WildFire™ Overview

Stallion Lunch and Learn

Markus Laaksonen

Systems Engineer Nordics

paloalto NETWORKS

the network security company™

The Lifecycle of Network Attacks

1

Bait the end-user

End-user lured to a dangerous application or website containing malicious content

2

Exploit

Infected content exploits the end-user, often without their knowledge

3

Download Backdoor

Secondary payload is downloaded in the background. Malware installed

4

Establish Back-Channel

Malware establishes an outbound connection to the attacker for ongoing control

5

Explore & Steal

Remote attacker has control inside the network and escalates the attack

paloalto NETWORKS

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

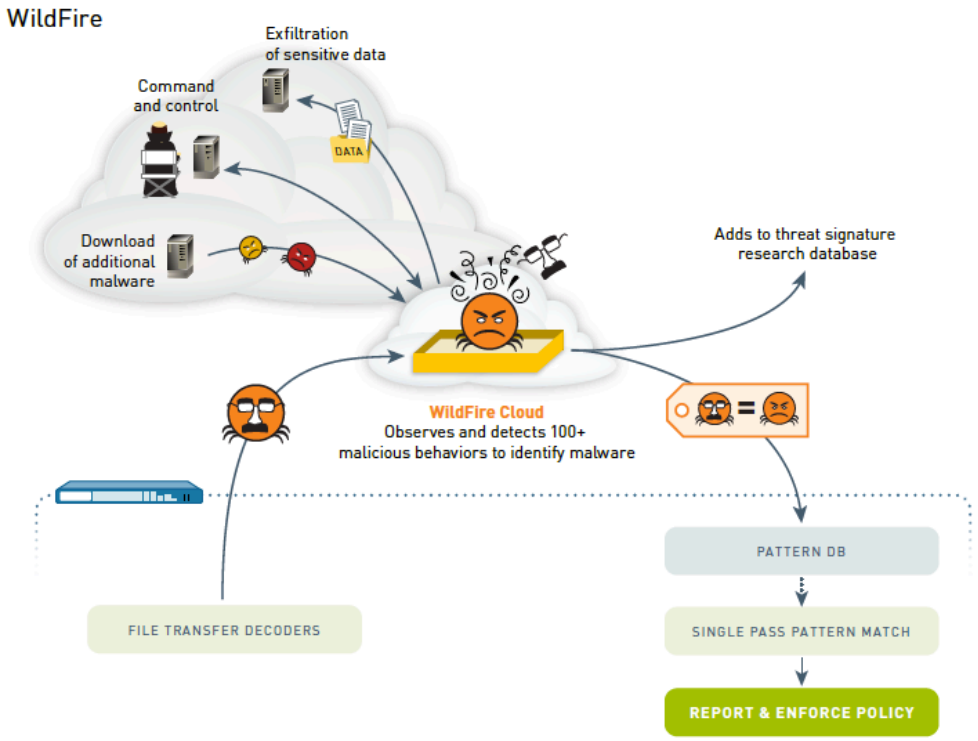
Enforcement

- 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

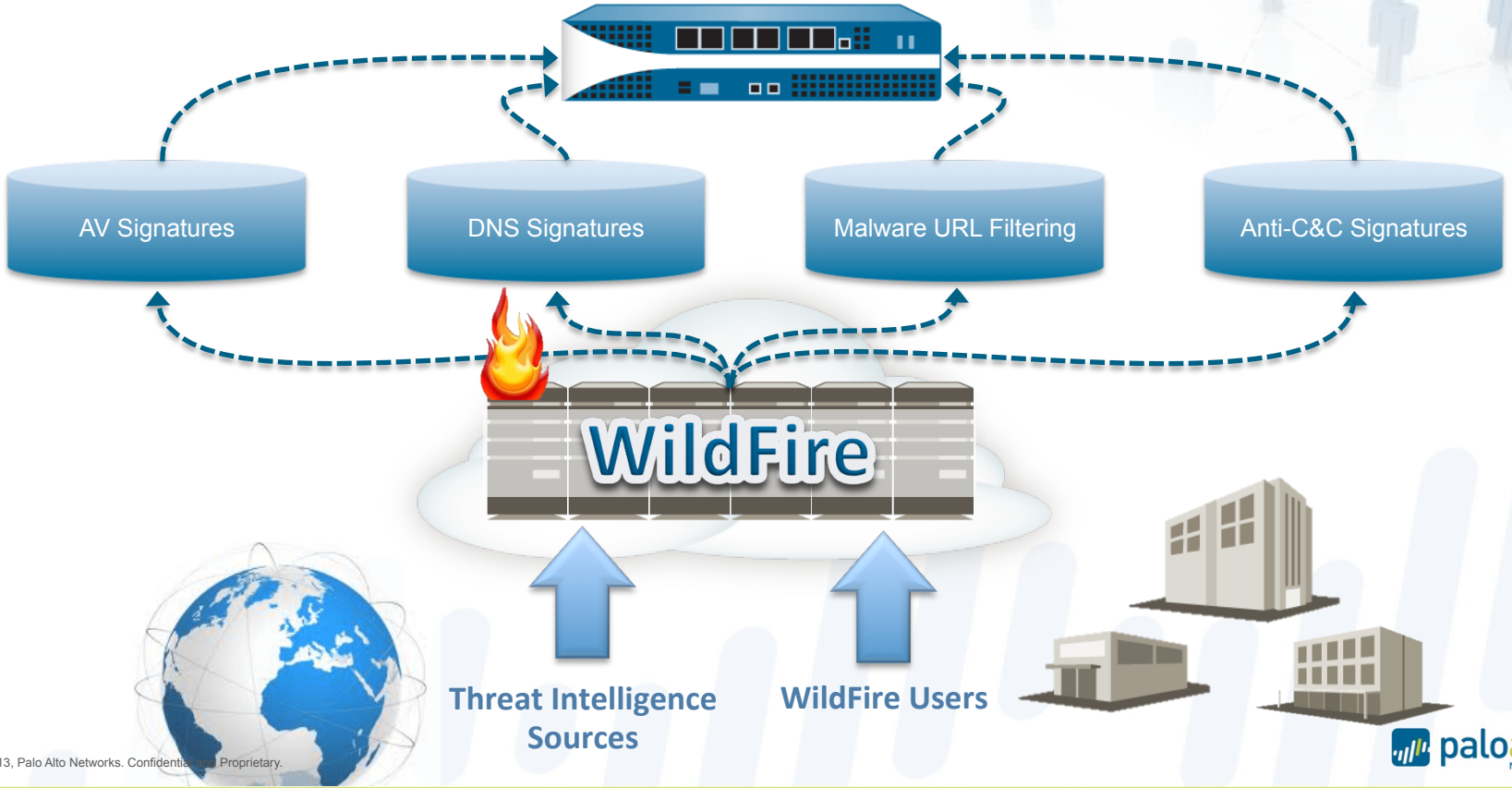
paloalto NETWORKS

WildFire Architecture

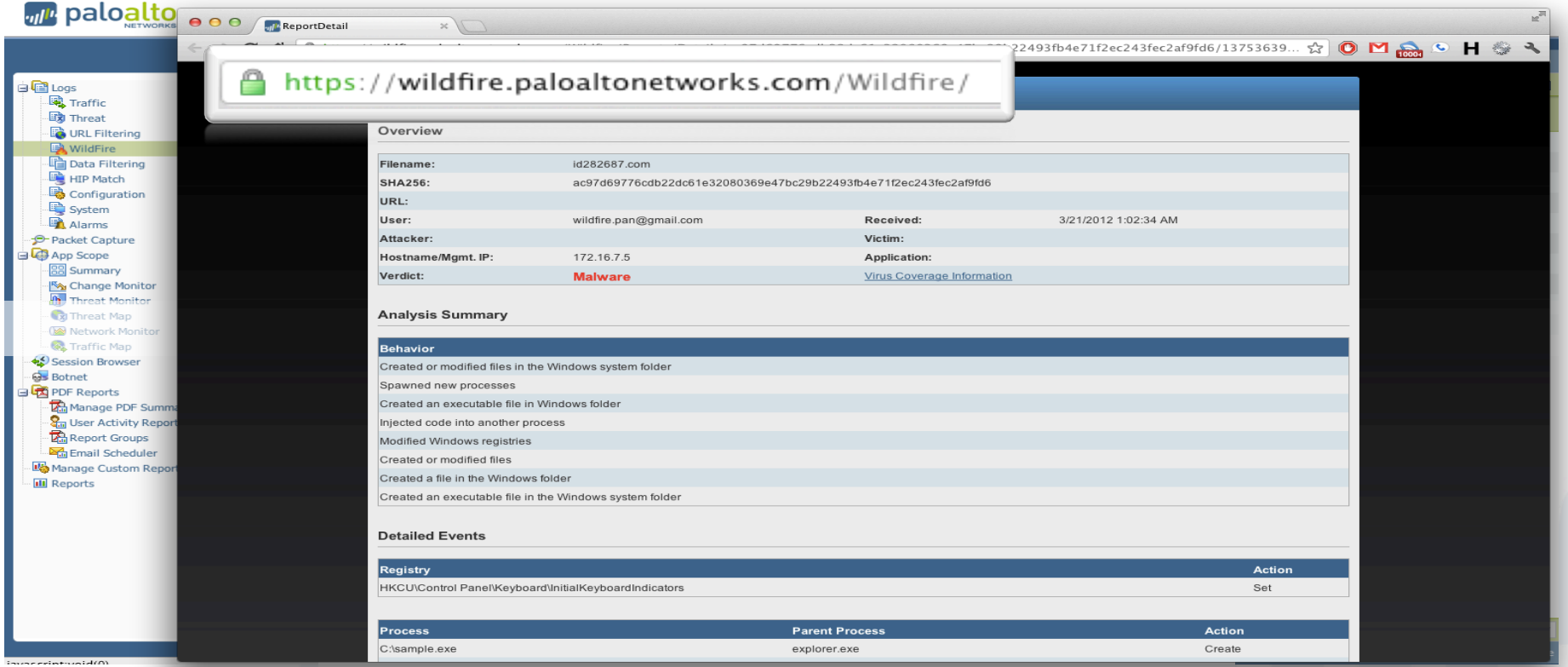
- 10Gbps threat prevention and file scanning on all traffic, all ports (web, email, SMB, etc.)
- Malware run in the cloud with open internet access to discover hidden behaviors
- Sandbox logic updated routinely with no customer impact
- Malware signatures automatically created based on payload data
- Stream-based malware engine performs true inline enforcement



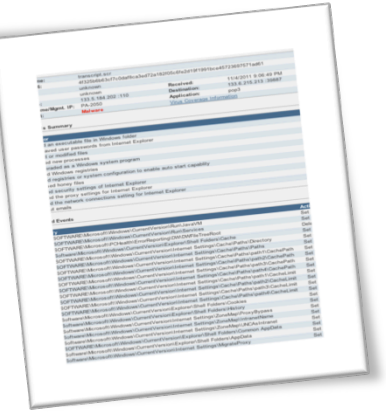
Reaching Effects of WildFire



WildFire Logs



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	Virus Coverage Information	

Verdict

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 capablity
- 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.

paloalto NETWORKS

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\DW\DWFileTreeRoot	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

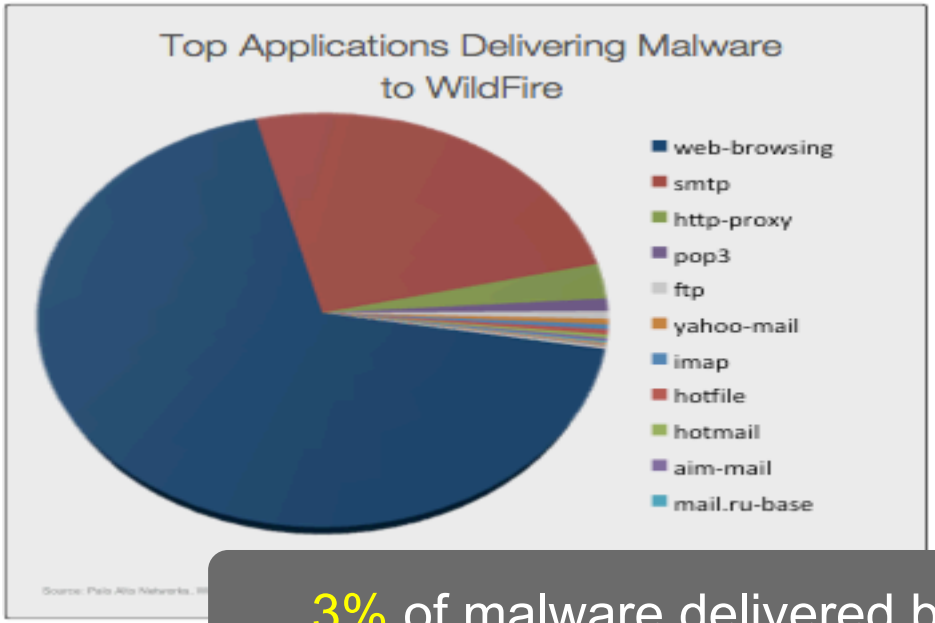
paloalto NETWORKS

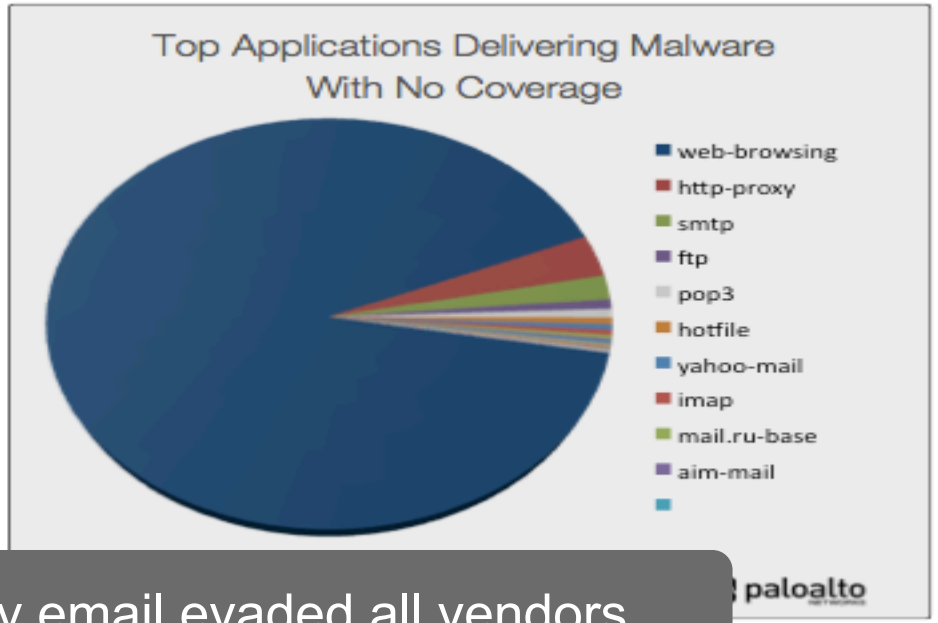
Large Scale Analysis of Unknown Malware

- 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.

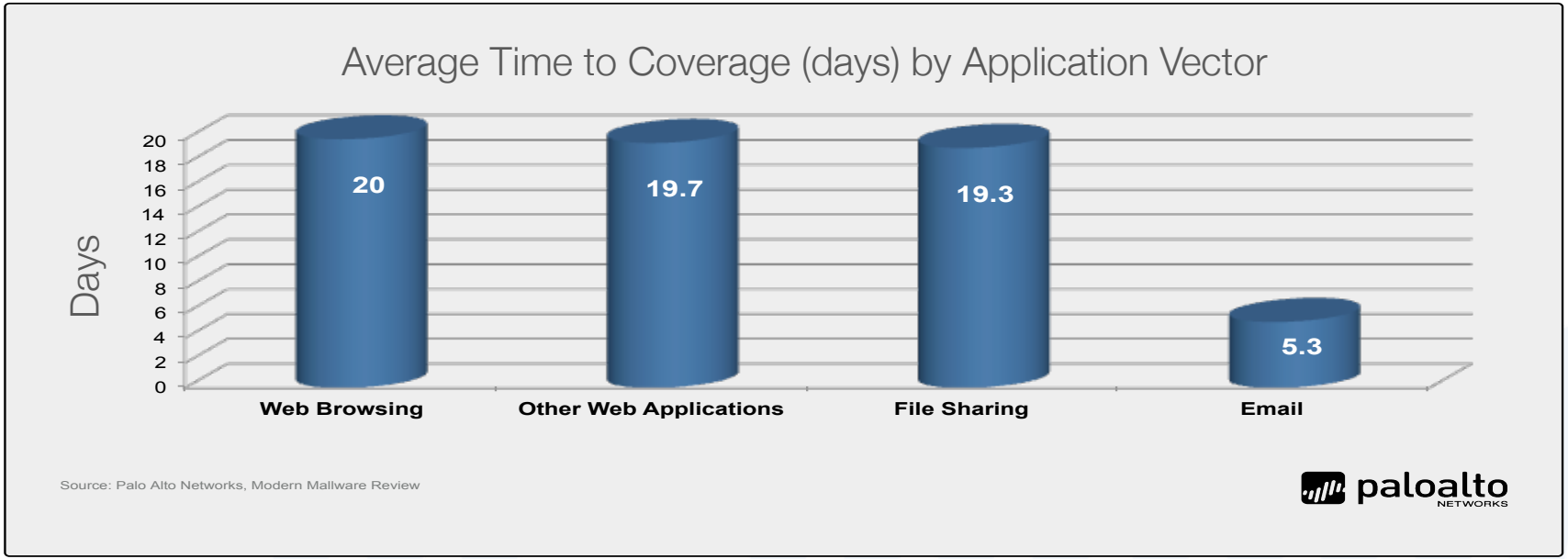




3% of malware delivered by email evaded all vendors
vs
More than 50% of malware delivered by the web

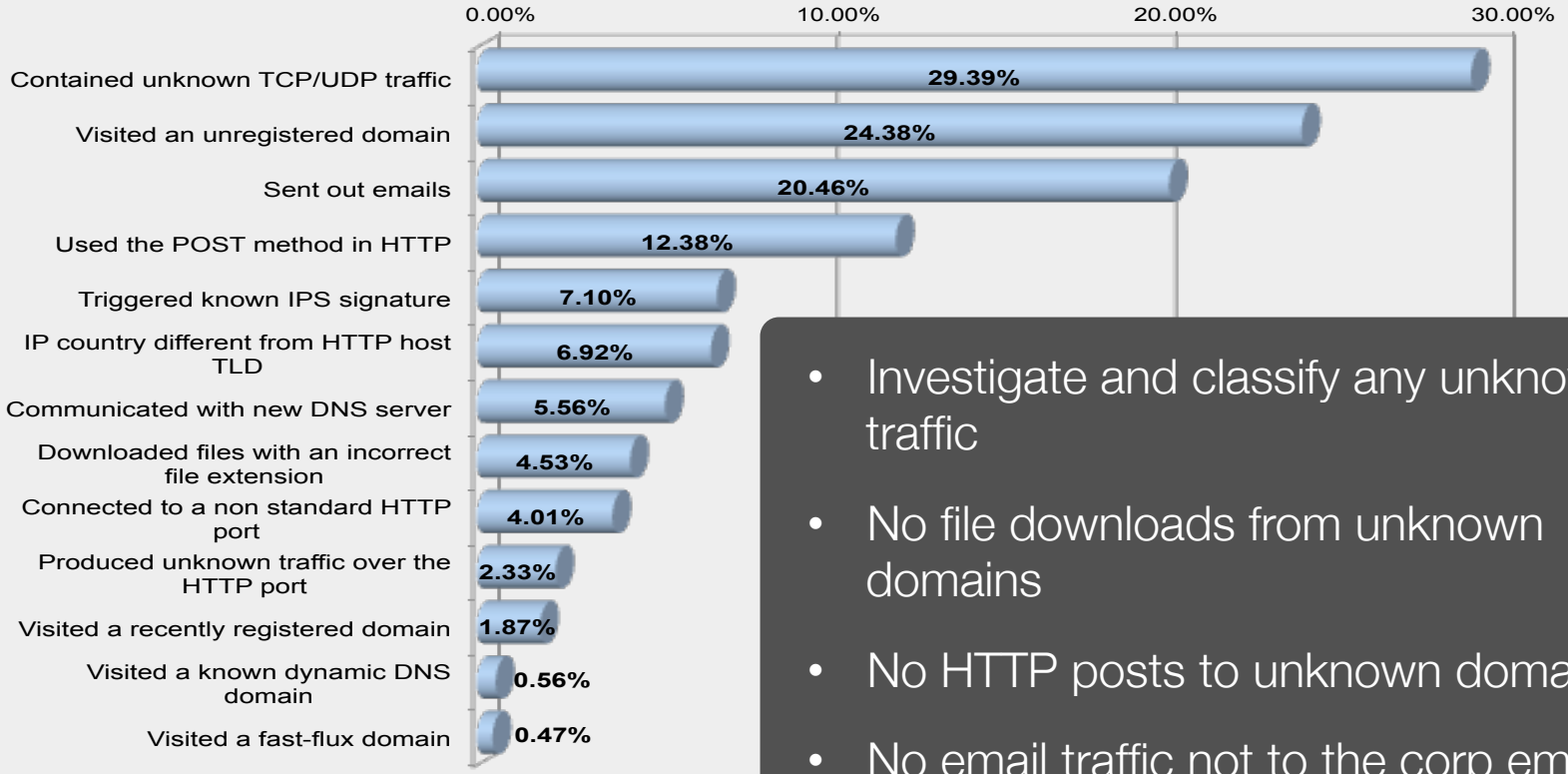
Average Time to Detection by Antivirus

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



paloalto NETWORKS

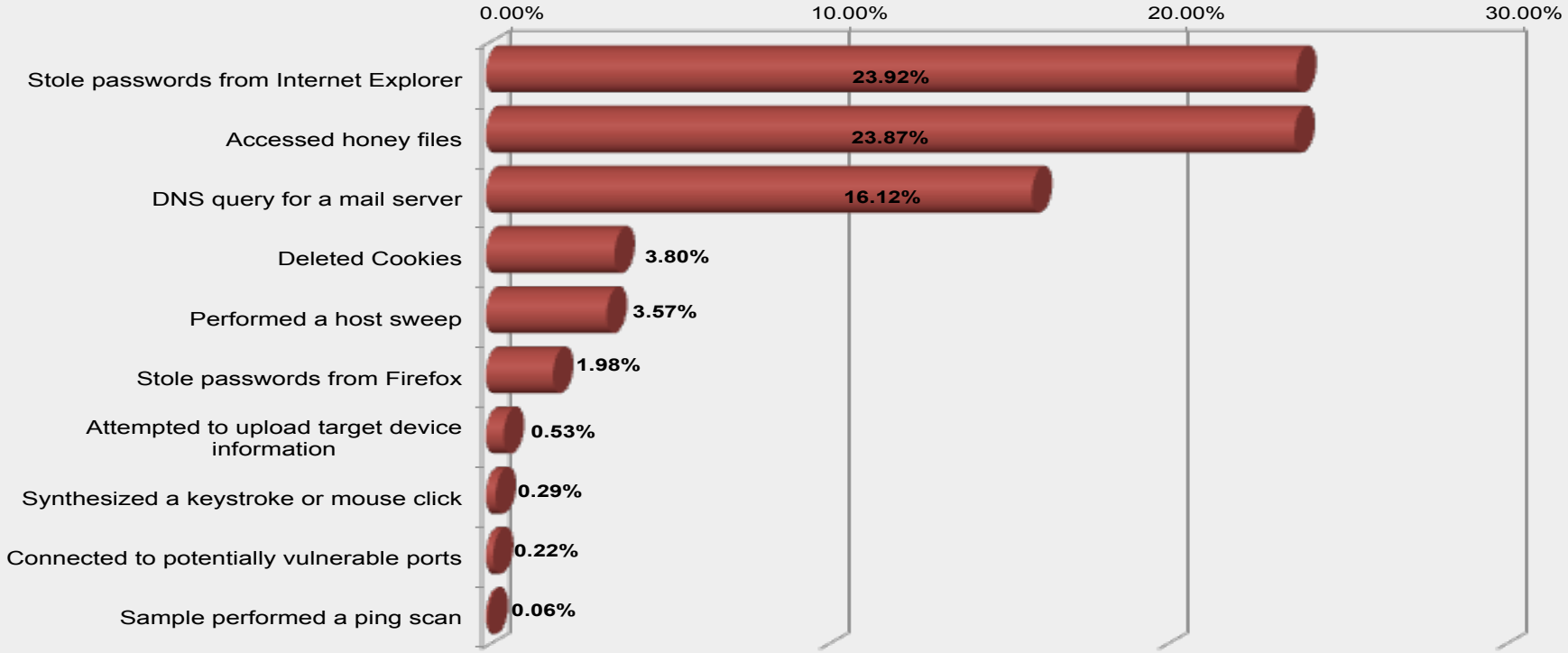
Most Commonly Observed Malware Behaviors on the Network



Source: Palo Alto Networks, WildFire Malware Report

- 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



paloalto NETWORKS

The Winner for Most Evasive Malware Vector Is…

Plain old FTP

- FTP was the 4th most common infection vector.
- 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 dominated the volume, but FTP was more targeted and better at remaining unknown.

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

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

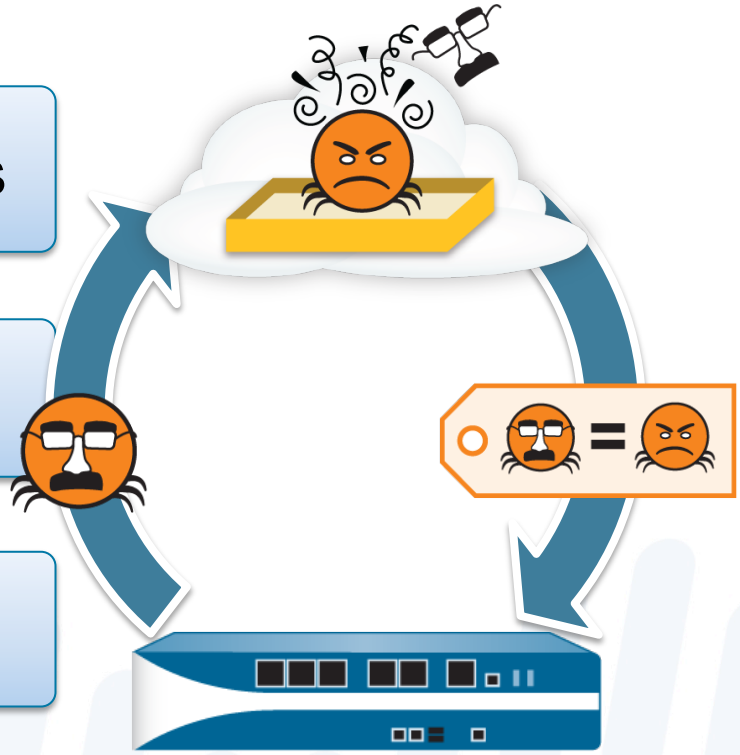
paloalto NETWORKS

WildFire Subscription Service

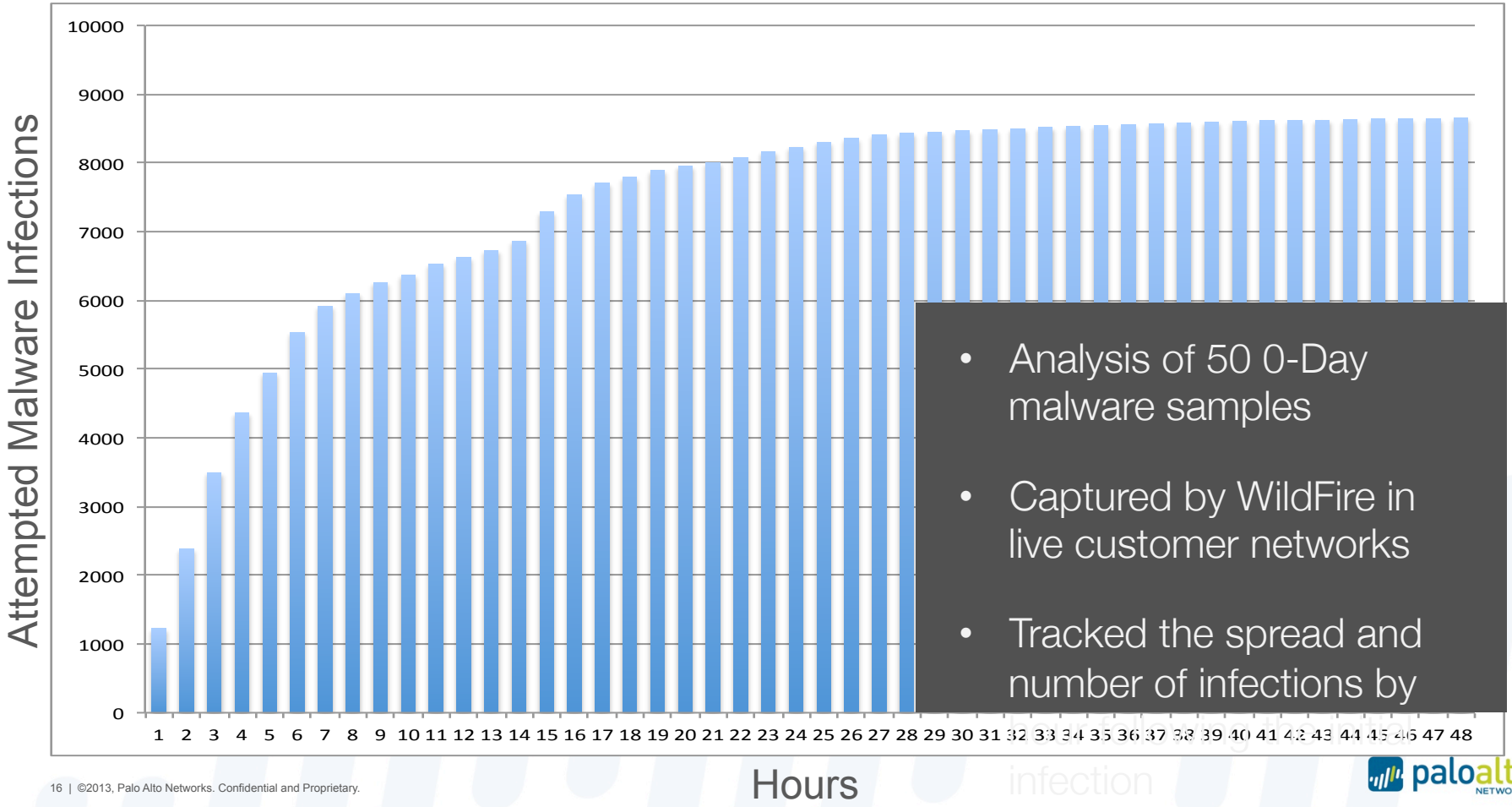
WildFire signatures every 30 minutes

Integrated logging & reporting

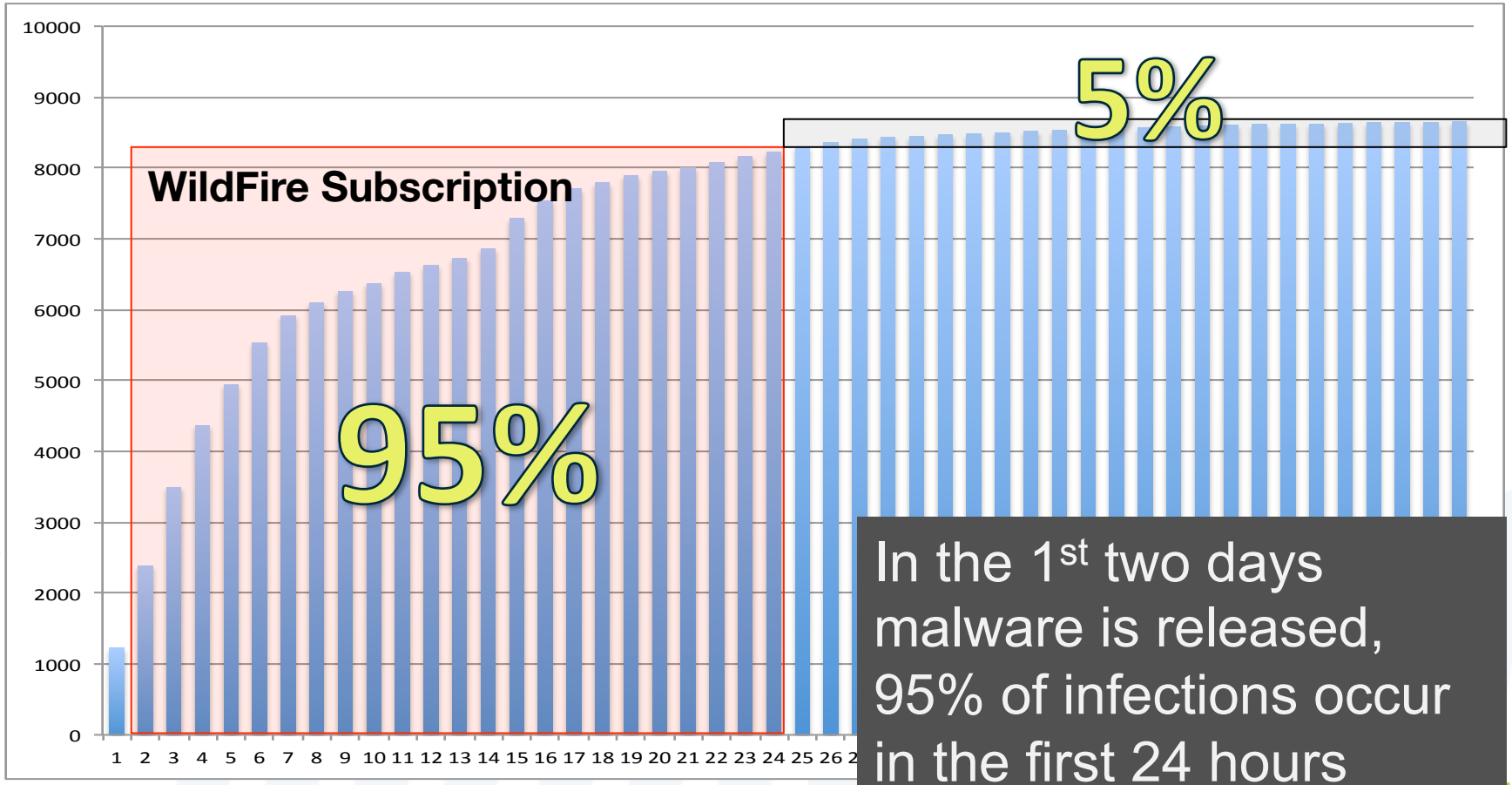
REST API for scripted file uploads



Real-World Spread of 0-Day Malware



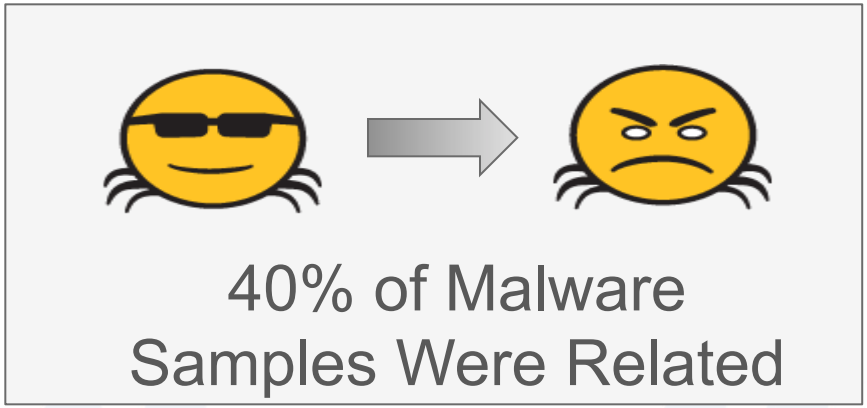
Real-World Spread of 0-Day Malware



In the 1st two days malware is released, 95% of infections occur in the first 24 hours

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

Case Study

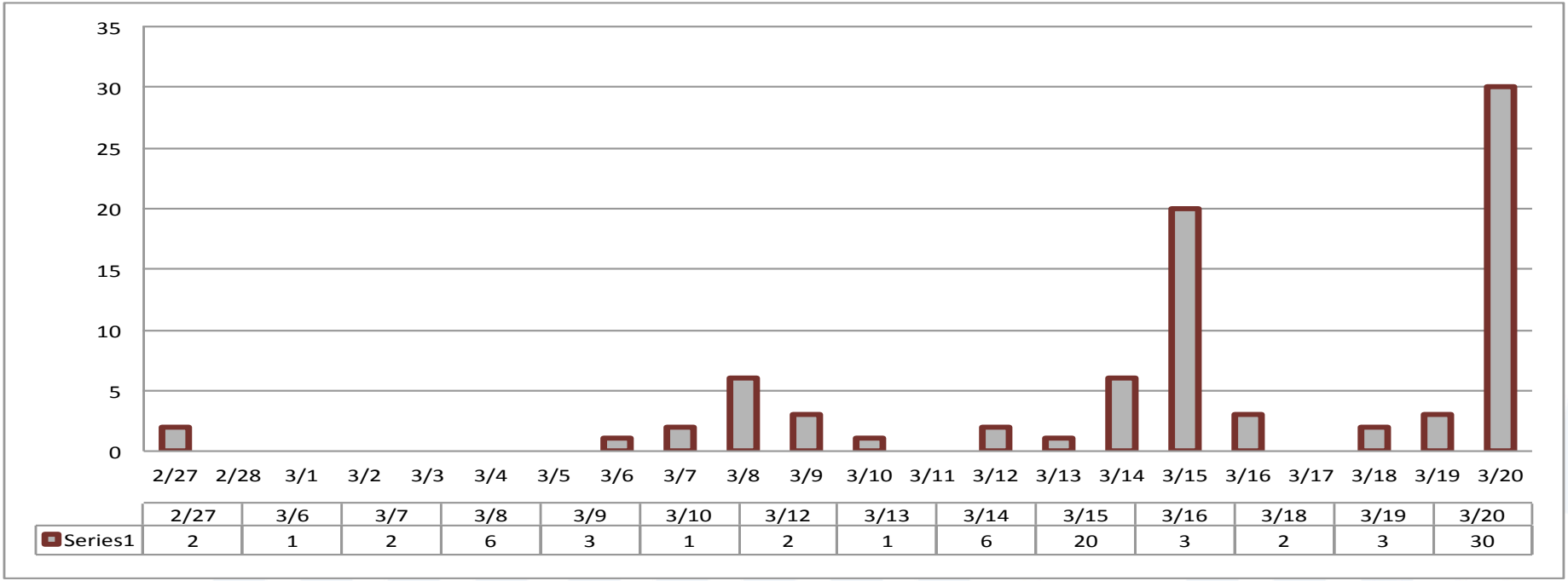
- Recent attack against South Korea using time-bombed malware that was set to wipe the Master Boot Record of an infected machine on March 20.
- Post-mortem analysis showed that we began detecting samples with WildFire on Feb 27th, and automatically generating signatures.
- The largest number of samples were collected on the day of the attack, March 20th.
- Coverage was provided within 30-60 minutes for each sample for WildFire customers.

paloalto NETWORKS

30 Minute Protection From New Malware

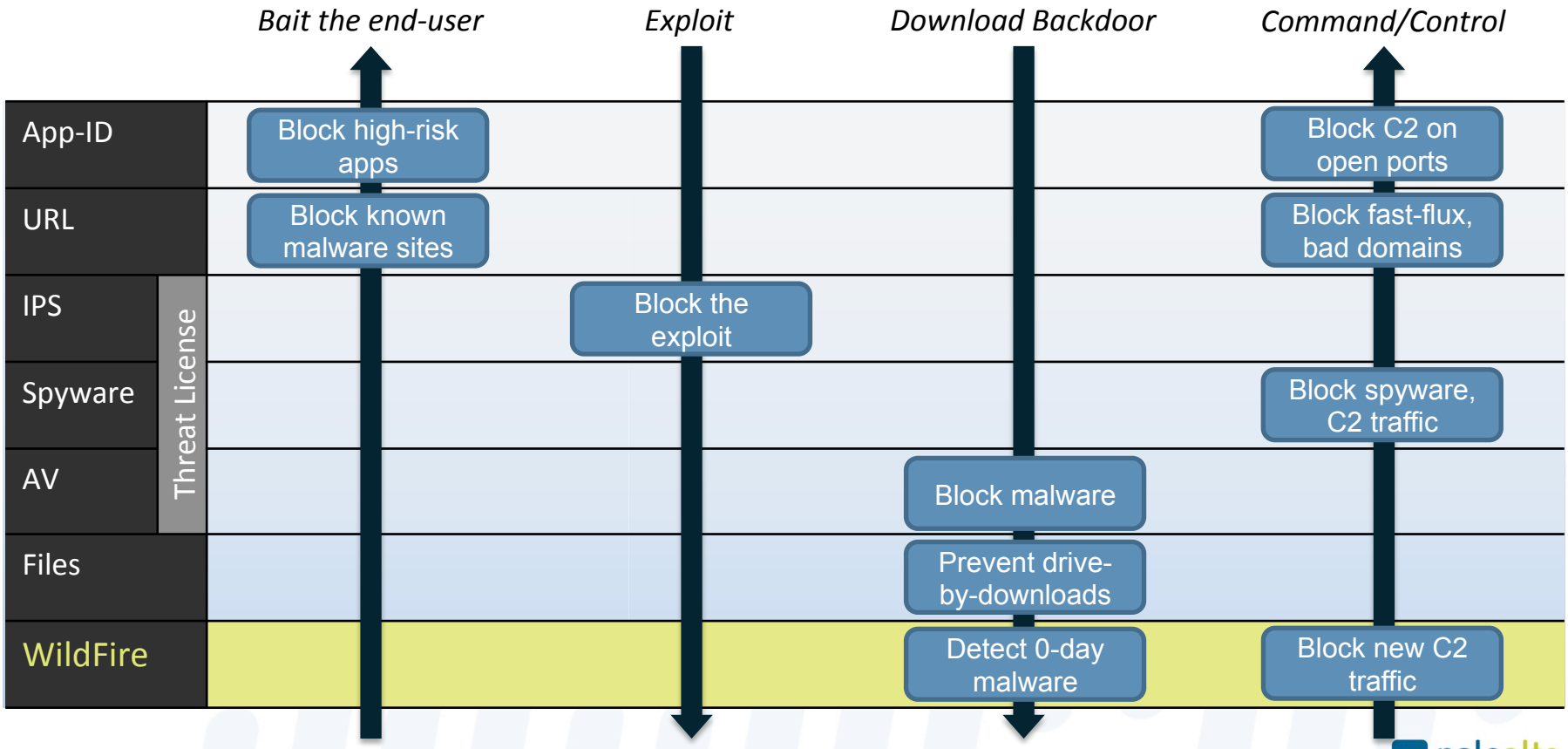
The day of the attack was the most active (fast response is crucial)

1 signature caught 15 variants = 14 infections that can be prevented



	2/27	3/6	3/7	3/8	3/9	3/10	3/12	3/13	3/14	3/15	3/16	3/18	3/19	3/20
Series1	2	1	2	6	3	1	2	1	6	20	3	2	3	30

An Integrated Approach to Threat Prevention



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.