STOP TARGETED ATTACKS WITHOUT DECRYPTING TRAFFIC

Executive Summary

Threat actors are crafty. They use a variety of techniques to conceal their attacks and evade detection. With HTTPS traffic now accounting for over two-thirds of all web traffic,[1] encryption has become their method of choice to bypass corporate defenses. Encryption is just one of many evasive tactics attackers have up their collective sleeves; they also encode traffic contents, compress and pack files, and employ many other techniques to slip past security controls.

Magnifier™ behavioral analytics, a cloud-based app for Palo Alto Networks® Application Framework, empowers organizations to detect and stop active attacks. Magnifier profiles user and device behavior by analyzing network metadata to uncover the telltale signs of intrusions. However, it does not need to inspect traffic content, so it's impervious to encryption and obfuscation techniques.

This paper describes how Magnifier detects in-progress attacks and how it works in concert with Palo Alto Networks Security Operating Platform to eradicate threats in encrypted traffic.

[1] Let's Encrypt with Firefox telemetry, https://letsencrypt.org/stats

The Rise of SSL Encryption

Use of Secure Sockets Layer, or SSL, encryption[2] has exploded over the past decade, growing from approximately 26 percent of all internet traffic in January 2014 to 69 percent in February 2018.[3] Heightened concerns over privacy and industry incentives to adopt encryption have motivated application owners of all sizes to encrypt website access. Additionally, the rapid proliferation of free and low-cost SSL certificates has brought encryption within reach of virtually all web developers.

Although SSL adoption boosts privacy and security, it also allows threat actors to conceal their malicious activity in encrypted traffic. To protect corporate assets, organizations need a robust way to detect and block threats hidden in SSL communications.

Palo Alto Networks Approach to Securing Encrypted Traffic

To ensure no attack remains undetected, Palo Alto Networks has developed multiple technologies to inspect and secure all communications, including encrypted traffic. These technologies include:

Behavioral Analytics

Once attackers have infiltrated a network, they must perform a series of steps to find and steal or destroy data. Magnifier behavioral analytics monitors network activity to profile behavior and detect anomalies indicative of intrusions.

Since Magnifier analyzes network metadata rather than the actual content, it can detect advanced attacks without requiring decryption.

High-Performance SSL Decryption

To inspect every packet, next-generation firewalls can decrypt HTTPS traffic at high speeds. Supporting flexible deployment options, next-generation firewalls can decrypt outbound or inbound SSL traffic or act as SSL decryption brokers.

Using next-generation firewalls, organizations can selectively decrypt traffic by application, category or user.

Advanced Endpoint Protection

Attacks hidden in HTTPS traffic ultimately target endpoints and their data.

Traps™ advanced endpoint protection uses multiple methods of prevention to stop exploits and malware before they can compromise corporate machines. It integrates with cloud and network security for threat analysis, shared intelligence and automated containment.

Palo Alto Networks Security Operating Platform provides ironclad protection against cyberattacks while eliminating blind spots encrypted traffic can introduce.

Detecting Internal Threats Without Decrypting Traffic

When attackers have gained access to a victim's network, they can use any number of evasive techniques to elude security controls. Instead of relying on malware, they can leverage common utilities, such as PowerShell® or native system tools, to explore a compromised network and transfer data. Attackers can steal credentials and move from endpoint to endpoint without necessarily violating security policies or setting off internal alarms.

However, attackers will inevitably betray themselves as they perform reconnaissance and expand their footprint in the network because their actions will deviate from past behavior and the behavior of other users or devices in the network. As they attempt to explore the network and control other devices, they will access new destinations, use new protocols, log in to systems with unusual user accounts, and exhibit other changes in behavior that reveal their malicious intent.

Magnifier behavioral analytics, a cloud-based app for Palo Alto Networks Application Framework, automatically detects behavioral anomalies indicative of active attacks. Magnifier examines rich network, endpoint and cloud data stored in Palo Alto Networks Logging Service to identify targeted attacks, malicious insiders and compromised endpoints with unparalleled accuracy (see Figure 1). It also streamlines investigations by providing a small number of actionable alerts with the context that security analysts need to confirm and respond to attacks.

[2] References in this paper to SSL encryption also apply to Transport Layer Security, or TLS, the successor to SSL.
[3] Let's Encrypt with Firefox telemetry, https://letsencrypt.org/stats/

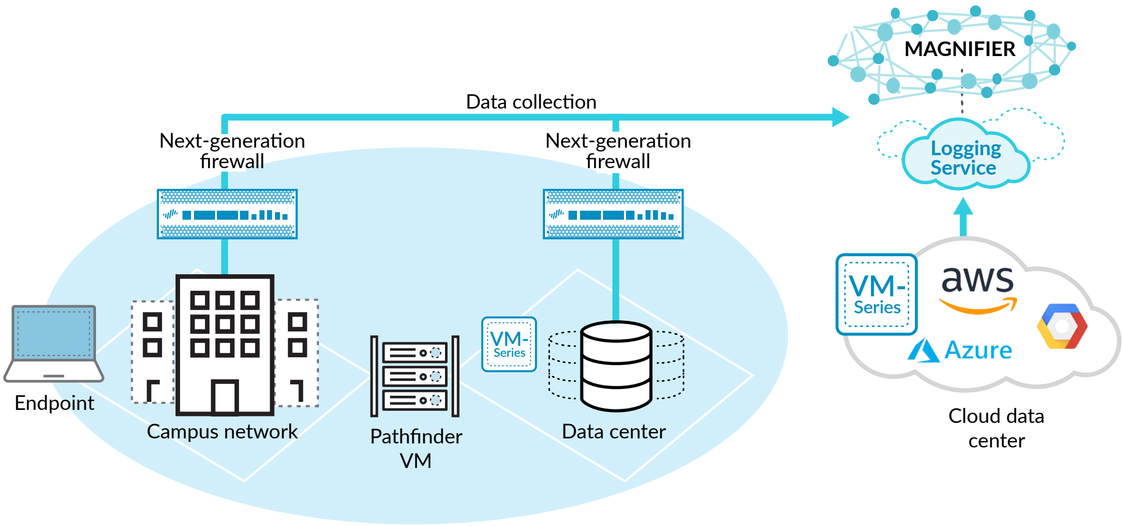


Figure 1: Magnifier analyzes data stored in Palo Alto Networks Logging Service from the Security Operating Platform to profile behavior and detect attacks

Evasion-Resistant Design

Rather than looking for attack signatures, Magnifier profiles user and device behavior to detect anomalies indicative of an attack. Its robust attack detection is based not on the content transferred but on the attributes of the communication, including which user and host initiated a connection, what destination they accessed, and what protocol they used.

Because Magnifier is not designed to detect predefined network patterns, such as the behavior of specific malware families, attackers cannot easily evade Magnifier's detection algorithms by changing packet lengths or exploit code. By dynamically learning the behavior of users and devices in the network, Magnifier detects changes in behavior that attackers cannot conceal. For example, if an attacker moves laterally from one host to the other, the attacker cannot avoid the communication between the machines.

By profiling many different dimensions of behavior, Magnifier can detect irregularities, such as a standard user connecting to multiple rarely accessed systems or attempting to manage remote computers, that suggest an attack is underway.

Magnifier detects network-based attack behaviors that are impossible to hide, even in encrypted traffic.

Because Magnifier analyzes network metadata and not transferred content or payloads, it can uncover network threats even in environments where traffic is encrypted.

Detect Every Stage of an In-Progress Attack With Behavioral Analytics

Once threat actors have infiltrated a network, they can take advantage of their existing access to explore their surroundings and expand their realm of control until they achieve their ultimate objective: stealing, manipulating or destroying sensitive data.

Magnifier detects every step threat actors take once they have gained a foothold in the network:

Lateral movement: To find sensitive data and maintain a persistent presence in the network, attackers steal credentials, conduct reconnaissance and take control of multiple endpoints. Magnifier monitors network traffic to model expected behavior and detect deviations suggestive of attacks. Magnifier profiles user and device behavior by analyzing protocol-level metadata collected by Palo Alto Networks next-generation firewalls.

By analyzing network data gathered from next-generation firewalls, including enhanced application logs and traffic logs with data from User-ID™ and App-ID™ technology, Magnifier can detect lateral movement and reconnaissance that attackers cannot avoid or hide.

Command-and-control activity: Magnifier recognizes the network behavior associated with command and control, or C2, such as repeated connections to rarely accessed sites or many failed DNS lookups. As a result, Magnifier can detect attacks without inspecting the transferred content.

Additionally, because Palo Alto Networks next-generation firewalls can extract Server Name Indication and other pertinent data from encrypted traffic and present this data in enhanced application logs, Magnifier can detect C2 traffic even when connections to C2 servers are encrypted.

Data exfiltration: After attackers have obtained sensitive data, they need to transfer it out of the network. Magnifier examines outbound connections and detects large uploads to rarely accessed sites or those using uncommon protocols.

Since Magnifier focuses on the amount of data sent, the port number, the destination popularity and other attributes of the destination site, Magnifier can detect exfiltration even when the uploaded traffic is encrypted or the contents are obfuscated.

Compromised endpoints: Using Pathfinder endpoint analysis service, Magnifier can uncover malware running on endpoints.

Because Pathfinder directly scans endpoints for running processes and then examines them with WildFire® cloud-based threat analysis service, it is not affected by network-level encryption.

How Magnifier Profiles Behavior When Traffic Is Encrypted

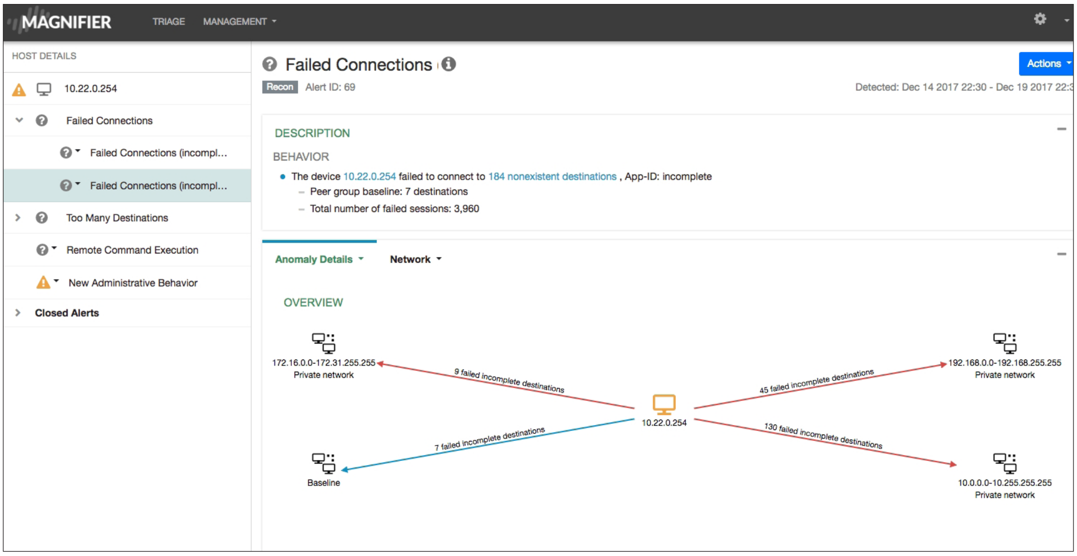
Magnifier detects attacks even when threat actors try to use encryption or obfuscation to evade detection. Application-level encryption does not affect the accuracy of Magnifier's attack detection algorithms for the reasons that follow.

Analyzes Network-Level Information

Magnifier primarily analyzes network-level information, such as traffic source, destination, domain, protocol, port number and volume, which it can obtain from packet headers even when application-level content is encrypted. For example, if an attacker attempts to map out the network to find servers with valuable data, the attacker cannot avoid abnormal network connections.

Magnifier analyzes data collected by next-generation firewalls to track the normal behavior of users and devices, including the systems they access, the protocols they use, the amount of traffic they send and receive, and many other dimensions of behavior. If Magnifier detects unusual activity – such as requests to many different ports on a host, including ports that are anomalous for the individual user and the user's peers – it will generate an alert. Magnifier can detect attacks without inspecting application contents, so it is not affected by application-level encryption (see Figure 2).

Figure 2: Magnifier detects network port scans even if individual requests are encrypted



Failed Connections

Alert ID: 69

Detected: Dec 14 2017 22:30 - Dec 19 2017 22:3

DESCRIPTION

BEHAVIOR

- The device 10.22.0.254 failed to connect to 184 nonexistent destinations , App-ID: incomplete
  - Peer group baseline: 7 destinations
  - Total number of failed sessions: 3,960

Streamlines Threat-Hunting Efforts

Magnifier has been designed from the ground up to streamline threat-hunting efforts. To that end, it generates a small number of accurate, actionable alerts with user, endpoint and application context. Although encryption does not impact Magnifier's detection capabilities, encryption can, in some cases, affect the amount of detail recorded in alerts. When traffic is encrypted, Magnifier alerts will still include information about the device, user, port number, and endpoint process or executable file associated with the attack, as well as information about the domain. However, alerts may not list the URL, browser agent or referrer for HTTPS-based attacks. In such instances, Magnifier will still detect attacks, but will not provide the detailed application data it usually presents in alerts.

Presents Full Application Details in Alerts

Magnifier presents full application details in alerts when organizations have configured their next-generation firewalls to decrypt HTTPS traffic. With proper configuration, firewalls will log full network metadata – including web browser agents, referrers and file names – in alerts to streamline investigations. By configuring their firewalls to decrypt traffic, organizations can also take advantage of their firewalls' application, user and content-based policies and threat prevention capabilities to block unauthorized access, exploits and malware.

When an attacker is inside a network, the targeted organization has the home-field advantage. Its IT and cybersecurity teams control the devices, applications and user rights; they can monitor network activity to detect anomalous behavior. Magnifier provides unprecedented visibility into this internal network traffic and enables organizations to uncover internal threats, even when traffic is encrypted.

Network Data Inspected by Magnifier

Magnifier analyzes protocol-level metadata in traffic logs, enhanced application logs and threat logs collected by Palo Alto Networks next-generation firewalls. It does not need to inspect the transferred contents or payloads. By building a profile based on more than 1,000 behavioral dimensions, including frequency of connections, source and destination of traffic, protocols used and more, Magnifier can learn the expected behavior of users and devices. Magnifier also monitors internal traffic as well as outbound traffic from clients and servers to the internet.

Session-Level Data

Palo Alto Networks next-generation firewalls extract the metadata needed to profile user and device behavior, including:

- Source IP, destination IP, source port, destination port
- Bytes sent and received
- Connection duration
- Enhanced application logs with transaction-level data on DNS, HTTP, DHCP, RPC, ARP, ICMP and more
- Application details from App-ID

User Data

Magnifier analyzes network traffic and endpoint data and extracts user context, such as:

- Logged-in user
- Typical user of a machine
- User creating the process that initiated the communication

Host Data

Magnifier identifies machines by tracking:

- Hostname
- MAC address

Find Attacks in Encrypted Traffic With Palo Alto Networks

Threat actors can develop never-before-seen techniques to trick users and compromise endpoints. With the rapid adoption of SSL encryption, they can hide their attacks in HTTPS traffic to bypass security controls. Once they have infiltrated a network, however, they must perform a step-by-step process of reconnaissance and lateral movement to gain access to valuable resources.

Palo Alto Networks provides powerful defenses against cyberattacks, especially those lurking in encrypted traffic. Palo Alto Networks next-generation firewalls can decrypt traffic to inspect and block network attacks. Traps advanced endpoint protection shields the ultimate targets of attacks, including laptops, personal computers, servers and IoT devices, from sophisticated threats.

Human adversaries, such as external attackers or malicious insiders, operating inside the network can often avoid the use of traditional exploits to stay under the radar. By profiling user and device behavior, organizations can detect changes in behavior that reveal active attacks. Magnifier focuses on network metadata, not application contents, allowing it to profile user and device behavior even when traffic is encrypted. By monitoring internal activity for anomalous behavior, Magnifier can automatically detect attacks and empower organizations to prevent costly data breaches.

paloalto NETWORKS®

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com