How hackers changed the security industry

Weld Pond @DEFCON Wall of Sheep
How did we get here?

We made trouble.
“Improving the Security of Your Site by Breaking Into It”

By Dan Farmer and Weitse Venema, 1993
Hackers Made Information Security a Participatory Sport
The First Hacker Tools

Crack – Alec Muffett - 1991
Targets guessable passwords

SATAN – Dan Farmer & Weitse Venema - 1995
Targets misconfiguration

Netcat – Hobbit - 1996
Network swiss army knife
Hacker Information Resources

Bugtraq

DEFCON
Hackers Write Commercial Security Software
Improve the Security of Your Product by Breaking Into It
Product companies selling security features

Identity & Access Management
Encryption
Firewalls

Accountancies selling compliance

SAS 70
NIST 80-153
Using Good Hackers to Battle Bad Hackers

If you have a murky past and doubt you could become a dot-com millionaire, think again. Last week a scraggly band of hackers known as “L0pht Heavy Industries” joined with some straitlaced tech execs to form @Stake, an Internet-security consulting firm.

Into the light: Once shadowy computer code warriors like Kingpin are going legit
In 2000 Launched @stake security consultancy

We conducted our own vulnerability research
We built our own attack/testing tools
We secured applications by breaking into them
Others soon followed:
  Guardent (acquired by Verisign)
  Foundstone (acquired by McAfee)

The L0pht + Dan Geer
Remember the Microsoft SDLC

--- Original Message --
From: Bill Gates
Sent: Tuesday, January 15, 2002 5:22 PM
To: Microsoft and Subsidiaries: All FTE
Subject: Trustworthy computing

Every few years I have sent out a memo talking about the highest priority for Microsoft. Two years ago, it was the kickoff of our .NET strategy. Before that, it was several memos about the importance of the Internet to our future and the ways we could make the Internet truly useful for people. Over the last year it has become clear that ensuring .NET is a platform for Trustworthy Computing is more important than any other part of our work. If we don’t do this, people simply won’t be willing -- or able -- to take advantage of all the other great work we do. Trustworthy Computing is the highest priority for all the work we are doing. We must lead the industry to a whole new level of Trustworthiness in computing.

When we started work on Microsoft .NET, more than two years ago, we set a new direction for the company -- and articulated a new way to think about our software. Rather than developing standalone applications and Web services, we’re moving towards smart clients with rich user interfaces. We’re driving the XML Web services that vendors can share information, while promoting standards for this new era.
What did we teach them?

• How to threat model
• How to exploit heap overflows
• How to fuzz software
• Built their first fuzzer – SPIKE
• How to use SysInternals Process Explorer to find attack surface
• Now Microsoft SDLC is the reference for the industry – literally, ISO 27034
Penetration testing is a requirement.

Companies have a product security response team.

Development teams use hacker techniques for security Testing. Look to Microsoft as a model.

And later came Bug Bounties!
Fast forward to 2017
Nation States pretend to be criminal hackers.
And Hackers are now Insiders
But we are **OLD** insiders

We need the next generation to keep making trouble
Make me nervous!
Security Champions
I BROKE INTO THE WEB SITE TO HELP YOU!

THANKS, BUT IT'S BETTER IF WE DON'T KNOW THE SITE IS INSECURE.

Weld Pond/Chris Wysopal
cwysopal@veracode.com
@weldpond