THE KNOWN UNKNOWNS

& OUTBIDDING CYBERCRIMIMALS

Dr. Stefan Frei

@stefan_frei

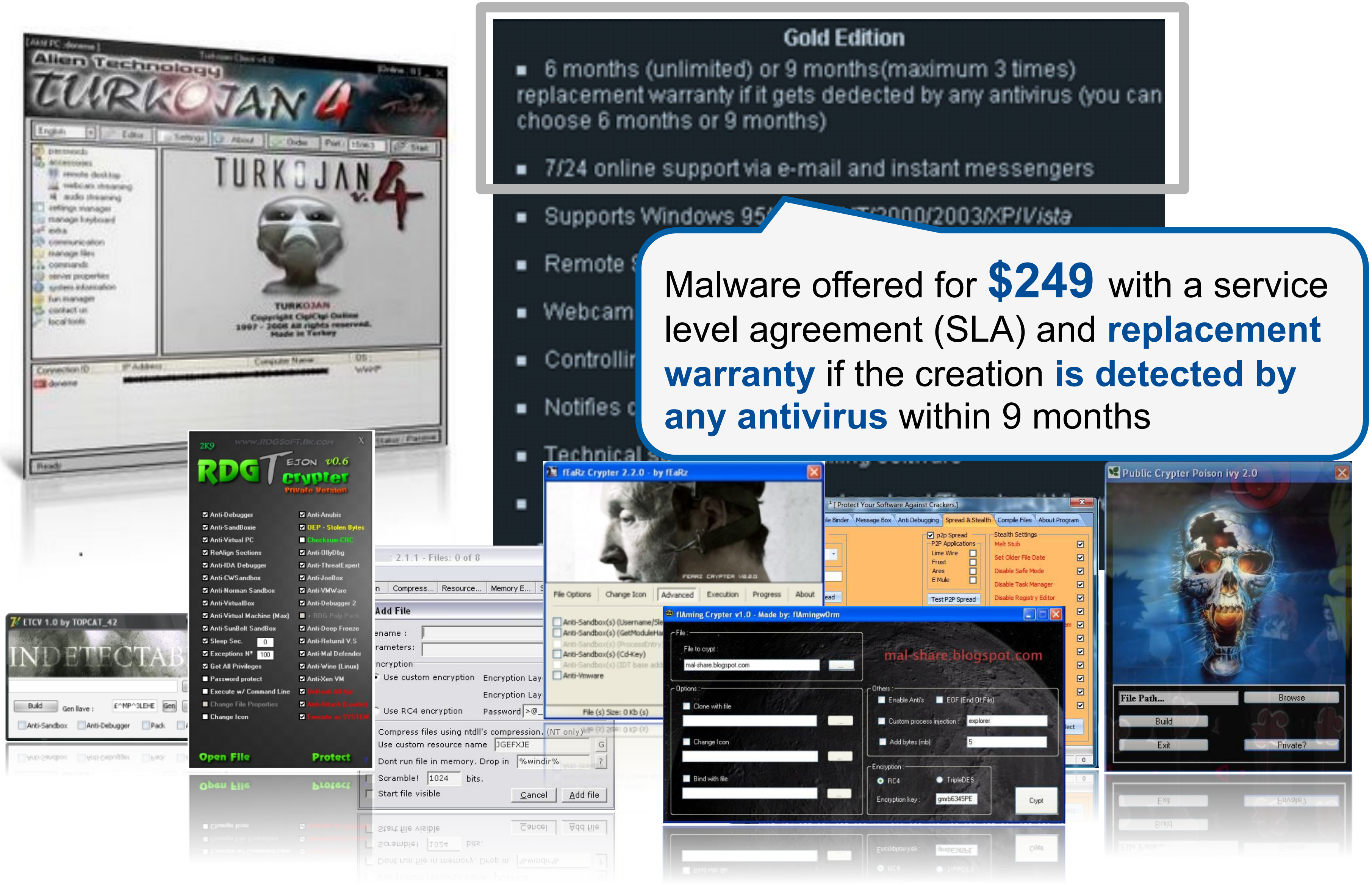
frei@techzoom.net

Throughout history, new technologies have revolutionized crime and warfare alike

- Chariot ..
- Gunpowder ..
- Tanks ..

Criminals proofed repeatedly to be very fast adopters of new technology

Thriving Underground Market



Gold Edition

- 6 months (unlimited) or 9 months(maximum 3 times) replacement warranty if it gets dedected by any antivirus (you can choose 6 months or 9 months)
- 7/24 online support via e-mail and instant messengers
- Supports Windows 95/ T/2000/2003/XP/Vista
- Remote
- Webcam
- Controllin
- Notifies
- Technical

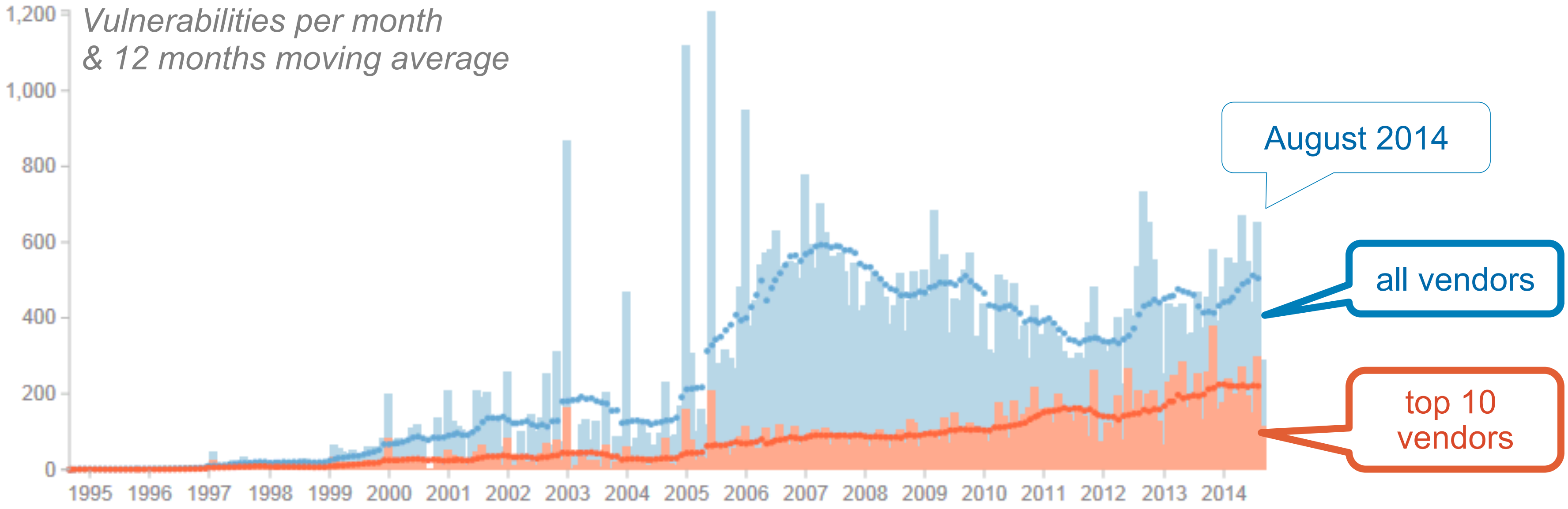
Malware offered for **$249** with a service level agreement (SLA) and **replacement warranty** if the creation **is detected by any antivirus** within 9 months information about

security vulnerabilities

has become a

valuable asset

Two decades of security investment ..

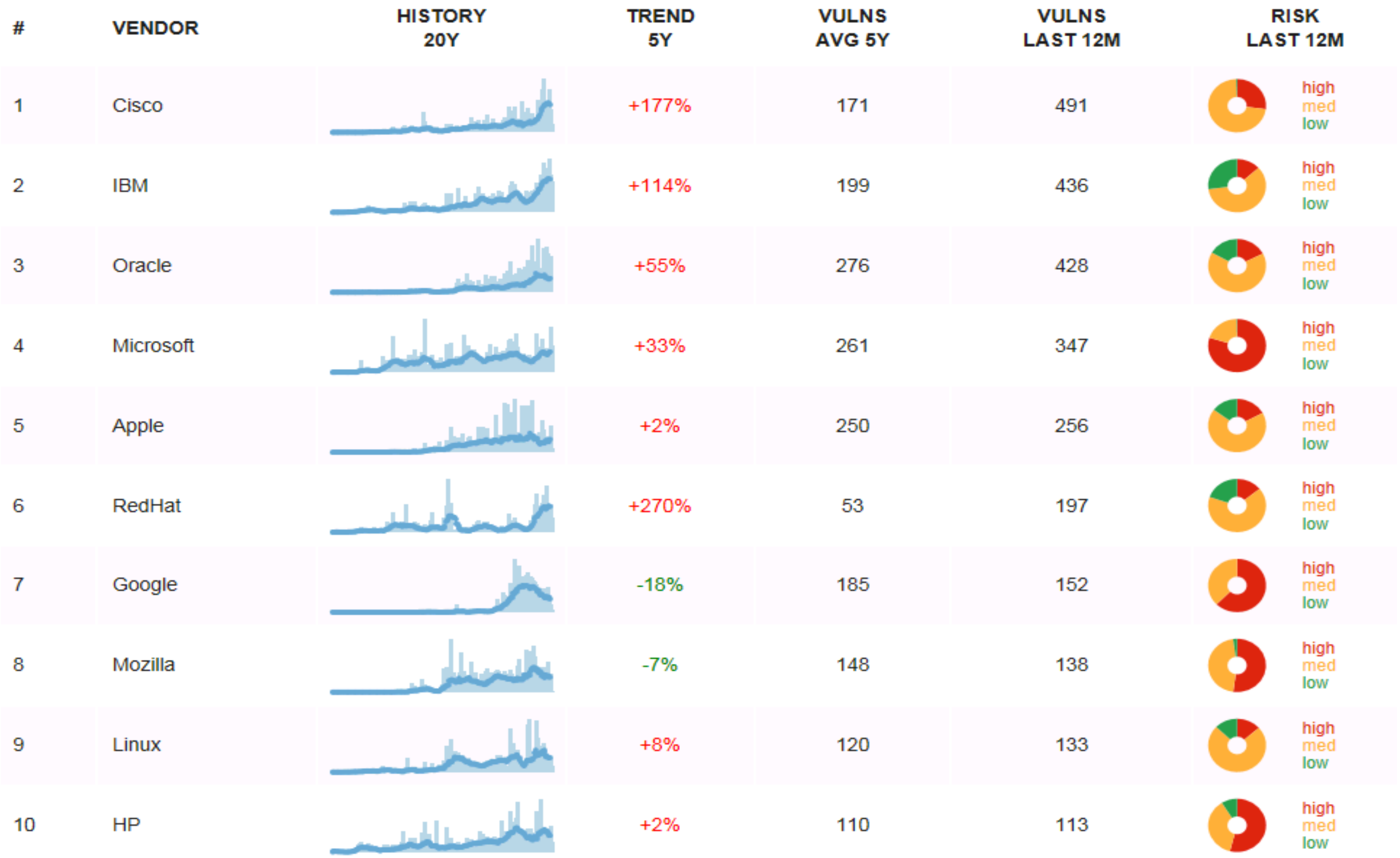


The top ten vendors *Cisco, IBM, Oracle, Microsoft, Apple, RedHat, Google, Mozilla, Linux, HP* account for more than 44 percent of all vulnerabilities published in the last 12 months.

Data source: http://www.techzoom.net/BugBounty/SecureSoftware

Long term trend

Five year average vs. last year

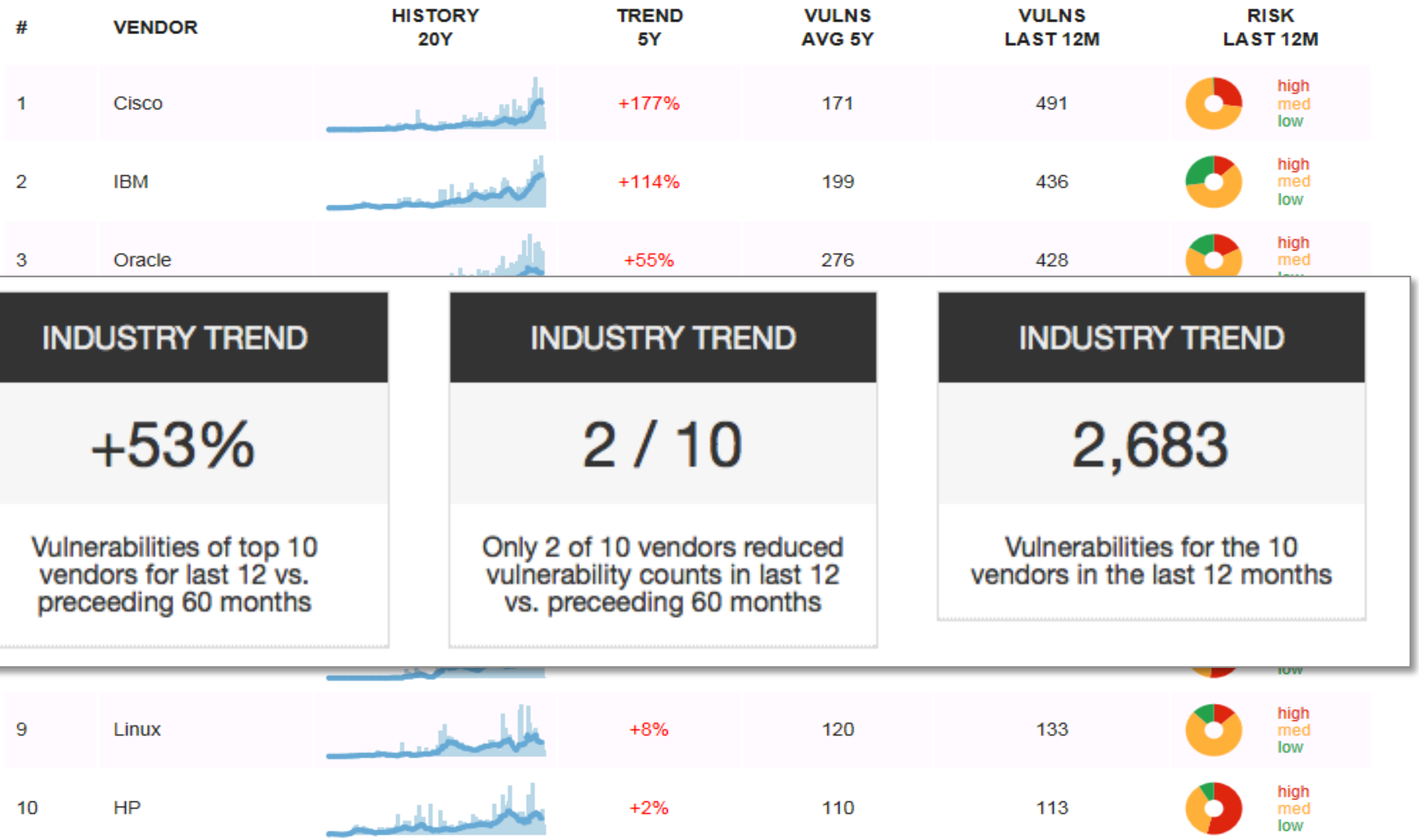


#	VENDOR	HISTORY 20Y	TREND 5Y	VULNS AVG 5Y	VULNS LAST 12M	RISK LAST 12M
1	Cisco		+177%	171	491	high med low
2	IBM		+114%	199	436	high med low
3	Oracle		+55%	276	428	high med low
4	Microsoft		+33%	261	347	high med low
5	Apple		+2%	250	256	high med low
6	RedHat		+270%	53	197	high med low
7	Google		-18%	185	152	high med low
8	Mozilla		-7%	148	138	high med low
9	Linux		+8%	120	133	high med low
10	HP		+2%	110	113	high med low

Data source: http://www.techzoom.net/BugBounty/SecureSoftware

Long term trend

Five year average vs. last year



#	VENDOR	HISTORY 20Y	TREND 5Y	VULNS AVG 5Y	VULNS LAST 12M	RISK LAST 12M
1	Cisco		+177%	171	491	high med low
2	IBM		+114%	199	436	high med low
3	Oracle		+55%	276	428	high med
9	Linux		+8%	120	133	high med low
10	HP		+2%	110	113	high med low

INDUSTRY TREND

+53%

Vulnerabilities of top 10 vendors for last 12 vs. preceeding 60 months

INDUSTRY TREND

2 / 10

Only 2 of 10 vendors reduced vulnerability counts in last 12 vs. preceeding 60 months

INDUSTRY TREND

2,683

Vulnerabilities for the 10 vendors in the last 12 months

Data source: http://www.techzoom.net/BugBounty/SecureSoftware

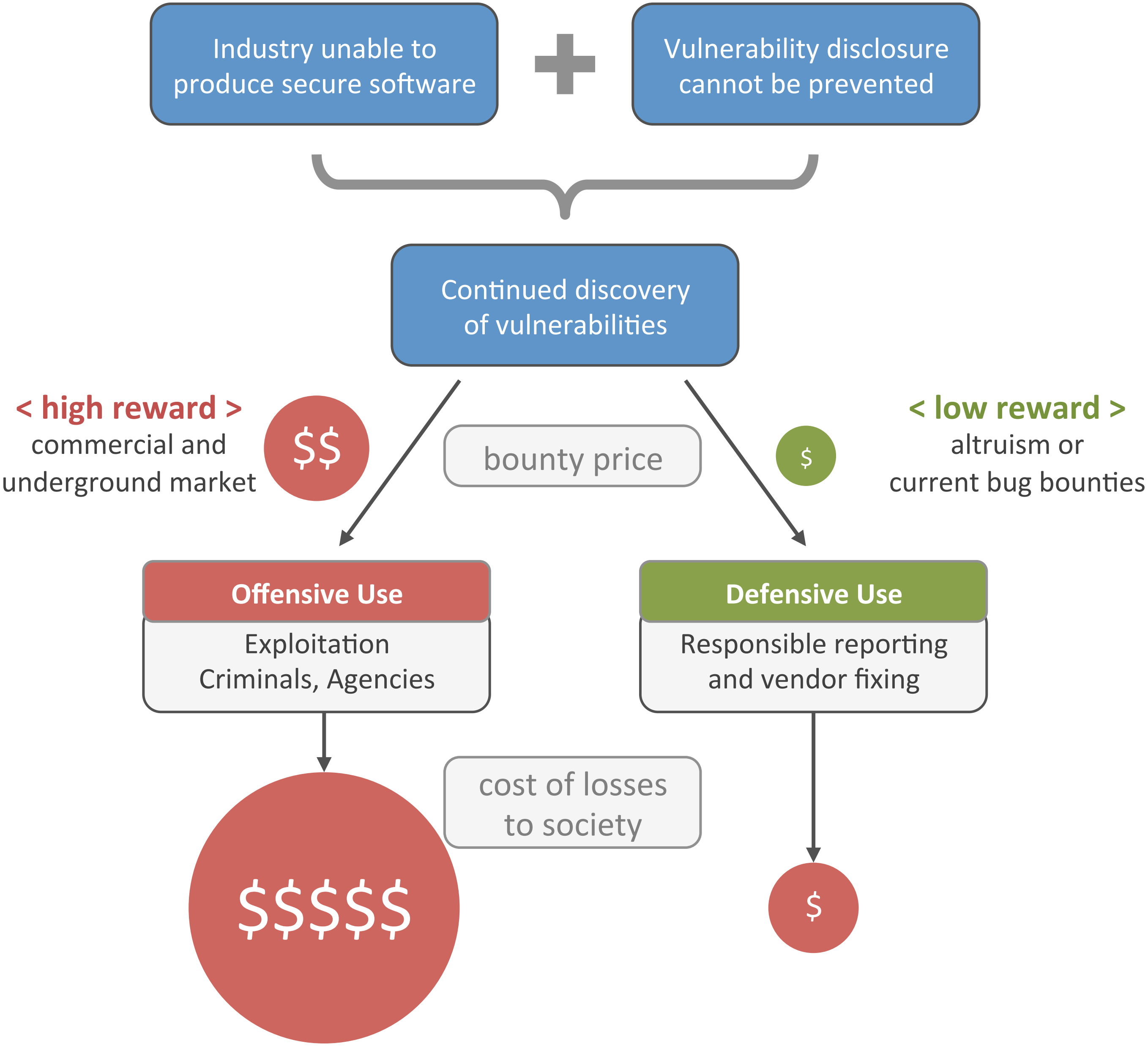
Vulnerabilities known only to **privileged closed groups** such as ..

Cyber Criminals

Brokers

Government Agencies

.. pose a **real** and **present risk** to all who use the affected software



Industry unable to produce secure software

Vulnerability disclosure cannot be prevented

Continued discovery of vulnerabilities

< high reward >
commercial and
underground market

$$

bounty price

$

< low reward >
altruism or
current bug bounties

Offensive Use
Exploitation
Criminals, Agencies

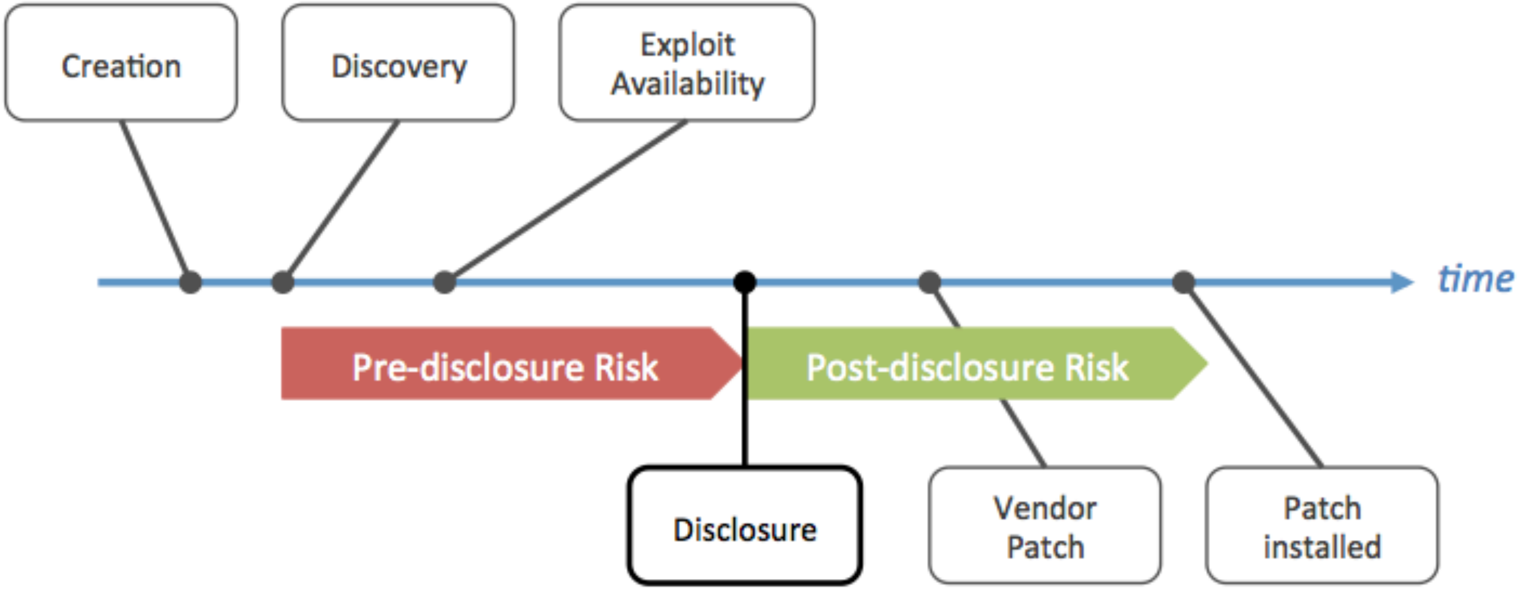
Defensive Use
Responsible reporting
and vendor fixing

$$$$$

cost of losses
to society

$

Lifecycle of a Vulnerability



The

Known Unknowns

vulnerabilities known to privileged groups only

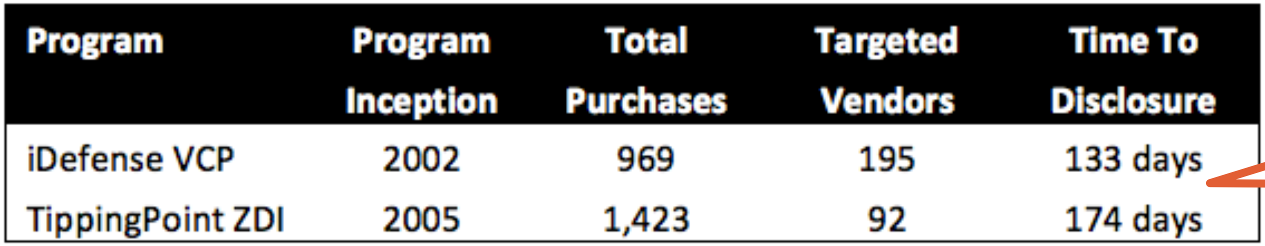
How many?

Unknown for how long?

How to measure?

Vulnerability Purchase Programs

Data of two vulnerability purchase programs covering 1,855 vulnerabilities from 2002 - 2013 allow the reconstruction of the vulnerability lifecycle after publication



Program	Program Inception	Total Purchases	Targeted Vendors	Time To Disclosure
iDefense VCP	2002	969	195	133 days
TippingPoint ZDI	2005	1,423	92	174 days

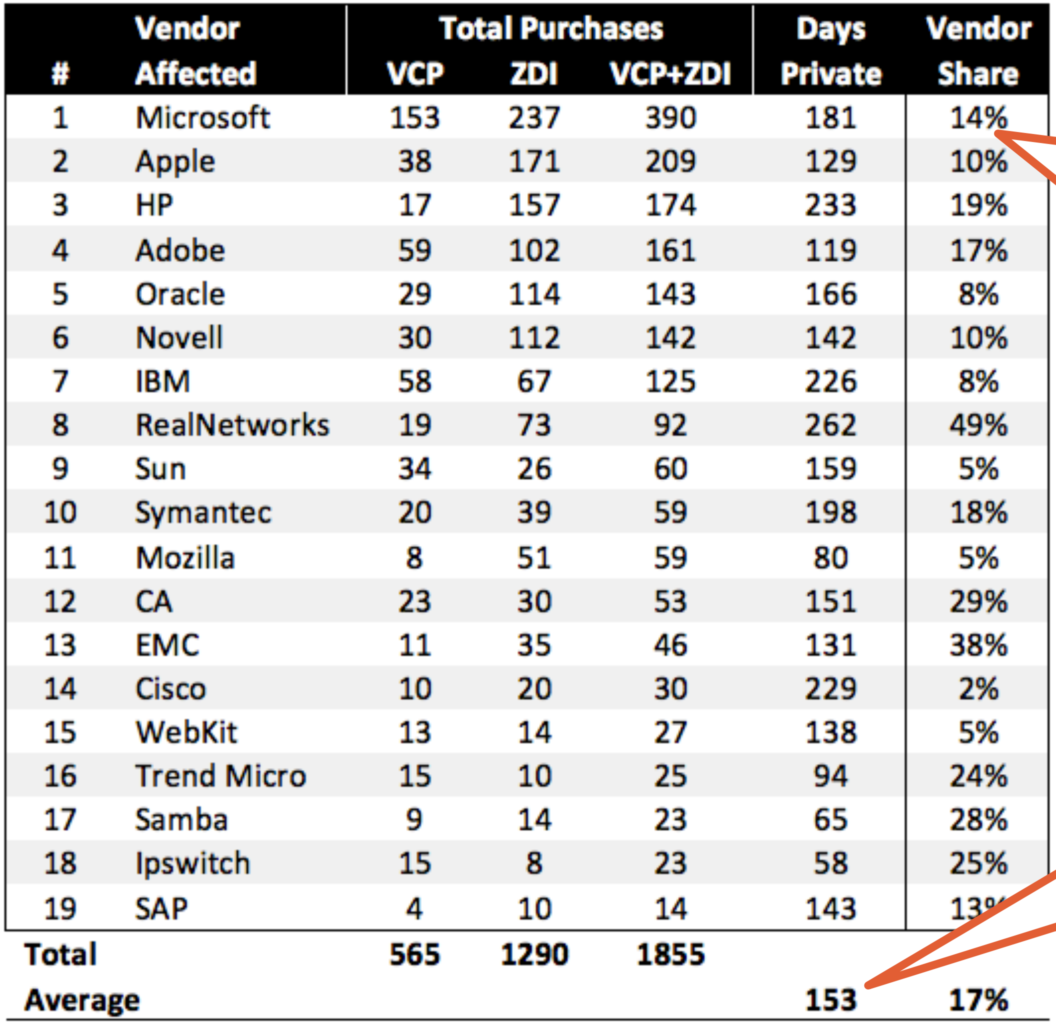
Pre-disclosure risk

These programs coordinate vulnerability information with the software vendor!

VERISIGN iDefense Vulnerability Contributor Program (VCP)

ZERO DAY INITIATIVE TippingPoint Zero Day Initiative (ZDI)

Relevant targets, considerable exposure



#	Vendor Affected	Total Purchases			Days	Vendor
		VCP	ZDI	VCP+ZDI	Private	Share
1	Microsoft	153	237	390	181	14%
2	Apple	38	171	209	129	10%
3	HP	17	157	174	233	19%
4	Adobe	59	102	161	119	17%
5	Oracle	29	114	143	166	8%
6	Novell	30	112	142	142	10%
7	IBM	58	67	125	226	8%
8	RealNetworks	19	73	92	262	49%
9	Sun	34	26	60	159	5%
10	Symantec	20	39	59	198	18%
11	Mozilla	8	51	59	80	5%
12	CA	23	30	53	151	29%
13	EMC	11	35	46	131	38%
14	Cisco	10	20	30	229	2%
15	WebKit	13	14	27	138	5%
16	Trend Micro	15	10	25	94	24%
17	Samba	9	14	23	65	28%
18	Ipswitch	15	8	23	58	25%
19	SAP	4	10	14	143	13%
Total		565	1290	1855		
Average					153	17%

14%

of all Microsoft vulnerabilities reported through a purchase program

153 days

from purchase to patch availability

Purchase programs …

- cover a considerable share of a vendors' vulnerabilities
- despite offering low prices compared to the "black market"

Exposure to "Known Unknowns"

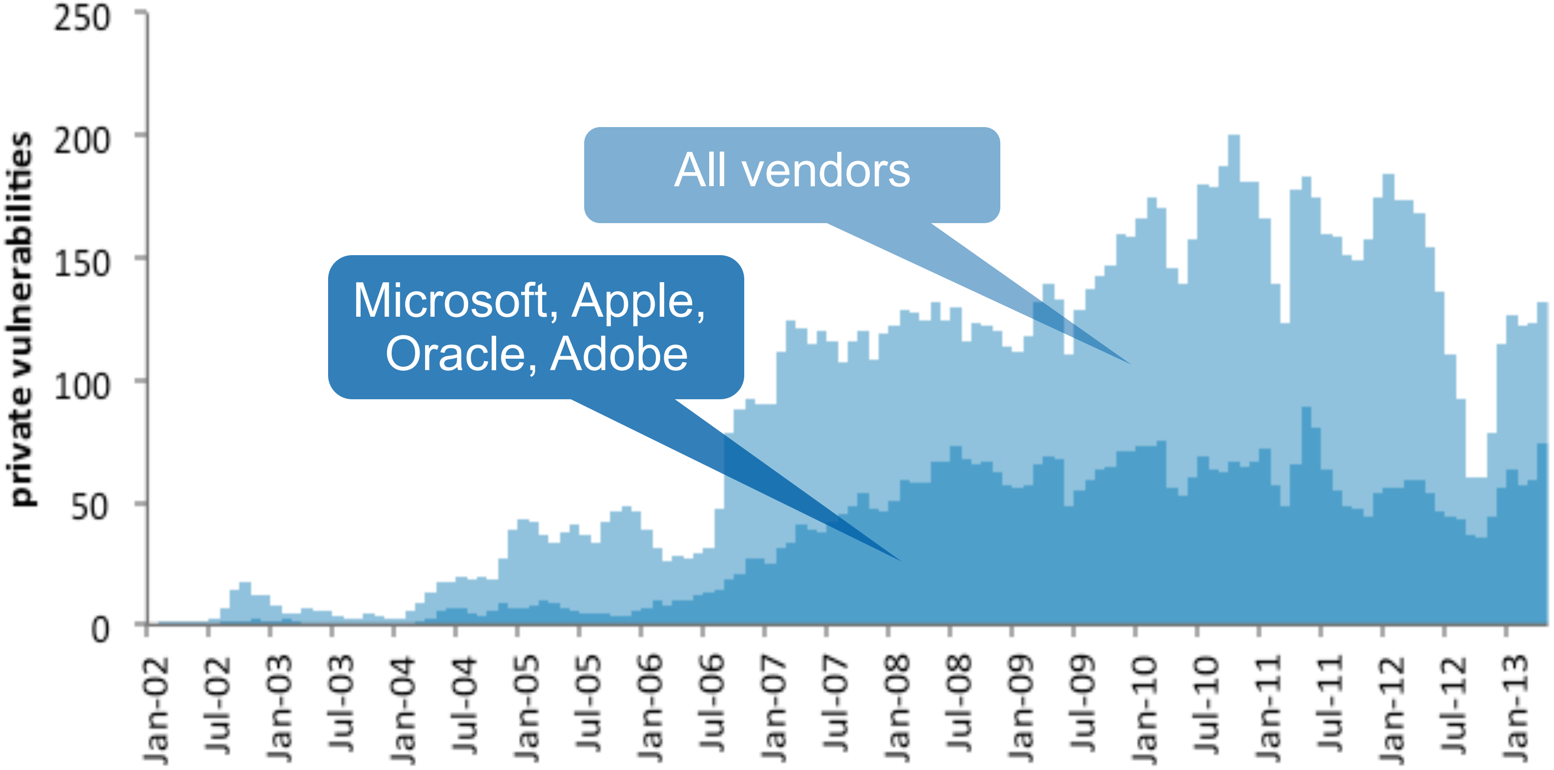
How many yet unpublished vulnerabilities are known to purchase programs exclusively ..

at any given day in the last years?

153 vulnerabilities known only to VCP and ZDI on any given day between 2010 and 2013

# of known unknowns, average per day

58 of which target Microsoft, Apple, Oracle, and Adobe



VCP & ZDI inform the vendor in order to release a patch

average exposure time: **153 days**

Critical vulnerabilities are available in considerable quantities for private groups, for extended periods and for a relatively low price

When the vendor is not informed about new vulnerabilities

average 0-day attack persists **312 days**

More Unknowns

Our measurement provides a **minimum estimate** of the known unknowns
(… criminals and government agencies don't share data)

What about vulnerabilities and exploits that are not publicly traded, and are definitively not coordinated with the software vendor?

- Boutique Exploit Providers
- Governments & Defense Contractors
- Commercial Security Consulting

ENDGAME.

[Re]Vuln

VUPEN security

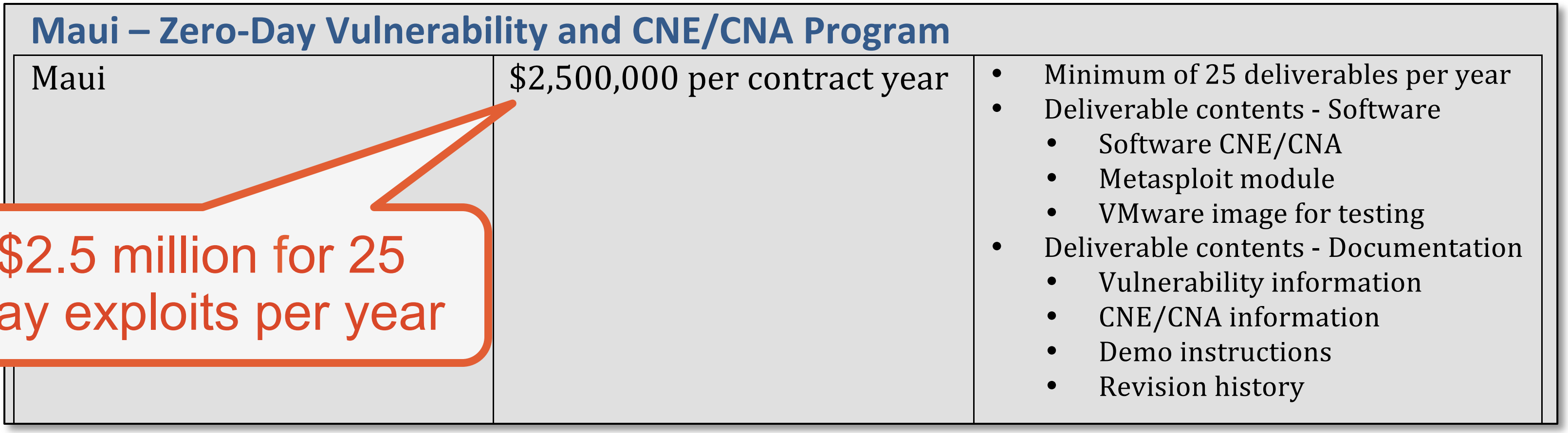
EXODUS INTELLIGENCE

Vulnerability & Exploit Providers

An increasing number of commercial players offer zero-day exploits for their subscribers:

- they do not reveal their clients
  (big buyers reportedly include government agencies)
- have a keen interest in a long pre-disclosure time
  (keep the zero-day private as long as possible)
- some firms restrict their clientele
  (by country, specific agencies)
- price for exploits between USD $40k and $160k

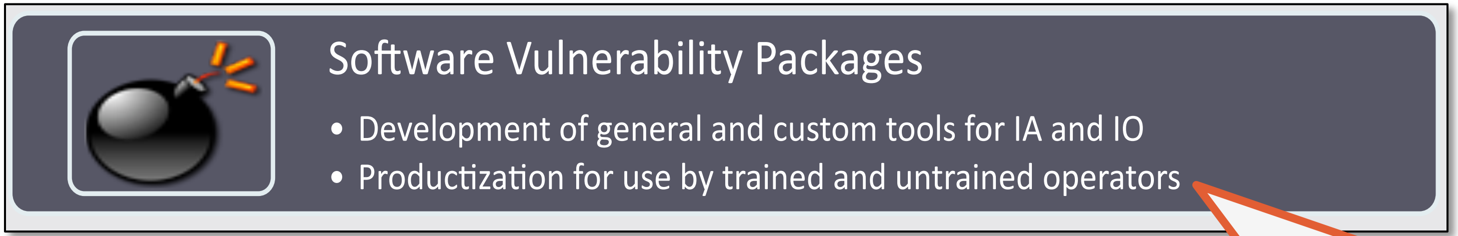
Shopping List



Maui – Zero-Day Vulnerability and CNE/CNA Program

Maui	$2,500,000 per contract year	• Minimum of 25 deliverables per year • Deliverable contents - Software • Software CNE/CNA • Metasploit module • VMware image for testing • Deliverable contents - Documentation • Vulnerability information • CNE/CNA information • Demo instructions • Revision history

USD $2.5 million for 25 zero-day exploits per year



Software Vulnerability Packages

- Development of general and custom tools for IA and IO
- Productization for use by trained and untrained operators

.. for use by trained and untrained operators

Challenge to Society

Our security depends largely on ethical researchers reporting vulnerabilities under the practices of coordinated disclosure for free

At the same time, the black market is expanding rapidly and offering large rewards for the same information

"Never was so much owed by so many to so few."

Winston Churchill's famous 1940 wartime speech

Cyber Crime Losses

Yearly losses due to cyber crime are estimated between

10 to 400 billion USD

Vulnerabilities are the root cause of considerable part of these losses

What if ..

.. we would purchase all vulnerabilities and report them to the vendor for remediation?

for USD

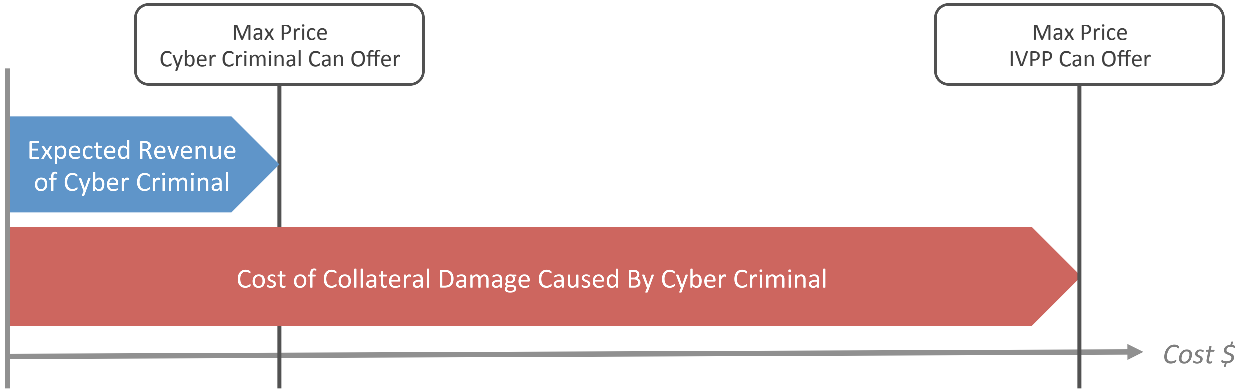
150,000.-

per vulnerability?

Online Cost Calculator
http://www.techzoom.net/BugBounty/EconomicsGlobal

We can outbid criminals

Buying vulnerabilities makes sense as long as the purchase cost is less than the cost of the prevented losses


Max Price
Cyber Criminal Can Offer
Max Price
IVPP Can Offer
Expected Revenue of Cyber Criminal
Cost of Collateral Damage Caused By Cyber Criminal
Cost $

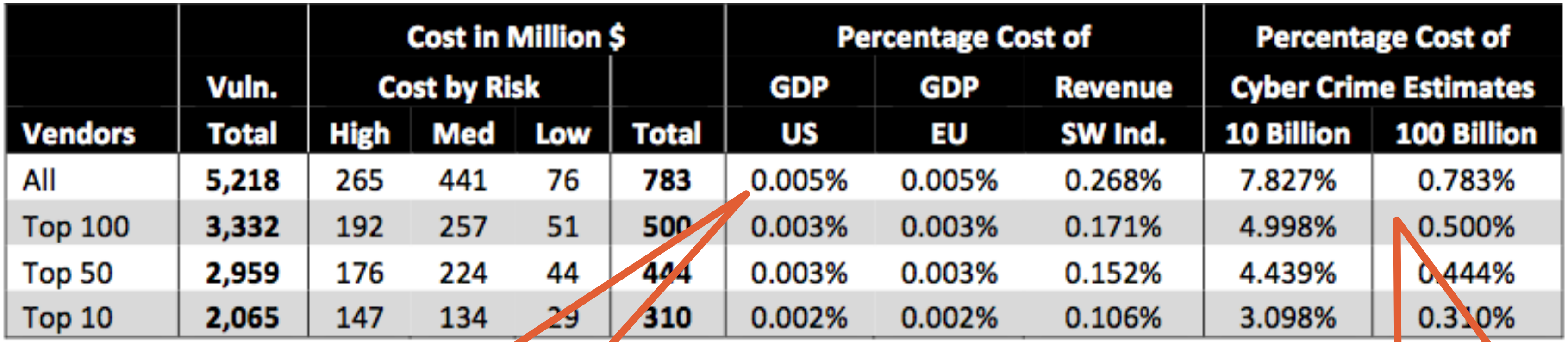
Vulnerability abuse incurs large collateral damage, exceeding criminals revenue

International Vulnerability Purchase Program

What would it cost society to buy all vulnerabilities from all vendors for USD 150,000 each?

This includes buying all non-critical vulnerabilites

Cost of buying all vulnerabilities in 2012



		Cost in Million $				Percentage Cost of			Percentage Cost of	
	Vuln.	Cost by Risk				GDP	GDP	Revenue	Cyber Crime Estimates	
Vendors	Total	High	Med	Low	Total	US	EU	SW Ind.	10 Billion	100 Billion
All	**5,218**	265	441	76	**783**	0.005%	0.005%	0.268%	7.827%	0.783%
Top 100	**3,332**	192	257	51	**500**	0.003%	0.003%	0.171%	4.998%	0.500%
Top 50	**2,959**	176	224	44	**444**	0.003%	0.003%	0.152%	4.439%	0.444%
Top 10	**2,065**	147	134	29	**310**	0.002%	0.002%	0.106%	3.098%	0.310%

less than
0.01%
of the **GDP** of the **US** or the **European Union**

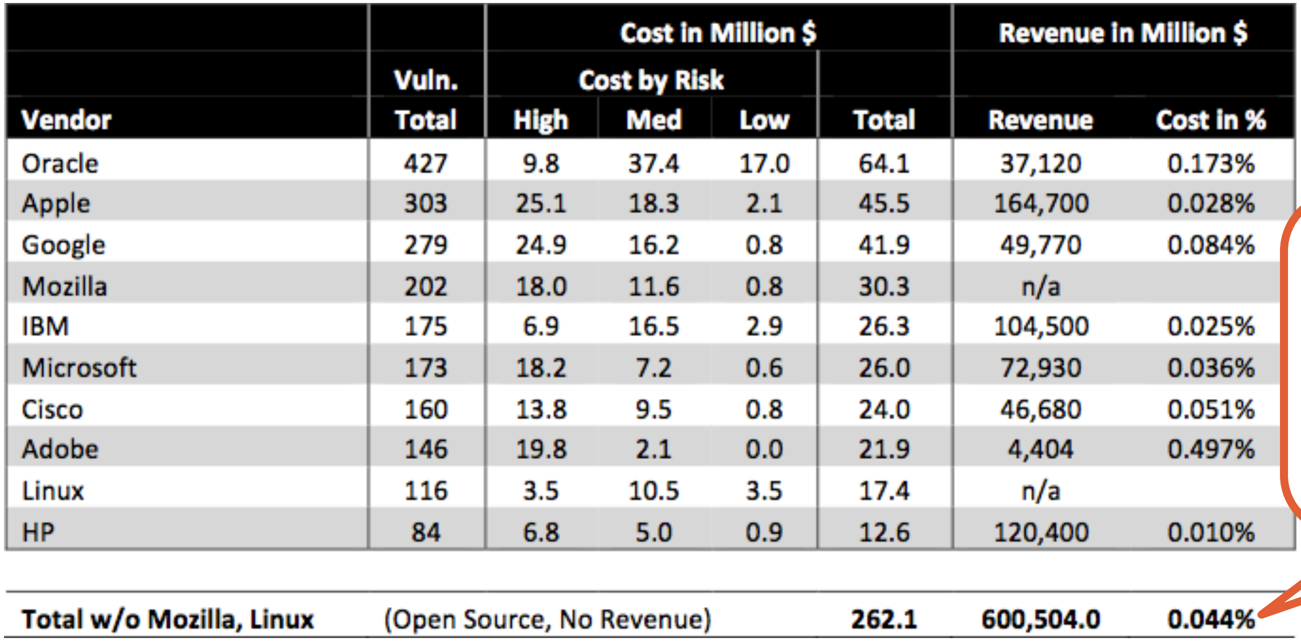
less than
1%
of the yearly cost of **cyber crime**

Software vendors buying their vulnerabilities

What would it cost software vendors to buy all their vulnerabilities for USD 150,000 each?

This includes buying all non-critical vulnerabilites

Cost of buying vendor vulnerabilities in 2012



		Cost in Million $				Revenue in Million $	
	Vuln.	Cost by Risk					
Vendor	**Total**	**High**	**Med**	**Low**	**Total**	**Revenue**	**Cost in %**
Oracle	427	9.8	37.4	17.0	64.1	37,120	0.173%
Apple	303	25.1	18.3	2.1	45.5	164,700	0.028%
Google	279	24.9	16.2	0.8	41.9	49,770	0.084%
Mozilla	202	18.0	11.6	0.8	30.3	n/a	
IBM	175	6.9	16.5	2.9	26.3	104,500	0.025%
Microsoft	173	18.2	7.2	0.6	26.0	72,930	0.036%
Cisco	160	13.8	9.5	0.8	24.0	46,680	0.051%
Adobe	146	19.8	2.1	0.0	21.9	4,404	0.497%
Linux	116	3.5	10.5	3.5	17.4	n/a	
HP	84	6.8	5.0	0.9	12.6	120,400	0.010%
Total w/o Mozilla, Linux	(Open Source, No Revenue)				**262.1**	**600,504.0**	**0.044%**

less than

1%

of the software vendors' **revenue**

Follow the money ...

The experience of past decades has shown that traditional approaches based on "more of the same" can not deliver adequate security

The question to ask is this:

> "How much are those that bear the costs willing to pay to reduce their losses incurred as a result of cyber crime?"

Conclusion
Recommendations

Conclusion

The software industry is yet unable to produce secure code.

Vulnerabilities and exploits continue to be available for abuse, for extended periods and unknown to the public.

Conclusion

We depend on researchers following coordinated disclosure for free, while the black market offers top money,

this current approach is not sustainable

It makes economic sense to purchase vulnerabilities, and we can outbid cyber criminals

Conclusion

What is the cost of doing nothing?

REFERENCES

References

- Online Vulnerability Purchase Cost Calculator
  http://www.techzoom.net/BugBounty

- The Known Unknowns in Cyber Security
  http://www.techzoom.net/Papers/The_Known_Unknowns_(2013).pdf

- International Vulnerability Purchase Program (IVPP)
  http://www.techzoom.net/Papers/International_Vulnerability_Purchase_Program_IVPP_(2013).pdf

- Cybercrime Kill Chain & Defense Layer Effectiveness (BlackHat)
  http://www.techzoom.net/Papers/Cybercrime_Kill_Chain_vs_Defense_Effectiveness_(2012).pdf

- Symantec Research
  http://www.symantec.com/connect/blogs/zero-day-world