

# Stallion Summer Shooting - WildFire™ Overview

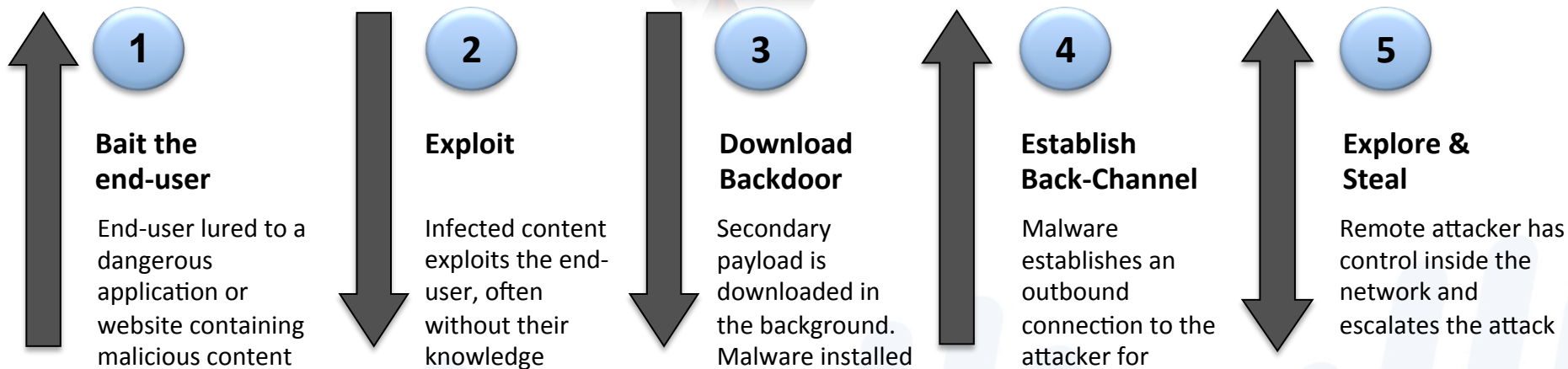
*Markus Laaksonen*

*Systems Engineer Nordics*



the network security company™

# The Lifecycle of Network Attacks



# Why Traditional Antivirus Protection Fails

Modern malware is increasingly able to:

- Avoid traditional AV honeypots with targeted malware
- Evolve before protection can be delivered, using polymorphism, re-encoding, and changing URLs



Targeted and custom malware



Polymorphic malware



Newly released malware

---

***Highly variable time to protection***

# Evolving Threats Require Intelligent Solutions

*An effective modern malware solution must provide:*



## Visibility

- See files in all applications, protocols, and ports at all times
- See files inside SSL, compression, and encoding
- Visibility into mobile devices and users



## Detection & Reaction

- Sandbox-based behavioral analysis of new unknown files
- Rapid alerting of malware discovered on the network
- Complete forensics report of the activity of the malware

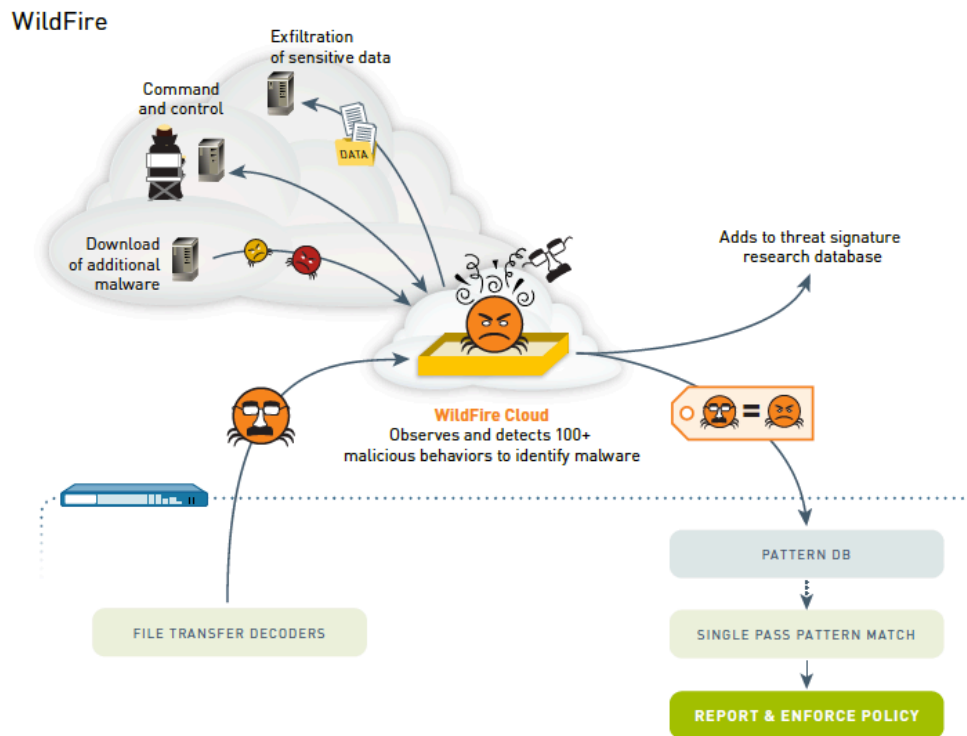


## Enforcement

- Automatic updates of signatures to block threats at the firewall
- True in-line blocking of infecting files and C&C traffic
- Stream-based malware blocking to preserve performance

# WildFire Architecture

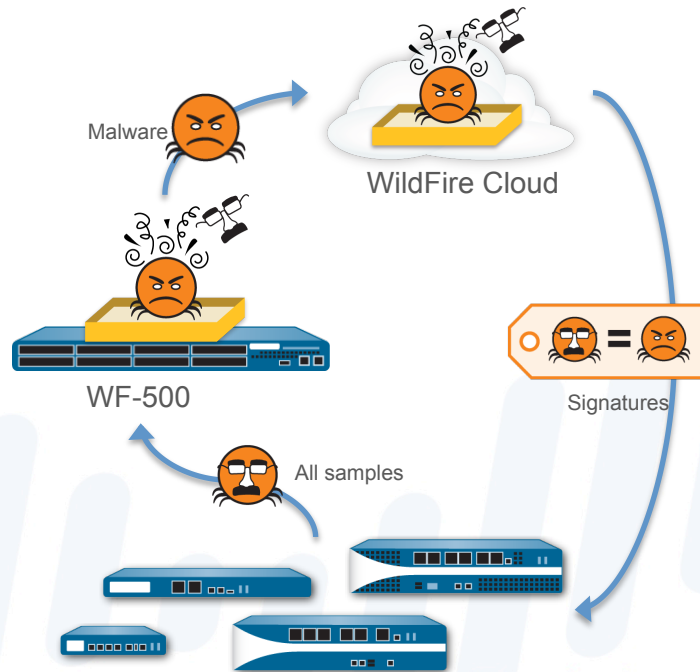
- File scanning on all traffic, all ports (web, email, SMB, etc.)
- Malware run in the cloud with open internet access to discover hidden behaviors
- Sandbox logic updated routinely with no customer impact
- Malware signatures automatically created based on payload data
- Stream-based malware engine performs true inline enforcement



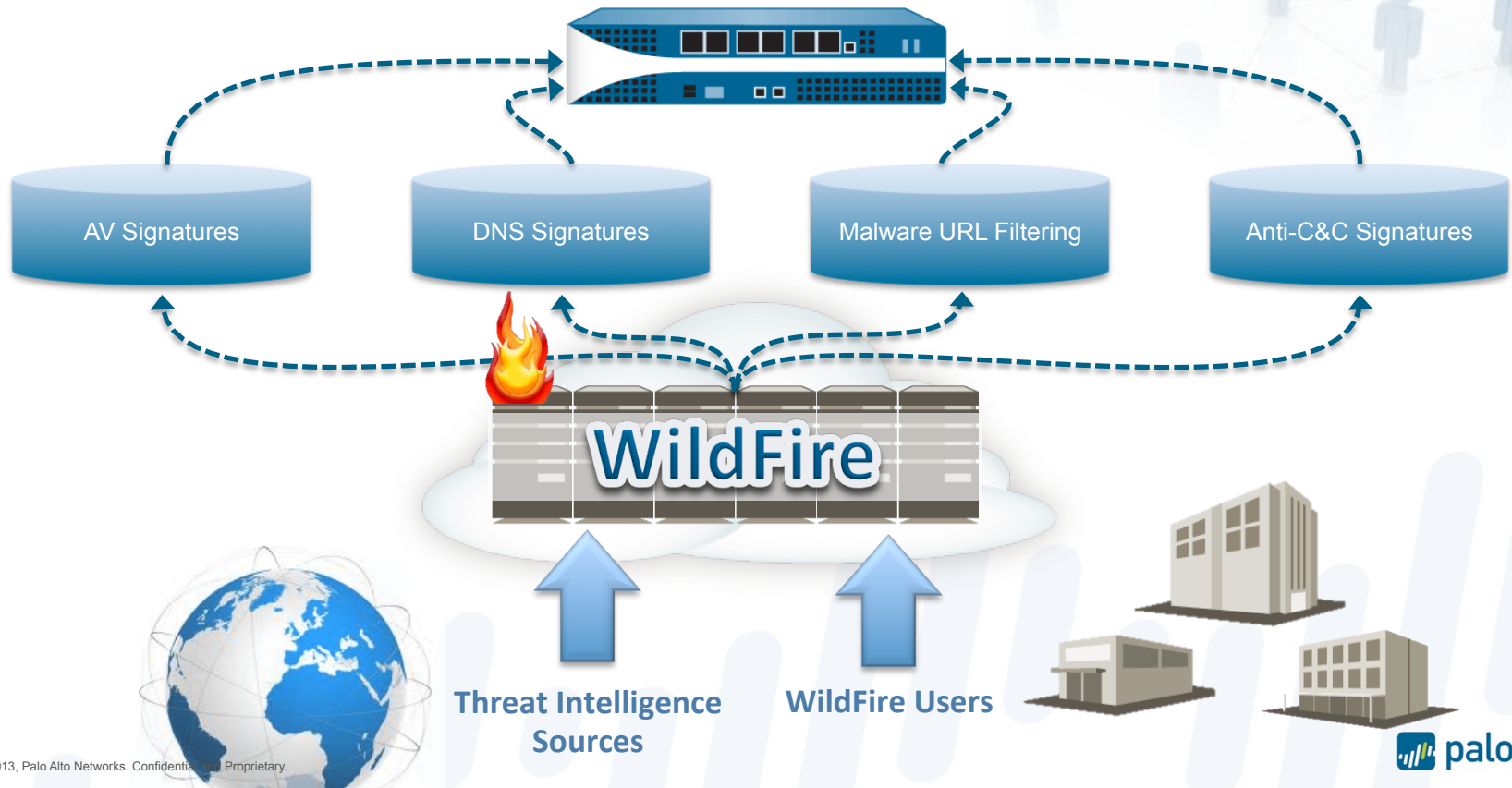
# Introducing the WildFire Appliance (WF-500)



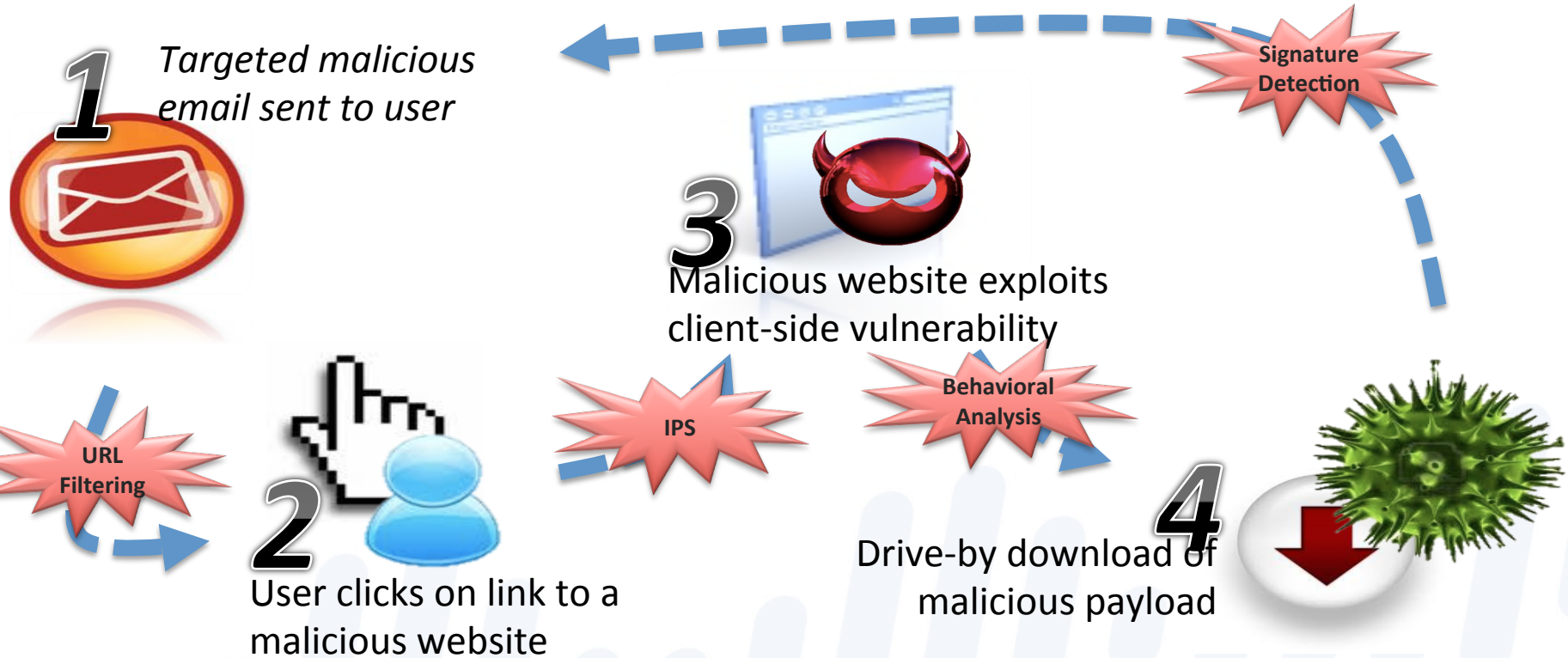
- Appliance-based version of WildFire for on-premises deployments
- All sandbox analysis performed locally on the WildFire appliance
- WF-500 has option to send locally identified malware to WildFire public cloud
  - Signatures only are created in public cloud
- WildFire signatures for all customers distributed via normal update service
- Detection capabilities in sync with public cloud



# Reaching Effects of WildFire



# Attack Stages of Modern Malware





# WildFire Logs

report@wildfire.paloaltonetworks.com

To: Malware  
Your Wildfire

The file  
URL: [https://wildfire.paloaltonetworks.com/Wildfire/](#)  
User: user@wildfire.paloaltonetworks.com  
Application: Application  
Source: Source  
Destination: Destination  
Device: Device

This sample  
Here is

-Create  
-Spawn  
-Cont  
-Modif  
-Chan  
-User A  
-Used  
-Creat  
-Inject  
-Stole  
-Chan  
-Modif  
-Disab  
-Execu  
-Starte

The details  
[https://wildfire.paloaltonetworks.com/Wildfire/](#)

ReportDetail

[https://wildfire.paloaltonetworks.com/Wildfire/](#)

Overview

Filename:	id282687.com		
SHA256:	ac97d69776cdb22dc61e32080369e47bc29b22493fb4e71f2ec243fec2af9fd6		
URL:			
User:	wildfire.pan@gmail.com	Received:	3/21/2012 1:02:34 AM
Attacker:		Victim:	
Hostname/Mgmt. IP:	172.16.7.5	Application:	
Verdict:	Malware		<a href="#">Virus Coverage Information</a>

Analysis Summary

Behavior

Created or modified files in the Windows system folder
Spawned new processes
Created an executable file in Windows folder
Injected code into another process
Modified Windows registries
Created or modified files
Created a file in the Windows folder
Created an executable file in the Windows system folder

Detailed Events

Registry	Action
HKCU\Control Panel\Keyboard\InitialKeyboardIndicators	Set

Process	Parent Process	Action
C:\sample.exe	explorer.exe	Create

# Detailed Report: Malware Example

## Overview

File name, hash, URL, source & destination, verdict (malware or benign), application

Filename:	transcript.scr		
SHA256:	4f325b6b63cf7c0daf8ca3ed72a182f05c6fe2d19f1991bce45723697571ad61		
URL:	unknown		
User:	unknown	Received:	11/4/2011 9:06:49 PM
Source:	133.5.184.202 :110	Destination:	133.6.215.213 :39887
Hostname/Mgmt. IP:	PA-2050	Application:	pop3
Verdict:	Malware	<a href="#">Virus Coverage Information</a>	Host AV Coverage

## Analysis Summary

Summarized list of the possibly suspicious behaviors exhibited by the sample

Created an executable file in windows folder
Stole saved user passwords from Internet Explorer
Created or modified files
Spawned new processes
Masqueraded as a Windows system program
Modified Windows registries
Modified registries or system configuration to enable auto start capability
Accessed honey files
Changed security settings of Internet Explorer
Changed the proxy settings for Internet Explorer
Modified the network connections setting for Internet Explorer
Sent out emails

WildFire looks for over 100 potentially malicious behaviors. Some behaviors are fairly benign by themselves, while others are almost exclusively performed by malware.

# Detailed Report: Malware Example (cont'd)

## Traffic

*Domain names and IPs of remote hosts contacted by sample, HTTP header summaries*

Method	URL	User Agent
GET	bcredretr.ru/forum/index.php?cmd=getload&login=54C43C4A DFF6BE07D&sel=77777&ver=5.1&bits=0&file=0	Mozilla/4.0
GET	bcredretr.ru/forum/index.php?cmd=getload&login=54C43C4A DFF6BE07D&sel=77777&ver=5.1&bits=0	Mozilla/4.0
GET	bcredretr.ru/forum/index.php?cmd=getload&login=54C43C4A	Mozilla/4.0

## Detailed Events

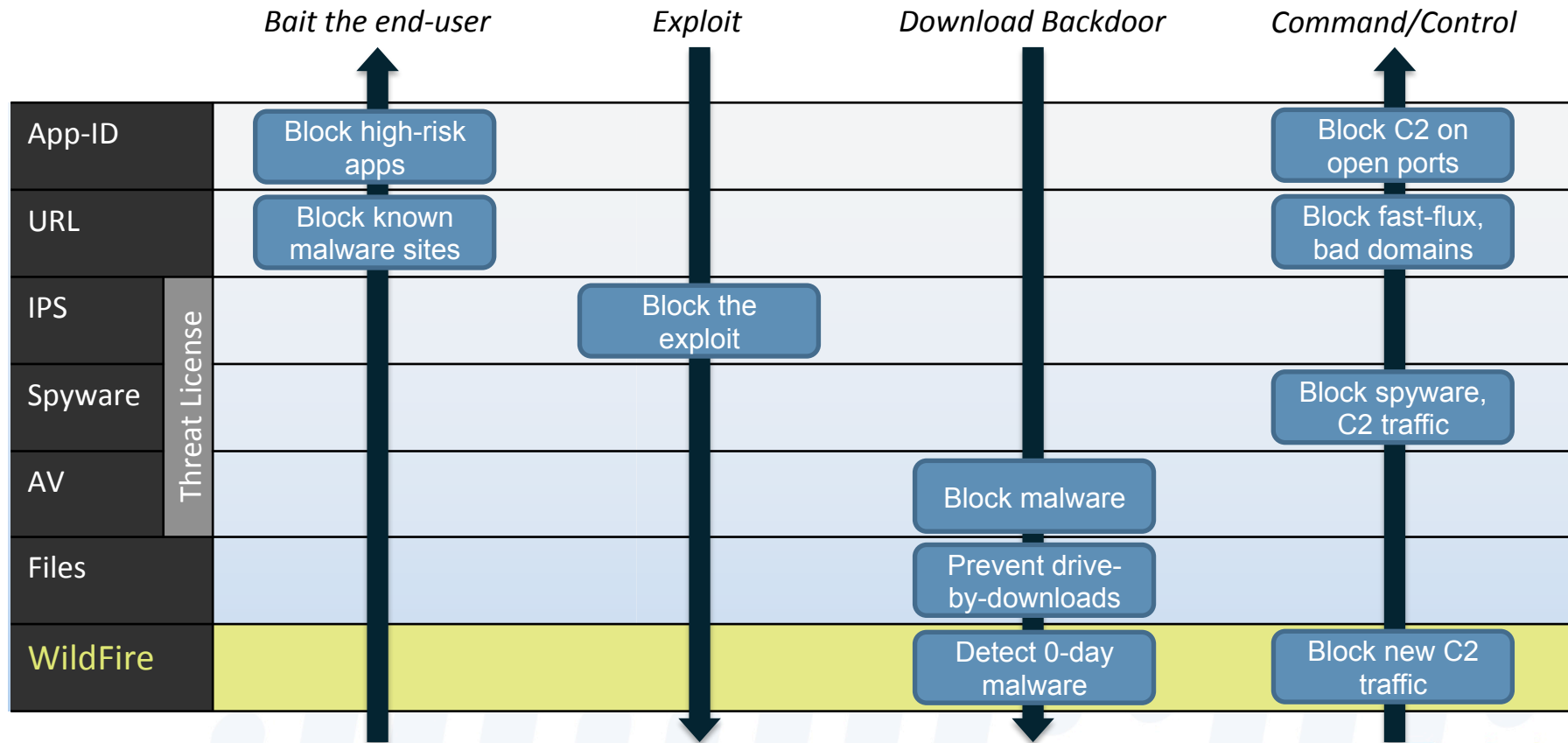
*List of modified registry keys, files, and processes started or stopped.*

Registry	Action
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\JavaVM	Set
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Services	Set
HKLM\SOFTWARE\Microsoft\PCHealth\ErrorReporting\DWDFWFileTreeRoot	Delete

Process	Parent Process	Action
C:\sample.exe	UNKNOWN	Create
C:\sample.exe	explorer.exe	Create
C:\WINDOWS\system32\svchost.exe	C:\sample.exe	Create

File	Process	Action
C:\Documents and Settings\Administrator\Local Settings\Temp\zincite.log	C:\sample.exe	Write
C:\WINDOWS\services.exe	C:\sample.exe	Write
C:\WINDOWS\java.exe	C:\sample.exe	Delete

# An Integrated Approach to Threat Prevention

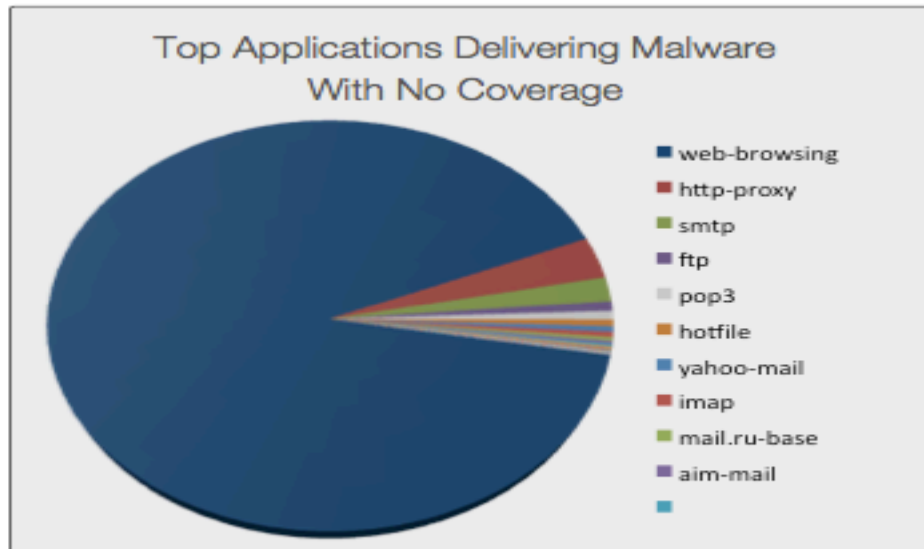
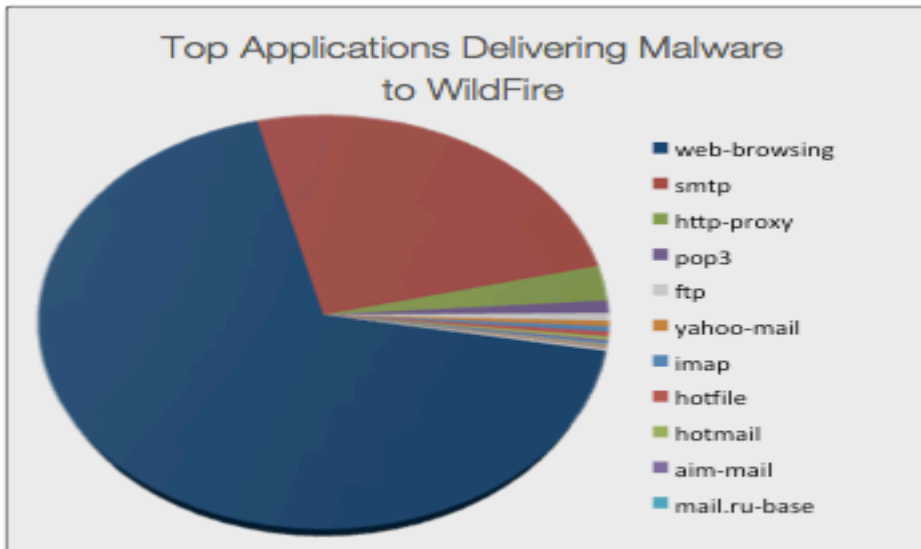


# Large Scale Analysis of Unknown Malware

- 3 months of WildFire Data
- 1,000+ participating networks
- 26,000+ malware samples that had no coverage from any of the top 6 AV vendors at the time of detection
- Full lifecycle analysis of the malware
  - Infection session
  - Behaviors on the target host
  - Malware generated traffic
- Focus on actionable advice

# Infection Vectors by Application

The web is where the actions is for unknown malware.

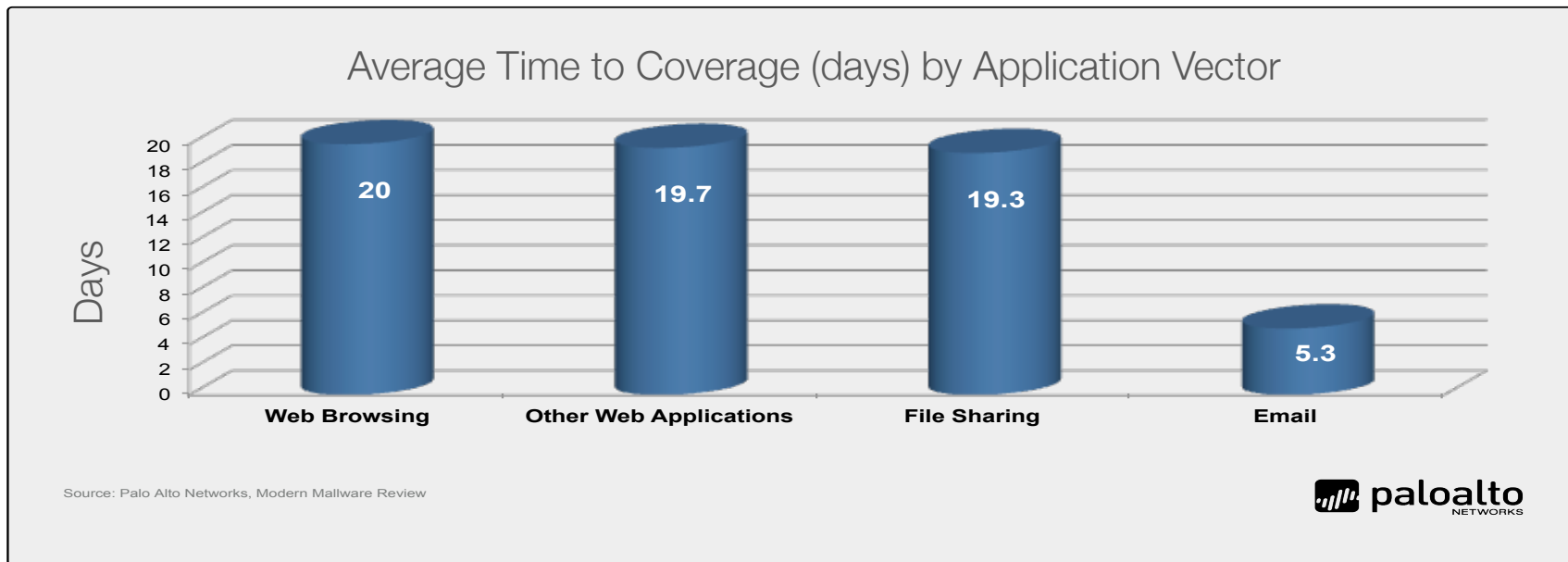


3% of malware delivered by email evaded all vendors  
vs

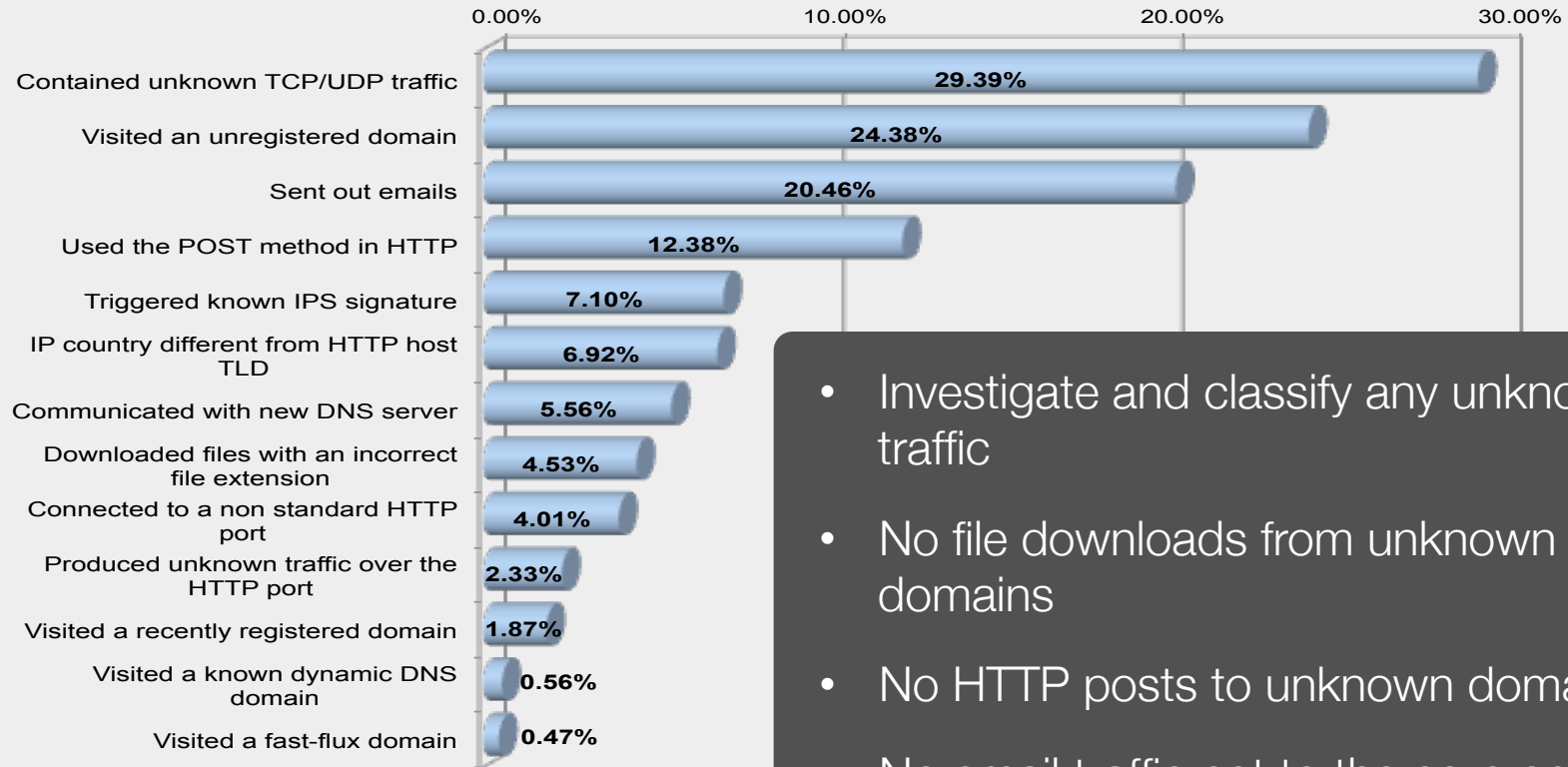
More than 50% of malware delivered by the web

# Average Time to Detection by Antivirus

On average, it took traditional antivirus 4x as long to provide coverage for malware delivered in applications other than email.



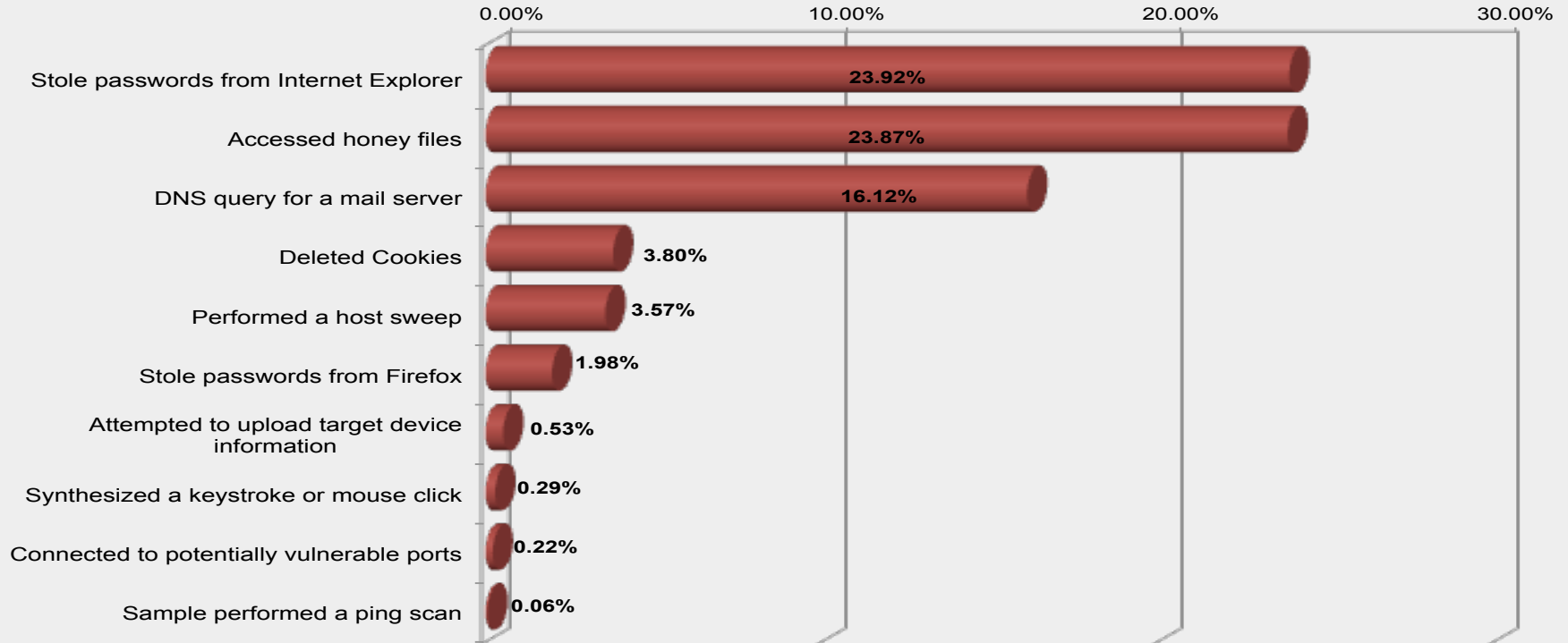
# Most Commonly Observed Malware Behaviors on the Network



- Investigate and classify any unknown traffic
- No file downloads from unknown domains
- No HTTP posts to unknown domains
- No email traffic not to the corp email server



# Most Common Hacking and Data Theft Behaviors



# Non-Standard Ports and Malware

## **FTP was the most evasive application observed\***

- 95% of unknown samples delivered via FTP were never covered by antivirus.
- 97% of malware FTP sessions used non-standard ports, and used 237 different non-standard ports.

## **Web-browsing delivered more malware, but was less evasive.**

- 10% of samples delivered over 90 different non-standard web ports



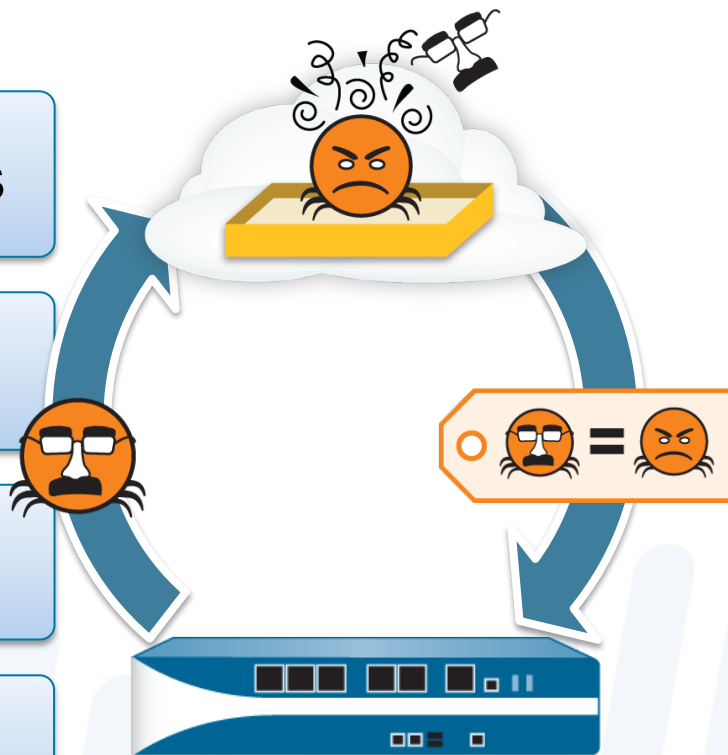
# WildFire Subscription Service

WildFire signatures every 30 minutes

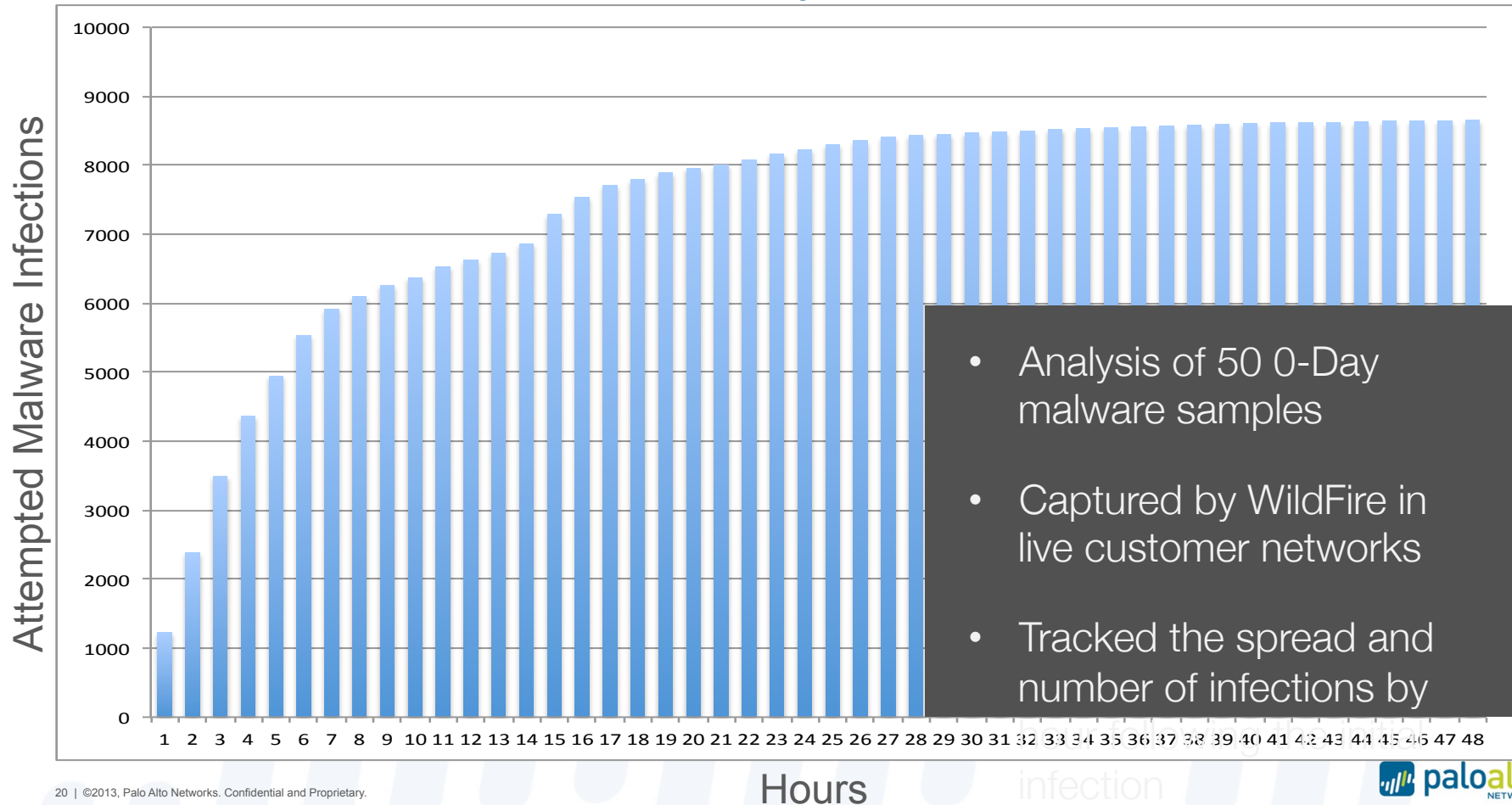
Integrated logging & reporting

REST API for scripted file uploads

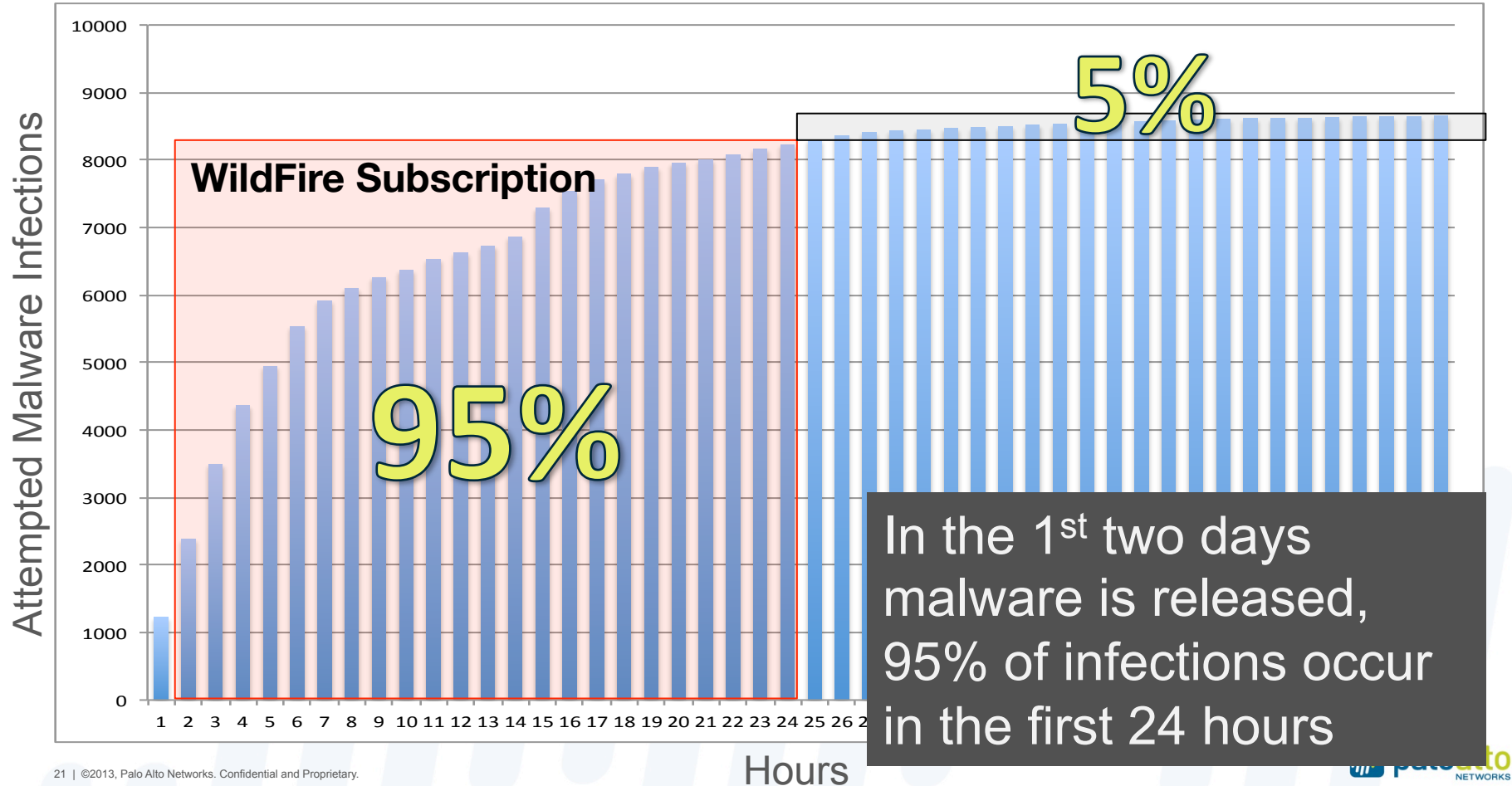
Possible New Features Forward



# Real-World Spread of 0-Day Malware



# Real-World Spread of 0-Day Malware



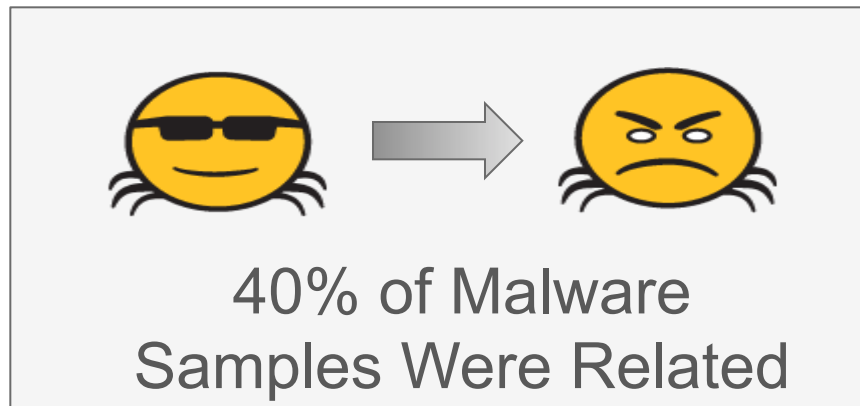
# 40% of Unknown Malware Files Were Variants

- Opportunity to Block Malware

- In 40% of cases, a single signatures matched multiple samples (variants)
- 1 signature hit 1,500+ unique SHA values
- Provides a way to block malware even when it is repackaged to avoid signatures

- WildFire Subscription

- Delivers signatures in 30 to 60 minutes of new malware being detected anywhere in the world



# WildFire Summary



Full visibility of the next-generation firewall extended to detect and prevent unknown malware.



Cloud-based analysis ensures scalable, safe and adaptable analysis.



Shared protection – all subscribers protected within 1 hour of first instance of malware detection.



True prevention – signatures based on payload that block multiple malware variants



Analysis within minutes and correlated with application, user, URL and file logs.

# What does WildFire exactly do for me?

- WildFire will deliver immediate visibility on:
  - The application used (no limitation to only HTTP, SMTP and SMB)
  - The user and system infected
  - The behavior of the malware
- 1 detection/execution of new unique (global) malware sample, results in protection
  - For all other customers as well
    - Often before they even see the first occurrence in their network
  - Against related malware (variants) where possible
    - The related signature is not just a hash of the original malware file...
- The WildFire sandbox also can help on adding additional coverage
  - Known malware URL category in the PANW-URL-DB → malware download prevention
  - DNS signatures → detect infected hosts, reaching out for secondary payload
  - C&C signatures → detect bots, talking to their controller (result of secondary payload)





the network security company<sup>™</sup>