknown Malicious Code

By Andrew Conry-Murray, Network Magazine
Jun 5, 2002 (7:36 AM)
URL: http://www.networkmagazine.com/article/NMG20020603S0009/1

Signature-based anti-virus (AV) software is running a losing race. Malicious code writers persistently out-pace the efforts of AV researchers to identify and halt the latest threats. This isn't due to a lack of effort: vendors have cut response time from days to hours. This is an admirable feat, considering they must ensure that the update detects and removes the virus, and that it doesn't interfere with the normal operations of their customers' myriad computer systems.

The problem is the race itself. Malicious code writers have a head start-they launch malware against live targets before AV researchers can analyze and counteract that code. Even if traditional AV vendors can release updates fast enough to protect nine-tenths of their customers, that still leaves one-tenth to deal with the damage. What network manager wants to be a sacrificial lamb, thrown to the wolves to save the rest of the flock?

And the virus problem is getting worse. According to ICSA Labs' 2001 virus prevalence survey, the likelihood of a company experiencing a worm or virus increased 15 percent in 2001. Average server downtime due to viruses was 14 hours. The median time to recover from a virus disaster was four person-days. (The study categorizes a disaster as 25 or more PCs or servers infected simultaneously.)

Traditional AV products clearly can't keep pace with the current threats. Many organizations are now investigating other options to fill the gap between virus attack and signature update. One such option is behavior-blocking technology, which has been around for several years, but is now gaining considerable traction because it provides what signature-based AV solutions can't: real-time protection against unknown malicious code.

Behavior blockers watch ActiveX, Java applets, various scripting languages, and other mobile code that arrives on a host via e-mail, the Internet, or other network connections. Some blockers isolate this code in a "sandbox," restricting the code's access to various OS resources and applications. Other blockers insert themselves into the kernel of a host's OS to intercept system calls.

From either vantage point, behavior blockers monitor the code as it runs in real time. If the code attempts a function that violates a predefined policy, the behavior blocker will halt that function (see Figure 1). You can also program

behavior blockers to quarantine or kill code and send a variety of alerts. It's this comparison of real-time behavior against a predefined rule set that enables behavior blockers to thwart zero-day attacks.

This article explores behavior-blocking technology, its benefits and drawbacks, and looks at several players in the market. It also discusses the future of signature-based AV software and whether behavior-blocking technology will support-or displace-its counterpart.

BEHAVIORAL SPECIALISTS

Companies turn to behavior blocking for two main reasons, says Dave Kroll, vice president of marketing and security research at Finjan (www.finjan.com), which makes behavior-blocking software. The first reason is to close the window of vulnerability. This window is defined by the time between the release of a new virus or worm onto the Internet and the creation of an AV signature that can be distributed to end users.

"It's a major headache to roll out emergency anti-virus updates," says Kroll. Administrators must reach every PC in the organization, including headquarters, branch and remote offices, laptop-toting road warriors, and home workers. Even a handful of PCs missing the update can compromise an entire corporate network.

Proactive solutions give harried administrators time to update signatures, apply software patches, reconfigure firewall rules, and take other steps to lock down the enterprise network. "If behavior blocking stops one or two viruses or worms a year, it's paid for itself," Kroll says.

The second reason companies use behavior-blocking software is that it's policy-based. Depending on the product, administrators can define very granular polices for specific departments, applications, and even end users. This granularity lets organizations distinguish between executable code that enables essential business functions and executable code that is either malicious or frivolous.

Ironically, policies are also often cited as a drawback to behavior blocking. Because the technology relies so heavily on policies, the burden is on the administrator to create a tight set of instructions for a host of applications, OS functions, and user groups. Poor policies will either halt benign processes or allow attacks to slip through.

This brings up a second flaw in behavior blocking: false positives. Like Intrusion Detection Systems (IDSs), behavior blockers are prone to trigger alarms for nonmalicious events. False positives have the same effect as the boy who cried wolf. "If you get too many alerts, you're going to start mistrusting the system," says Vince Weafer, senior director of Symantec Security Response. Weafer says too many false alarms will encourage admins to ignore future alerts, or to turn the system off.

Despite these drawbacks, behavior-blocking technology has made headway in the security market. The next section examines several players and their offerings.

PRODUCT LINEUP

Finjan

Finjan leads the behavior-blocking market, according to analysts at IDC (www.idc.com). Finjan has three offerings in the behavior-blocking space: SurfinGate and SurfinGate for E-mail, which guard the gateway, and SurfinShield, which sits on desktop PCs.

At the gateway, SurfinGate inspects HTTP and FTP traffic for the presence of ActiveX, Java, Visual Basic Script (VBS), and JavaScript. It scans this code in real time for potentially malicious behavior, such as file-system operations and network operations. If such behavior is detected, SurfinGate checks it against an administrator-defined policy. If the action violates the policy, SurfinGate stops the code from entering the network, logs its action, and sends an alert to an administrator. Policies can be defined for groups, departments, and individuals.

SurfinGate for E-Mail scans both in-bound and outbound SMTP traffic for naughty code, including Trojan Horses and scripts planted as attachments, inside .zip files, or in HTML e-mail. Code that violates a policy is blocked at the gateway or quarantined for later inspection. The current version of SurfinGate for E-Mail only allows for global policy creation.

You can deploy SurfinGate for E-Mail as an SMTP mail relay or as a plug-in for Microsoft Exchange 2000.

The gateway products run on Windows NT/2000 and Solaris 6,7, and 8. They are also available as appliances. SurfinGate and SurfinGate for E-Mail are available on an IBM eServer Series 330 box running Windows 2000. In addition, SurfinGate is available on a Sun Nextra X1 server running Solaris.

SurfinShield Corporate is installed on individual desktops. The software inserts itself near the kernel of the OS and monitors executables, ActiveX controls, Java applets, and Windows scripting hosts that arrive at the desktop via the Internet, e-mail, and Instant Messaging (IM).

If code attempts to open a network connection, delete or write files, access the system registry, or make OS calls, the desktop client acts and the code is sandboxed. Code that violates administrator-defined security policies is either halted or deleted. Finjan says the client software can surgically delete malicious code without interfering with any applications or Web browsers that might be running.

SurfinShield Corporate consists of a console component, a server component, and a client module. The console functions as an enterprise-wide mission

control where policies are defined. The server holds those policies and maintains event logs. The client agent enforces policies and sandboxes all executables. The client can run independent of the server, making it suitable for laptops that might be disconnected from the corporate network for extended periods of time. All three components run on Windows OSs.

Aladdin

Aladdin's (www.esafe.com) eSafe Gateway is a software-based solution that scans HTTP, FTP, and SMTP traffic for executable code, including Java, ActiveX, and scripting languages such as VBScript and JavaScript. As traffic passes through the eSafe Gateway, it sends that traffic to both the client that requested the traffic and to an inspection engine.

However, the gateway will withhold the final packet in the transmission from the client until the inspection engine has scanned executable code. If the scanned code is clean, the gateway completes the transmission to the end user. If the scanned code is malicious, the gateway alerts an administrator. The gateway also informs the end user that the transfer has been blocked.

The eSafe Gateway supports the Content Vectoring Protocol (CVP), which lets the gateway communicate with any OPSEC-compliant firewall and allows more targeted inspection capabilities. That is, the firewall will only pass potentially infectable files to the gateway for scanning. Noninfectable files, such as plain text or graphic images, are simply forwarded to their destination. The gateway can also communicate with OPSEC-compliant firewalls to request policy changes, such as allowing executable code to pass from trusted sources.

The gateway also includes a signature-based AV engine to block known viruses. The eSafe Gateway software runs on Windows NT/2000 servers. A specialized version integrates with Microsoft's Internet Security and Acceleration (ISA) server. The eSafe Gateway is also available as a Linux-based appliance for small and medium-sized organizations.

eSafe Enterprise sits on individual desktops and uses sandboxing and a personal firewall to thwart malicious code. The client software monitors each active process and application on the desktop via a system driver. The sandbox matches the executable code's behavior against an administrator-defined rule set and halts any action that violates that rule set.

The desktop client also functions as a personal firewall. Administrators can selectively block IP ports from being opened on the desktop. The desktop client also stops Trojan Horses that might have been inadvertently installed from opening ports to contact the attacker who installed the virus.

The eSafe client gives administrators substantial control over the user's machine. Administrators can lock users out of inappropriate Web sites (or restrict them to a set of trusted sites), block the use of certain words in e-mail, chat rooms, and Instant Messaging (IM), and stop users from reconfiguring

the PC or installing software. The client also includes a signature-based AV engine to halt known viruses that find their way onto the PC.

Client agents are controlled from the eConsole, which configures, deploys, and manages those agents. Administrators can monitor security events from the console, adjust settings, and distribute network-, group-, or user-based policies.

The eSafe Enterprise client runs on Windows desktops. The console runs on either Windows NT/2000 or Novell Netware.

Pelican Security

Pelican Security's (www.pelicansecurity.com) SafeTNet is a desktop agent that monitors applications that can download executable code, including Web browsers, e-mail, Office applications, and chat clients. Whenever code is executed, SafeTNet's Dynamic Sandbox intercepts the system calls the code makes to the Windows OS. The sandbox checks these calls against a policy database, and acceptable system calls are allowed to proceed. Unacceptable calls, such as attempts to modify registry settings or open a network connection, are blocked. End users can't turn off or modify the SafeTNet client. The client can stop end users from downloading or installing unauthorized programs.

You can customize SafeTNet's out-of-the-box policies to allow particular processes to run, or you can create new policies to match the enterprise's needs. Administrators can apply policies globally or by groups, including groups already established in the enterprise via Windows NT.

SafeTNet has three components: the client agent, a server, and a management console. The server installs the client agent and sends policy updates. The client reports security events to the server. Administrators can manage those security events from the console. You can also integrate the product with management software, including UniCenter, HP OpenView, and Tivoli.

The client agent runs on Windows 95/98/NT, the server runs on Windows NT, and the management console runs on an NT workstation.

Trend Micro

The InterScan AppletTrap from Trend Micro is an HTTP proxy server that scans incoming Internet traffic for the presence of ActiveX, Java applets, and scripts. AppletTrap performs three checks on incoming mobile code. First, it looks for code with digital certificates; that is, ActiveX controls that have been digitally signed via Microsoft Authenticode, or Java applets containing digital certificates. Unsigned code, or code with signatures from unknown sources, can be blocked at the gateway.

Second, the product can block known malicious Java applets and JavaScript. Trend Micro maintains and continuously updates a database of known

malicious applets. Administrators can add to this database and also block any Java applets coming from blacklisted URLs.

Third, Java applets that pass the first two checks are wrapped in monitoring code at the proxy server and then transferred to the client. The client runs the applet in a sandbox. As the applet runs, the monitoring code checks its behavior against a list of administrator-defined policies. If the applet demonstrates malicious behavior, the monitoring code halts the action, notifies the user and administrator of the policy violation, and adds the applet to the database of malicious vandals. Applets that don't violate security polices are removed from the sandbox and allowed to run unimpeded. No client agent is required for this sandboxing function.

The proxy server runs on Windows NT/2000 and Solaris 2.6. The administration console uses Internet Explorer or Netscape Navigator for both local and remote access. AppletTrap runs as a standalone proxy or as a plug-in to Check Point's Firewall-1. It also integrates with other Trend Micro AV solutions.

Tiny Software

Tiny Software (www.tinysoftware.com) includes sandboxing functionality in its Personal Firewall 3.0 Network Edition. The sandbox throws up a barrier around ActiveX, Java, and other executables. It monitors the Windows registry, system services, system calls, file system, and IP ports. The sandbox prevents any actions that resemble administrator-defined malicious behavior, such as attempts to alter or delete particular files.

Administrators can configure and monitor personal firewall clients via a Windows NT/2000 domain controller. The client runs on the gamut of Microsoft OSs, from Windows 98 up to XP.

Okena

StormWatch, from Okena (www.okena.com), is a multifunction client agent that acts as a host-based IDS, personal firewall, and proactive worm and virus blocker. For instance, besides blocking the execution of malicious code, StormWatch can prevent port scanning and stop buffer overflows. StormWatch is available for both servers and desktops.

StormWatch deploys an agent that shims itself into the kernel of the host's OS, where it intercepts system calls in real time. The agent compares the system calls to predefined polices. System calls pointing to malicious or unwanted behavior (as defined by the policies) are blocked.

Rather than use a sandbox, the Storm-Watch agent simply monitors every application on the desktop. Four modules-the file interceptor, the network interceptor, the registry interceptor, and the COM interceptor-sit in front of the kernel to gather system calls. These interceptors coordinate with a rules engine to determine which actions are allowed and which should be denied.

A management console feeds policy updates to the rules engine. The rules engine then sends alerts and log data back to the console for analysis. StormWatch includes 12 out-of-the-box policies for a variety of applications, such as Microsoft Office (including Outlook) and Instant Messenger. Administrators can also create customized policies.

The StormWatch desktop agent and management server run on Windows NT/2000. The management browser requires Internet Explorer 5 or Netscape 4.7x.

WHAT THE USERS SAY

According to several administrators using behavior-blocking products, the technology generally fulfills its function-catching unknown worms, viruses, and other malicious mobile code that AV signatures miss. Of course, they also noted several problems, including false positives, deployment hassles, and sometimes buggy products.

The security administrator at a major outdoor equipment and apparel company uses Finjan's SurfinShield desktop software on approximately 600 machines.

He was first attracted to the product by a rash of Outlook-based viruses. Although his company wasn't hit, he saw enough to convince him to seal a deal with Finjan. His experience with the behavior-blocking software has been mixed. "You can't underestimate the time and effort to get it out there."

He notes that false positives have been a problem, and not just with homegrown applications. "It doesn't play well with everything," he says. "It's not something you can just roll out without an impact."

On the other hand, he's also seen firsthand Finjan's protective capabilities. During a transition from Windows NT desktops to Windows 2000, the Goner virus struck. Several Windows 2000 machines, which hadn't been installed with Finjan's SurfinShield, fell victim to Goner. Windows NT machines running SurfinShield successfully repelled the virus.

The administrator says he'll continue to run SurfinShield in tandem with traditional AV software. He counts on behavior blocking to act as insurance against zero-day exploits, providing him some breathing room to apply more long-term fixes.

Tony Nelson is director of IT operations at StarPoint Solutions (www.starpoint.com), which designs digital business applications. He uses Aladdin's eSafe Enterprise and eSafe Gateway software to protect four Internet gateways and approximately 400 desktops.

Nelson sought out a proactive virus solution after the Melissa virus slipped into the network and shut down the New York office for a full day. Although he was running anti-virus software, not all of his users had the latest updates.

His experience with eSafe has been positive. "The gateway catches 99 percent of our viruses," says Nelson. "The only time we find them on the desktop is when somebody has a laptop from out in the wild." He also likes the fact that end users can't turn off eSafe's desktop client or tamper with its settings. Despite eSafe's excellent track record, he has no plans to give up on signature-based AV. "I like having the dual vendor system. In today's times, you can't be too careful."

The security administrator for a large insurance company is using Okena's StormWatch on 500 desktops for remote employees who access the corporate network via the Internet. He uses the product as a personal firewall, but also appreciates its capacity to thwart unwanted code execution. "It's smart enough to know the difference between a system file and Nimda," he says.

He says he has been pleasantly surprised at how easy it is to configure and deploy policies. He also likes that it's invisible to end users and doesn't trouble them with lots of pop-ups and alerts, which in turn minimizes help-desk calls. "If they do run into trouble, [the agent] logs back to a master console and I can monitor that," he says. "Then I can change the policy and distribute it back to the folks that are connected."

THE NEW FACE OF ANTI-VIRUS SOFTWARE

Some experts see behavior blocking as the wave of the future, a wave that will wash away signature-based AV products. After all, if the blockers you've installed successfully catch both known and unknown threats, why bother running a second, unnecessary layer of software-especially if all it does is demand updates and generate subscription fees?

It's a good question, and the answer has two components. The first is economic. In terms of market share, behavior-blocking software is a ripple, not a wave. Companies making behavior-blocking software own 1.5 percent of the market, according to a report from research firm IDC (see Figure 2). By contrast, AV companies own nearly 83 percent. (The remainder belongs to e-mail scanning and Internet access control software.)

Even though IDC predicts that behavior blocking will grow faster than standard AV software (29 percent compound annual growth vs. 14 percent compound annual growth), AV vendors will still be sitting on an estimated $2.7 billion market in 2005; the behavior blockers won't even crack $90 million. Thus, it's unlikely that traditional AV companies will dry up any time soon.

Second, a major appeal of traditional AV technology is its certainty. Digital fingerprints clearly identify viruses, and the AV software removes it without fuss. That means network administrators don't have to spend time constructing detailed mobile code policies, examining quarantined code for malicious intent, or explaining to irate vice presidents why Web apps keep shorting out. In addition, AV technology can also clean out infected systems, a feature that no behavior blocker can match.

The upshot is that signature-based anti-virus solutions aren't going away. Still, traditional AV vendors would be foolish to ignore behavior blocking (ever hear of David and Goliath?), because they can't escape the fact that their current methods are ineffective against the new breed of blended threats.

What's likely to happen is the major vendors will use their market dominance to absorb, Borg-like, the behavior blockers, either through partnerships, acquisitions, or by developing their own blocking technology.

AV market leader McAfee has already begun this process. In November 2001, it launched a partnership with Finjan to integrate McAfee's anti-virus scanning engine into Finjan's product line. In April 2002, Aladdin announced a partnership with Kaspersky Labs that offers Kaspersky's anti-virus module to eSafe customers.

Symantec has also hinted that it's pursuing a behavior-blocking strategy. In March 2002, Carey Nachenberg, chief architect of Symantec's security response team, published a paper entitled "Behavior Blocking: The Next Step in Anti-Virus Protection" on the SecurityFocus.com Web site (see Resources). While the paper doesn't directly state that the company is developing a behavior-blocking product, it indicates that Symantec is thinking hard about the future of AV technology.

Trend Micro is launching a service, known as the Outbreak Commander, that uses policy-based behavior-blocking to shorten the gap between the appearance of virus and the creation and distribution of signatures. When Trend Micro obtains a virus or worm sample, it writes a policy specifically geared to identify and halt any malicious behaviors.

For example, during a recent worm outbreak, Trend Micro engineers had a policy ready for customers in just 20 minutes; by comparison, the full signature took nearly an hour to develop. This is a clever use of policy-based behavior blocking, and it greatly reduces the window of vulnerability; however, it is not a truly proactive mechanism because customers must still wait for Outbreak Commander to acquire a virus or worm sample and make updates available.

And as for administrators, it would be unwise to give up anti-virus signatures, but perhaps just as unwise not to investigate behavior blocking. As new threats continue to evade standard defenses, behavior blocking offers a proactive solution to zero-day exploits. The time you spend fine-tuning behavioral policies and weeding out false positives will be well worth seeing unknown malicious code bounced from your network, hours before the first AV signature arrives at your inbox. Suddenly, the race is fair again.

Andrew Conry-Murray, business editor, can be reached at amurray@cmp.com.

Products Mentioned

Aladdin www.esafe.com- eSafe Gateway, eSafe Enterprise

Finjan Software www.finjan.com - SurfinGate, SurfinGate for E-mail, SurfinShield Corporate

Okena www.okena.com - StormWatch

Pelican Security www.pelicansecurity.com - SafeTNet

Tiny Software www.tinysoftware.com - Personal Firewall 3.0 Network Edition

Trend Micro www.trendmicro.com - InterScan AppletTrap

Resources

For more information on server-based behavior-blocking products, check out "Web Server Lockdown," in the February 2002 issue of Network Magazine.

To read Carey Nachenberg's short paper, titled "Behavior Blocking: The Next Step in Anti-Virus Protection," go to online.securityfocus.com/infocus/1557/.