TYPES OF CYBER-ATTACKS — AND HOW TO PREVENT THEM

Today's cyber-criminals employ several complex techniques to avoid detection as they sneak quietly into corporate networks to steal intellectual property or hold files for ransom. Their threats are often encrypted to evade detection.

Once they have exploited a target, attackers will attempt to download and install malware onto the compromised system. In many instances, the malware used is a newly evolved variant that traditional anti-virus solutions don't yet know about.

This ebook details the strategies and tools that cyber-criminals use to infiltrate your network and how you can stop them.

SONIC**WALL**®

Bombard networks with malware around the clock

Attacks come in from all vectors: in email, on mobile devices, in web traffic as well as via automated exploits. On top of this, the size of your company doesn't matter. To a hacker you are an IP address, an email address or a prospect for a watering hole attack. Attackers use automated tools to execute exploits or to launch phishing emails throughout the day and night.

The problem that many organizations face is not having the right tools for the job. Many lack automated tools to help scrub traffic, protect endpoints and filter out bad email. Others run firewalls that can't see into encrypted traffic for hidden threats or rely on limited onboard system memory to store malware signatures.
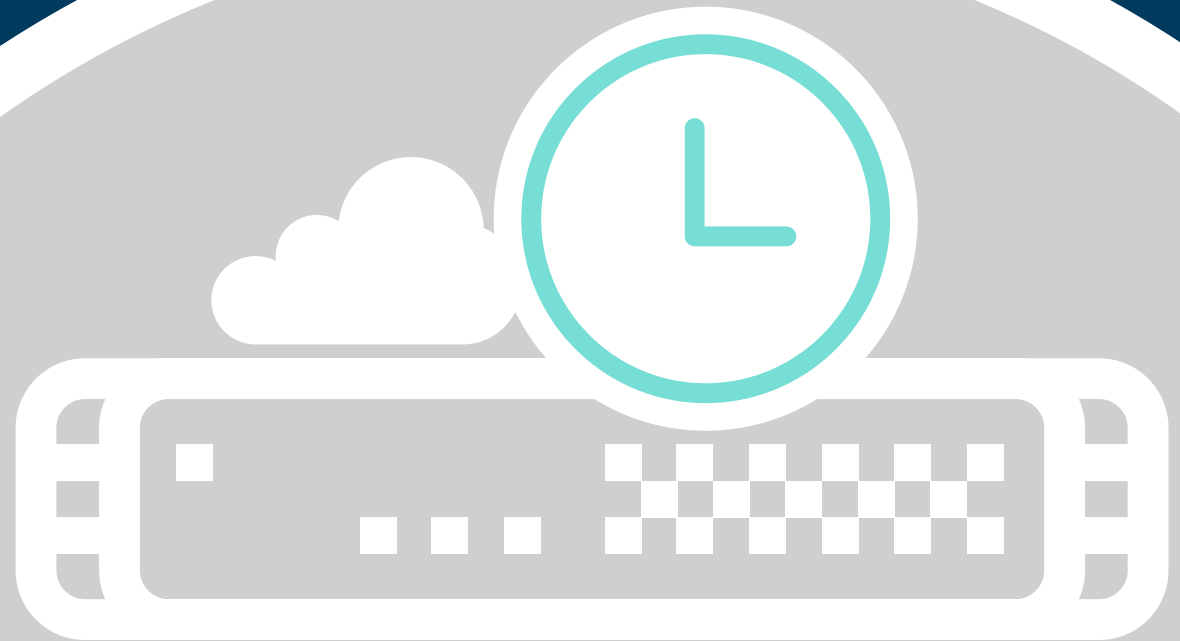
Cyber-criminals work 24/7
to exploit your weaknesses.

SONIC**WALL**®

Protect your network every minute of every day

With hundreds of new malware variants developed every hour, organizations need up-to-the-minute, real-time protection against the latest threats. An effective security solution needs to be continuously updated, 24 hours a day, 7 days a week. In addition, because the number of malware types and variants is so large, it exceeds the available memory of any firewall.

Firewalls should use a network sandbox and the cloud in order to provide the broadest view of malware and discover brand new variants and best identify them. Plus, make sure your security solution also supports dynamically updated protection not only at the firewall gateway, but at mobile and remote endpoints, as well as for your email.

Insist on a security platform that leverages the power of the cloud for real-time countermeasures to the latest malware threats.

Infect networks with different forms of malware

Cyber-criminals use different types of attack vectors and malware to compromise networks. The five most typical types are viruses, worms, Trojans, spyware and ransomware.
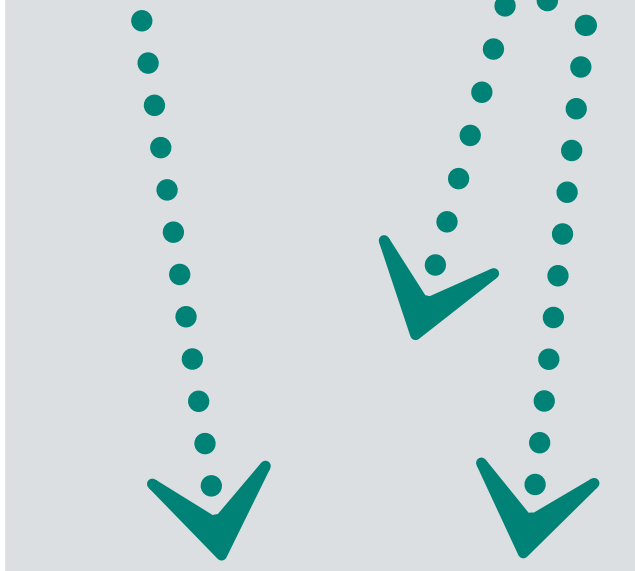
Computer viruses were originally spread through the sharing of infected floppy disks. As technology evolved, so too did the distribution method. Today, viruses are commonly spread through file sharing, web downloads and email attachments.

Computer worms have existed since the late 1980s but were not prevalent until networking infrastructures within organizations became common. Unlike computer viruses, worms can crawl through networks without any human interaction.

Trojans are designed specifically to extract sensitive data from the network. Many types of Trojans will take control of the infected system, opening up a back door for an attacker to access later. Trojans are often used in the creation of botnets.

Spyware is not typically malicious in nature, but it is a major nuisance because it often infects web browsers, making them nearly inoperable. At times, spyware has been disguised as a legitimate application, providing the user with some benefit while secretly recording behavior and usage patterns.

Ransomware is an attack that often encrypts the files on an endpoint or server demanding the end-user to pay a ransom in bitcoin to receive the encryption key. When it spreads to business-critical systems, the cost of the ransom can swell to hundreds of thousands of dollars.

Cyber-criminals use different types of malware to catch you off guard.

Ensure that your network is protected against all types of malware

All firewalls should safeguard organizations from viruses, worms, Trojans, spyware and ransomware. This is best accomplished by integrating these protections into a single-pass, low-latency approach that blocks attack vectors not only at the gateway, but also at endpoints beyond the traditional perimeter. Look for features that include:

- **Network-based malware protection** to block attackers from downloading or transmitting malware to a compromised system

- **Continuous and timely updates** to safeguard networks around the clock from millions of new malware variants as soon as they are discovered

- **Intrusion prevention service (IPS)** to prevent attackers from exploiting network vulnerabilities

- **Network sandboxing** to send suspicious code to a cloud-based isolated environment for detonation and analysis to find never-before-seen malware

- **Access security** to apply security countermeasures at mobile and remote endpoints, both inside and outside of the network perimeter

- **Email security** to block phishing, spam, Trojans and social engineering attacks transmitted via email

Ensuring each device that accesses your network is running up-to-date anti-virus software provides an additional layer of network malware protection. Pairing a PC running anti-virus with network firewalls can reduce many of the tools cyber-criminals have for compromising the network.

To stay ahead of threats, consider multiple layers of protection against malware.

Find and compromise the weakest networks

Although many firewall vendors claim to offer superior threat protection, few have been able to demonstrate the effectiveness of their solutions. Organizations that use inferior firewalls may believe their networks are protected, even though skilled criminals can sneak past the intrusion prevention system by using complicated algorithms to evade detection and compromise the system.

Because some firewalls offer protection at the expense of performance, organizations that use them may be tempted to turn off or limit their security measures in order to keep up with the demand of high network performance. This is an extremely risky practice that should be avoided.

Another weak link in network security is the human factor. Criminals use phishing scams to gain login and other authorization information that can enable them to simply sidestep firewall protections by instigating attacks from the inside. Also, employees can lose mobile devices or expose them to breach when they are used outside of the network security perimeter.

Cyber-criminals often target their victims based on the network weaknesses they discover.

Choose a comprehensive security platform that offers superior threat protection and high performance

Look for security solutions that have been independently tested and certified for network-based malware protection by ICSA Labs.

Consider a multi-core platform design that can scan files of any size and type to respond to changing traffic flows. All firewalls need an engine that protects networks from both internal and external attacks — without compromising performance.

Look for a firewall that offers a network sandbox to help discover brand new malware that may be targeted at your environment. This may mean the difference between a normal work day and one that holds files hostage.

Your security strategy must include protection of mobile and remote endpoints both inside and outside the perimeter.

In addition, you need email security to protect against phishing, spam, viruses, social engineering and other threats transmitted via email.

All firewalls need an engine that protects networks from both internal and external attacks — without compromising performance.
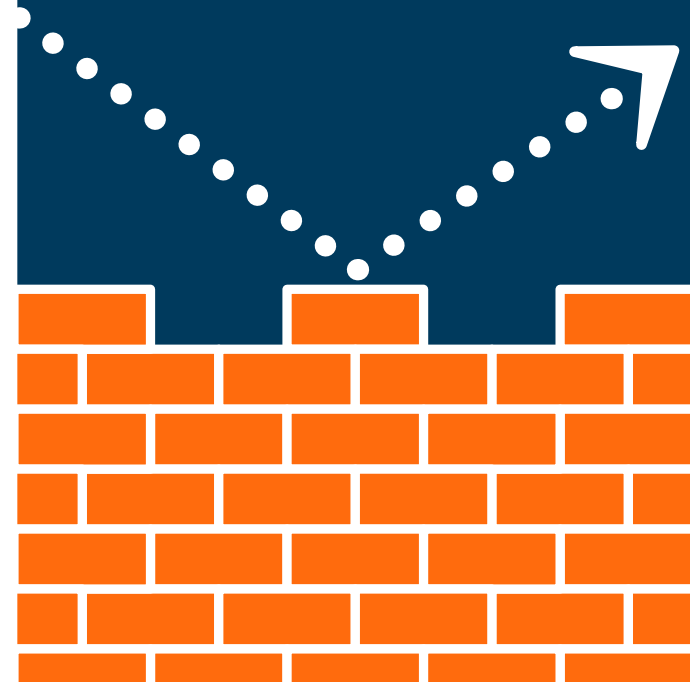
New threats are popping up every hour on all continents.

Morph frequently and attack globally

Many cyber-criminals succeed by continually reinventing new malware and sharing it with their counterparts around the globe. This means that new threats are popping up every hour on all continents. Many cyber-criminals use a "smash and grab" approach to attacks: get in, take what they can, and get out before anyone can raise the alarm. Then they repeat the attack elsewhere.

Others go low and slow in an attempt to gain access to more data over a longer period of time. Some attacks come through the web while others through email or into the network on infected devices that were previously roaming outside the network security perimeter.

SONIC**WALL**®

Choose a firewall that protects against global threats

Reacting quickly to threats is critical for maximizing protection. In order to rapidly deploy countermeasures against emerging threats onto your firewall, look for a security solutions provider that has its own rapid-response, in-house team of countermeasure experts. In addition, that team should extend its reach by collaborating with the broader security community.

A broad-spectrum solution utilizes a globally comprehensive cloud-based malware catalogue to augment local firewall analysis.

Finally, while a simple firewall can identify and block by geography, a sophisticated firewall will add botnet filtering capabilities to reduce exposure to known global threats by blocking traffic from dangerous domains or blocking connections to and from a particular location.

To block the latest global threats, invest in a security solution with global reach.

Conclusion

Cyber-attacks are on the rise, but there are effective defenses. When you are ready to evaluate counter-attack solutions to fit your network environment, learn more by downloading our white paper, Achieve Deeper Network Security.

SONICWALL®

About Us

SonicWall has been fighting the cyber-criminal industry for over 25 years, defending small, medium size businesses and enterprises worldwide. Our combination of products and partners has enabled a real-time cyber defense solution tuned to the specific needs of the more than 500,000 global businesses in over 150 countries, so you can do more business with less fear.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Refer to our website for additional information.
www.sonicwall.com

SONIC**WALL**®