Mind your Own Business: A Longitudinal Study of Threats and Vulnerabilities

Platon Kotzias, Leyla Bilge, Pierre-Antoine Vervier, Juan Caballero

Cyber attacks against enterprises

Vulnerabilities

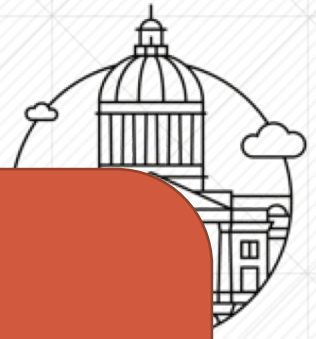
EQUIFAX

Equifax breach
basic security

LILY HAY NEWMAN SEC

EQUIFAX
EXCUSE

Malware



anta
ecover
Sam
vare

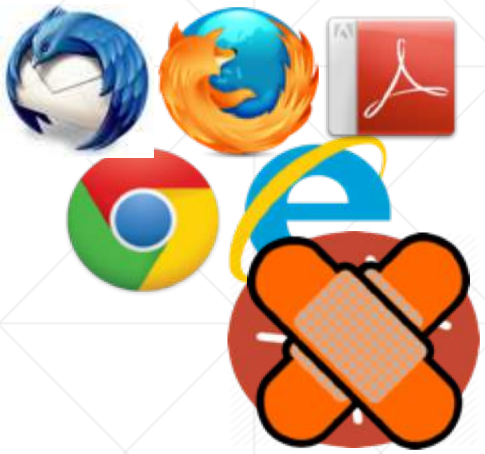
What is the security posture of enterprises?

Does the investment pays off?

Verizon partner data breach exposes millions of customer records

Accessed through an unprotected Amazon S3 storage server

Vulnerabilities and Malware



What is the patching behavior of enterprise client and server software?

What are the malware encounters?

Exploitation

Prior Work

1
enterprise

85K
hosts

4
months

[Yen et al ‘14]

28K
Enterprises

82M
hosts

~3 years

Consumers

[Nappa et al ‘15]

Servers

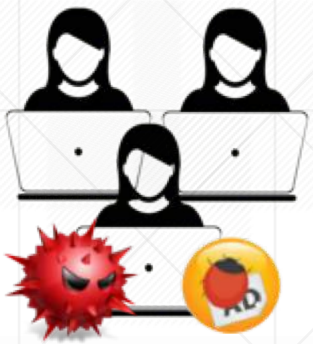
[Rescorla ’03]
[Yilek ’09]
[Durumeric et al ‘14]

In this work

Internal

External

Malware Encounters

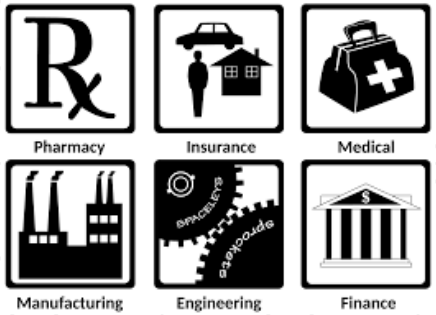


Patching Behavior

Symantec Datasets – Internal View

28K
Enterprises

82M
Hosts



67
Sectors

137
Countries

~3 years
(Apr15 - Dec17)

Public Datasets

Outside View

censys

(Oct15 – Nov17)

IPv4 scans

38 Blacklists

(Jul15 – Dec17)

Spam, Botnet infections, C&C

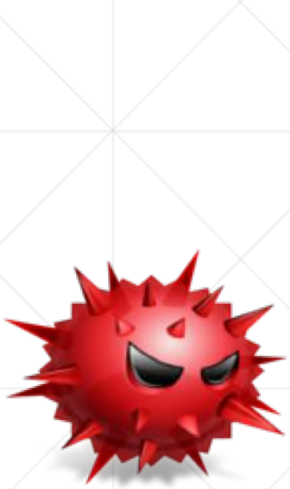
Other

NVD

(Apr15 – Dec17)

virustotal

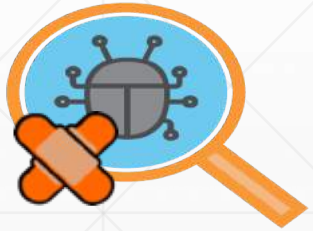
Road Map – Malware Encounters



Malware Encounters

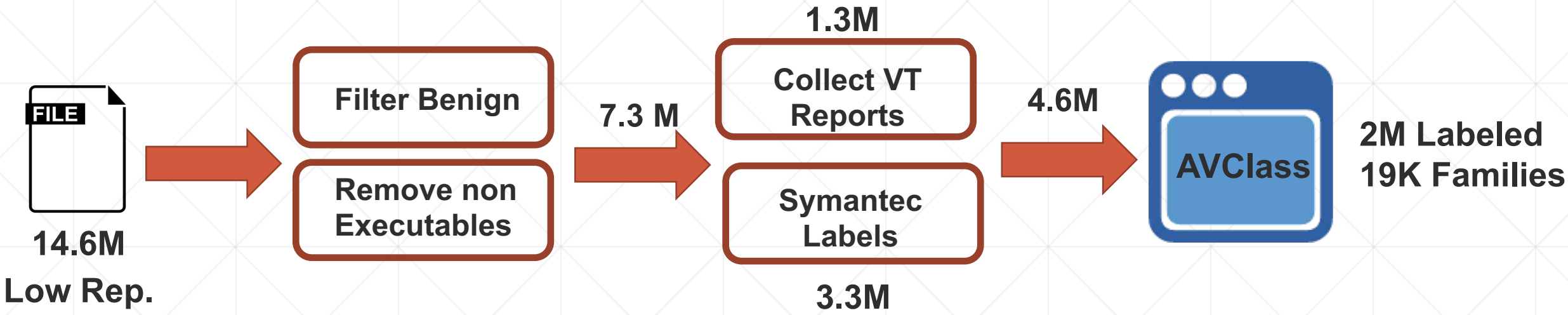
Internal

External



Patching Behavior

Family Classification



Only 27% of our queried hashes were found in VirusTotal

57% no AVClass families

Family Classification – Winactivator

Family	Type	Hosts
opencandy	pup	1.1M
winactivator	malware	470.8K
installcore	pup	453.4K
autoit	malware	398.4K
remoteadmin	pup	333K
sogou	pup	282.8K
mictraylog	pup	264K
asparnet	pup	232.8K
elex	pup	218K
donex	pup	142.3K
dealply	pup	176.5K
nssm	malware	171.2K
ramnit	malware	142.3K

34% (9.4K)
Enterprises

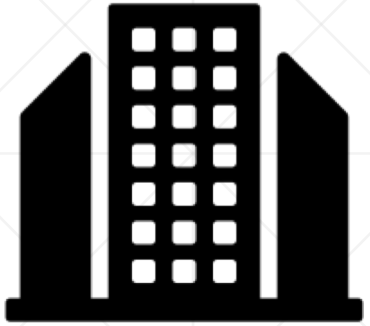
470K
Hosts

Malware and PUP prevalence

Hosts

41%

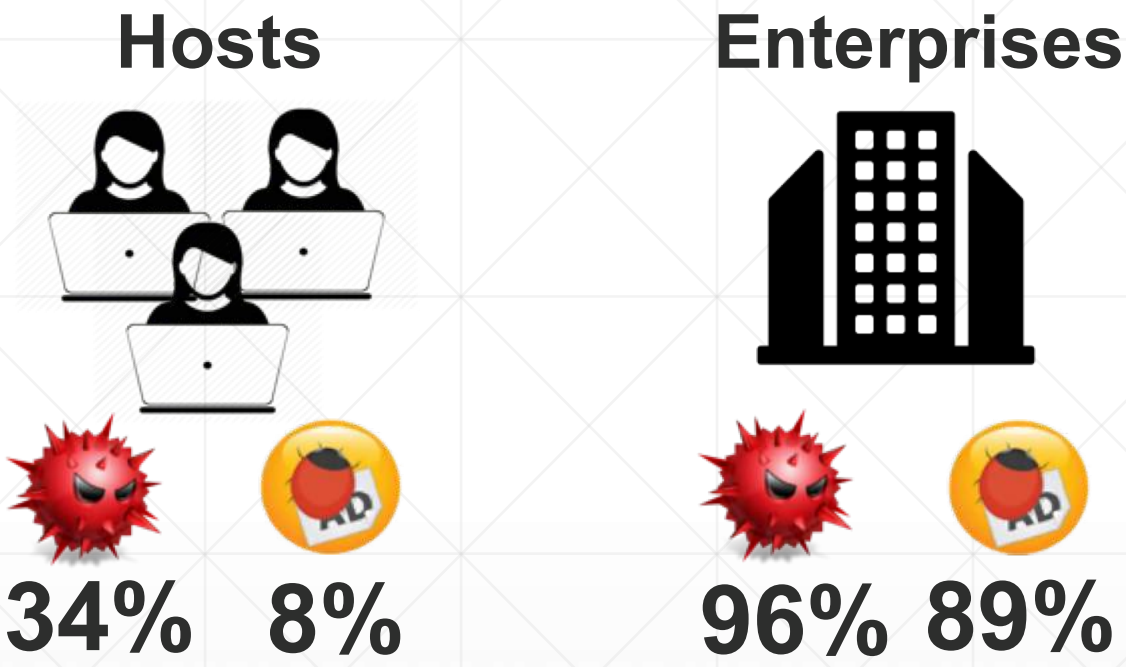
Enterprises



97%

Almost all enterprises will suffer at least one encounter in 3 years

Malware vs PUP

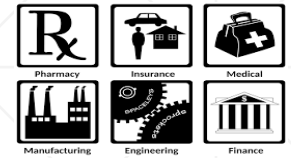


Enterprises encounter malware much more often than PUP

PUP is less prevalent in enterprise than in consumer hosts

[Kotzias et al ‘16]

Industry prevalence – Malware and PUP



67
sectors

Industry	Hosts
Banks	15.7%
Consumer Finance	15.9%
Biotechnology	20.5%
Wireless Telecommunication	28.6%

Industry	Hosts
Electrical Equipment	76.4%
Automobiles	75.5%
Construction Materials	74.4%
Marine	74.3%

Some industries are doing much better than others

4/10 least affected industries are finance-related

Ransomware Case Study – Modest prevalence

Families

22

Enterprises

31%
(8.8K)

Hosts

0.02%
(103K)

Family	Hosts	Enterprises
wannacry	30.1K	872
locky	20.3K	5.2K
petya	11.2K	155
ransomkd	10.2K	1.1K
teslascrypt	9.4K	2.9K
cryptolocker	8.7K	1.7K
cerber	6.1K	2.2K
cryptowall	2.6K	1.4K
dcryptor	2.0K	468
torrentlocker	785	443

- Wannacry (worm/ransomware):
  - Eternal Blue SMB patched in Windows 7
  - Enterprises with Windows XP affected

Outside-in Perspective

- Weekly basis
- IP blocks owned & cloud servers rented

Blacklists serve only for high-level perspective of the threat landscape

IT Services sector

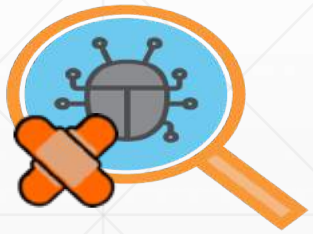
16 times more encounters from internal view

Road Map – Patching Behavior

Internal

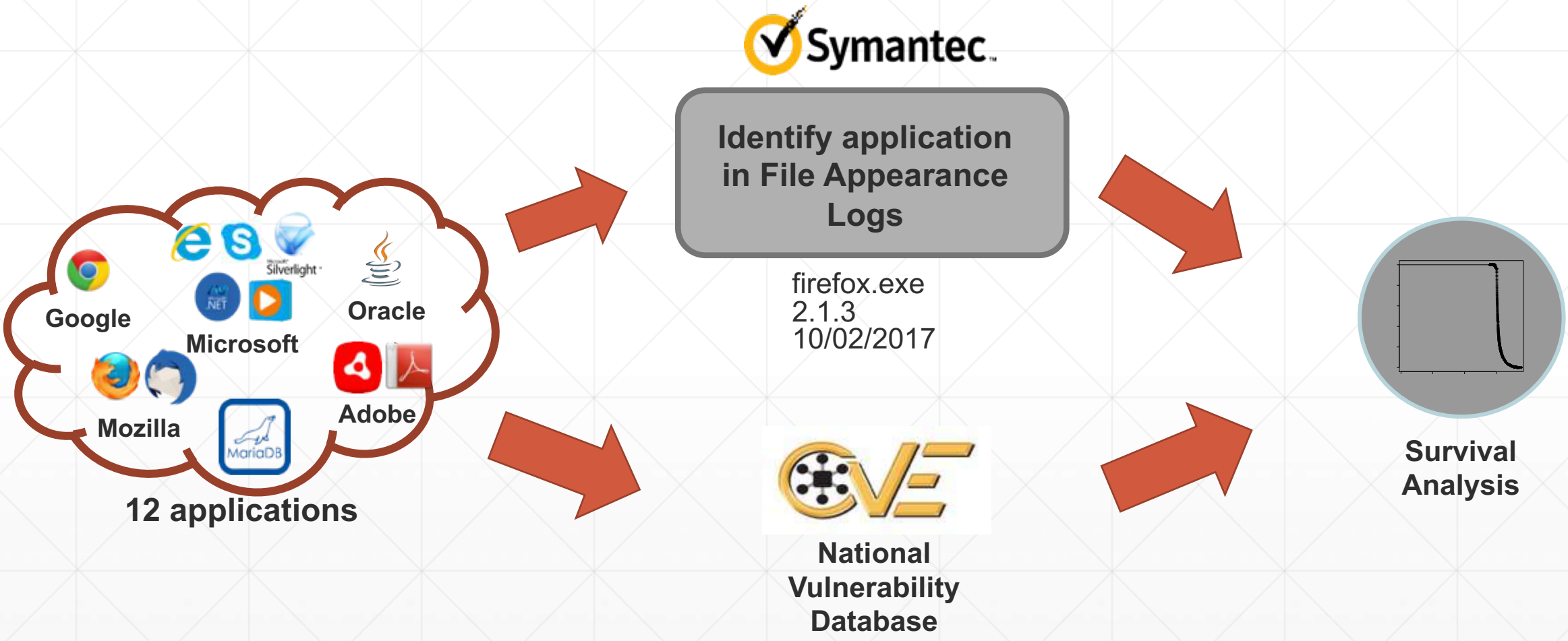
External

Malware Encounters

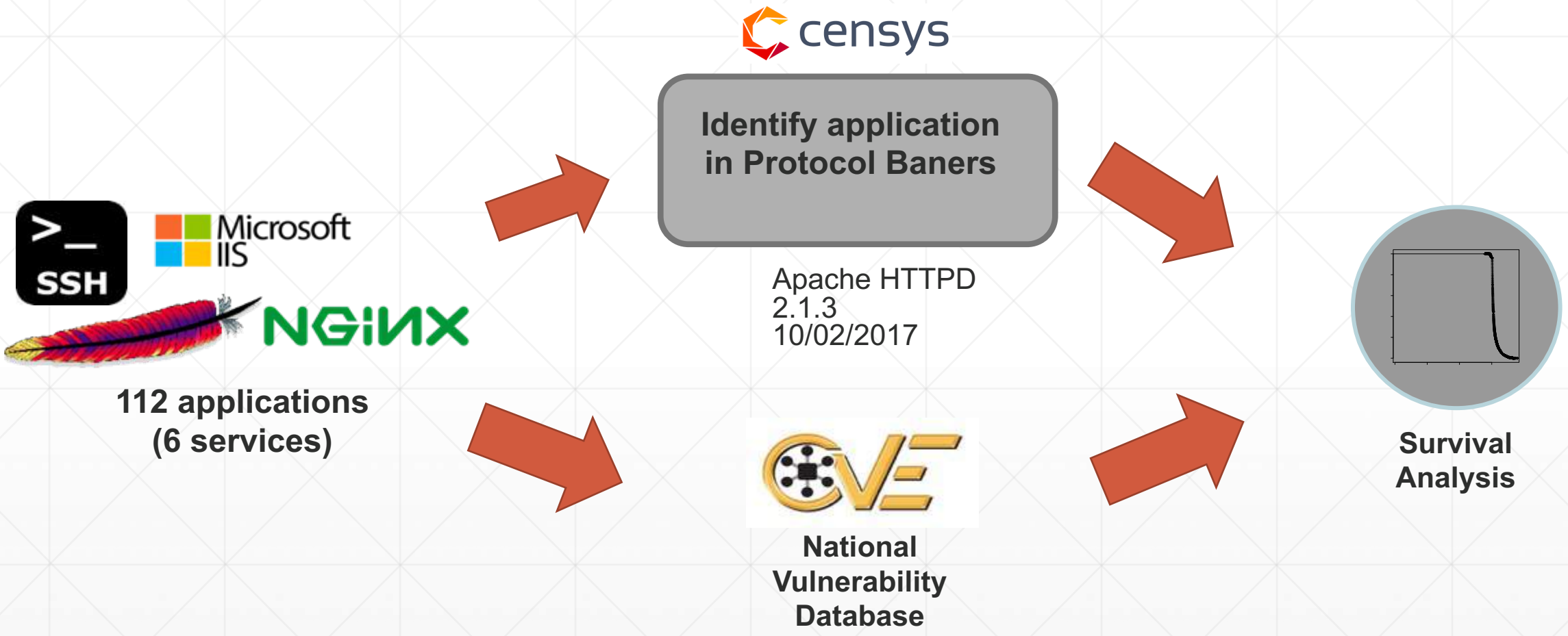


Patching Behavior

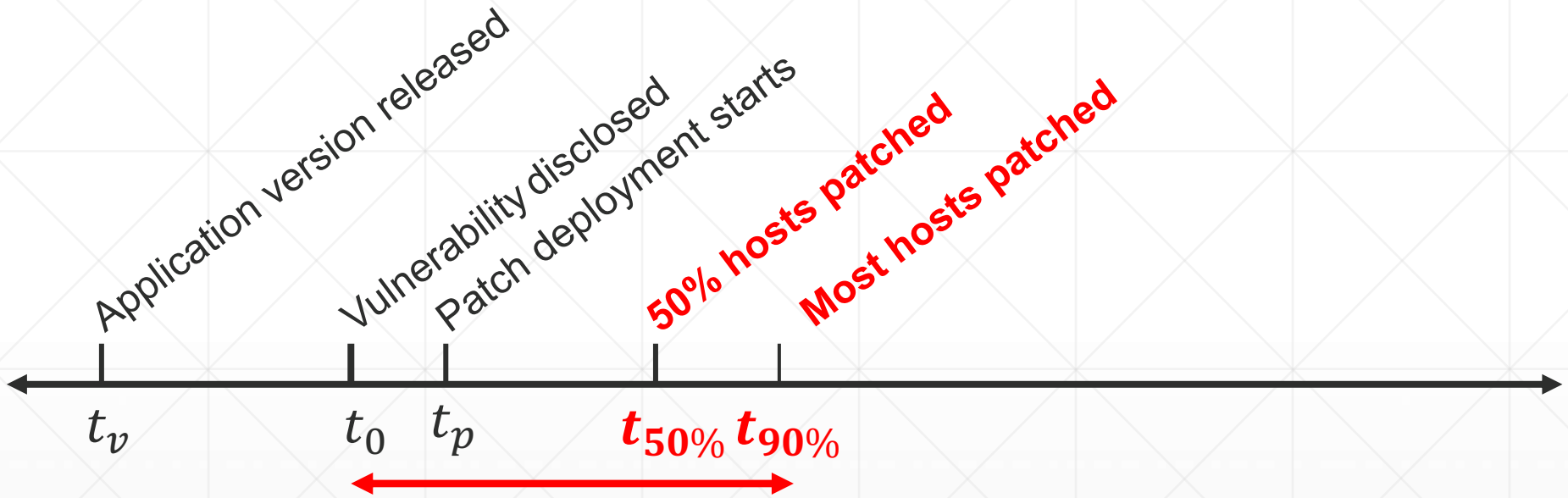
Identifying Vulnerable client applications



Identifying Vulnerable Server Applications



Vulnerability Lifecycle



Client Side Vulnerabilities – 12 Applications

Application	90% Patched (days)
Chrome	72
Skype	89
Adobe Reader	234
Media Player	314

Over **6 months** on average to patch 90% of vulnerable population across all applications

Compare with consumer hosts

[Nappa et al. ‘15]

Enterprises are slightly faster than consumers to patch applications

Server Side Vulnerabilities – Patching behavior

112 applications

233 to **575** days
for patching 90% of vulnerable hosts

216 to **287** days
for patching 90% of vulnerable hosts

282 days
for patching 90% of vulnerable hosts

200 days
for patching 90% of vulnerable hosts

Patching of enterprise clients better than enterprise servers

Key Takeaways

Malware Encounters

- Almost all enterprises should expect a malicious appearance in 3 years
- Significant differences among industries

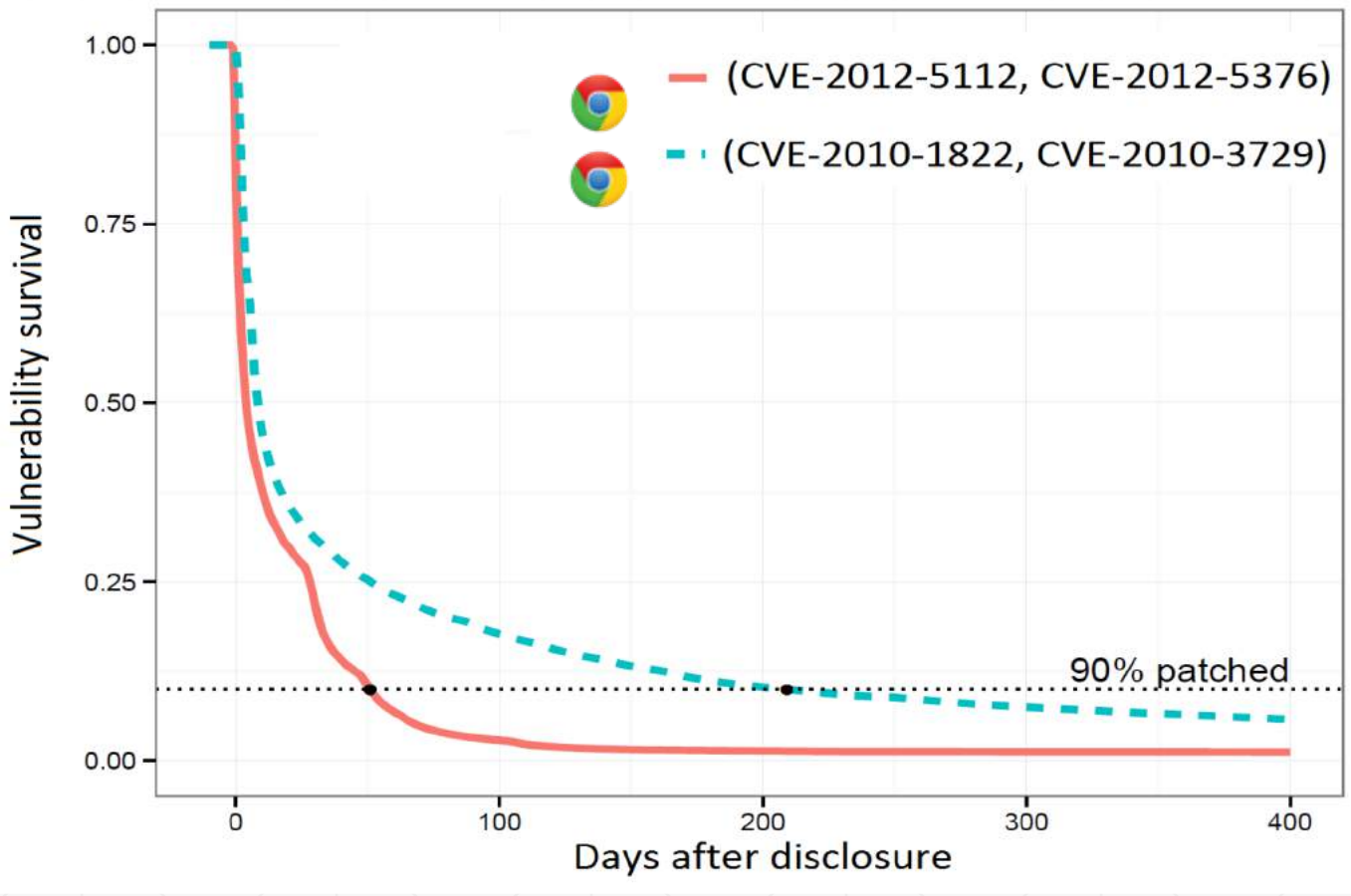
Patching Behavior

- Enterprise client patching better than consumers but still slow
- Server patching is worse than client patching

Mind your Own Business: A Longitudinal Study of Threats and Vulnerabilities

Platon Kotzias, Leyla Bilge, Pierre-Antoine Vervier, Juan Caballero

Survival Analysis



Survival Function

$$S(t) = \Pr[T < t] = 1 - F(t)$$

Patching Milestones

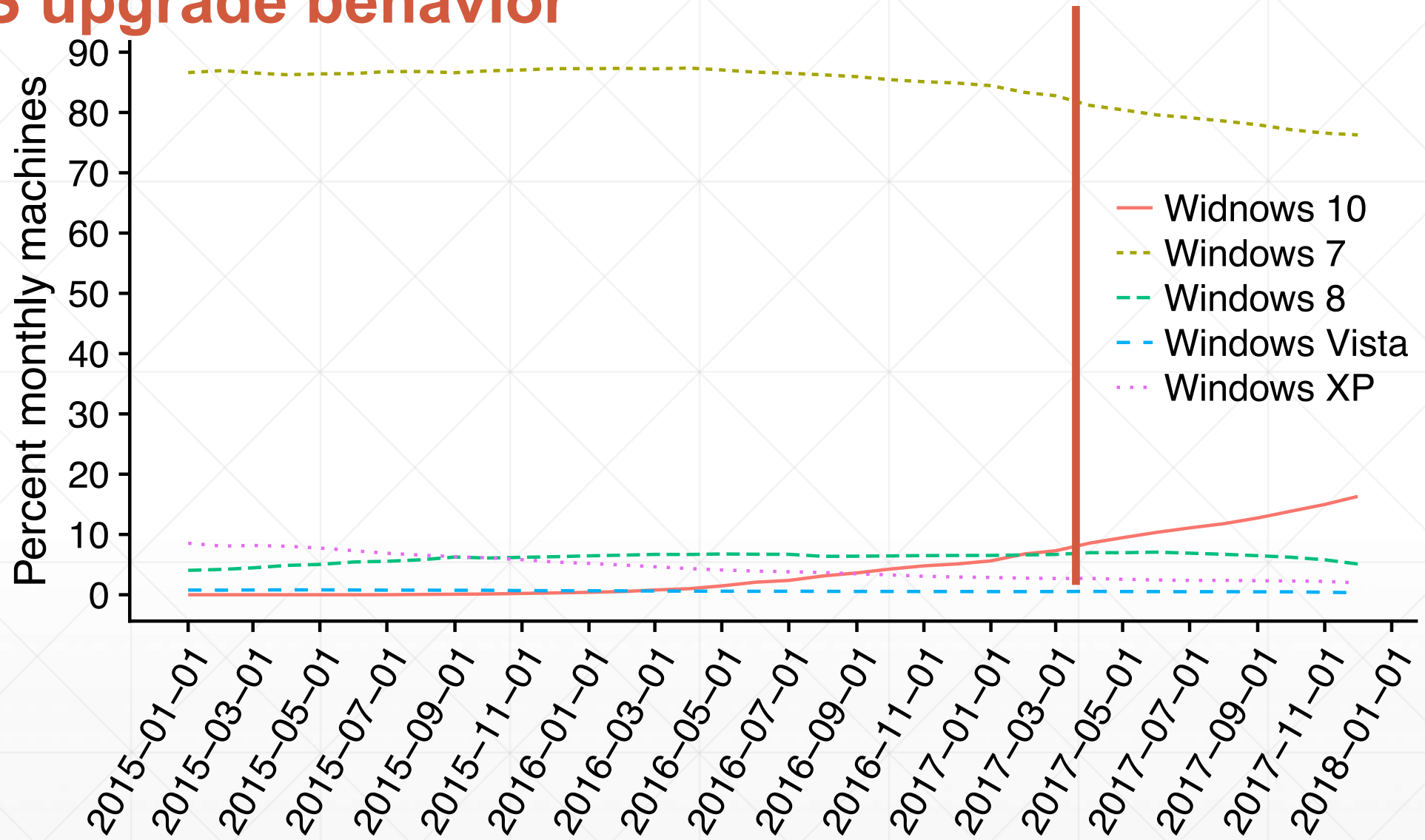
$$t_a = S^{-1}(1 - a)$$

Calculated from the inverse of the survival function

$$t_{90\%} = S^{-1}(0.1)$$

Antonio Nappa, Richard Johnson, Leyla Bilge, Juan Caballero, Tudor Dumitras, **The Attack of the Clones: A Study of the Impact of Shared Code on Vulnerability Patching**, 2015 IEEE symposium on security and privacy, 692-708

OS upgrade behavior



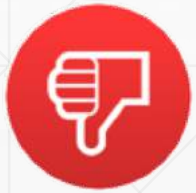
43% of enterprises with at least one Windows XP machine in 2017

Client Side Vulnerabilities – By Industry

- Using the 5 most prevalent applications (IE, Chrome, Adobe Reader, Firefox, JRE)

Industry	90% Patched
Telecommunication Services	141
Consumer Finance	152
Communications Equipment	152

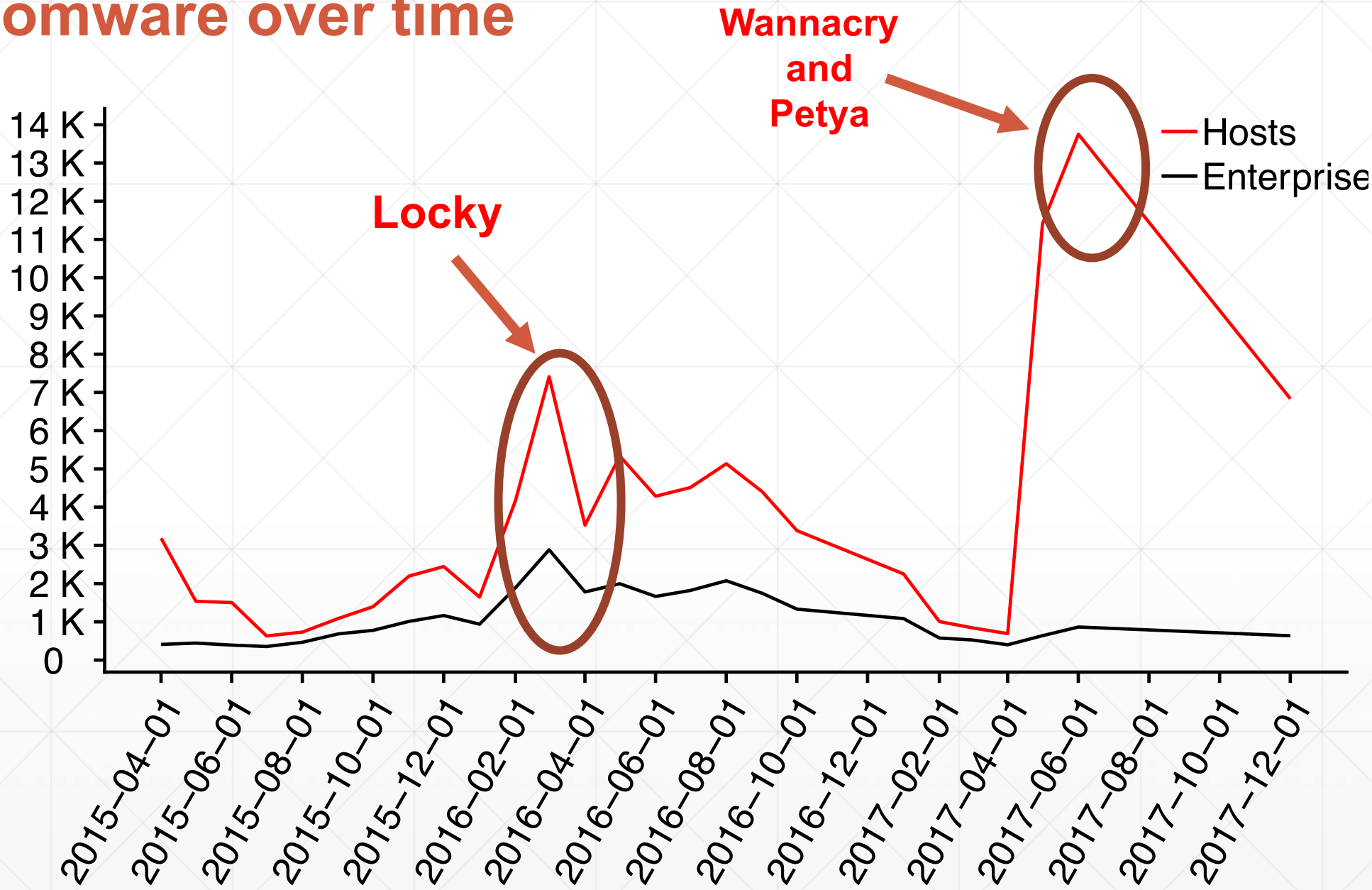
- Finance, Software and Communications are faster
- Invest more in cyber security products



Industry	90% Patched
Multiline Retail	193
Construction Materials	187
Gas Utilities	197

- Some industries are worse than consumer hosts

Ransomware over time



Client Side Vulnerabilities - Best and worst

- Compare patching time among enterprises with more than 1K hosts

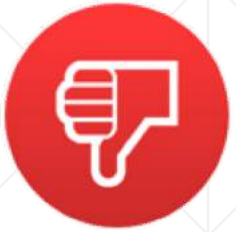
TOP 10

Patch 90% of machines in
< 10 days

Most in Financial and Insurance industry

Best patcher from the Hotels, Restaurants and Leisure industry

Bottom 10



Patch 90% of machines in
500 days

Spread in multiple industries: Media, Healthcare etc.

Worst patcher from the Capital Market industry

Best patchers have less malware encounters than worst patchers

Industry Sector Coverage – Top 15 Industries

Industry Sector	Enterprises	Hosts
Banks	1.1K	16.6M
IT Services	1.0K	7.5M
Healthcare Services	1.1K	6.5M
Professional Services	875	3.8M
Commercial Services	1.2K	3.2M
Insurance	597	3.2M
Capital Markets	851	2.0M
Software	832	2.0M
Electronic Equipment	1.0K	1.7M
Machinery	1.4K	1.5M
Specialty Retail	601	1.5M
Constructions & Engineering	1.3K	1.1M
Media	971	1.5M
Chemicals	850	1.0M
Food Procuts	846	872K