License to hack

Leo Niemelä

LÄHITAPIOLA

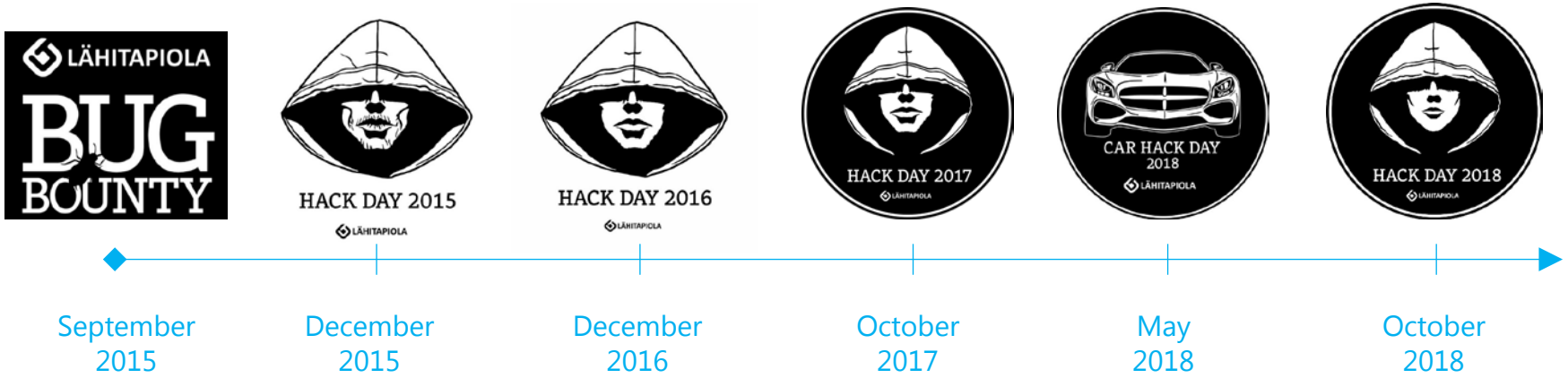
Leo Niemelä, CSO, LähiTapiola
Twitter @leoniemela

LÄHITAPIOLA

“Hack for good and like a pro”

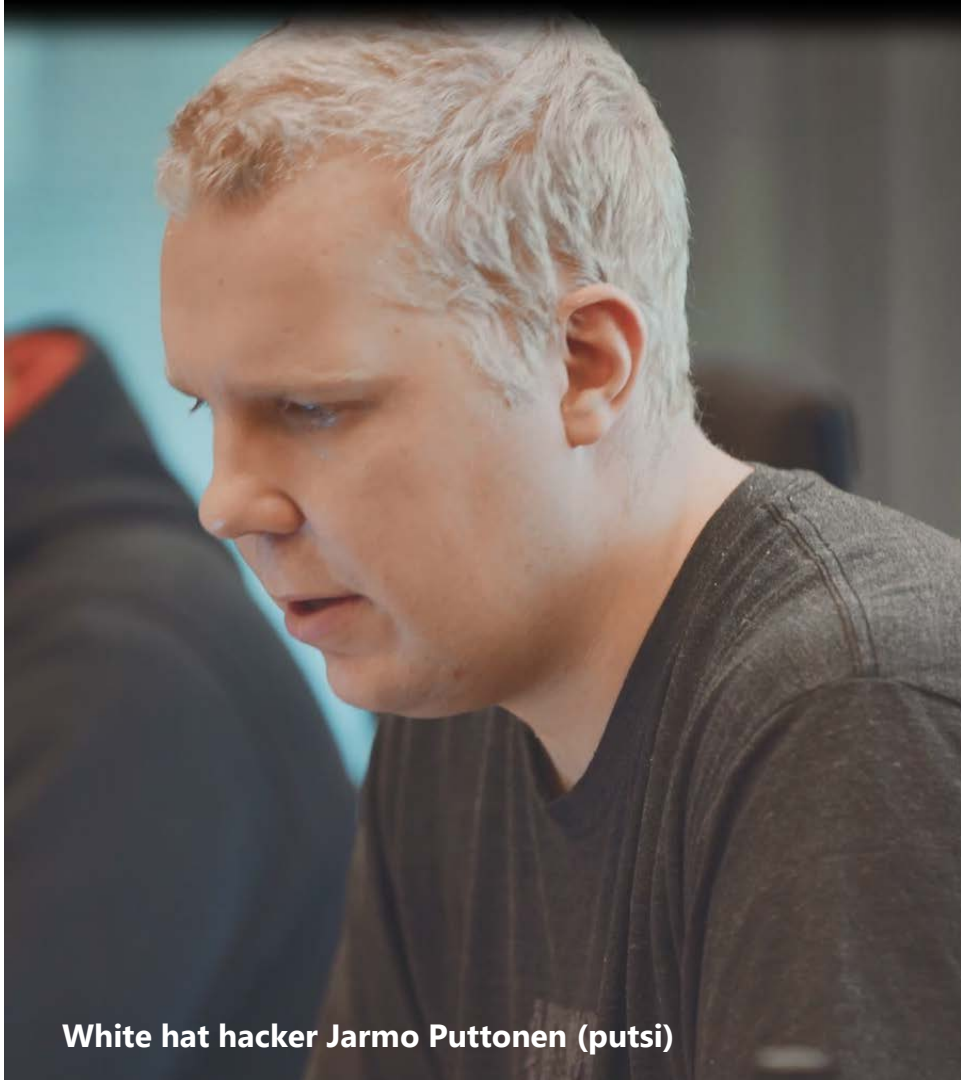
LÄHITAPIOLA

How we hack


LÄHITAPIOLA
BUG
BOUNTY
HACK DAY 2015
LÄHITAPIOLA
HACK DAY 2016
LÄHITAPIOLA
HACK DAY 2017
LÄHITAPIOLA
CAR HACK DAY
2018
LÄHITAPIOLA
HACK DAY 2018
LÄHITAPIOLA
September
2015
December
2015
December
2016
October
2017
May
2018
October
2018

Our Bug Bounty journey so far

- First opened 14.9.2015 and Hackerone since 1.4.2016
- Total bounties paid $126 000
- Friendly hackers have been thanked rather than hit with a lawsuit
- Over 200 (quality) reports from hackers, 600+ in total
- Dozens of potential criminal cases
- Huge amount of vulnerability fix rollouts to production environment
- Enterprise software 0 days forwarded to Cert-FI



White hat hacker Jarmo Puttonen (putsi)

Benefits

- Traditional pen-testing gives coverage – but they are usually limited by scope and time allocated
  - Your pen-testers have pretty good knowledge on the common solutions and technologies
- With Bug Bounty you have no idea about the coverage, but the hackers are not limited by scope or time
  - Your Bug Bounty hunter is your average pen-tester, just having more difficulties following instructions and staying within scope

White hat hacker Sean Melia (seanmeals)

Key takeaways

- We work with hackers and build trust-based relationships (Bug Bounty, Hack Day´s)
- Bug Bounty programs are cost-effective for finding security issues on target systems and different platforms
- Current trend is that Bug Bounty programs are becoming industry best practice
- Online services will be hacked anyway (illegally)
- Increases awareness of security in software development and personnel in general

Online Services - Secure Software Fruit Tree

High Fruit	Vulnerability Disclosure Program
Bulk Fruit	Secure Development Process (Privacy by Design)
Low Hanging Fruit	Security Testing and Audits
Ground Fruit	Training and Threat Modeling

Courtesy: Leo Niemelä

“When good hackers find the bugs before the bad hackers do, that’s a huge win for the company.

LÄHITAPIOLA

Thank you!

LÄHITAPIOLA

TERVEYS • TURVALLISUUS • TALOUS