Trellix

SOLUTION BRIEF

Intelligent server defense

Counter advanced attacks with both network and endpoint security

Overview

Employees operate in a world where mobile devices constantly interact with servers in data centers and in the cloud, and share sensitive data. As remote work becomes the norm, business is more often conducted outside the office. This can leave an open attack path to your organization's crown jewels: data, customer information, and intellectual property stored on your servers.

Servers often run web-facing applications that provide direct attack surfaces from both the internet and within the managing organization. Threat actors can attack the server directly with an outside-in attack that scans the server and determines what OS, web services, and applications are running. They can then use this information to identify vulnerabilities or exploits for compromise.

The cybersecurity industry offers many solutions to protect client endpoints and the network itself, but servers—both Linux and Windows—have different attack surfaces, vulnerabilities, and patterns than client endpoints. Adversaries stay hidden on the servers. In fact, the median time before attackers are discovered is 24 days. This gives adversaries time to perform reconnaissance, escalate privileges, steal your organization's most sensitive data, and cover their tracks.

Key benefits

- Address attacks targeted to a server's unique attack surfaces, vulnerabilities, and patterns
- Detect malicious traffic moving laterally between clients and network devices communicating over SMB
- Reduce time to detect and resolve server attacks from weeks to hours
- Detect attacks others miss with advanced Trellix threat intelligence

How adversaries approach servers

The attack on a server is often quite different than a client endpoint. An adversary's goal is to stay resident on the system and collect network reconnaissance data, personally identifiable information, or financial transaction information.

The longer an adversary can stay hidden, the more value they'll gain. Basic attacks such as malware or worms are easily defeated, so modern attackers use web shells as a remote access trojan; a few simple lines of code installed on the web server provide backdoor access or access to the server file system.

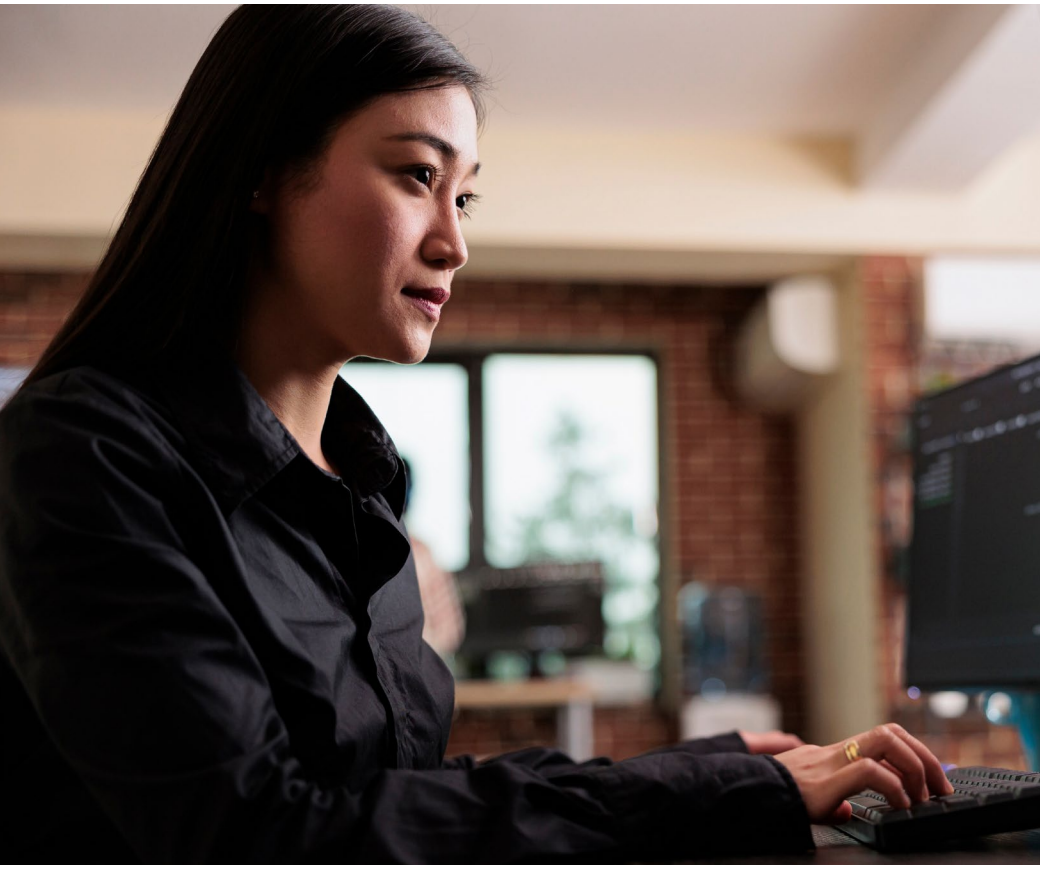
These few lines of code look similar to code that exists on the server, and unless the web shell is active, it's not easy to detect. Using web shells, adversaries can modify web servers to redirect search engine requests to a compromised web page. Or they can present content to the search engine that's different from what the user sees. Locating a web shell usually requires a user-agent change of the crawler bot.

How server attacks are detected

Automated tools to detect a web shell attack offer only limited means of detection. Administrators must use indicators to find a web shell attack, such as:

- Abnormally high web server usage (due to heavy downloading and uploading by the attacker)
- Files with an abnormal timestamp (for example, newer than the last modification date)
- Unknown files on the server
- Files with dubious references, such as cmd.exe or evals
- Unknown connections in web server logs

Analyzing web server logs can determine the location of the web shell, but the process is time consuming because every suspect log must be reviewed. And during the process, the attack continues.



Traditional security tools are ineffective against modern server attacks. Firewalls and intrusion detection systems typically rely on signatures, which web shells can easily bypass. Secure web gateways and other products may look at content, but web shells can easily fool these scanners because they are legitimate code.

Your organization requires a solution that can emulate a system completely, interact with code, look for indicators, and only then determine whether code is malicious.

The Trellix solution

Trellix Network Security and Trellix Endpoint Security detect web shell traffic, determine whether a server has been infected, and enable investigation to respond to the attack.

Trellix Network Security

For network traffic, customers can enable SmartVision mode in the Network Security solution to detect malicious traffic moving between clients and network devices communicating over Server Message Block (SMB). Trellix can detect web shell traffic, determine what the web shell is doing, when it is active, and what devices are being used. Incident responders can use this information to determine if an attack is in progress and how to begin an investigation.

Trellix Endpoint Security

Endpoint Security uses multiple specialized engines to help protect, detect, and respond to an attack on clients using Windows, macOS, and Linux. It also provides incident responders with real-time detection and investigation capabilities for Windows and Linux servers.

With these two solutions, an investigator can use Network Security to determine when a web shell is being used as part of an attack involving servers, and to identify affected servers. The investigator can use Endpoint Security to perform a deep dive investigation on those servers, and determine which web pages or applications have been compromised with the web shell. They can then isolate those web pages or applications, remediate the environment, and resume normal operations.

After they determine how the attack occurred, your security team can prevent further infection by resolving vulnerabilities or patching infected systems. Similar proactive fixes can be applied across uninfected servers as a preventative measure.

Better together

With this combined solution, Trellix cuts the time to detect and resolve attacks from weeks to hours. Dealing with infected files or applications drops from days to minutes. Trellix provides your organization with an end-to-end detection and investigation lifecycle for deep data center attacks that no other vendor can match.

To learn more about Trellix, visit trellix.com.

Trellix
6220 American Center Drive
San Jose, CA 95002
www.trellix.com