



Weak Points in an Enterprise: People and External Access

Because worms, viruses and other hybrid attacks take advantage of identity vulnerabilities, the enterprise protection strategies must change. Current strategies focus on attempting to change the users behavior, while this is important, it is equally important to ensure vendor behavior changes to shielding the users and vulnerable software from attack.

Problems

Ongoing attacks from worms, keyloggers, spyware and malware prove the sanity of a corporate network requires proactive preventive mechanisms. In enterprise environments, it further validates that Anti-Virus (AV) and Intrusion Detection Systems (IDS) are not enough to catch up with the pace of bad guys. AV and IDS are reactive only and rely on signatures that are available only after an attack has started.

Industry experts believe that new attacks occur less than 30 days after a patch is released and such attacks will continue to increase significantly. Enterprise's can search for better patching technology, but they will never be able to catch up or become as fast as the attackers.

How Attackers Find Vulnerability

Attackers generally monitor vendor patch announcements and start reverse-engineering of the patch to immediately discover its vulnerability. For example, the Blaster attack occurred only a few weeks after the patch was released. As sophistication increases these types of attacks scenarios will become increasingly more common.

What Attackers Look For

In the past, the majority of worm attacks were destructive, but today they are increasingly becoming more related to cyber crime. These attacks are related to hacking for financial gain. Worms with Trojan horse payloads provide support for identity theft, credit card fraud and the snaring of financial-system password. Businesses that rely on their web sites for revenue have noticed a large increase in the growth of Denial of Service attacks..

Actions that limit damages to networks from malware

Network connection vulnerabilities must be addressed with a combination of the following mechanisms:

- Proactive actions - allowing network connections only for computers that are approved and authenticated.
- Reactive actions - detect suspicious activities of a computer and deny services from the network.
- The combination of these two should not cause unpleasant user experience and/or impede user productivity.

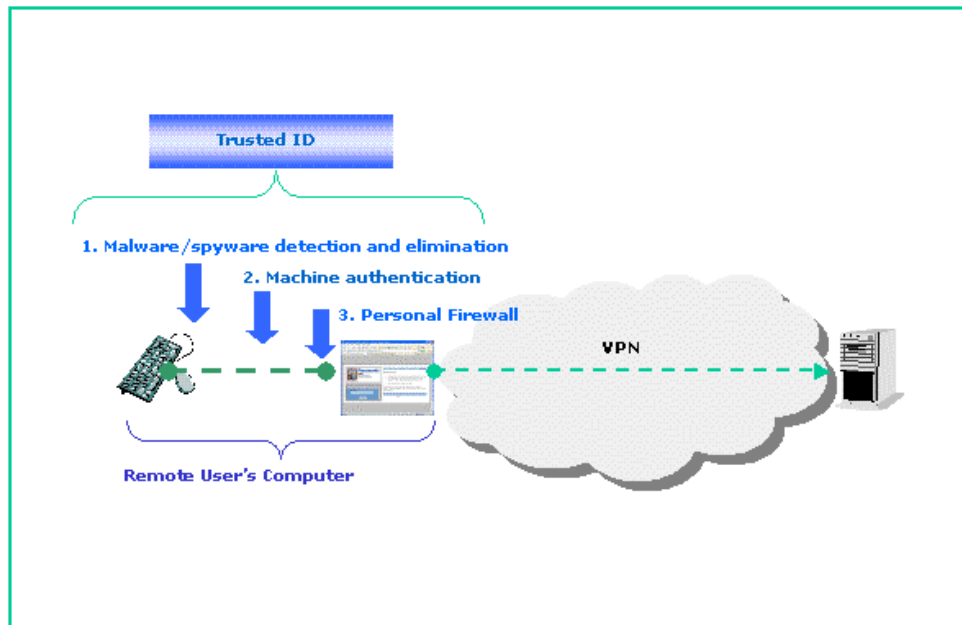
How StrikeForce Technologies meets the challenge

StrikeForce Technologies uses a holistic approach to prevent a remote users machine from being used as a launch pad by attackers against an enterprise network. Our Trusted ID solution provides the following functions:

- Machine Authentication
- Malware scanning before the network connection opens
- Personal Firewall throughout VPN connection

StrikeForce believes that all the above functions need to be addressed simultaneously to effectively preserve the sanctity of the remote machine. Having these functions work concurrently,

the enterprise is ensured that the remote machines are not infected and are not an origin spreading spyware.



1. Machine Authentication

The objective of “machine authentication” is to verify a remote users machine before allowing a connection to the enterprise VPN or to block the connection if the machine fails to comply to the established security policies. This authentication process is separate from the users identity authentication that is performed by our flagship product ProtectID™.

2. Spyware scanning before the network connection opens

Spyware defenses remove established malware and filter incoming spyware programs that record online activities such as keystroke, instant messages, email, chats, web site visits and

personal information. Spyware can arrive in hidden downloads one may think are legitimate or in email attachments like virus's. On a remote users computer, spyware may create standard registry entry to call itself at startup.

3. Personal firewall

The objective of activating a personal firewall is to protect a single Internet-connected computer from intruders. The need for personal firewalls is increasingly important as users connect to “always on” broadband connection with a static IP address that makes the computer vulnerable to hackers. Once a personal firewall is configured, it performs the following basic functions:

- Filters inbound and outbound web traffic
- Detects and logs intrusion attempts
- Deters identified viruses, worms, Trojan horses and other intrusions