



Controlling Modern Malware

Introducing WildFire: the Next-Generation of Malware Defense

November 2011

Palo Alto Networks
3300 Olcott St
Santa Clara, CA
95054
www.paloaltonetworks.com

Table of Contents

Modern Malware: The Threat Landscape Has Changed	3
Why Existing Solutions Can't Fix The Problem.....	3
Introducing WildFire®.....	4
WildFire In Action.....	5
Advantages of Combating Malware in the Cloud	6
Fully Integrated Threat Prevention	6
Frequently Asked Questions	7

Modern Malware: The Threat Landscape Has Changed

Modern malware is at the heart of many of today's most sophisticated attacks, enabling attackers to gain a foothold within the enterprise from which they can dig deeper into the network, control their attack, and steal information. As malware has become more advanced, it has also become more targeted and customized for a particular network, thus helping it to avoid traditional signature-based anti-malware and network security products. This shift has put IT security teams at a disadvantage inasmuch as the malware that represents the greatest risk to the enterprise is also the most difficult to detect.

As the modern threat has grown more sophisticated and persistent, the malware employed to assist in an attack has grown increasingly customized and tailored to remain undetected by traditional anti-malware products. This continuous evolution and repackaging of malware has increased the time it takes for antivirus vendors to acquire samples and develop signatures, sometimes to weeks or months, while enterprises remain unprotected.

Why Existing Solutions Can't Fix The Problem

Traditional firewalls only look at packet headers, and are not designed to detect malware. Even traditional antivirus products are flawed because they are signature-based and thus only detect malware that has previously been analyzed by the antivirus vendor. Vendors of most antivirus web-proxy and email gateway products today are signature-based and positioned to respond mostly to the quick-spreading and far-reaching malware of yesterday, relying on "honeypots" to collect only the most widely spread malware samples for characterization and signature generation. As a result, traditional antivirus vendors have increasingly delayed visibility into the highly targeted and sophisticated malware threats facing most enterprises today. Many firewalls and IPS solutions with antivirus capabilities rely solely on these same signature-based technologies, and thus have the same weaknesses.

Another problem facing many IPS antivirus products is the growing use of encryption. Traditional network security infrastructure is now blind to as much as 33% of traffic because of the growing use of SSL encryption. This trend is expected to continue, as many web-based email, social networking, and other Enterprise 2.0 web applications default to HTTPS to protect data in transit. This is a double-edged sword, however, and provides an encrypted channel to distribute malware to hosts on a network that is not adequately equipped to handle this new threat vector. This is just the tip of the iceberg, as malware and their authors have increasingly adopted a variety of additional techniques to obscure both the infecting files as well as the ongoing command and control traffic that modern malware depends on. This includes tunneling communications within approved protocols or traffic as well as using proxies, circumventors and non-standard ports in order to avoid traditional security solutions. These techniques, like SSL allow threats to remain hidden even as they repeatedly cross the perimeter without inspection.

While most anti-malware vendors view modern malware as a host problem, Palo Alto Networks views modern malware as a network security problem. Attackers and their malware use your network to infect a host and establish a beachhead, to initiate backdoors and covert channels for command & control, and to exfiltrate proprietary or sensitive data. With modern malware being a network problem, the firewall is ideally positioned to protect networks from advanced attacks. A next-generation firewall has visibility into all network traffic and can provide multiple opportunities to detect the modern malware lifecycle, from exploitation to compromise to command and control.

Introducing WildFire®

To meet the challenge of modern-day malware, Palo Alto Networks has developed WildFire, which provides the ability to identify malicious files by directly executing them in a virtual environment and observing malicious behavior. This enables Palo Alto Networks to identify malware quickly and accurately, even if the malware has never been seen in the wild before.

WildFire makes use of a customer's on-premises firewalls in conjunction with the Palo Alto Networks cloud-based analysis engine to protect in-line performance, while using the cloud to ensure the fastest protections for all enterprise locations.

- **Virtualized Sandbox:** When the firewall encounters an unknown file (PE files initially), the file can be submitted to the WildFire virtualized sandbox. Submissions can be made manually or automatically based on policy. The sandbox provides virtual targets where Palo Alto Networks can directly observe more than 70 malicious behaviors that can reveal the presence of malware.
- **Automated Signature Generator:** When a sample is identified as malware, it is passed on to a signature generator, which automatically generates a signature for the sample and tests it for accuracy. With WildFire in the cloud, signatures can be automatically regression tested against an extensive database of samples, and then delivered to all Palo Alto Networks customers as part of the daily malware signature updates. Palo Alto Networks also generates signatures for the all-important command and control traffic, allowing staff to disrupt active attacks.
- **Deep Visibility:** The WildFire solution makes extensive use of Palo Alto Networks App-ID technology by identifying file transfers within all applications, not just email attachments or browser-based file downloads. Additionally, on-device SSL decryption enables administrators to configure policies that detect file transfers through HTTPS-encrypted web applications and send them to WildFire for analysis.
- **Actionable Intelligence:** In addition to protection, administrators have access to a wealth of actionable information about the detected malware through the WildFire portal. A detailed behavioral report of the malware is produced, along with information on the user that was targeted, the application that delivered the malware, and all URLs involved in the delivery or phone-home of the malware.

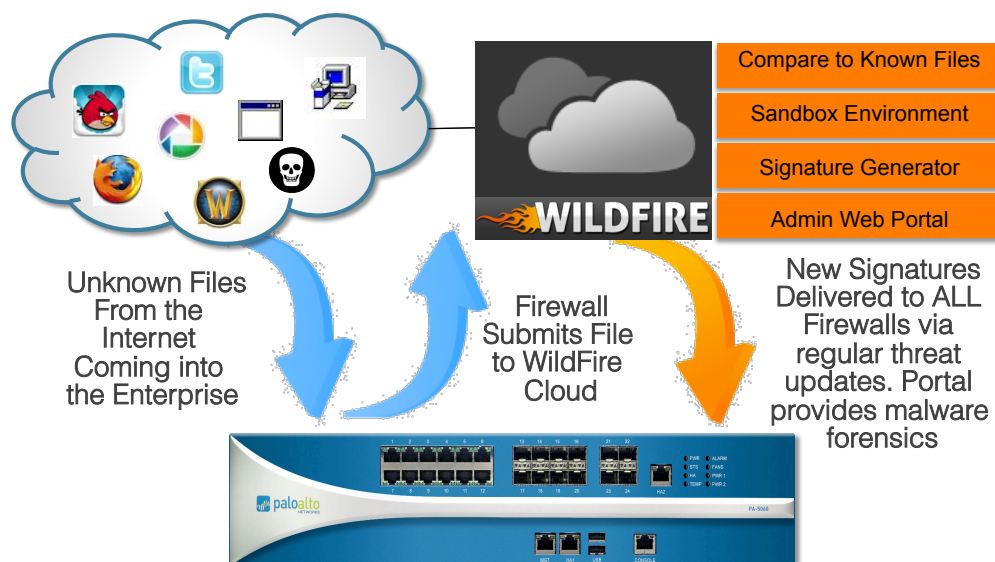
Analysis Summary		
Behavior		
Modified registries or system configuration to enable auto start capability		
Registered a file as auto-start from a local directory		
Executed external DLLs with rundll32.exe		
Spawned new processes		
Modified Windows registries		
Created or modified files		
Created an executable file in a user document folder		
Detailed Events		
Registry		
		Action
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2{e86064ca-57e4-11e0-bef8-806d6172696f}\BaseClass		Set
HKCU\Software\WinGLRpi\WygMamo		Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Local AppData		Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\sysMobilenet		Set
HKCU\Software\WinGLRpi\UGKT		Set
HKCU\Software\WinGLRpi\pqVJrMI		Set
Process		
	Parent Process	Action
C:\sample.exe	UNKNOWN	Create
C:\sample.exe	explorer.exe	Create
UNKNOWN	C:\sample.exe	Create

Excerpt from a malware analysis report

- Behavioral Botnet Report:** In addition to the direct analysis of malware in WildFire, the Palo Alto Networks solution also includes the ability to identify the presence of modern malware through the monitoring and correlation of suspicious network traffic. The behavioral botnet report looks for a variety of telltale signs of a botnet infection, such as the presence of unknown application traffic, IRC traffic, repeated attempts to download files, and connections to unknown or newly registered domains. The report leverages User-ID to identify the infected user and the factors that contributed to the analysis.

WildFire In Action

WildFire is easily put into action by configuring a simple policy on a Palo Alto Networks next-generation firewall. Policies can control what types of files are submitted and any correlating information that should be included or not. When the firewall encounters a file within traffic that matches a WildFire forwarding policy, the file is first checked to see if a known reputable software author has signed it. If not, the cloud is then queried to determine if the WildFire service has already analyzed the same file, before sending a duplicate and repeating the process needlessly. The file is then sent up to the WildFire service if it has not been analyzed previously.



When a new sample is sent to WildFire, the file is executed within a virtual machine, and analyzed for malicious behavior. WildFire monitors activity on the virtual machine, looking for over seventy behaviors that may indicate maliciousness, including modifications to the Windows registry and browser security settings, injection of code into other processes, and modification of files in the Windows system folder. When the analysis is complete, a determination is made as to whether the sample is considered benign or malicious, and a report is made available to the administrator via the WildFire web portal, and via configurable automatic email reports.

WildFire automatically generates signatures for samples that are deemed malicious, and immediately regression tests the signatures against an extensive database of clean and malicious samples to ensure signature quality. In addition to creating signatures for the infecting files, Palo Alto Networks also creates signatures that identify the command and control traffic of the malware, ensuring that staff can also instantly stop and quarantine any active threats already in the network. The signatures of all malicious WildFire submissions are then bundled with the daily antivirus updates and distributed to Palo Alto Networks customers that have a threat protection subscription.

Frequently Asked Questions

Q) How do I control what is sent to the cloud?

A) The user has total control over what is sent to the WildFire service using policy control. In a typical deployment, a policy is configured that sends incoming high-risk file types to WildFire that originate from an untrusted zone (i.e. the internet) to a trusted zone. In this deployment, the only files that are uploaded to the WildFire service are files that had already entered the network from an outside, untrusted network. Additionally, all file uploads from the device to the cloud are encrypted (see below).

Q) How do I know the files I upload are safe in transit to the cloud?

A) All data uploaded from the appliance to the cloud is encrypted and sent via HTTPS using a client certificate present on the device. This ensures the data is secure in transit between the Palo Alto Networks firewall and the servers that form the WildFire cloud.

Q) How is data in the cloud protected?

A) The WildFire data centers that store and process files uploaded from Palo Alto Networks devices is protected by Palo Alto Network firewalls, and access to the data centers is strictly limited to select servers on the Palo Alto Networks company network that perform automated regression testing of malware signatures.

Q) How long does my data reside in the cloud?

A) All samples uploaded to WildFire are promptly removed from the cloud service infrastructure after processing completes (typically less than 5 minutes). This policy limits the lifetime of files uploaded to the cloud to be as brief as possible.