SONICWALL

EXECUTIVE BRIEF: STOPPING RANSOMWARE WITH ADVANCED THREAT DETECTION CAPABILITIES

Why you need to use static and dynamic defenses

Abstract

Threat detection platforms such as next-generation firewalls (NGFWs) and email security leverage signatures and heuristics with great success. But when defending against today's malicious attacks, they are no longer sufficient. The challenges of targeted attacks and zero-day threats make the addition of advanced threat detection critical to an effective security posture.

Understanding the real challenge – and what to do about it

The growth of external threats today is astounding. Attackers combine the opportunistic nature of automation with a software vendor's mindset to continually evolve their threats — all in an effort to have as broad a reach as possible, without detection. And given the negative impact incurred by any organization that suffers a data breach or ransomware attack, detecting malicious code before it has an impact within your network is imperative for IT organizations.

The real challenge isn't the ransomware that has already spread around the internet; it's targeted attacks and zero-day threats. Targeted attacks involve never-before-seen code purpose-built for the organization being attacked, while zero day threats exploit newly discovered vulnerabilities for which vendors have yet to issue patches. Organizations need to be most concerned with these types of attacks, which are usually far more successful than their older counterparts. So, what's the best way to prevent a threat from emanating from within your network?

You have a few choices in terms of where you choose to address malicious attacks and how you detect and eliminate them. The goal is to detect and remove malicious code as close to the source of the attack as possible. As far as where to address an attack, organizations typically fall into two camps: the endpoint security camp, in which malicious code makes its way to an endpoint and is then detected and destroyed, and the perimeter camp, in which malicious code is identified and destroyed at the

WAN edge before it enters the network. Until there's a 100% effective solution, both technologies will likely remain important layers of defense. Advanced threat detection platforms can provide a pre-emptive edge for both camps – if it's deployed in the right way.

> Today's malicious code is so advanced that detection requires a multifaceted approach. However, both signatures and heuristics have limitations.

Stopping malware at the edge

If you think of your network as a castle, there's no better place to stop an attack than at the gate — a choke point at which anyone and anything can be inspected before being allowed entry. By placing a solution that can detect malicious code just inside your next-generation firewall (NGFW) or email security service/appliance, you place a guard at the castle gate. Nothing gets in without the guard knowing about it. As data comes in, the traffic data is scanned, using several methods to detect malicious code:

- **Signatures/static protections**
  Using a database of malicious digital signatures, traffic is scanned to seek out any data that matches a signature. Should a match be found, the code or file is flagged as malicious.
- **Heuristics/dynamic protections**
  Unlike signatures, which look for specific matches within a database, heuristic-based scanning uses rules and algorithms to detect code that might have malicious intent.
- **Sandboxing**
  Rather than try to comb through code to find malicious signatures or intent, the sandbox allows the code to be detonated, or run as intended in an isolated environment, and monitors the behavior for malicious activity. This process is accomplished in a purpose-built environment, or sandbox, where no harm can be done.

Using this combination of tactics is more efficient and effective, since low hanging fruit can be caught by the faster, less resource-intensive traditional technologies. This allows the sandbox to concentrate on remaining content that actually requires its level of scrutiny.

In time when nearly 100% of your workforce can be a mobile workforce, you can think of advanced endpoint security as the primary line of defense against threats – a multi-use tool against almost everything an employee could face. Endpoint security has come a long way in the past number of years and by placing a heuristics-based advanced threat detection platform directly on the endpoint, you can allow many things in but convict them before they can execute and cause damage. As data, code, and files come in, several methods are used to protect the end user.

- **Pre-execution methods**
  By using a combination of dynamic allow and block listing and static protection (not signatures which slow down endpoints), the goal is to mitigate as many attacks as possible to avoid any remediation steps on behalf of IT.
- **On-execution methods**
  Dynamic behavior detection is used to detect attacks as they execute but not before they fully do. Processes are arrested and malicious files, code and scripts are quarantined and/or removed to mitigate damage or loss of data.
- **Sandboxing**
  Many threats on endpoints can lay dormant awaiting execution via a timer or command. By leveraging an advanced threat detection platform with your endpoint protection solution, organizations can test suspicious artifacts that can't be fully convicted by endpoint security. Sandboxes have more freedom to manipulate code, scripts, and files that endpoints are not allowed to do such as fast forward through time.

This combination of methods helps IT administrators mitigate a lot of the remediation work that falls on them when an attack causes a system change, damage, or a loss of data. All advanced threat protection platforms need to have a post-execution set of methods to remediate problems, but the goal is to never use them which is why sandboxing is vital to that goal.

Why signatures and heuristics alone aren't good enough

Signature-based detection is only as good as the database that it uses to identify malicious code. Even if your database isn't updated to the minute, you might miss an attack because it takes time for AV vendors to identify malware, update their database and distribute it to you. In addition, those who write malicious code are aware of signature-based detection and frequently check to see if their code is listed on public feeds like VirusTotal before making updates.

Heuristics can also be inaccurate. In order for a malicious script or batch of code to be convicted, it has to do something malicious. This is also why many Advanced Endpoint Protection (AEP) platforms perform worse in third-party testing when test malware is involved. Today, many forms of malware execute over several processes to masquerade as benign traffic.

Take ransomware, for example. The initially downloaded code isn't harmful. The code becomes weaponized when it connects to a command and control (C2) server and downloads additional code. Another example is a macro within a Microsoft Word document. Unless the malicious macro uses a suspicious or known attack method, neither signatures nor heuristics can tell whether the macro itself is good or bad.

Using signatures or heuristics to do a passive scan of traffic has its limitations. Scanning doesn't allow the code an opportunity to become active, and attackers are skilled at obfuscating their bad code (from a scanning perspective) within "good" code. Therefore, the most effective way to detect malicious code is to interact with a completely weaponized version.

Playing with fire

The only way to catch advanced malicious code is to "detonate" it.

The detonation process is much different from simply scanning code. It is similar to culturing a dangerous microbe in a biohazard containment lab or blowing up a bomb in a containment chamber. An advanced threat analysis platform provides a safe place to let intercepted data open and run its course under observation. Should suspicious or malicious behavior be confirmed, the file and the threat it contains can both be eliminated.

Advanced threat analysis platforms like sandboxes attempt to detonate every kind of file:

- **Active content files**
  These files include executables, scripts and DLLs. The files are allowed to run and interact with the sandbox as normal, to monitor them for malicious actions such as modifying OS firewall settings or establishing outbound connections across the Internet.

- **Passive content files**
  These files include any kind of document, PDFs, compressed files (e.g., ZIP, JZIP, RAR) and even image files. These files are parsed using their default application to monitor for malicious activity, such as a Word macro attempting to download additional code from across the internet. Without having every piece of software available in a sandbox, it's impossible to parse every passive file. In the end, your advanced threat analysis platform should be configured with the ability to inspect as many file types as possible.

Malware in an image

You might wonder why image files should be scrutinized, as they represent one of the most seemingly benign data types. But image files can contain malicious payload data. Take the example of a recent attack in Brazil, in which a PDF attachment contained a link to a ZIP file. Within that ZIP file was an executable and a portable network graphics (PNG) file. The PNG was small (less than 64 pixels square) but had a file size of over 1MB. Upon inspection of the adjacent executable, it became evident that the code was designed to extract and run a hidden malicious binary from within the PNG.

Improving signatures with your advanced threat analysis platform

As previously mentioned, a multifaceted approach is the best way to detect malicious code. Improving either passive scanning method can help make the detection process more efficient, as it takes far fewer CPU cycles to check against a signature database than it does to generate and sustain a sandbox capable of detonating a single instance of malicious code.

In addition to detonation, sandboxing can be used to create security definitions when code is determined to be malicious — after all, it has a front row seat to the malicious code running. When malicious code is identified, a signature is created and a signature database can be updated, improving the speed and accuracy of future malicious code detection.

Still, passive scanning techniques have their shortfalls around detection. So it's fair to ask whether or not a sandbox is more successful.

Memory-based attacks

Many payloads try to execute within the memory of a system in order to bypass static and dynamic detection systems and mitigate forensic detection. You advanced threat detection platform must be able to analyze malware with memory-based inspection to hunt for threats, namely those that use processor-based vulnerabilities.

How a sandbox works

The sandbox acts as a "sacrificial lamb" environment, monitoring malicious code and its interaction with the OS. Sandboxes look for the following:

- OS calls: Including monitoring system calls and API functions
- File system changes: Any kind of action, including creating, modifying, deleting and encrypting files
- Network changes: Any kind of abnormal establishment of outbound connections

- Registry changes: Any modifications to establish persistence or changes to security or network settings
- Beyond and between: Monitoring of instructions that a program executes between OS calls, to supplement context of other observations
- Fileless malware: malware wants to run within memory to avoid detection and forensic analysis

How effective is an advanced threat analysis platform like a sandbox?

Signature-based detection is perfect for discovering yesterday's malicious code but does nothing to stop zero-day attacks or attacks that are simply mutated or polymorphic (i.e., specific malware that does not match a signature because of mutation). Heuristics take detection a step in the right direction, looking for abnormal patterns in code. But as demonstrated in the use of an image file to deliver a payload, the initial files (e.g., a PDF with a link to an external ZIP file) don't raise any red flags.

This issue is why the sandbox is such an effective detection method. Even with zero-day attacks that have no signature and code that has never been seen before, sandboxing is the only method that detects malicious behavior. At the end of the day, malicious code takes a limited number of actions, including making an external connection, downloading additional payloads, connecting to a C2 server, and attempting to make OS changes. None of these actions are necessarily normal for work-related files.

Conclusion

There are several ways to protect your organization against malicious code. While protecting the endpoint is important, it can put an organization at an even greater risk by allowing malicious code into the network. Sandboxing provides a means to stop threats before they enter the network.

Learn more. Discover key differentiators to consider in your sandbox strategy. Read our solution brief, "Putting a solid sandbox strategy in place."

The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON- INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

About Us

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com.

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

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

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