Vulnerability Disclosure in IoT: The good, the bad and the legal threats

Mark Neve, Copper Horse
@copperhorseuk

IoT Security Foundation Annual Conference
26th November 2019

Vulnerability Disclosure – Introduction

"Many well-intentioned people simply give up and don't report serious security incidents when the effort is too high or the risk is too great" — security expert Troy Hunt

Department for Digital, Culture, Media & Sport

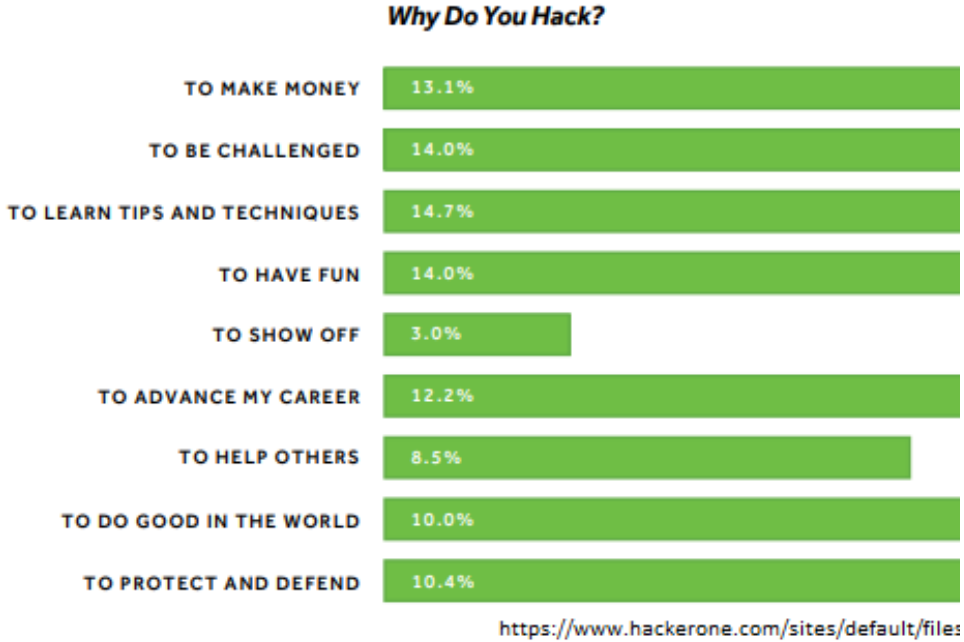
Code of Practice for Consumer IoT Security

2) Implement a vulnerability disclosure policy

All companies that provide internet-connected devices and services shall provide a public point of contact as part of a vulnerability disclosure policy in order that security researchers and others are able to report issues. Disclosed vulnerabilities should be acted on in a timely manner.

https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security/code-of-practice-for-consumer-iot-security

Who's Testing Your Security?



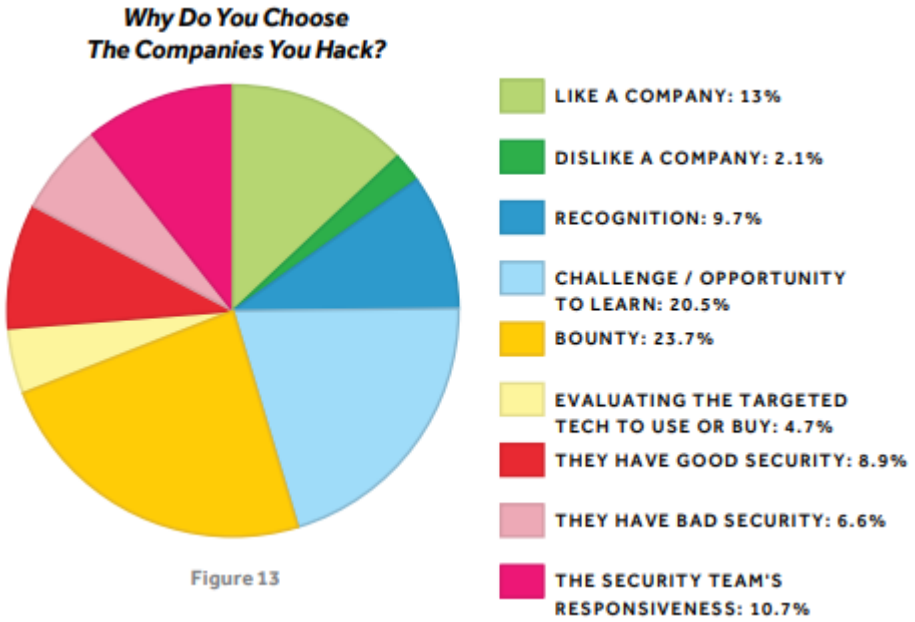


Figure 13

- Other bad reasons, not always discovered through disclosure!

Best Practice

- Coordinated Vulnerability Disclosure
- Define your disclosure policy
- What's "acceptable" testing?
- Specify your disclosure timeline – usually 90 days
- Nominate a Head of Security Response

Vulnerability Disclosure: Best Practice 2/2

- <companydomain>/security page
- Thank you page
- Setup contact email addresses:
  - security@<companydomain> and securityalert@<companydomain>
- PGP key

Proxy Disclosure

Bug Bounty Payouts Up 73% Per Vulnerability: Bugcrowd

Bug bounty programs grew along with payouts, which averaged $781 per vulnerability this year, researchers report.

WHAT IS HACKER101?

Hacker101 is a collection of videos, resources, and hands-on activities that will teach you everything you need to operate as a bug bounty hunter. The material is available to learn for free from HackerOne. Led by HackerOne's Cody Brocious, the Hacker101 material is ideal for beginners through to intermediate hackers and located at https://hacker101.com/. Feel free to share and join the conversation on Twitter with hashtag #hacker101.

Bugcrowd University Expands Education and Training for Whitehat Hackers

Bugcrowd Pays Out Over $500K in Bounties in One Week

In all, bug hunters from around the world submitted over 6,500 vulnerabilities in October alone.

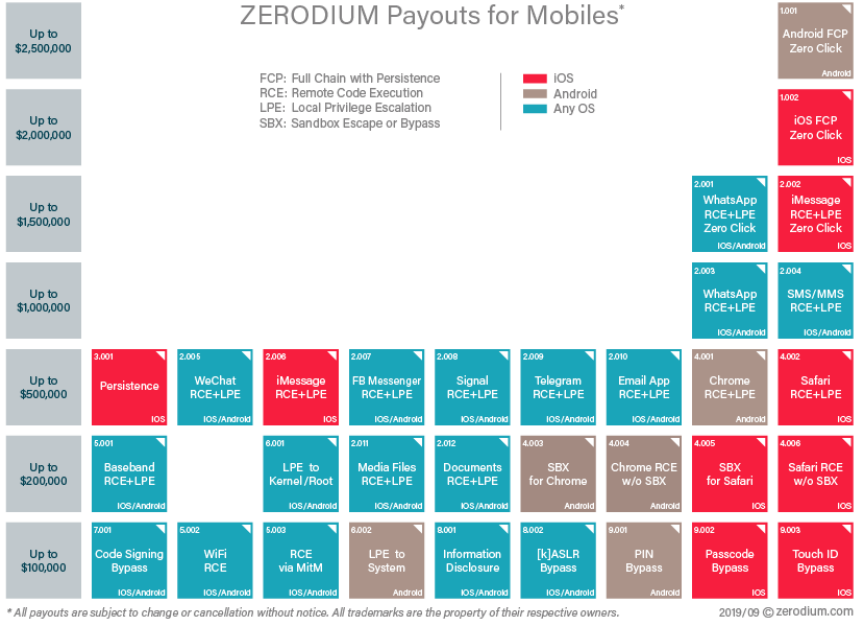
https://www.darkreading.com/vulnerabilities---threats/bugcrowd-pays-out-over-$500k-in-bounties-in-one-week/d/d-id/1336307

Zero-Day Market

We are Zerodium

The leading exploit acquisition platform for premium zero-days and advanced cybersecurity capabilities.

"We pay BIG bounties, not bug bounties"



The Legal Threats

York council app users hacked: Nearly 6,000 affected

20 November 2018 Share

Screenshot of the Council's justification for reporting our developer to the police

One Planet York: 'Ethical hacker' exposed council app flaw

28 November 2018 Share

Screenshot f

On Monday, the council tweeted: "Despite attempts to contact [the hacker], they did not respond and as a result of what appears to be a deliberate and unauthorised access we informed the police".

More stories from around Yorkshire

The local authority, which has since revised its stance, said: "Following further review it has become clear that the person who identified the issue with the app had tried to contact us but their email had not been received due to security settings.

https://www.rapidspike.com/blog/one-planet-york-data-breach-update/

Passing the Responsibility

Five million customers affected by Vtech database hack

By Zoe Kleinman
Technology reporter, BBC News

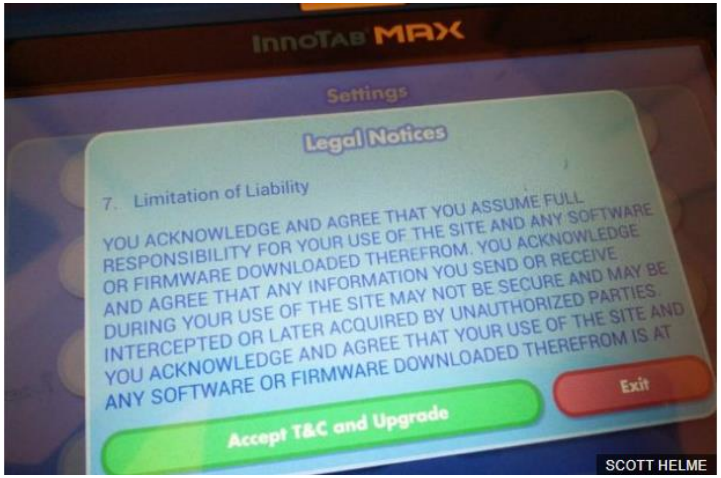
30 November 2015 Share

The hacked database included a lot of customer data, including some details about children, and the company was told about the breach by a journalist.

It did not contain any credit card information, Vtech said, but it did store the "name, email address, encrypted password, secret question and answer for password retrieval, IP address, mailing address and download history" of customers.

VTech issues new T&Cs telling parents to take responsibility if children's tablets and toys get hacked

VTech was hacked in December leading to breach of personal data and 'pictures of kids'



https://www.bbc.co.uk/news/technology-35532644
https://www.independent.co.uk/news/uk/home-news/vtech-issues-new-terms-and-conditions-telling-parents-to-take-responsibility-if-childrens-tablets-a6865331.html

Doing it Right

- Keep a timeline
- Be nice
- Proof of concept
- Communicate
- Deploy fixes
- Joint disclosure
- Say thanks
- Security Advisory

2018 vs 2019 Research Data

Thanks!

@copperhorseuk

mark.neve@copperhorse.co.uk