SONICWALL®

EXECUTIVE BRIEF: 5 WAYS YOUR FIREWALL SANDBOXES CAN FAIL

What you need to know to stay ahead of advanced persistent threats (APTs)

An advanced persistent threat (APT) is a set of stealthy and continuous computer hacking processes, often orchestrated by criminals targeting a specific entity. These threats often include unknown and undocumented malware, including zero-day threats. They are designed to be evolving, polymorphic and dynamic. And they are targeted to extract or compromise sensitive data, including identity, access and control information. While these types of attacks are less common than automated or commoditized threats that are more broadly targeted, APTs pose a serious threat.

To better detect APTs, security professionals are deploying advanced threat detection technologies, often including virtual sandboxes that analyze the behavior of suspicious files and uncover hidden, previously unknown malware. However, threats are getting smarter, and many vendors' sandbox techniques simply have not kept up. This brief examines five areas where legacy sandboxing techniques fail, and explores what is needed for your enterprise to stay ahead of APTs.

Today's advanced threat detection technologies often only report on the presence and behavior of malware.

1. Infiltration before analysis

First, some sandboxing solutions do not come to an analysis verdict until a potentially dangerous file has already entered the network perimeter. This increases the possible vectors an executed malware file has to infiltrate throughout the network behind the perimeter.

2. Limited file analyses

Second, some gateway sandboxing solutions are limited in the size and type of files or operating environment they can analyze. They may only address threats targeted at a single computing environment. And yet enterprises today operate across multiple operating systems, including Windows, Android and Mac OSX.

Also, increased adoption of mobile and connected devices has broadened the attack surface that threats are targeting. In 2015, Dell SonicWALL saw a wide range of new offensive and defensive techniques that attempted to increase the strength of attacks against the Android ecosystem, which accounts for nearly 85 percent of all smartphones globally. 1 Today's advanced threat detection technologies often only analyze and detect threats targeted to legacy office productivity operating systems and applications. This can leave organizations vulnerable to attacks targeted at modern mobile and connected device environments.

In addition, they might not be able to process a broad range of standard business file types, including executable programs (PE), DLL, PDFs, MS Office documents, archives, JAR and APK files. These limitations can result in unknown zero-day threats being passed through to the network without analysis and identification.

3. Siloed sandbox engines

Third, standalone single-engine sandbox solutions are no longer adequate.

Malware is now being designed to detect the presence of a virtual sandbox and evade discovery, limiting the effectiveness of first generation sandbox technologies. Single-engine sandboxing solutions present a particularly easy target for evasion techniques.

What's more, single-engine techniques create analytical gaps. For instance, analysis looking at calls between applications and operating systems may be less granular than analysis looking at calls between hardware and operating systems, because many of those calls are hidden from application layers.

A more effective technique would be to integrate layers of multiple sandbox engines. And yet, today's sandboxing solutions are often siloed, single-engine, standalone appliances or cloud services. Deploying multiple sandboxing technologies, if even viable, would significantly increase configuration complexity, administrative overhead and costs.

4. Encrypted threats

For many years, financial institutions and other companies that deal with sensitive information have opted for the secure HTTPS protocol that encrypts information being shared. Now other sites like Google, Facebook and Twitter are adopting this practice as well in response to a growing demand for user privacy and security. Although there are many benefits to using more internet encryption, a less positive trend emerges as hackers exploit this encryption as a way of "hiding" malware from corporate firewalls.

Using Secure Sockets Layer (SSL) and Transport Layer Security (TLS) encryption (SSL/TLS), or HTTPS traffic, skilled attackers can cipher command and control communications and malicious code to evade intrusion prevention systems (IPS) and anti-malware inspection systems. These attacks can be extremely effective, simply because most companies do not have the right infrastructure to detect them. Legacy network security solutions typically either don't have the ability to inspect SSL/TLS-encrypted traffic, or their performance is so low that they become unusable when conducting the inspection.

5. Stymied remediation

In addition, today's advanced threat detection technologies often only report on the presence and behavior of malware. Even if the sandbox technique effectively identifies a newly evolved threat at a specific endpoint, organizations then have no clear way to remediate the threat. They do not have a simple, efficient way to have firewall signatures updated across a global distributed network.

Once malware is discovered, likely after a system is infected, remediation falls to the IT organization, leaving IT with the time-consuming task of tracking down and eradicating malware and associated damage from infected systems. Plus, IT also needs to quickly create and deploy new malware signatures across the organization to prevent additional attacks.

What is needed

While legacy sandboxes may be flawed, their underlying principle is sound. Still, these shortcomings need to be addressed for sandboxing to be effective. To do so, your sandboxing solution should:

- Apply cloud-based analysis to suspicious files to detect and block unknown threats outside the gateway until a verdict is determined
- Analyze a broad range of file types and operating environments, regardless of file size or encryption
- Rapidly and automatically update remediation signatures
- Integrate multiple sandbox engines to better resist evasion tactics, gain better visibility to malicious behavior and increase threat detection.
- Lower costs and complexity

Learn more.

Discover how multi-layer sandboxing detects more zero-day threats. Watch this on-demand webcast.

A more effective technique would be to integrate layers of multiple sandbox engines.

About Us

Over a 25 year history, SonicWall has been the industry's trusted security partner. From network security to access security to email security, SonicWall has continuously evolved its product portfolio, enabling organizations to innovate, accelerate and grow. With over a million security devices in almost 200 countries and territories worldwide, SonicWall enables its customers to confidently say yes to the future.

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