Why are systems (still) not updated after all these attacks?

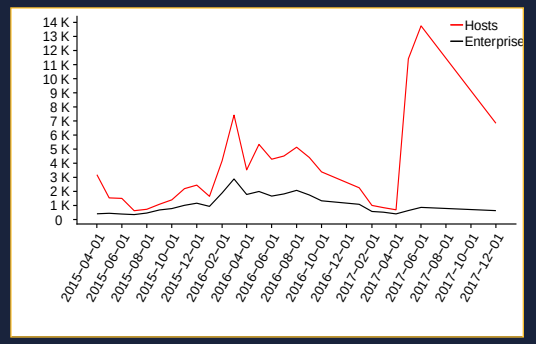
A measurement study on the enterprise security

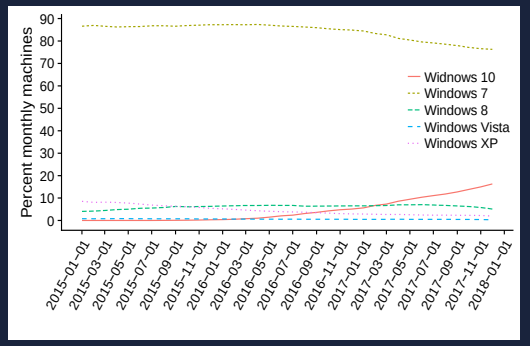
- We perform a deep investigation of enterprise threat and vulnerability landscape
  - The largest study to date, covers 3 years of data
    - Symantec Telemetry (28K enterprises, 80M machines, 69 industry sectors)
    - Public datasets (NVD, Virus Total, Censys, Blacklists)

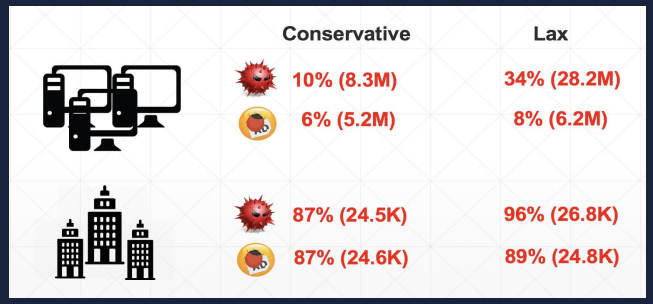
	INTERNAL	EXTERNAL
		
		

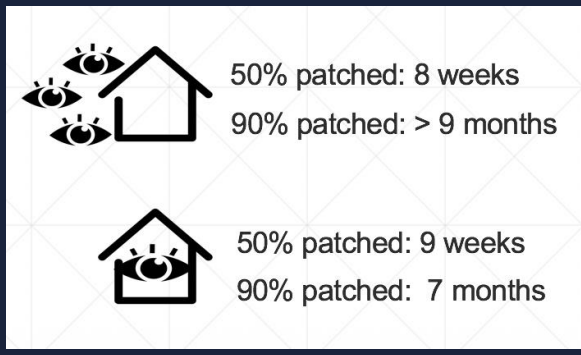
2

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









Application	50% Patched	90% Patched
Chrome	18 (<1 month)	72 (2.4 months)
Skype	17 (<1 month)	89 (~3 months)
Adobe Reader	78 (2.5 months)	234 (~ 8 months)
Media Player	147 (~5 months)	314 (10.4 months)

Industry	Hosts	Top 3 Families
Banks	15.7%	opencandy, remoteadmin, installcore
Consumer Finance	15.9%	remoteadmin, opencandy, ramnit
Biotechnology	20.5%	opencandy, staser, installcore

Industry	50% Patched	90% Patched
Communications Equipment	53	152
Consumer Finance	52	152
Diversified Financial Services	56	164

Industry	Hosts	Top 3 families
Electrical Equipment	76.4%	winactivator, opencandy, ramnit
Automobiles	75.5%	autoit, winactivator, opencandy
Construction Materials	74.4%	opencandy, remoteadmin, installcore

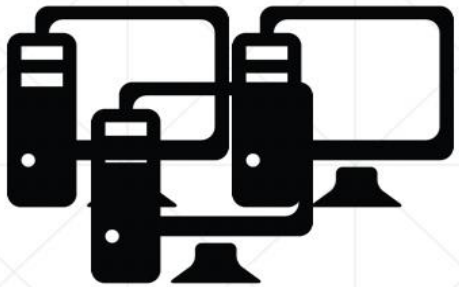
Industry	50% Patched	90% Patched
Gas Utilities	68	197
Construction Materials	66	187
Multiline Retail	61	193

Threat labeling does more harm than good!

- Inconsistencies on threat labeling among different security firms constitute a big problem in our community
  - It is hard to judge whether a particular malware family still constitutes a threat
  - Attribution becomes difficult if not impossible (the origin, the age)
  - Per-threat risk /predictive analytics becomes challenging as the accuracy of the ground-truth is questionable

Only 27% are found in VT and 57% of the signatures are generic …

Malware is still a problem!

	Conservative	Lax
	10% (8.3M)	34% (28.2M)
	6% (5.2M)	8% (6.2M)
	87% (24.5K)	96% (26.8K)
	87% (24.6K)	89% (24.8K)

All enterprises encounter malware

Industry prevalence

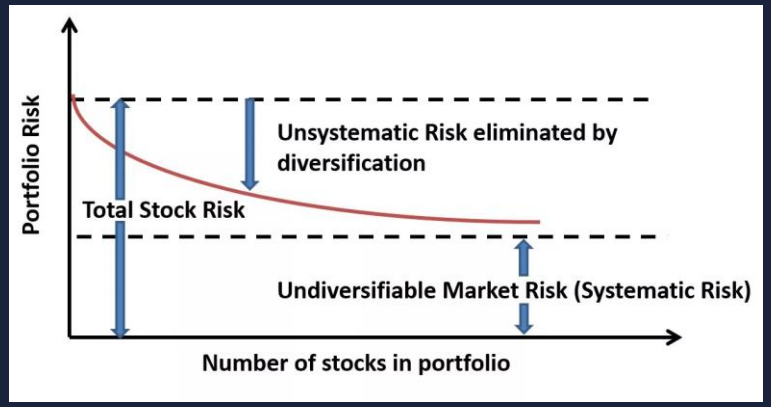
Industry	Hosts	Top 3 Families
Banks	15.7%	opencandy, remoteadmin, installcore
Consumer Finance	15.9%	remoteadmin, opencandy, ramnit
Biotechnology	20.5%	opencandy, staser, installcore

Industry	Hosts	Top 3 families
Electrical Equipment	76.4%	winactivator, opencandy, ramnit
Automobiles	75.5%	autoit, winactivator, opencandy
Construction Materials	74.4%	opencandy, remoteadmin, installcore

Industry sectors that invest on security product the most, encounter considerably less malware!

Systematic and Unsystematic Risk

- Systematic risk – market risk:
  - “Uncertainty inherent to the entire market”
  - It cannot be avoided with diversification, or behavioral changes
- Unsystematic risk:
  - “Uncertainty that comes with the company or industry you invest in”



- Mapping these concepts to the cyber domain
  - Systematic risk:
    - The threats that appear on all sectors and company types regardless of their security posture
    - It can be measured only with the volume of activities
    - Only 3 malware families that are seen in all industries, 13 families that are seen in 25% of enterprises
  - Unsystematic risk:
    - Depending on the security behavior of the company, the risk can go down or up
    - Measurements are more complicated
    - 91% of the threat families are seen in less than 5% of the enterprises

Unsystematic Risk Analytics is more appropriate for cyber security and this is good news!

Outside-in Perspective

- Detect IP addresses allocated to the enterprise
  - Get all allocated blocks from Regional Internet Registries
  - Identify cloud infrastructure:
    - Get Whois info for domains of a company
    - Passive DNS to remove IP addresses mapped to multiple IPs

- Correlate enterprise IPs with datasets of external IOCs (e.g, spam senders, C&C servers)

Outside-in analysis provides insights on successful enterprise infections

Outside-in Perspective – Industry posture

- Spam is still predominant
  - > 1.3M hosts in 3 worse industries (Media, Communication Equipment, Software)
  - Heavily monitored --> Better datasets compared to other malicious activities
- High prevalence of malware (>40K), phishing (>13K) and C&C servers (> 7K in top3)
- 4 Industries in both top 10 of malware appearances and infections
  - Software, Electronic Equipment, Commercial Services, Professional Services

Blacklists ideal for only a high-level perspective of the threat landscape

Vulnerability landscape

Identifying Vulnerable applications

12 applications

Identify versions in File Appearance Logs

National Vulnerability Database

Patch Time

112 applications (6 services)

Identify versions in protocol banners

National Vulnerability Database

1,882 Vulnerabilities: 50% Critical, 40% High Impact

Client Side Vulnerabilities – 12 Applications

- High percentage of unpatched hosts
  - **42% of the 14M** hosts with Adobe Reader

Application	50% Patched	90% Patched
Chrome	18 (<1 month)	72 (2.4 months)
Skype	17 (<1 month)	89 (~3 months)
Adobe Reader	78 (2.5 months)	234 (~ 8 months)
Media Player	147 (~5 months)	314 (10.4 months)

- It takes over 6 months to patch 90% of the population across all applications and vulnerabilities

- Enterprises are on average faster to apply patches than consumers (Nappa et al. 2008-2013)

Client Side Vulnerabilities – By Industry

- Compare patching time among industries using 5 most popular applications (IE, Chrome, Adobe Reader, Firefox, JRE)

Industry	50% Patched	90% Patched
Communications Equipment	53	152
Consumer Finance	52	152
Diversified Financial Services	56	164

- Industries that typically invest more in cyber security products

Industry	50% Patched	90% Patched
Gas Utilities	68	197
Construction Materials	66	187
Multiline Retail	61	193

- Some industries are worse than consumer hosts

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

Simplistic risk analytics that only relies on business sector as a risk factor have serious flaws!

Server Side Vulnerabilities – Patching behaviour

- Compare 112 server side applications
- Patched time → Time first observed by scans

112 applications

- From the 73.1M publicly accessible IPs
  - **24%** had at leas one vulnerable service
  - **10%** are affected by more than 15 vulnerabilities
  - **1.5M** servers in **~12K** enterprises have never been upgraded

50% patched: 8 weeks

90% patched: > 9 months

50% patched: 9 weeks

90% patched: 7 months

Popular software (Apache, OpenSSH, Microsoft IIS) needs > 10 months to patch

Server Side Vulnerabilities – Industry posture

- Compare patching time among industries using all 112 applications (6 services)
  - FTP, SSH, SMTP, HTTP(S), POP(S), IMAP(S)

Industry	50% Patched	90% Patched
Multi-Utilities	78 (2.6 months)	412 (~14 months)
Communications Equipment	159 (5.3 months)	679 (~23 months)
Thrifts and Mortgage Finance	162 (5.4 months)	705 (~23 months)

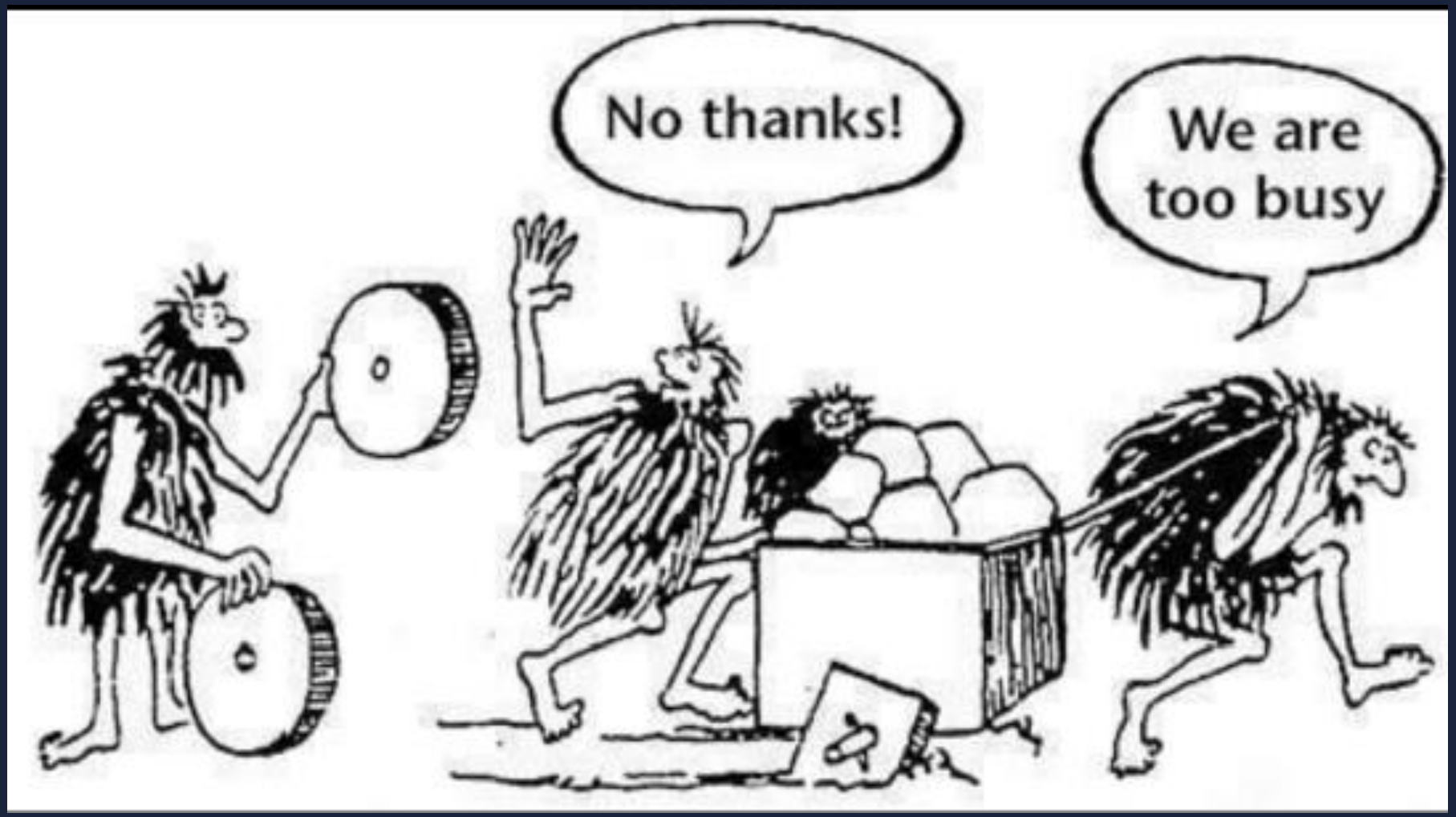
- Best patchers not so good

Industry	50% Patched	90% Patched
Energy Services	279 (~9 months)	625 (~21 months)
Transportation Infrastructure	279 (~9 months)	703 (~23 months)
Marine	292(~10 months)	691 (~23 months)

- HTTPS(S) and SSH bear the worst patch time
- Worst 10 includes critical infrastructures (Gas, Transportation, Energy)

Server patching behavior worryingly bad across all applications and services

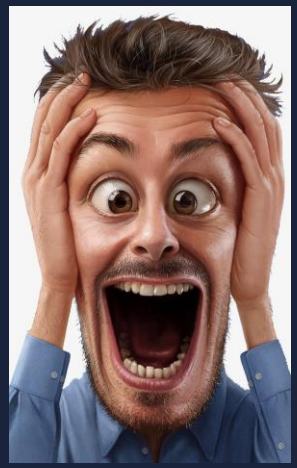
Proactive vs Reactive Behavior



Thank You!

Summary of Findings…

- All enterprises eventually encounter malware (90% - 97%)
- Only one fourth of the low reputation files are found in Virus Total
- Enterprise computers encounter very low percentages of unwanted software
  - The user behavior has significant impact on cyber risk
- Industry sectors that invest on security product the most, encounter considerably less malware (15% vs 70%)
- Vulnerability patching still a very important issue in enterprise settings
  - To patch 90% of the population it takes at average 6 months
- There are many malware and PUP families only seen in one or a small number of industries, potentially indicating targeting of those industries.



Client Application Patching Window

						Unpatched	Enterprise PT		Consumer PT [32]	
Program	**Vendor**	**Versions**	**Hosts**	**Enterprises**	**CVE**	**Hosts**	**50%**	**90%**	**50%**	**90%**
Chrome	Google	267	10.2M	23,814	454	1.7M	18	78	15	246
Firefox	Mozilla	205	4.2M	20,575	308	1.1M	25	161	36	179
Thunderbird		10	159K	6,132	40	15K	23	98	27	129
Skype	Microsoft	41	1.1M	18,120	2	8K	17	89	-	-
Internet Explorer		1,035	15.8M	24,543	428	11M	47	138	-	-
.NET		197	8.5 M	22,474	21	2.5M	60	162	-	-
Silverlight		43	8.9M	22,763	17	5M	82	182	-	-
Media Player		141	9.5M	22,700	1	7.5M	147	314	-	-
JRE	Oracle	340	5.7M	22,367	21	1.4M	56	141	-	-
Air	Adobe	11	1.2M	15,136	316	216K	44	152	-	-
Reader		47	13.9M	23,563	221	6.2M	78	234	188	219
MariaDB	-	35	13.5K	1,106	53	3K	75	246	-	-
	TOTAL	2,372	23M	25,367	1,882	AVG	67	200		

Server Apps Patching Window

Rank	Program	Service	Vulnerable			Patch Time			Avg. Vul. Window
			Machines	Ent.	CVEs	Avg.	50%	90%	
1	OpenSSH	SSH	4,517,497	10,764	84	96	22	317	132
2	Apache Httpd	HTTP	2,691,805	10,655	182	108	24	323	165
3	Microsoft IIS	HTTP	2,690,361	13,738	22	140	32	552	208
4	Lighttpd	HTTP	1,133,379	908	26	78	15	233	88
5	vsftpd	FTP	825,480	2,045	5	59	7	216	89
6	mini_httpd	HTTP	810,859	349	2	89	15	253	111
7	Nginx	HTTP	413,911	4,890	14	175	162	346	191
8	ProFTPD	FTP	266,929	2,427	27	70	7	287	106
9	Apache Coyote	HTTP	208,213	2,834	1	168	71	575	241
10	Exim	SMTP	52,260	1,867	13	135	16	480	211
				Total 112 Apps.		108	56	282	230