Lessons from a decade of bug hunting

Atlantic Security Conference 2019

xen1thLabs

A DARKMATTER COMPANY

SMART AND SAFE DIGITAL

Content

`whoami`

Eldar Marcussen

Lead security researcher

Proven history of performing security research that result in 0day vulnerabilities, conference presentation and security tools. I have written a source code scanner and auditing source code is often part of my security research process. My past research and security tools have also featured in industry related cyber security text books.

A former	Developer	Currently	Husband and Father
	System administrator		Security researcher
	Penetration tester		Trainer

01
BUG HUNTING

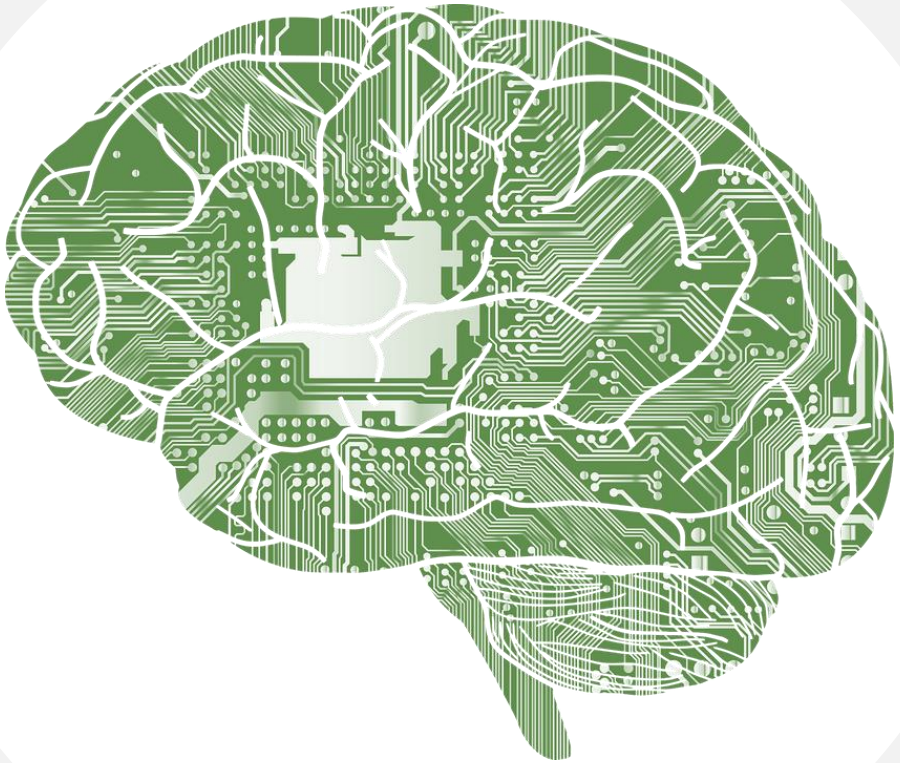
Bughunting

Identifying weaknesses

- Read the documentation
- Learn to recognize weakness patterns in source code
- Learn to recognize weakness patterns in design/process
- Anticipate poor decision making
- Implement short test cases to verify behavior if unsure
- Take breaks from complex/difficult code

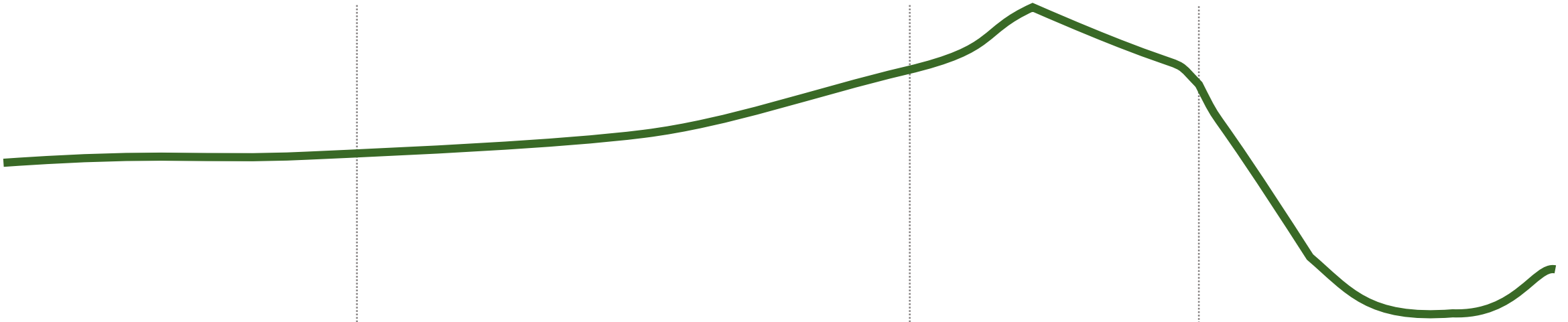
Simplifying bug hunting

- AVOID FALSE POSITIVES
- THIS MIGHT MEAN MISSING VULNERABILITIES (false negatives)
  - ➢ You can always take another look later
- SHORTLIST OF VULNERABILITY CLASSES
  - ➢ Easy to analyse
  - ➢ Avoids drowning in XSS



Reporting vulnerabilities

Vulnerability enthusiasm



DISCOVERY

- Spotting something worth a second look

VALIDATION

- Reading some code or
- Analysing a crash
- Confirming the vulnerability

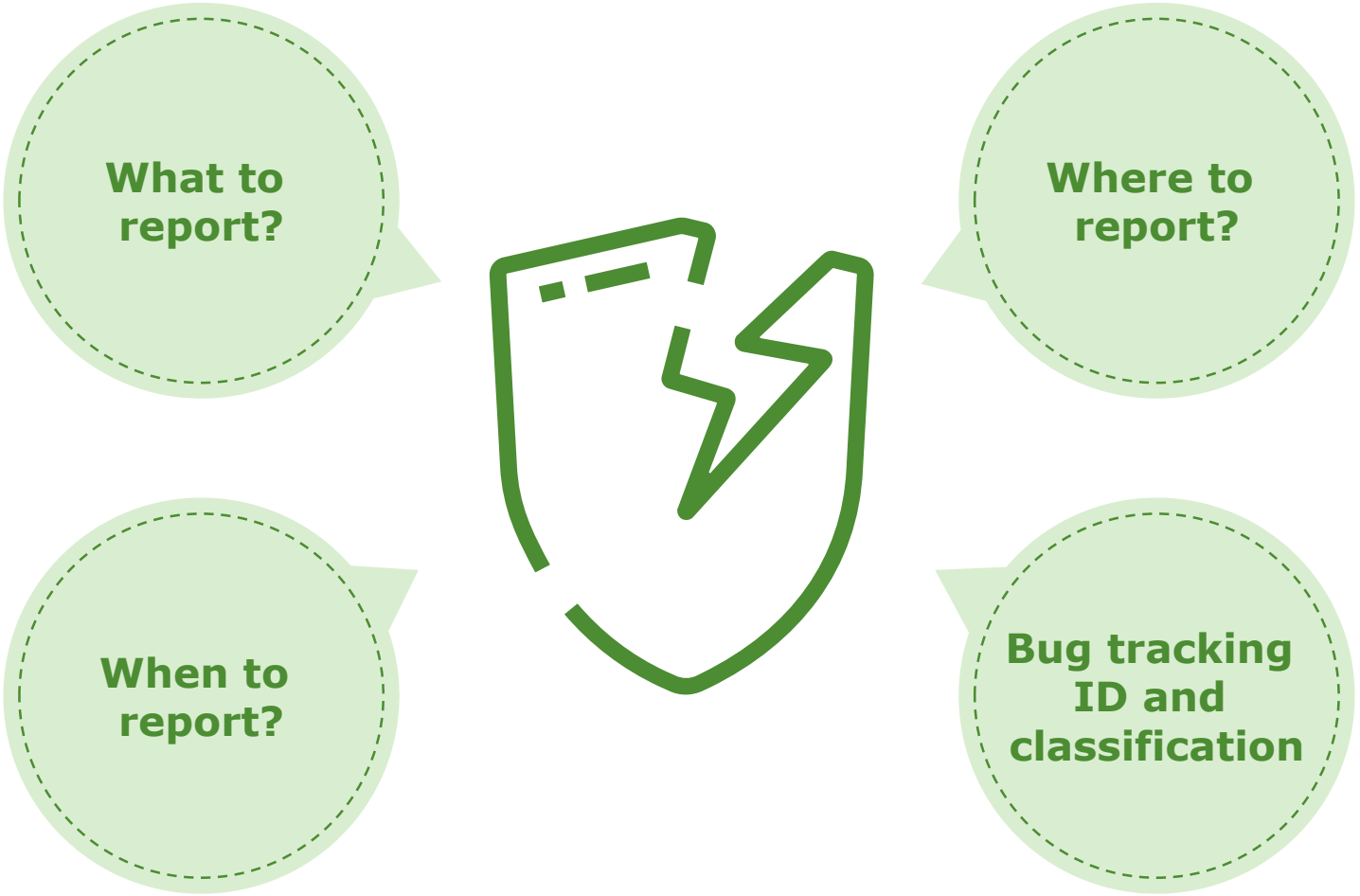
EXPLOITATION

- Overcoming technical challenges
- “Popping shells”

DISCLOSURE

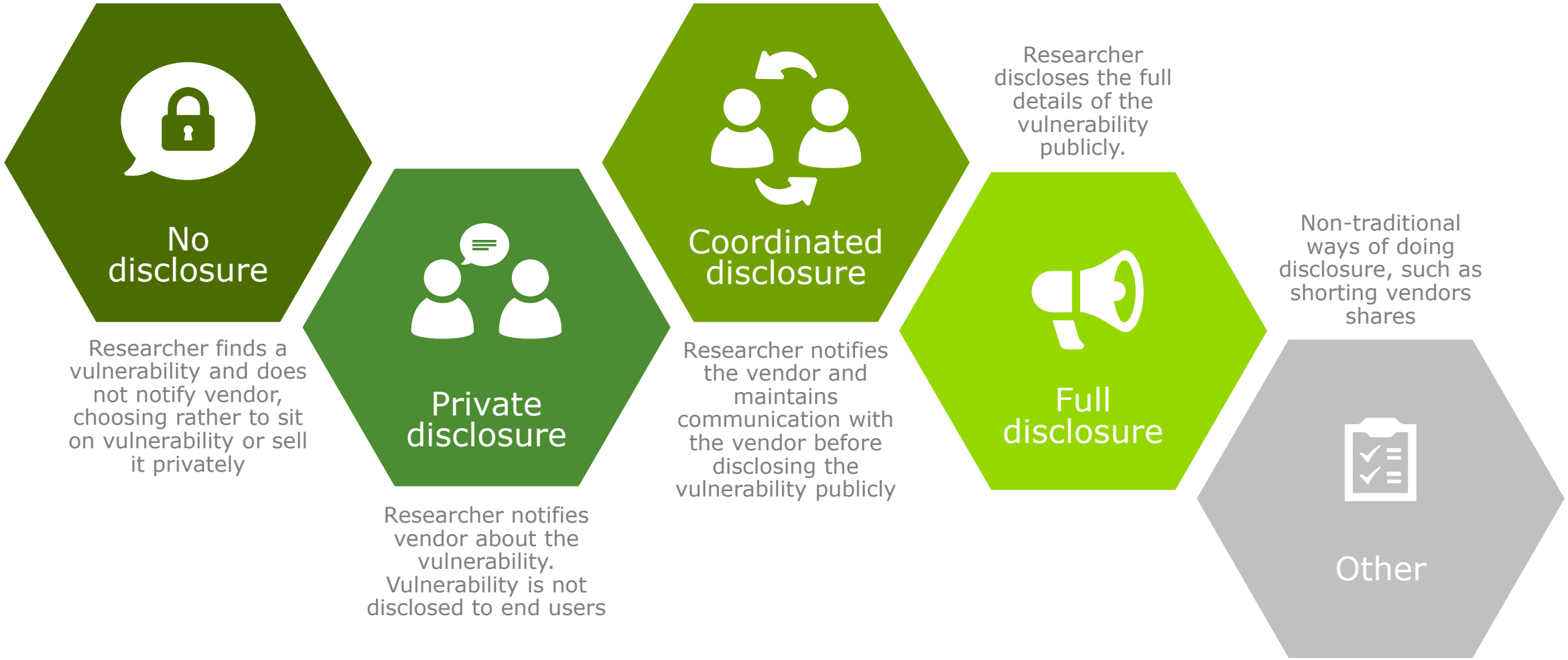
- Writing advisory
- Advisory QA
- Contacting vendor
- Requesting CVE
- Lots of emails
- Waiting for patch
- Publishing advisory

Reporting vulnerabilities



02
DISCLOSURE

“Types” of disclosure



COORDINATED, NOT RESPONSIBLE

Problems with the disclosure debate

Vulnerability tourism

Assumptions

Strawman arguments

Lack of empirical data

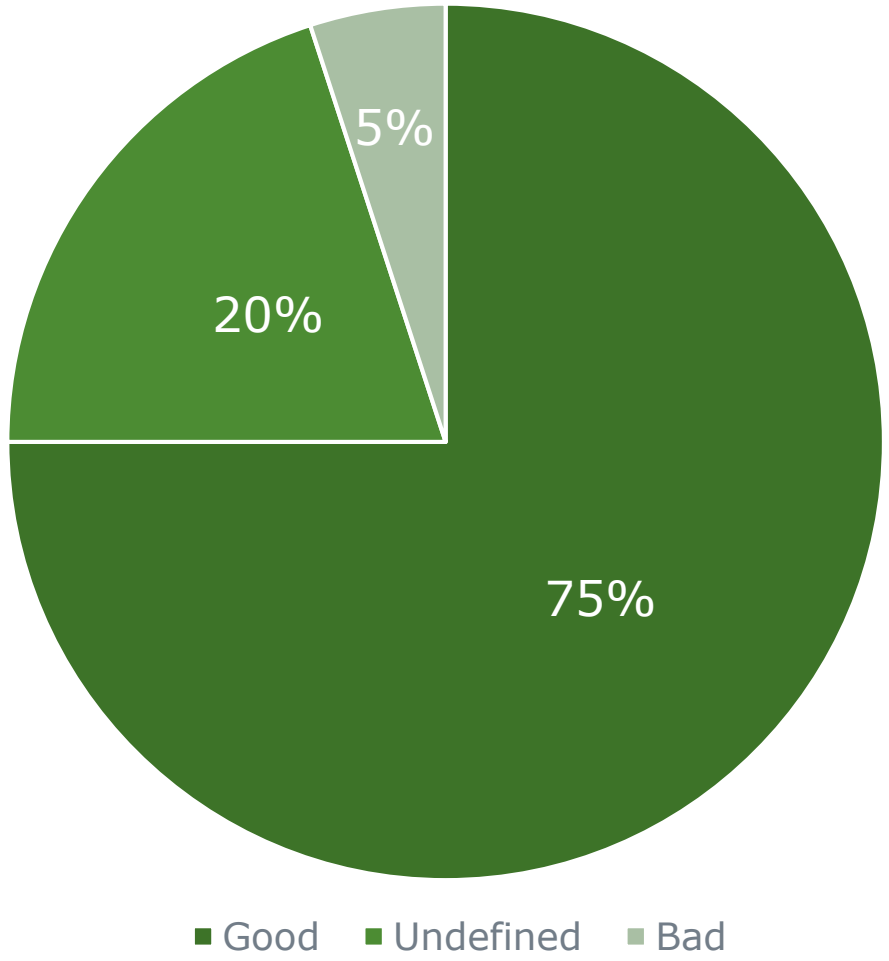
Shallow arguments

Disclosure policy compliance

Don’t be that guy

Personal stories

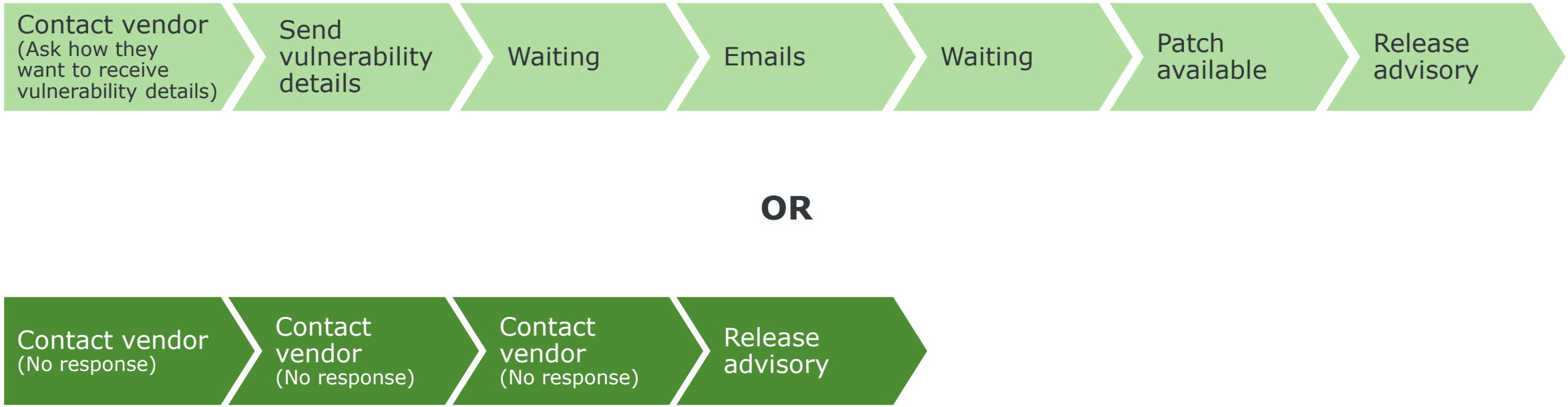
Disclosure experiences



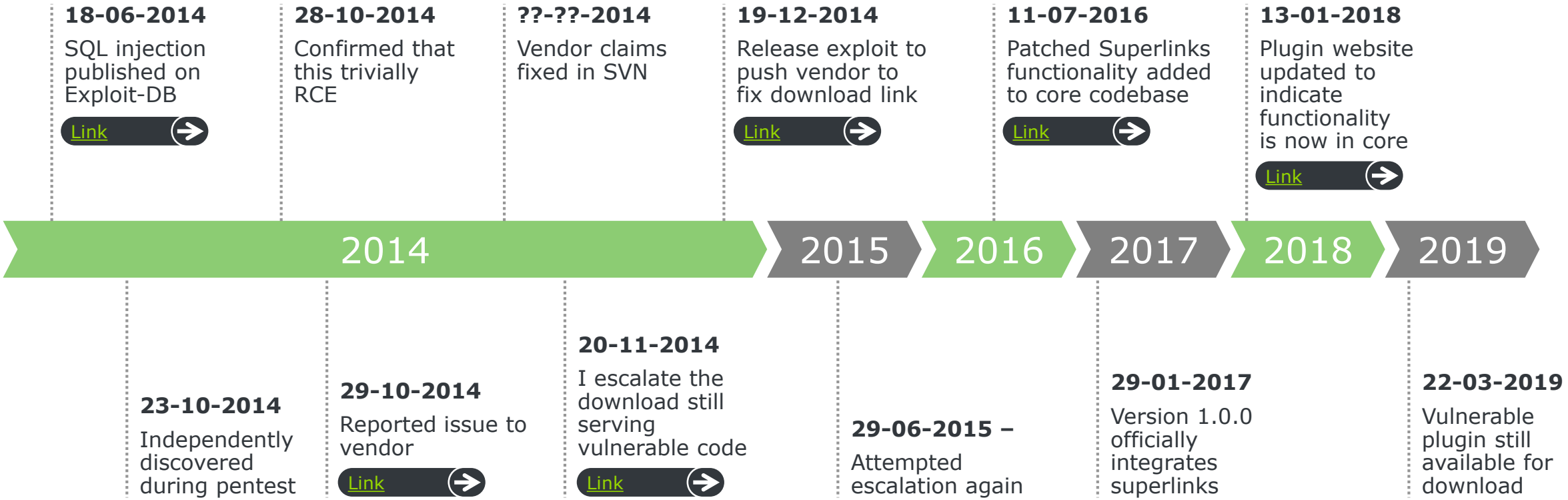
DEALING WITH VENDORS

- This is a placeholder text.
- This text can be replaced with your own text.

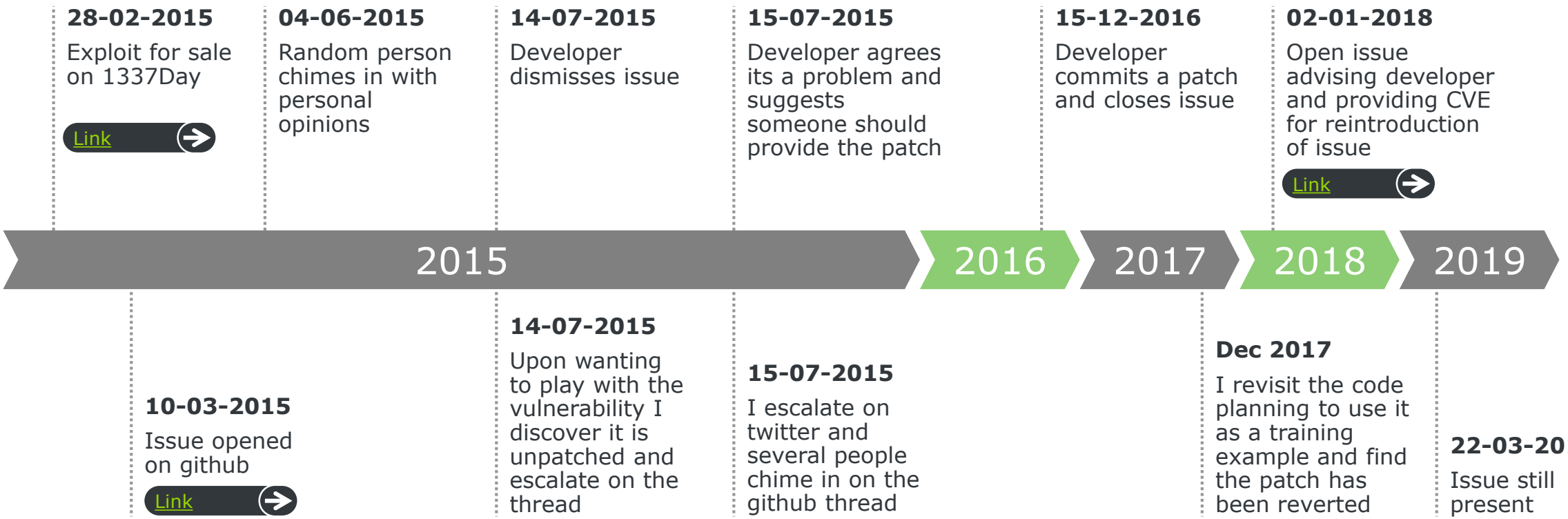
Disclosure experiences



Cacti superlinks plugin



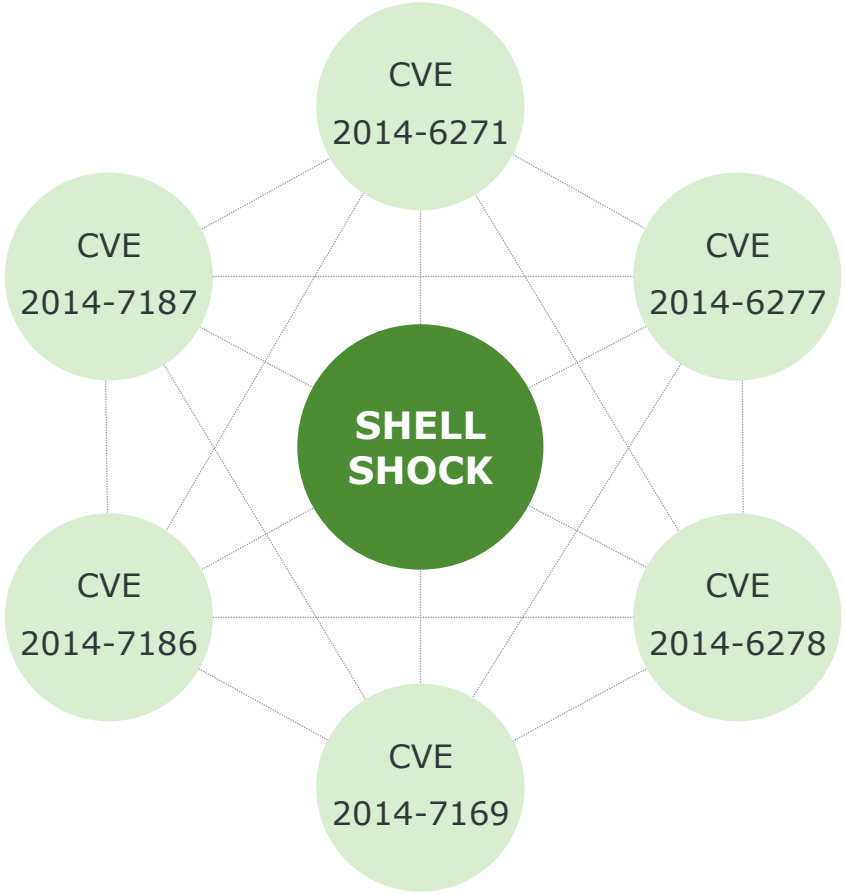
phpMoAdmin


28-02-2015
Exploit for sale on 1337Day
Link
04-06-2015
Random person chimes in with personal opinions
14-07-2015
Developer dismisses issue
15-07-2015
Developer agrees its a problem and suggests someone should provide the patch
15-12-2016
Developer commits a patch and closes issue
02-01-2018
Open issue advising developer and providing CVE for reintroduction of issue
Link
2015
2016
2017
2018
2019
10-03-2015
Issue opened on github
Link
14-07-2015
Upon wanting to play with the vulnerability I discover it is unpatched and escalate on the thread
15-07-2015
I escalate on twitter and several people chime in on the github thread
Dec 2017
I revisit the code planning to use it as a training example and find the patch has been reverted
22-03-2019
Issue still present

Public disclosure stories

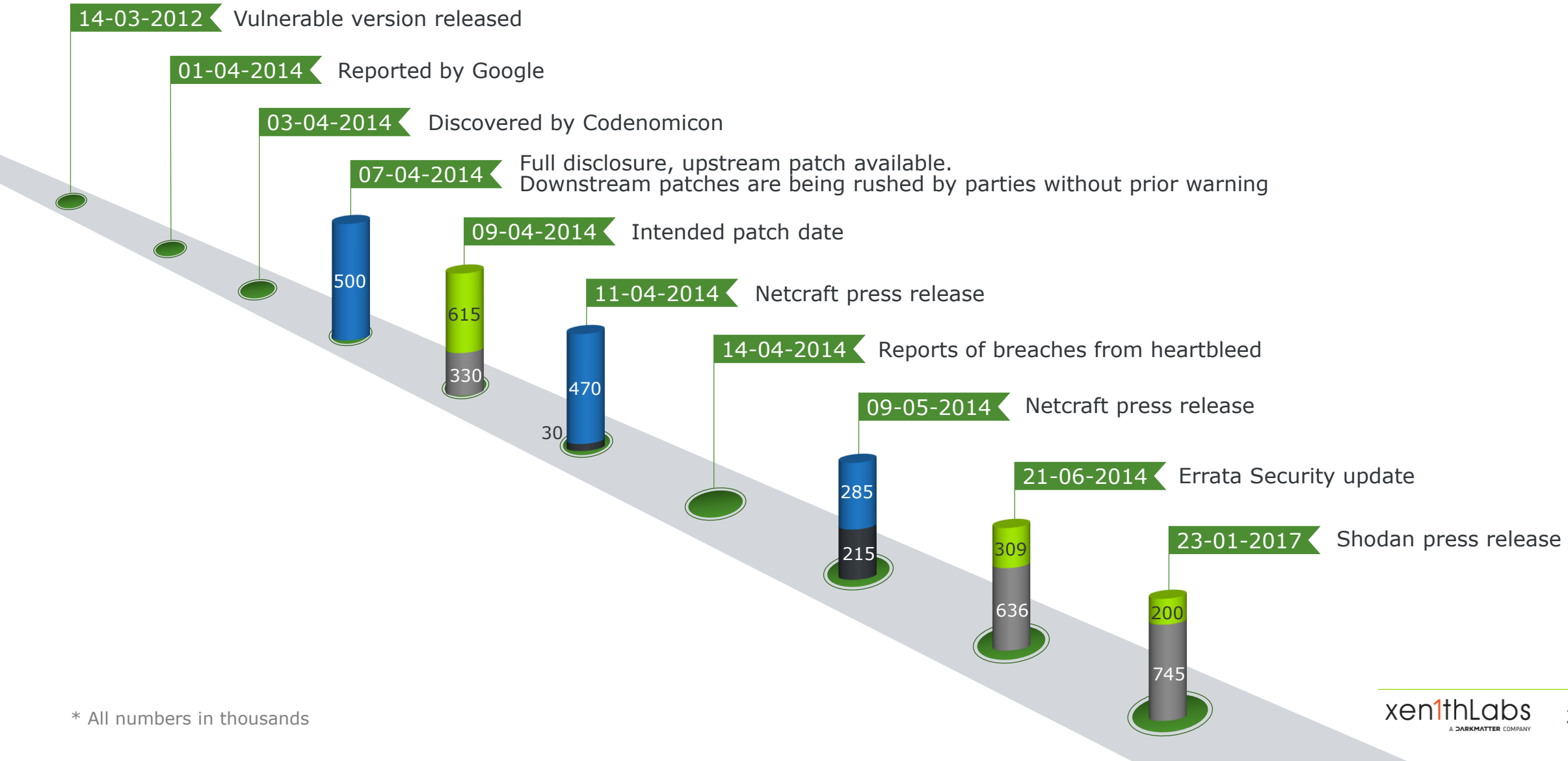
Shell shock (bashdoor)

- Initial report: 12 September 2014
- Initial patch: 24 September 2014
- Wide spread abuse: Within hours of disclosure
- Additional patches: 25-30 September 2014
- Abuse slowly died off



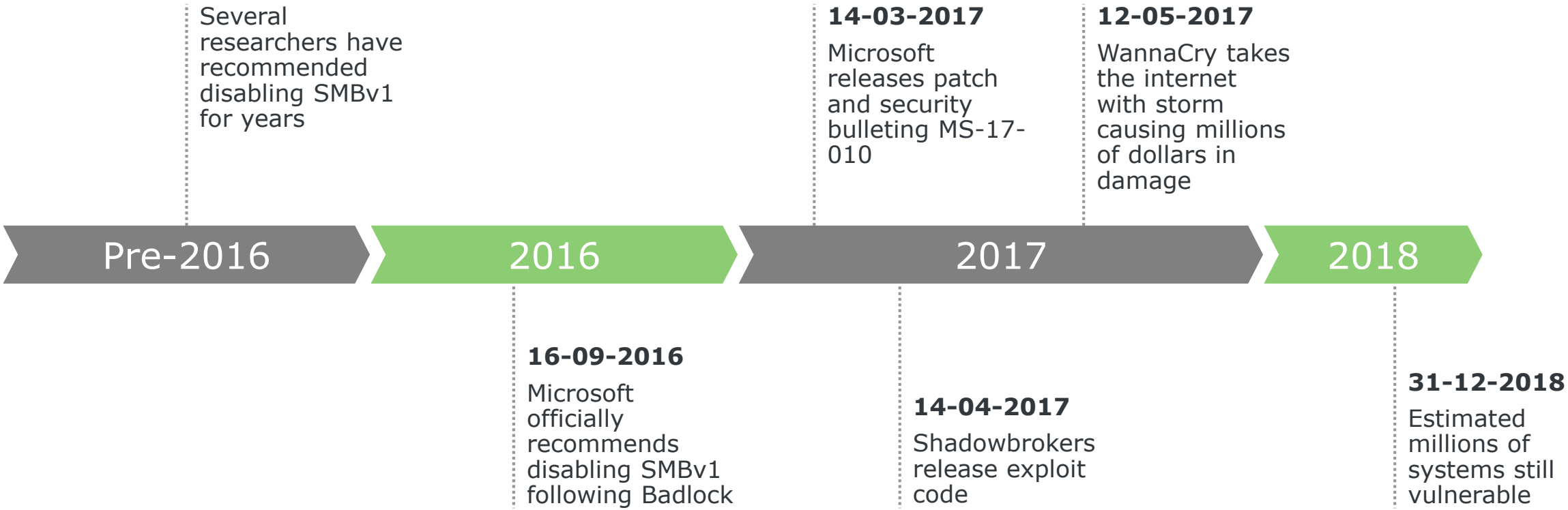
Attackers exploited Shellshock within hours of the initial disclosure by creating botnets of compromised computers to perform distributed denial-of-service attacks and vulnerability scanning. Security companies recorded millions of attacks and probes related to the bug in the days following the disclosure.

Heartbleed



* All numbers in thousands

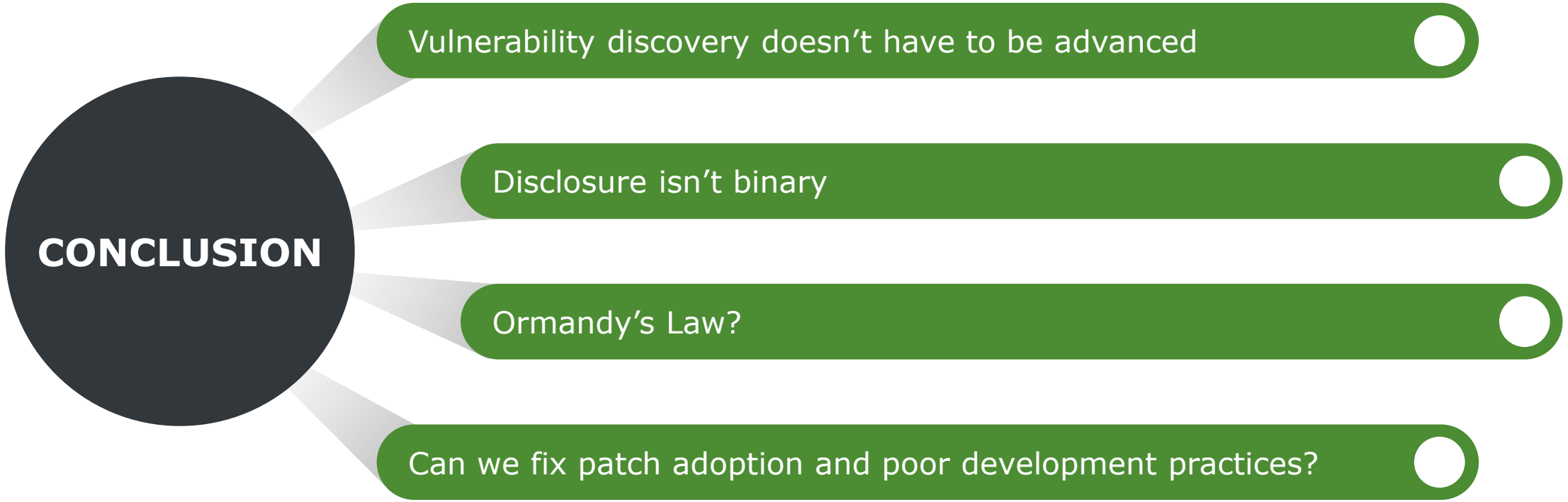
Eternal blue



Other disclosure stories

- https://www.csoonline.com/article/3338112/vendor-allegedly-assaults-security-researcher-who-disclosed-massive-vulnerability.html
- https://beyondbinary.io/articles/seagate-nas-rce/
- https://www.ring0.lol/posts/2014/07/27/coindrawer-bug-bounty-finale/
- https://twitter.com/Agarri_FR/status/1112401090023170049
- https://medsec.com/entries/stj-lawsuit-response.html
- https://threatpost.com/the-vulnerability-disclosure-process-still-broken/137180/
- https://www.wired.com/2015/09/fireeye-enrw-injunction-bizarre-twist-in-the-debate-over-vulnerability-disclosures/

03
CONCLUSION


CONCLUSION
Vulnerability discovery doesn’t have to be advanced
Disclosure isn’t binary
Ormandy’s Law?
Can we fix patch adoption and poor development practices?