RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Follow the Money: Security Researchers, Disclosure, Confidence and Profit

SESSION ID: ASEC-R04A

Jake Kouns

Chief Information Security Officer
Risk Based Security
@jkouns

Carsten Eiram

Chief Research Officer
Risk Based Security
@carsteneiram

SHOW ME THE AGENDA!

A Quick Overview To Set The Stage

Researcher Motivation in the ”Old” Days

- Reporting vulnerabilities to vendors looked good, as it got you credited in vendor advisories. Great for CV.
- Unemployed researchers with solid discoveries could get jobs in the industry, turning a hobby into a (profitable) professional gig. Employed ones could get better jobs / higher salary. This still applies today!
  - These jobs could even be at the companies in whose products the vulnerabilities were discovered.
- There was nothing altruistic about it!

Researcher Motivation in the ”Old” Days

- Reporting vulnerabilities to vendors back then was often a hassle, though – and can still be even today.
- Many would, therefore, instead:
  - Just publish somewhere to get social recognition, fame, and glory
  - Trade / give away for goodwil and respect
  - Use offensively for fun – or profit
  - Store in a digital box somewhere and move on

Several Money Options Exist!

- Grey Market (3/4 letter agencies)
- Black Market

Some Early Bug Bounties

- Some vendors / lone developers and security companies realized that rewarding vulnerability discoveries would be a good incentive for researchers to report their findings.
- August 2002, iDefense created the VCP (Vulnerability Coordination Program).
- August 2004, Mozilla created their bug bounty program, paying USD 500 for critical bugs.

But There Are Older Ones...

- Netscape actually launched the Netscape Bugs Bounty back in October 1995 to improve the security of their products.
- Interestingly, their approach was to offer cash for vulnerabilities reported in the latest beta
  - Wanted to incentive researchers to help secure it before going into stable release
  - Not unlike part of Microsoft’s bounty program today.

Full Disclosure

- Disclosure was a huge battle ground between vendors and researchers from 2000 to 2008 timeframe
- Researchers were still having problems getting vendors to respond
- More importantly perception (true or not) was that vendors only fixed bugs when they were dropped
- Researchers were hard core Full Disclosure the ”right” way
  - Importance placed on getting bugs fixed / improving security

Pwn2Own – A Bug Bounty Contest

- Created in 2007 for CanSecWest
  - Chance to win x2 Macbook Pro and 10k from ZDI
- Big money on the line in 2010
  - Total cash prize pool of US$100,000
- Competition brings lots of PR and growing cash incentives

No More Free Bugs

- In March 2009 at CanSecWest, security researchers announce their new philosophy: ”No More Free Bugs”.

- It’s not really clear how much effect this had

- At least sparked a debate about the issue, and made (some) security researchers’ expectations of monetary compensation more publicly known.

Bug Bounties become all the rage!

Bug Bounties - Do They Make A Difference?

Bug Bounties

- When researchers started reporting vulnerabilities to vendors, they were thrilled when:
  - They actually got a response
  - It wasn't a threat from a lawyer.
- Had you told a researcher back then that vendors today would be offering bug bounties, they would have smiled and shook their heads in disbelief.

Types of Bug Bounties

- Vendor bug bounties
- 3rd party bug bounties (ZDI, iDefense VCP, etc.)
- Company website bug bounties
- Crowd-sourced programs (Bugcrowd, HackerOne, etc.)

Types of Rewards

- Cash
- Prizes (T-shirt, mug, ...)
- Fame and glory

Bug Bounties – Interesting Ones!

- Google, probably one of the more serious vendor bounties
  - Big reason bounties took off (Pwnium 4 announces **USD 2.7M** in prizes)
  - Latest twist (bounties for other software)

- Microsoft's bounty for vulnerabilities
  - Originally defensive “bounties only”
  - Specifically bypassing security mechanisms
  - Focus on their beta software prior to stable release to ensure less customers are impacted

Getting Bug Bounties Right

- Needs to provide rewards compared to the bug bounty requirements/rules.
- Both reward types and sizes should be clear as well as the criteria for getting them.
- Rules/requirements should be clear (e.g. what is considered a valid submission, restrictions/limitations, how are duplicate reports handled, how should it be reported, what information should be included, what is the expected response time)

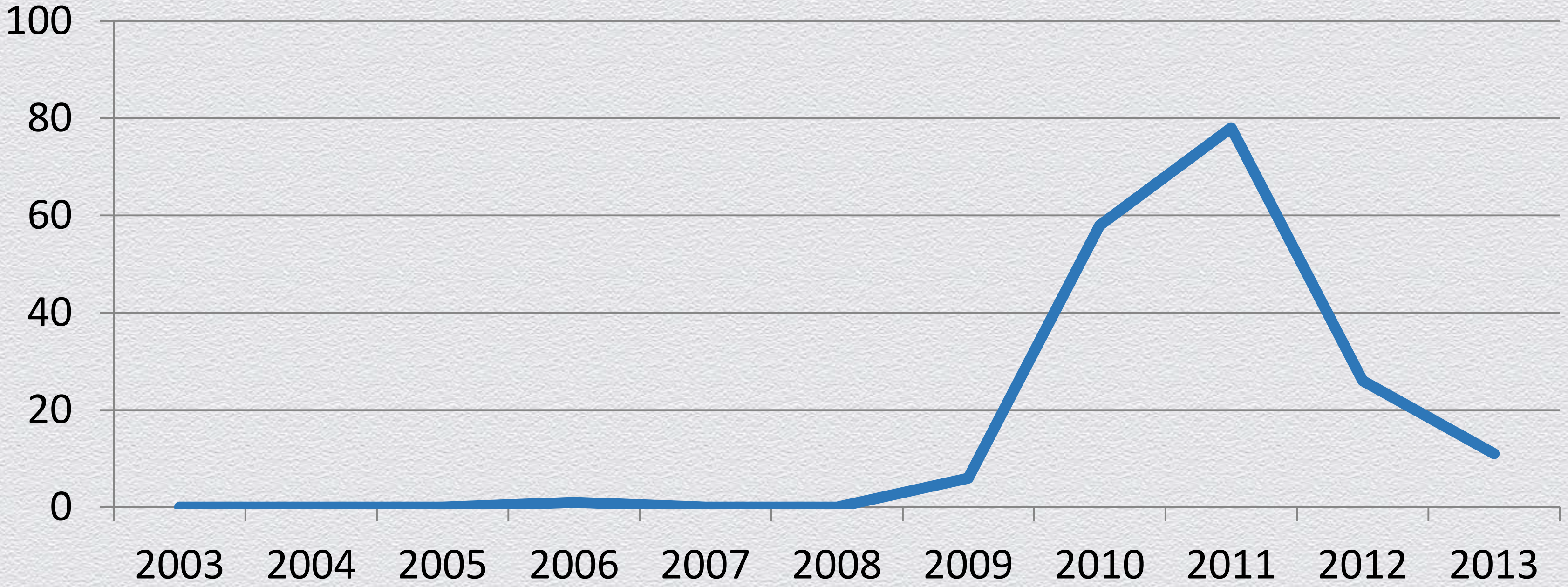
Yahoo Case – Getting Bug Bounties Wrong

- September 2013, High-Tech Bridge discovers XSS vulnerabilities in the Yahoo! website.
- Yahoo! responds with a discount code of **USD 12.50** per vulnerability to be used for purchasing trinkets in the Yahoo! store.
- That's a recipe for bad press – and they got it.
- November 2013, Yahoo! releases a proper bug bounty program now paying between USD 150 – 15K. The XSS vulnerabilities were rewarded USD 1K.

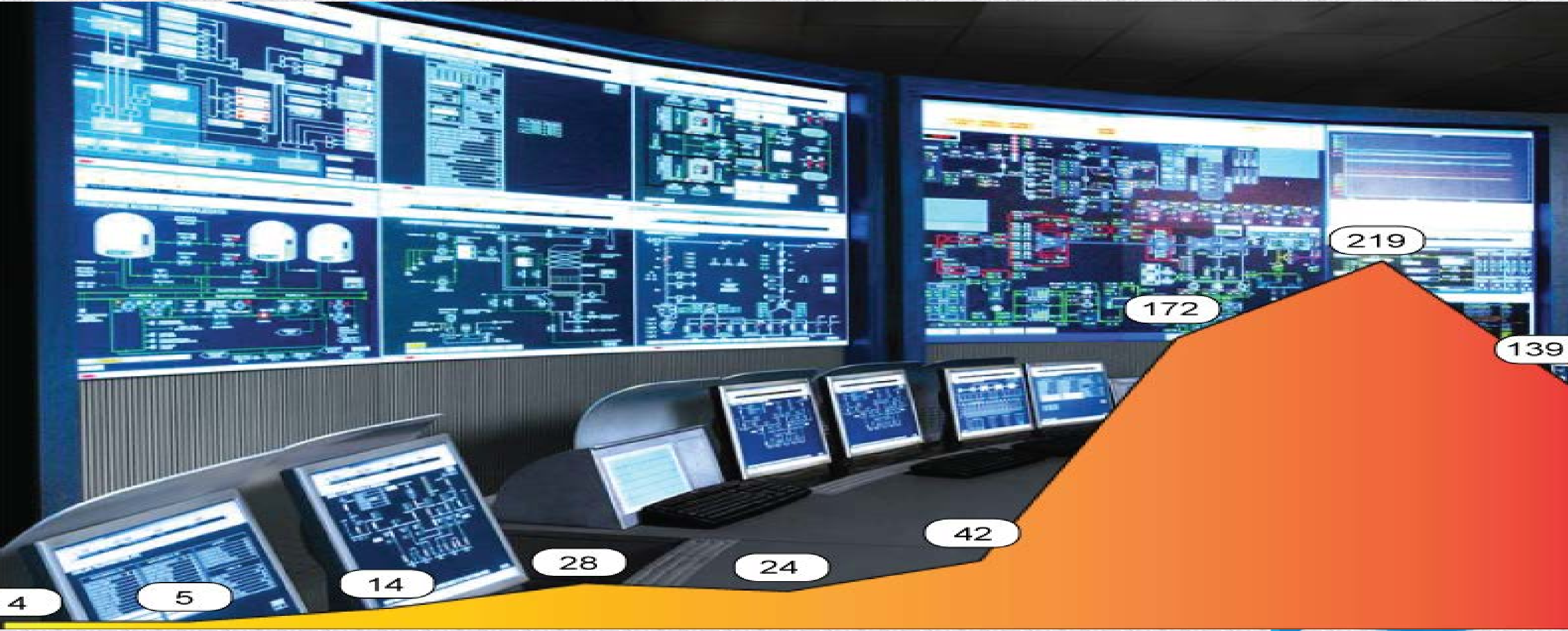
Website / SaaS / Cloud Vulnerabilities

- Even major companies and cloud providers don’t get the security of their websites and SaaS perfect!
- Companies with bounties for such as Facebook, Paypal, AT&T etc.
- Considerations for such initiatives incl.
  - Monitoring and how to react if things go wrong (e.g. site is wiped)
  - How do you differentiate between attacks and testing?

Shockwave Player Vulnerability Trend



Researcher Focus and SCADA



Bug Bounties – Are We There Yet?

Attitude Adjustment (Researchers)

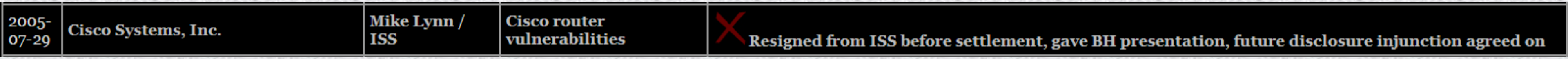
- Stop feeling entitled to compensation – instead appreciate it.
- Main complaint is that finding vulnerabilities takes time and provides value to the vendors - which is perfectly true.
- However, if volunteering to audit a product / website (often out of curiosity, which drives most of us), the researcher is not entitled to anything from that uncommissioned work!
- Testing a live website without permission or not following the vendor bounty's rules of engagement = potential legal issues!

Attitude Adjustment (Vendors)

- If not offering to pay for a researcher’s findings, do not think you in any way have a say in when and how the information is disclosed.
- Legal threats, complaints, and claims of ”irresponsible disclosure” should all be sent to /dev/null.
- Think through the logistics of running a bounty program or seek help!
- Should not rely solely on bug bounties for security testing!

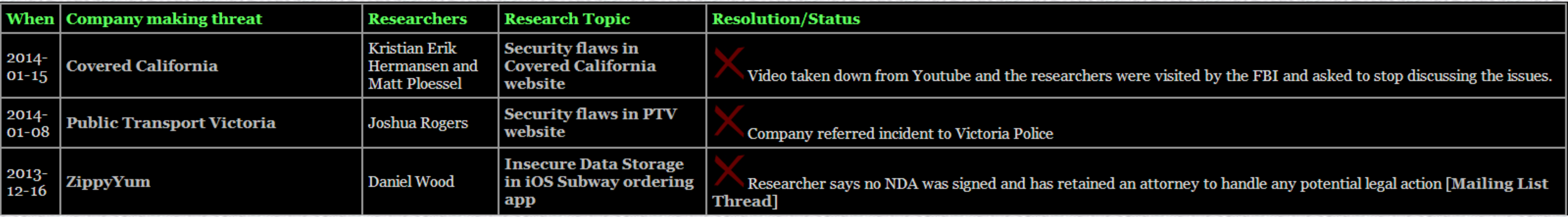
Legal Threats…

- Cisco vs Mike Lynn (2005)



2005-07-29	Cisco Systems, Inc.	Mike Lynn / ISS	Cisco router vulnerabilities	✗ Resigned from ISS before settlement, gave BH presentation, future disclosure injunction agreed on

- Still happens today... And unfortunately with some success!



When	Company making threat	Researchers	Research Topic	Resolution/Status
2014-01-15	Covered California	Kristian Erik Hermansen and Matt Ploessel	Security flaws in Covered California website	✗ Video taken down from Youtube and the researchers were visited by the FBI and asked to stop discussing the issues.
2014-01-08	Public Transport Victoria	Joshua Rogers	Security flaws in PTV website	✗ Company referred incident to Victoria Police
2013-12-16	ZippyYum	Daniel Wood	Insecure Data Storage in iOS Subway ordering app	✗ Researcher says no NDA was signed and has retained an attorney to handle any potential legal action [Mailing List Thread]

Source: http://attrition.org/errata/legal_threats/

Bug Bounties

- There has definitely been a shift in how vendors perceive bug bounties.
- It’s clear to us that if a vendor wants to encourage researchers to look at their code and report findings in a coordinated manner
  - Then bug bounties are very effective - when done right!
- There even seems to be a perception these days that a serious vendor offers a bug bounty.
  - So it’s useful even as a marketing stunt.

Bug Bounties Do…

- Allow you to control the disclosure process
- Increase the scrutiny and number of vulnerabilities reported in the software – that’s a GOOD thing!
- Cost effective method to (potentially) access top security talent

Bug Bounties Do Not…

- Replace a solid SDL process during devlopment
- Replace internal QA
- Replace external consultants

Future Of Bug Bounties

THE UNITED STATES OF AMERICA
THIS NOTE IS LEGAL TENDER FOR ALL DEBTS, PUBLIC AND PRIVATE
I 35060360 A
ONE DOLLAR

Discussion!

RiskBased SECURITY

#RSAC

RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Follow the Money: Security Researchers, Disclosure, Confidence and Profit

SESSION ID: ASEC-R04A

Jake Kouns

Chief Information Security Officer
Risk Based Security
jake@riskbasedsecurity.com

Carsten Eiram

Chief Research Officer
Risk Based Security
che@riskbasedsecurity.com