Kaspersky Industrial Cybersecurity Conference 2019

September 18-20, 2019, Sochi, Russia

kaspersky

Industrial Bug Bounty: Fantasy or Reality?

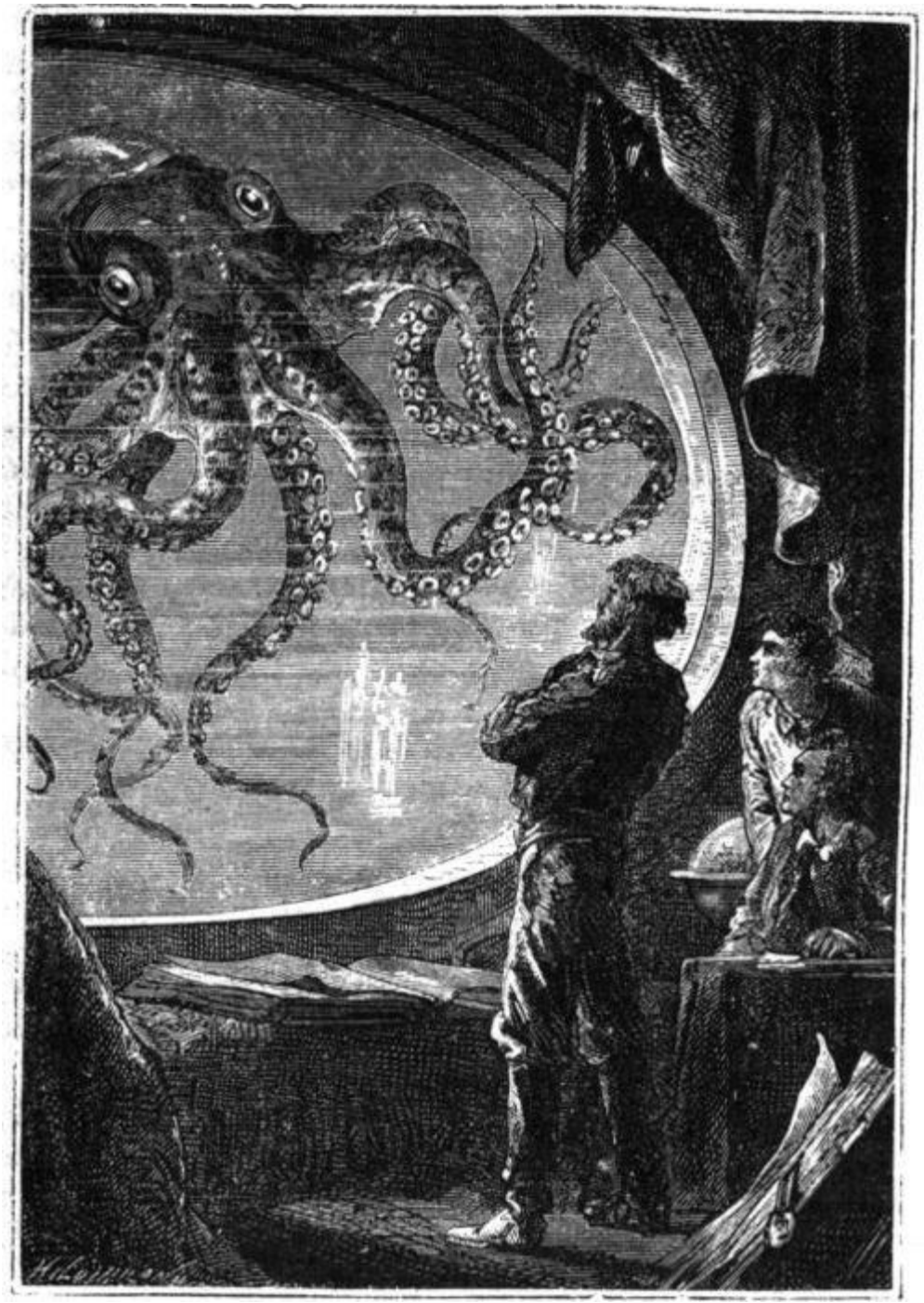
Vladimir Dashchenko,

Kaspersky ICS CERT

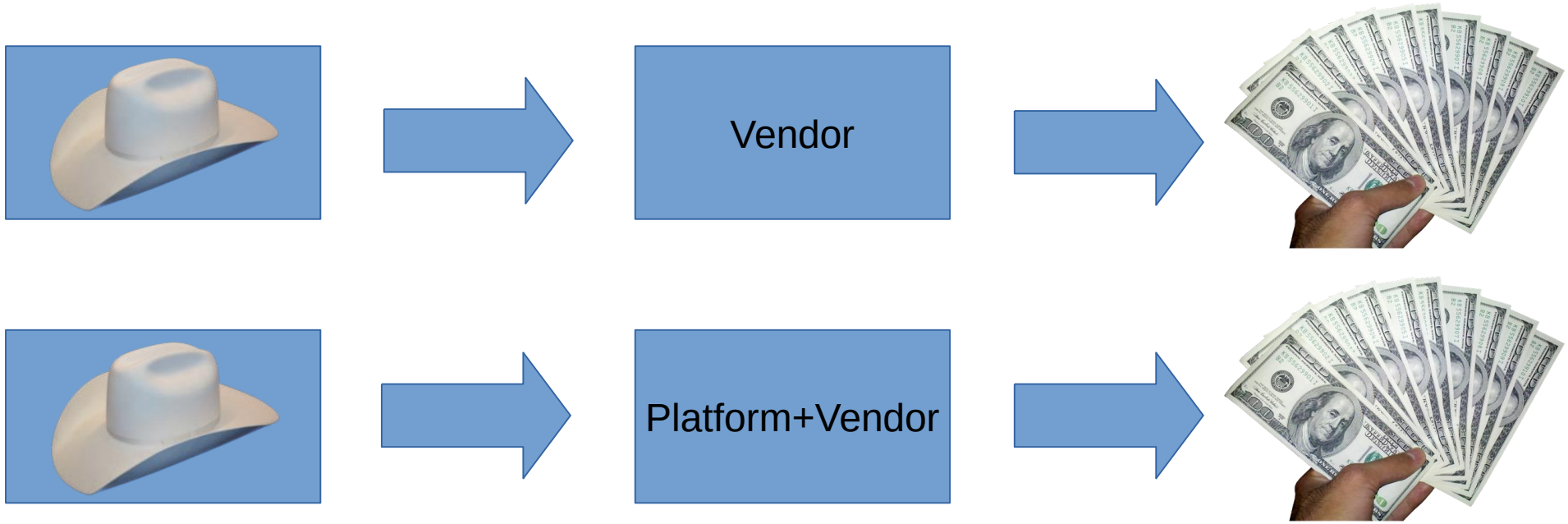
What is a bug bounty?

What is that

You hack – they pay



Who pays



Quick statistics. Platforms

Hackerone: 340+

Bugcrowd: 950+

The average bounty for critical issues rose to more than $2,000

From HackerOne’s inception in 2012 through June 2018, organizations have awarded hackers over $31 million

$11.7 million in bug bounties was awarded in 2017 alone

Quick statistics. Vendors

Microsoft: Up to $300 000 (Azure); up to $250 000 (Hyper-V)

Intel: Up to $100 000 (Intel firmware)

Kaspersky: Up to $100 000

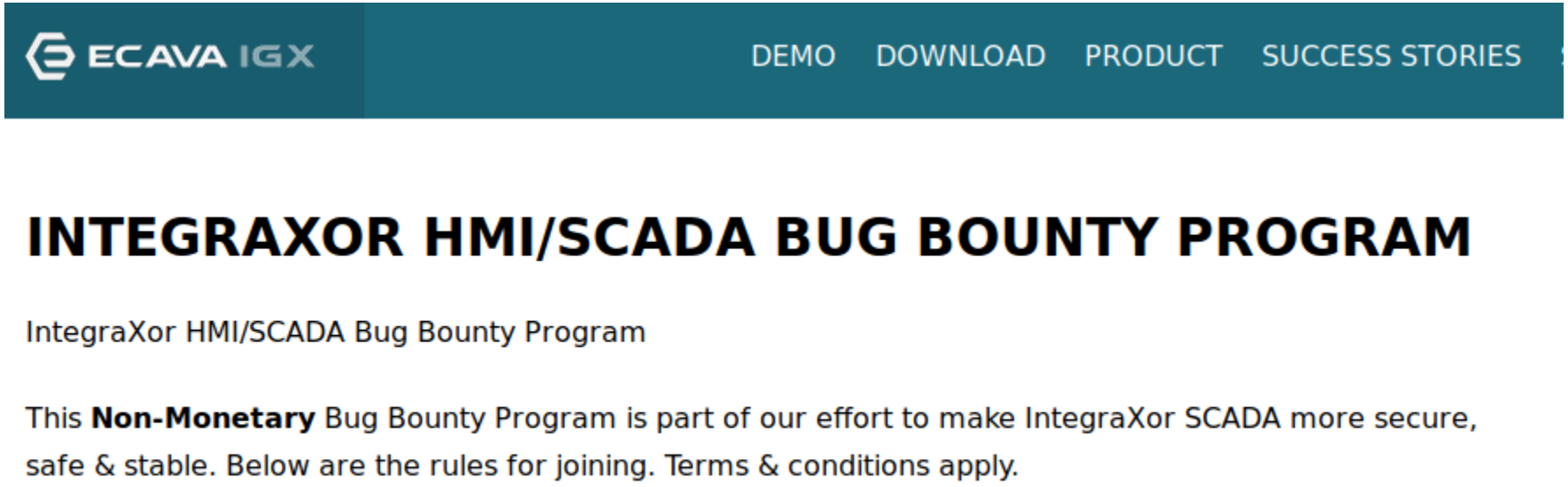
Google: Up to $150 000 (exploit chains that can compromise a Chromebook or Chromebox with persistence in guest mode)

ICS Bug Bounties

ICS Bug Bounty

THERE WAS THE ONLY ONE:

https://www.integraxor.com/integraxor-hmi-scada-bug-bounty-program/



ICS Bug Bounty

I/O Point Reward Table

Issue \ System	IGX Backend	IGX Frontend	Project Editor	Inkscape /SAGE	Browser *	Plugin
Security Vulnerability	8k	8k	1k	128	128	0
Program Crash	1k	1k	1k	128	128	0
Program Hang	1k	1k	1k	128	128	0

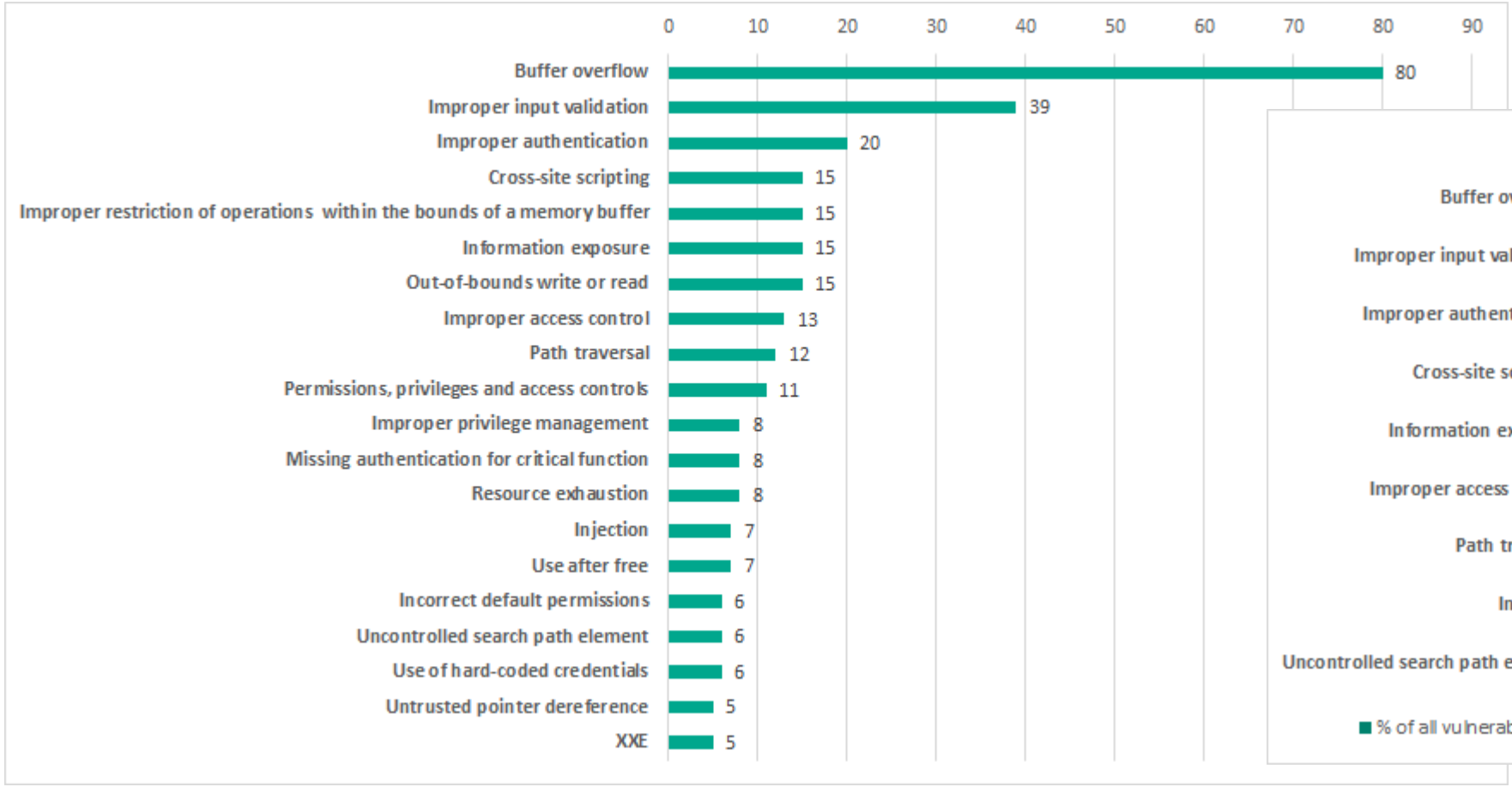
* The concerned browsers are latest version of AS, FX, GC & IE that showing IGX SCADA content, not this commercial web domain.

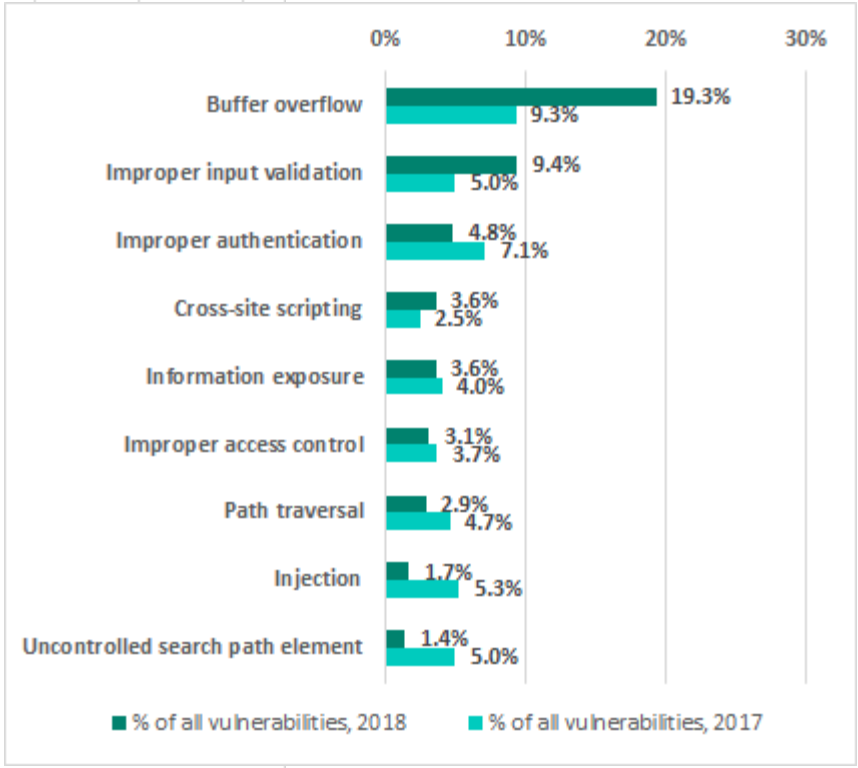
- We do not pay out monetary reward but only pay off I/O point to use our software license. The reward point is valid for 10 years from the date that the issue is fixed. If you are not an IntegraXor SCADA user, then you are allowed to resell the reward point in our forum or anywhere else.
- The value of rewards worth from USD $149 to $3999 which is according to how our license being sold. And the amount will be awarded according to the severity that completely judge by our technical team.

2013-07-22	John Carroll	Frontend	@n0x00
2013-07-23	Siddhesh Gawde	Blog	pen3t3r
2013-07-23	Ajay Singh Negi & Prashants Negi	Forum	@_prashantnegi
2013-07-23	Harsha Vardhan Boppana	Forum	@hvboppana
2013-07-30	Ashish Kamble	Front-end & Backend	Qualys
2013-08-15	Kope	Front-end & Backend	–
2013-11-07	Alphazorx aka technically.screwed	Backend	ZDI
2013-11-14	Omer Iqbal	Blog	@omerbutt26
2014-04-01	Andrea Micalizzi aka rgod	Backend	Retrogod
2015-01-30	Praveen Darshanam	Backend	~~Linkedin~~
2015-08-28	Marcus Richerson	Backend	San Diego State University
2016-08-12	John Carroll	Backend	@n0x00
2017-01-31	Brian Gorenc and Juan Pablo Lopez	Backend	Trend Micro
2017-06-07	Brian Martin	Backend	Tenable Security
2017-12-20	Steven Seeley	Backend	Source Incite
	Michael DePlante and Brad Taylor		Zero Day Initiative

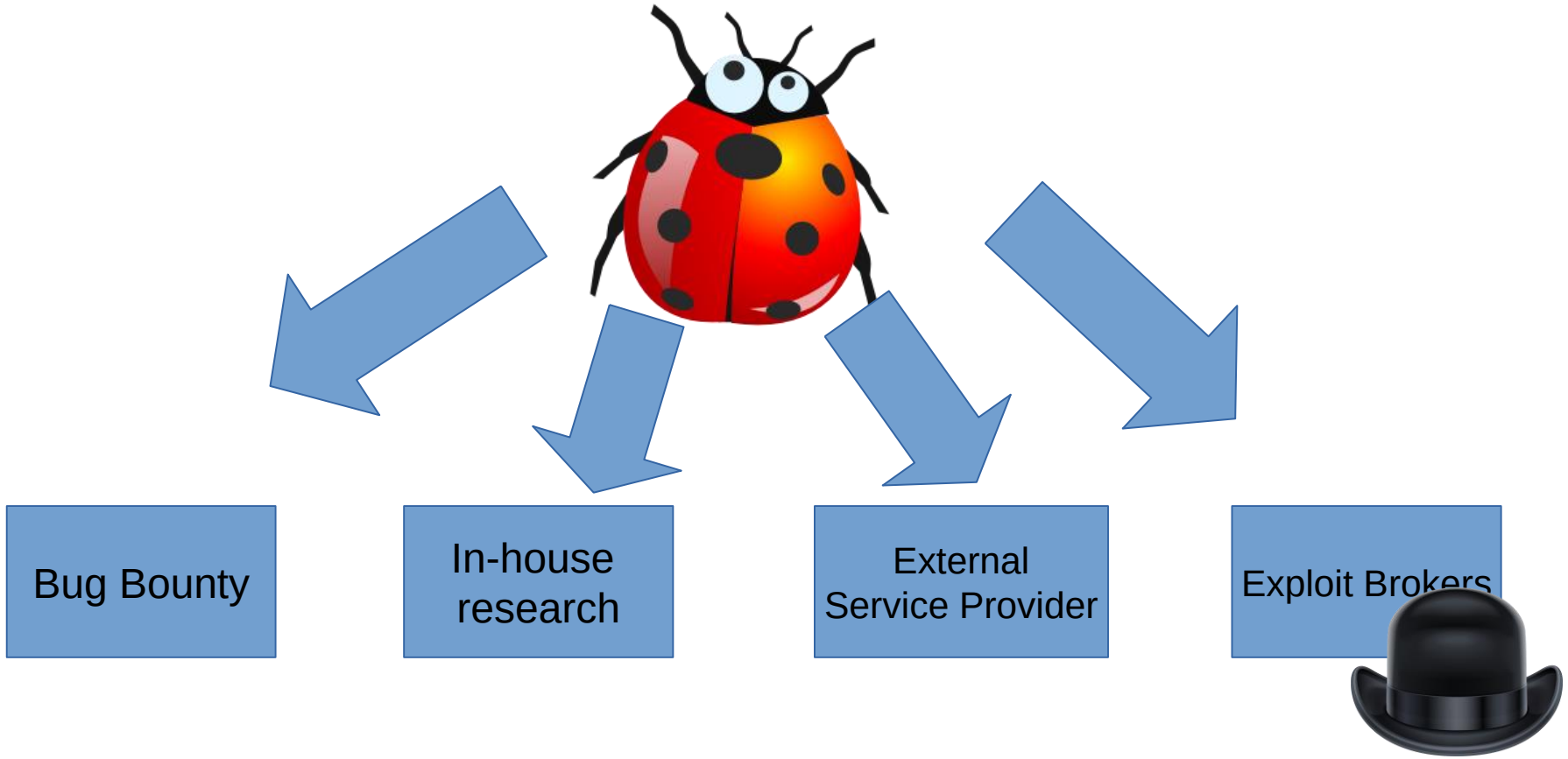
Statistics

415 (2018), US ICS-CERT stats





The bug was born!



Stop factors

Reason 1: “That’s too expensive for us”

IT

DOS – $500

XSS – $250 – $1000

SQLi – $2 000 - $6 000

Information disclosure – up to $20 000

RCE – $4 000 - $25 000

XXE – $500 - 10 000

Path traversal – $5 000 - $12 000

DOS –

XSS –

SQLi –

Inform

RCE –

XXE –

Path tr

Reason 1: “That’s too expensive for us”

Approximate payouts per company

Average number of vulnerabilities – 17 (from top 20 vendors; KL ICS CERT Statistics based on US ICS-CERT information)

One vendor – 40 vulnerabilities

RCE – 5 – $25 000

DOS - 29 ~ $29 000

Certificate validation – 1 - $1 500

XSS – 2 - $500

Missing Authentication (leads to DoS) – 1 - $1 000

Path traversal – 1 - $3 000

LPE – 1 – $3 000

Total: $63 000

Reason 2: Maturity problem

Denial, anger, bargaining, depression, acceptance – we see all the stages (ZN talk 2018)

Only

Sma

Diffic

Vuln

le

Reason 3: In-house research challenge

Vendor thinks that’s enough

Early bug discovery

Reason 4: “Oh, we have an external security team”

It’s more convenient

It’s more confidential

Counter arguments

Counter arguments

Factor	**Counter argument**
Too expensive	Yes, that might be expensive. But depends on vendor
Maturity	The sleeping fox catches no chickens
In-house research challenge	Challenge to build a strong offensive team Offensive in-house research is based on the methodology agreed with R&D
Established relationship with one external security team	Expensive Limited time and scope Blurred eyes (better to have rotation)

Bug bounty arguments

Motivation to build internal processes

Opportunity to enhance internal security team by improving skills and techniques

Increasing level of trust to your product

Making your product more secure

Making this world safer place

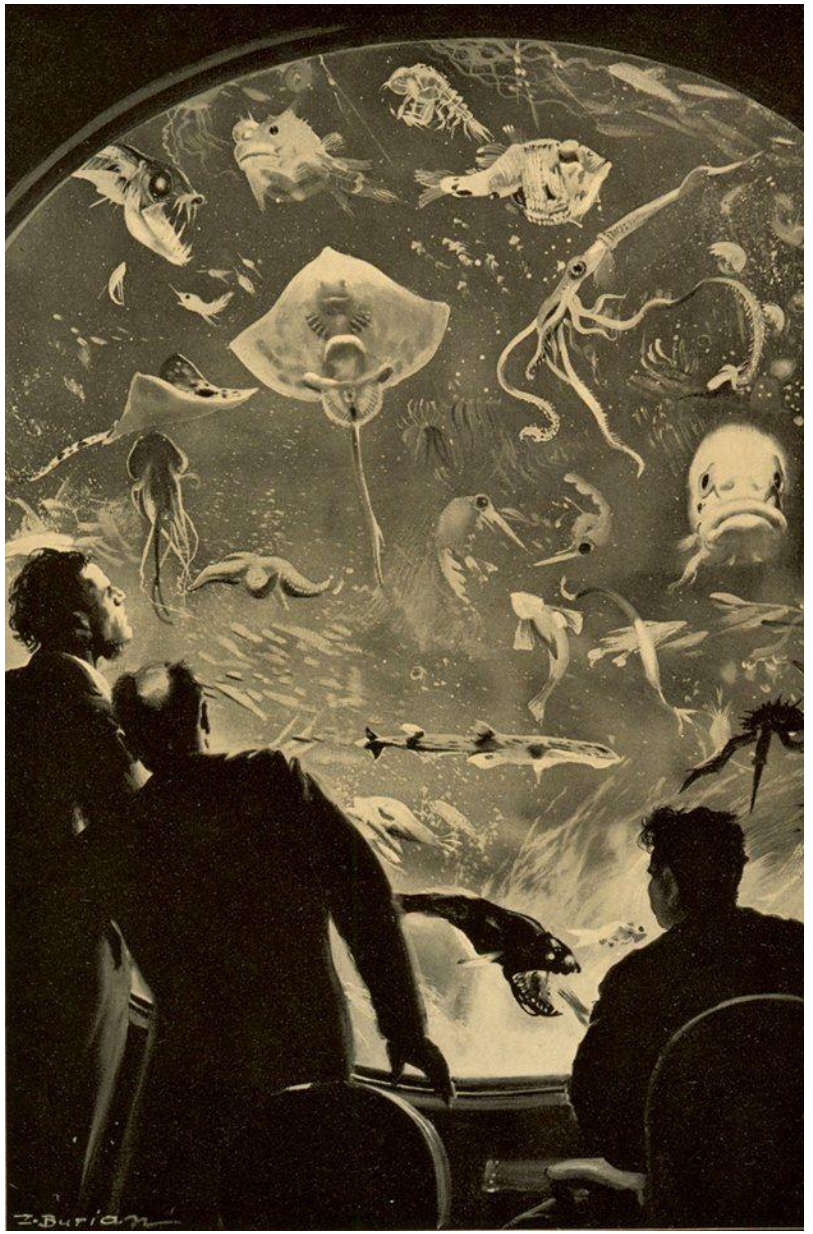
From Fantasy to Reality

From Fantasy to Reality

A good start – private invite-only bug bounty

for a limited number of products.

Inviting security companies?



Kaspersky Industrial Cybersecurity Conference 2019

September 18-20, 2019, Sochi, Russia

kaspersky

Thank you!

Vladimir Dashchenko (@VDashchenko)

Kaspersky ICS CERT

Ics-cert.kaspersky.com