INFORMATION SECURITY
JUNE 2002 A TruSecure Publication

test CENTER

BY JP VOSSEN

NEW PRODUCTS TESTED IN REAL-WORLD ENVIRONMENTS

STAT Neutralizer

Harris delivers a simple, effective solution that blocks unauthorized activities.

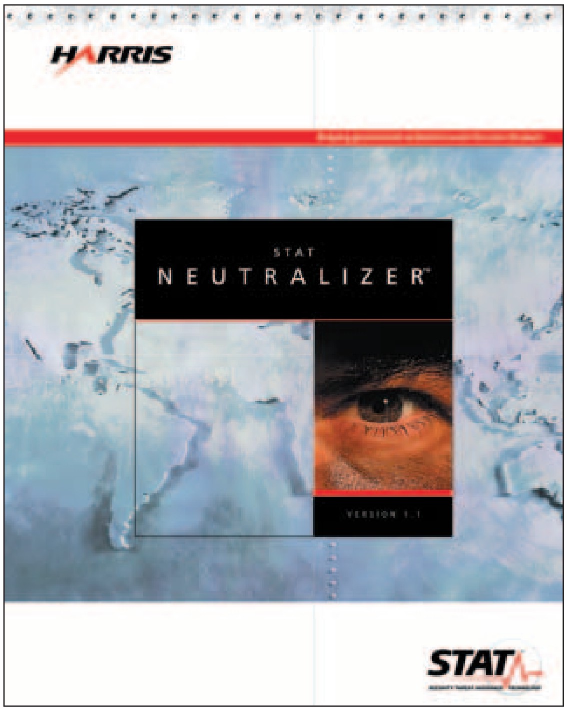
Harris' STAT Neutralizer implements a simple, yet surprisingly effective idea. If you hook the kernel calls that control file and registry key creation, reading, writing and deletion, you can add a significant layer to your defense-in-depth. Because those actions are at the crux of all activity, malevolent or otherwise, if you block unexpected or undesirable actions, you can eliminate a lot of risk at a higher level than with similar products—notably AV solutions. Since it's activity based, you don't have to worry about constantly updating signatures, and it's flexible enough to be useful in almost any environment—since you can write or refine rules as needed.

Neutralizer has two typical uses: preventing malware from executing, and hardening systems for use in untrusted environments or while waiting for a patch to address a vulnerability. Neutralizer's distributed architecture consists of an agent running on each protected machine and an administrative/logging server. The only supported platforms are Windows NT 4.0 SP3+ and Windows 2000. According to Harris, Windows XP, Linux and Sun Solaris will eventually be supported.

Getting Started

I installed the Neutralizer server on an existing Windows 2000 SP2 server running IIS and several other services. When choosing a machine to host the server, keep in mind that the Web server takes over port 443 (HTTPS) for the Web-based administration interface, and the software license is based partly on the server's IP address. Thus, you won't want to run the Neutralizer server on a machine that's also running an HTTPS server, or has frequent IP address changes.

Aside from the simplicity, I especially liked two aspects of the installation. Even though I was intercepting kernel calls, I didn't have to reboot Windows 2000 or, amazingly, NT. And I was pleased to see that Apache provides the interface (on port 443), not IIS.



I installed the agent on the Neutralizer server, as well as on some other Windows 2000 machines and an NT 4.0 server in a different domain. Like the server, the agent requires admin rights for the install only. I also installed it remotely, and it worked very well. The installation doesn't allow you to enter different credentials for different machines, but an easy workaround is only installing groups of machines with the same credentials.

The only thing the agent requires is the host name or the server's IP address, which is already provided in the installation. Once the installation directory is chosen, there's nothing to configure on the agent—everything is done through the Web interface to the server. The agent communicates with the server over an SSL-encrypted session. Once it has obtained a policy, it will work whether or not it can connect to the server. On agent start-up or reconnection following a disruption, the agent will transmit its logs and look for policy updates.

What to Expect

The server runs Apache/1.3.20 (Win32), PHP/4.0.6, mod_ssl/2.8.4 and OpenSSL/0.9.6b to provide the Web-based administrative interface. New to version 1.1 is a Sybase back-end database for event logging.

The performance hit on the server and agents depends mainly on the complexity of the enabled rules, so keep that in mind when defining groups and rules. The rule description language is Perl-style "Regular Expressions." Far more prevalent in the Unix world than in Windows, RegExs are an immensely powerful way to define a pattern you wish to match, though they're admittedly sometimes obscure.

The Neutralizer interface has a navigation bar that allows you to choose between seven main function areas: logs, agents, groups, rules, variables, settings and interface users. The heart of the system is the rules section. The management architecture is well designed and very usable, with the groups mapping which rules are applied to which agents. Rules may belong to more than one group, but agents can only belong to a single group. Each of the four default groups (Default, Default Apache Server, Default IIS Server and Default Workstation) has some subset of the 29 built-in rules assigned to it. The built-in rules focus mainly on denying Outlook, Outlook Express, Internet Explorer and Netscape Communicator the ability to perform various actions, such as accessing the system repair directory or modifying various registry keys. This is probably a good way to provide basic coverage with little chance of false positives, but I was looking for more comprehensive rules. These would be easy enough to create, and Harris says it's developing a strategy to do exactly that. In the meantime, both groups and rules may be "cloned" or copied, so you can find a rule similar to what you want to create, clone and then modify it.

The point of Neutralizer is to stop malicious activity before it has a chance to do any damage, so in many ways it is similar to an AV product. Once you've installed and configured Neutralizer, there's just not much else to do, except fine-tune the rules.

Shortcomings

The first problem I ran into while testing Neutralizer occurred when I tried to update the agent policy. The update function told me that the policy was already updated, but the "Current Agents" screen correctly told me that the policy wasn't current. The problem turned out to be that the NeutServer service wasn't running on my server, though I could get the same symptom by turning off the NeutAgent on an agent as well. Either way, there's no way to tell if the services are running, or to start or stop them, from the Neutralizer interface.

Some issues also arose in rule creation and enforcement, where rules aren't always intuitive and seemingly don't always work as expected. It turns out that the mechanisms by which Windows does certain things aren't consistent. The user notification function also worked inconsistently, but this is a known issue that Harris says it's addressing.

SNAPSHOT

STAT Neutralizer v1.1

Harris

www.statonline.com

Price: Contact vendor

PROS

- Simple to install, especially the remote agent.
- Doesn't require significant resources to deploy and implement once configurations have been created.
- Rules are defined using Perl-style Regular Expressions, which are powerful and subtle.
- Uses Apache, not IIS, as the administrative interface Web server.

CONS

- Install doesn't force you to choose an administrator password—it uses a default.
- Rules aren't always intuitive, nor do they always work quite as expected (due to various idiosyncrasies of Windows APIs), and thus should be tested extensively.
- Regular Expressions are powerful, but can be confusing.

VERDICT

The idea is simple, yet surprisingly effective—a product that monitors files and registry keys for creation, reading, writing and deletion. By blocking unexpected or undesirable actions, you can add a significant layer to your defense-in-depth, and STAT Neutralizer is one implementation of this idea that doesn't require adding a lot of extra infrastructure, management and administration.

What's Coming Down the Pike

One thing I'd like to see improved in future revs is log handling. I'm not confident that the Web interface will scale well in large environments. There's no automated way to archive logs, or to log to an independent central log host such as a syslog server or even the Event Log. I'd also like to see the ability to use local and global NT groups (not to mention Active Directory) to define permissions for user groups.

While Neutralizer is quite usable, it's still a little rough around the edges. All the basics are in place, and the existing product is already manageable and scaleable. It's under active development, and I expect it will mature rapidly. Version 1.2, which has a strong emphasis on usability and interface improvements, is scheduled for release in Q3. In addition to a new Java-based interface, it's slated to have automated rule creation functionality, a learning or base-lining mode, alerting via SMTP and support for Windows XP.

Neutralizer doesn't claim to solve all of your security problems, but rather adds another layer of security. In one of the product brochures, Harris even discusses how it complements AV, IDS and firewall products. The basic concept is sound, and this implementation of STAT Neutralizer definitely shows promise. ◗

JP VOSSEN, CISSP (**jpvossen@infosecuritymag.com**), is a technical editor for *Information Security* and an integration manager for Counterpane Internet Security.