WildFire

WildFire™ automatically protects your networks from new and customized malware across a wide range of applications, including malware hidden within SSL-encrypted traffic. WildFire easily extends the threat prevention capabilities of the next-generation firewall to tackle some of the most challenging threats in the world today, and does so with full visibility and enforcement at up to 10Gbps.

- Proactively executes suspicious files in a safe environment to identify malware based on more than 100 malicious behaviors.
- Combines the visibility of the next-generation firewall with cloud-based analysis to ensure accurate, safe and scalable malware analysis.
- True in-line blocking of malware infecting files and command-and=control traffic at the firewall.

Modern malware has changed the way networks are attacked, and enabled criminals to target and steal an enterprise's most valuable assets. By evolving new techniques to avoid traditional antivirus controls, this new breed of malware provides attackers with a method for infecting a target and patiently attacking a network from the inside without detection. As a result, finding and controlling new and unknown malware has quickly become one of the most important requirements for enterprise network security teams. To meet this challenge, Palo Alto Networks™ has developed WildFire, which easily and efficiently extends the power of the next-generation firewall to automatically detect and stop threats from new, evolving or targeted malware.

Unlike traditional antivirus solutions that look to match known malware, WildFire captures unknown files entering the network and proactively executes them in a safe cloud-based environment where any and all malicious actions and network activity are observed and recorded. Using active analysis, Palo Alto Networks proactively identifies malicious files within minutes based on their actual behavior to conclusively identify new or customized malware that may be unknown to the industry. When new malware is detected, WildFire automatically generates and delivers protections to all WildFire subscribers within an hour of the initial detection. This allows enterprises to not only find unknown or custom malware, but also stop new malware outbreaks before they spread. And as with all Palo Alto Networks analysis, this threat prevention is performed on all traffic, across all ports at up to 10 Gbps.

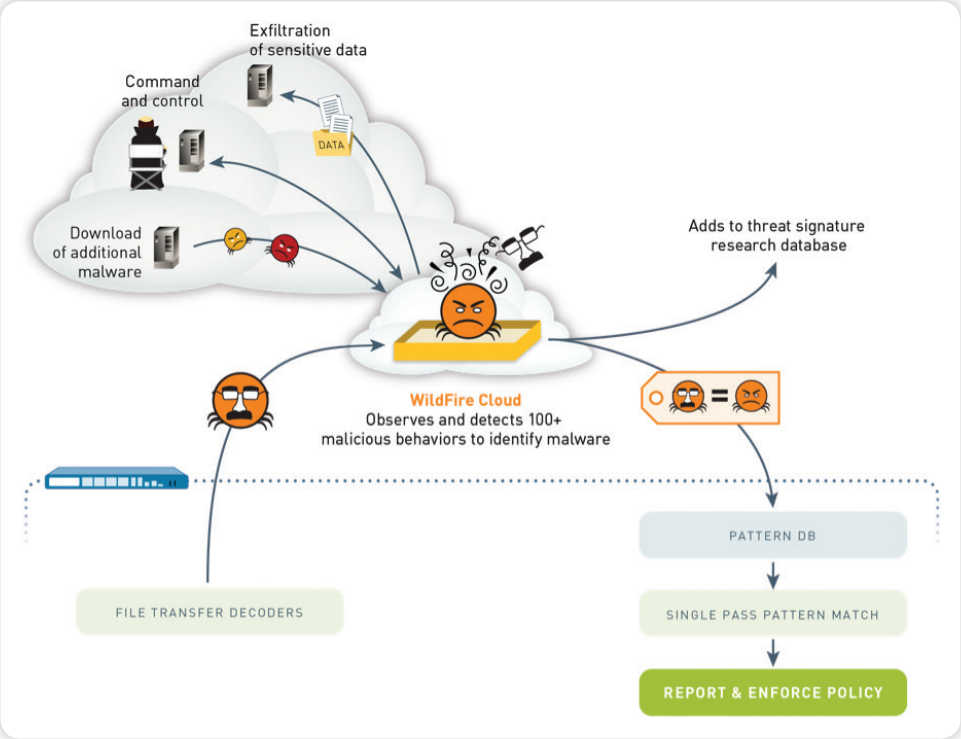
Preparing for Modern Network Attacks

As attacks have grown more sophisticated, the attack strategy has grown more patient, and developed a focus on stealth and evading security measures. Malware is increasingly the key to executing on these sophisticated attacks. Malware is easily modified or customized in order to avoid known antivirus signatures, and once the malware is delivered, it can act as an ongoing control point for the attacker inside the target network. This has made malware not only a very serious threat in its own right, but also a critical enabler of long-term network attacks or so-called advanced persistent threats (APTs).

This evolution demands that security teams adapt their network security models to integrate anti-malware techniques into the network security layer, and most importantly expect and prepare for malware that will not be identified by a pre-existing signature. With Palo Alto Networks WildFire, security teams can take this critical step and extend their existing integrated approach to threat prevention to include the behavioral analysis, detection and prevention of modern malware.

paloalto NETWORKS

the network security company™



How WildFire Works

WildFire provides a logical combination of next-generation firewall hardware and cloud-based malware analysis. WildFire takes advantage of the unique visibility, enforcement and performance advantages of the next-generation firewall appliances, and likewise uses the scale and power of the cloud to safely test malware in virtualized environments, and deliver coordinated protections to all firewalls worldwide.

Next-Generation Visibility and Performance

As with all Palo Alto Networks threat prevention, the process begins with the full visibility provided by the next-generation firewall. All traffic is inspected across all ports to identify potentially malicious files hidden in traffic. When a file is detected, WildFire automatically checks the hash value of the file to determine if the file has previously been analyzed. If the file is unknown, it is securely copied and uploaded from the firewall to Palo Alto Networks cloud-based environment. This upload process is protected at all times by encryption signed by Palo Alto Networks certificates on both ends of the connection. Customers with the additional WildFire license also gain access to WildFire API for programmatic submission of up to 100 samples per day and up to 1,000 report queries by file hash per day.

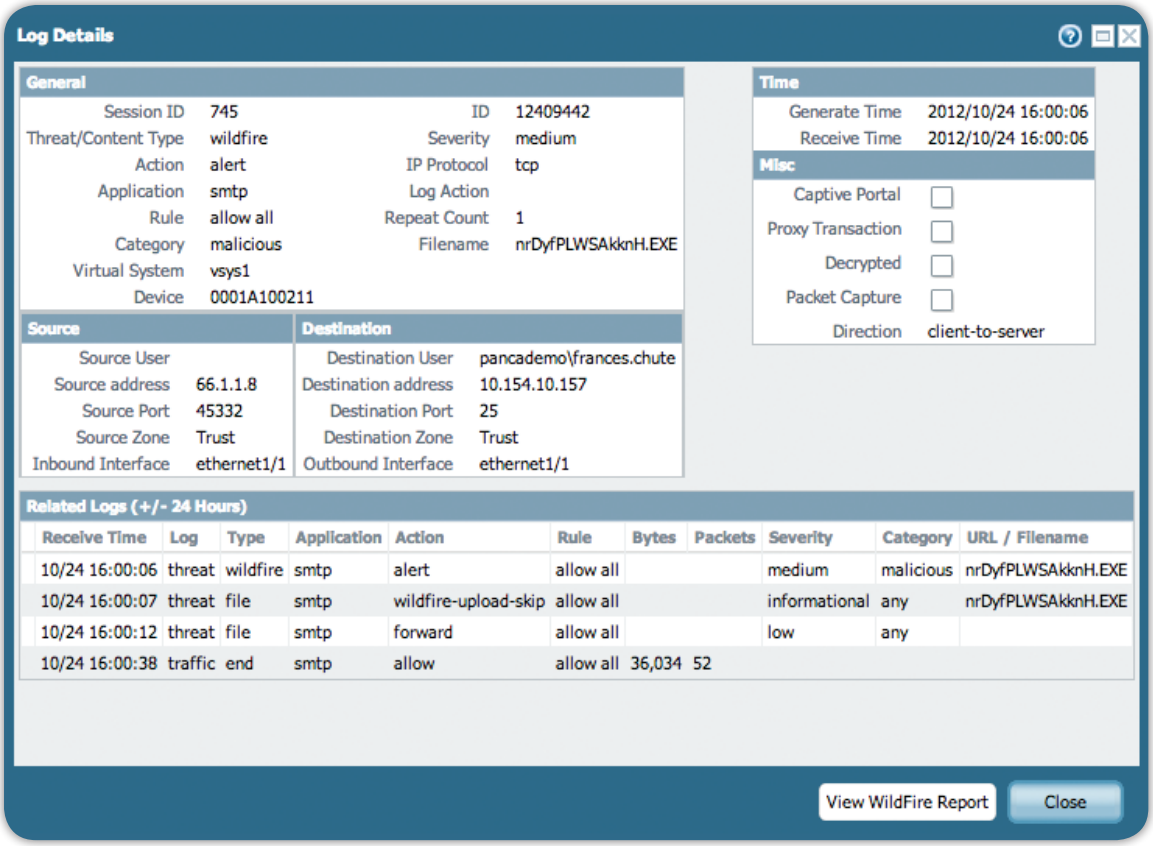
Turning the Power of the Cloud Against Malware

Once in the cloud, the file is executed in a virtualized computing environment, where all behaviors can be observed. WildFire monitors for more than 100 malicious behaviors to identify the true nature of malicious files based on their actions as opposed to a pre-existing signature. WildFire observes all process and hooking behaviors, changes made to registries, auto-run modifications, changes to security settings and any files that are created or modified. Likewise, WildFire looks for suspicious or malicious network behaviors such as establishing backdoors, downloading additional executables, visiting dynamic DNS domains, scanning for vulnerabilities and much more. By performing this analysis in the cloud, WildFire can scale to analyze any volume of malware while providing malware with unfettered access to the Internet to ensure all command-and-control behavior is observed.

Automated Prevention

Once a file is determined to be malicious, WildFire automatically develops protections for the new threat. WildFire subscribers are immediately notified of the verdict of the analysis via integrated WildFire logs in the Palo Alto Networks user interface, and also by email notification based on policy. The WildFire cloud includes an automated signature engine that generates true malware signatures for the infecting file, which are delivered to all subscribed firewalls worldwide within 1 hour of the malware first being discovered. Signatures are true malware signatures and are enforced using the stream-based malware engine to ensure that security teams can provide true in-line enforcement while maintaining high throughput and network performance.

In addition to creating protections for the infecting file, WildFire also builds additional network-based detections. WildFire observes DNS behavior of the malware as well as any URLs that the malware uses, which are automatically added to Palo Alto Networks DNS-based malware signatures and PAN-DB URL filtering categorization. The Palo Alto Networks Threat Research Team also builds command-and-control signatures for the malware, which augment the IPS and spyware signatures available in the Threat Prevention license.



Integrated WildFire Logs

Malware Forensics and Event Analysis

Integrated Logging and Reporting

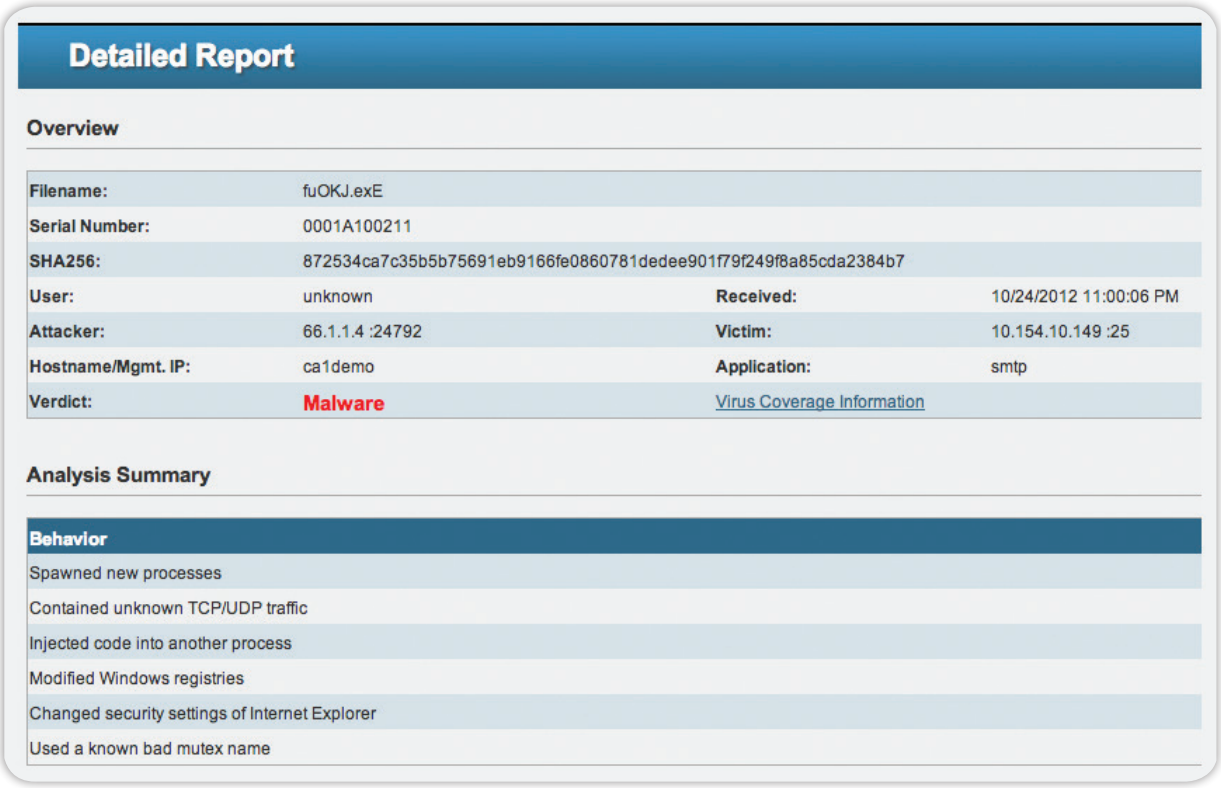
WildFire subscribers receive integrated WildFire logs on their firewalls, enabling teams to correlate WildFire events with other important events observed by the firewall. This ensures that staff can quickly and seamlessly tie applications, URLs, files, known threats and unknown threats into a coordinated approach to threat prevention. Additionally, Palo Alto Networks provides pre-built reports for WildFire events to provide ongoing documentation of emerging threats.

WildFire Portal

When dealing with new and emerging threats, it's important that security teams be able to quickly and easily investigate malware in order to correlate an infection with other security events or simply to aid in the cleanup in the case of an infection.

The WildFire Portal provides detailed analysis and forensics for every file analyzed by WildFire. Staff can track the overall rates of malware detected, and can drill down into detailed analysis on any given file. Staff can easily see the verdict of a file, the application, IP address and/or URL that delivered the file as well as the user that was targeted.

The analysis then provides granular details of the malware including all observed malicious behaviors, a list of any and all domains the malware visited, registry keys added or modified as well as any files created or modified. This analysis provides the context to know exactly how the malware attempted to enter the network, how it tries to communicate back out of the network and actions it performed on the target host. This information can provide teams with details to establish host-based indicators for infected machines, as well as providing the real-world data needed to adapt security policies to changing attack strategies. This data also helps security teams to teach and train network users by showing the names, locations and applications that have been used against them in phishing or social engineering attempts.



Detailed Report

Overview

Filename:	fuOKJ.exE		
Serial Number:	0001A100211		
SHA256:	872534ca7c35b5b75691eb9166fe0860781dedee901f79f249f8a85cda2384b7		
User:	unknown	**Received:**	10/24/2012 11:00:06 PM
Attacker:	66.1.1.4 :24792	**Victim:**	10.154.10.149 :25
Hostname/Mgmt. IP:	ca1demo	**Application:**	smtp
Verdict:	**Malware**	Virus Coverage Information	

Analysis Summary

Behavior
Spawned new processes
Contained unknown TCP/UDP traffic
Injected code into another process
Modified Windows registries
Changed security settings of Internet Explorer
Used a known bad mutex name

Analysis from the WildFire Portal

The Importance of Cloud-Based Analysis

The rapid pace of malware evolution has increasingly made the cloud the most logical place to perform malware behavioral analysis and sandboxing. The cloud provides safe, scalable environment for malware testing and offers the flexibility to keep pace with the daily changes in the fight between malware creators and security teams.

Active malware analysis depends heavily on virtualization, with each malware sample being executed in a fully independent virtual environment. This means that large numbers of virtual machines are required in order to keep pace with the growing demands of analyzing new malware and suspicious files. By moving analysis to the cloud, WildFire can elastically scale computing resources as needed instead of being limited by the capacity of on-premise customer hardware. This architecture ensures that malware analysis is always available and removes the need to constantly add additional hardware as the rate and sophistication of modern malware continues to accelerate.

However, even beyond the simple need to scale, the cloud provides important functional advantages when performing malware analysis. By using the cloud, WildFire provides malware with full, unfettered access to the Internet ensuring that the malware can perform all actions without interruption, and thus ensure an accurate diagnosis. This is an important distinction given that a great deal of malware will perform a variety of checks to ensure that it has access to the real Internet prior to launching any malicious behaviors.

Secondly, malware authors and security vendors are in a daily battle to detect one another's techniques and respond. By performing malware analysis in the cloud, Palo Alto Networks researchers can make updates to WildFire logic or techniques at any time without impacting customers in any way. For example, if Palo Alto Networks researchers observe malware using a new method of detecting a virtual machine or hooking a process, they can easily update WildFire's logic to adapt. Since this logic is removed from the customer's local hardware, the benefits are instantaneous and require no actions at all on the customer's side.

Maintaining the Privacy of Your Files

As with any use the cloud, an enterprise must ensure that the cloud is used safely and without exposing enterprise data. WildFire is no exception, and provides customers with full control over what data is shared with WildFire and the additional protection of multiple layers of professionally managed security to ensure data is never exposed.

Security teams can set policies to determine exactly which files should be sent to the WildFire cloud. Teams may want to analyze all unknown files or simply those files coming from the Internet or other untrusted zones. In addition to control over which files are sent for analysis, policies can be set to control what relevant session information should be included with the sample for analysis. Session information refers to the context of the network session responsible for delivering the unknown file such as the application, the target user, the port number, the source IP address, AND. This data is often particularly useful for correlation purposes if a file is found to be malicious, but is not required for WildFire to determine the status of the file.

When a file is sent for analysis, the firewall establishes a secure connection between the local firewall and Palo Alto Networks WildFire cloud. This connection is secured on both ends by client certificates signed by Palo Alto Networks ensuring that data remains secure in transit and preventing the possibility of a man-in-the-middle attack. Once delivered to the WildFire cloud, the file is protected behind multiple layers of professionally managed security. Files are only allowed inbound to the WildFire cloud to ensure that benign files never leave the WildFire environment. Following analysis, benign files are destroyed and only the hash value retained in order to prevent future re-analysis.

Requirements:
PAN-OS version 5.0 or higher.

Licensing Information:
Basic WildFire functionality is available to all Palo Alto Networks customers at no charge. These users can automatically submit suspicious files to WildFire and protections are delivered with regular threat prevention content updates (threat prevention license is required). An additional WildFire license provides WildFire protection within 1 hour of new malware being detected anywhere in the world, integrated logging/reporting; access to WildFire API for programmatic submission of up to 100 samples per day and up to 1,000 report queries by file hash per day.

paloalto NETWORKS
the network security company™

3300 Olcott Street
Santa Clara, CA 95054

Main: +1.408.573.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com