Cybersecurity: From State Actors to Bedroom Hackers

BCS, May '19

Rahul

1980
Earth - Born

Warwick - MEng.
1998

2002
Shazam - Technical Architect.
(Acquired)

Apsmart - Founder &
CEO (Acquired)
2009

2012
Thomson Reuters -
Head of Advanced
Products

Red Sift -
Founder &
CEO
2015

Today
2019

2018
Co-
op
-
Independent
Non-
Executive
Director
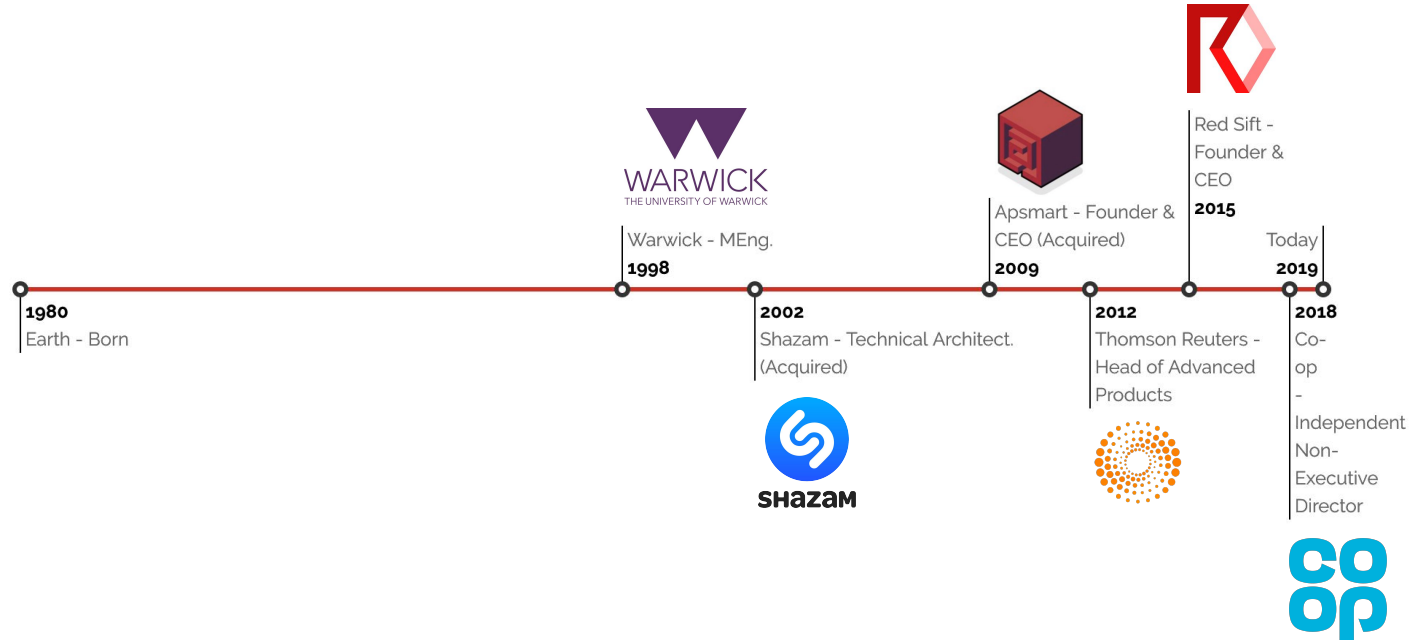
A history of making software

1980
Earth – Born

1998
Warwick – MEng.

2002
Shazam – Technical Architect.
(Acquired)

2009
Apsmart – Founder &
CEO (Acquired)

2012
Thomson Reuters –
Head of Advanced
Products

2015
Red Sift –
Founder &
CEO

2018
Co-
op
–
Independent
Non-
Executive
Director

2019
Today

1980

1992
Basic

1995
Pascal

1997
C

1998
Java

1999
ML

2002
C++

2005
C#

2008
Objective-C

2009
Javascript

2012
D

2014
Swift

2015
Go

2017
Python

2019
Rust

RED SIFT

The cognitive security platform

We exist to democratise the technology essential for cybersecurity.

What makes us different?

Computers
not
Consultants

Everyone
not
Exclusive

Platform
not
Point

We help > 200 Organisations

"According to the email our cyber experts sent to our teams, they believe a hacker tool Metasploit was used. The automation network and Siemens hardware were attacked and shut down."*

"After shutting down the network, the attackers played the song *Thunderstruck* by the hard rock band AC/DC at maximum volume."*

Hacking goes OSS

What do you want to do:

1. E-Mail Attack Single Email Address
2. E-Mail Attack Mass Mailer
3. Return to main menu.

Enter your choice: 1

Do you want to use a predefined template or craft a one time email template.

1. Pre-Defined Template
2. One-Time Use Email Template

Enter your choice: 1
Below is a list of available templates:

1: Baby Pics
2: Strange Internet usage from your computer
3: New Update
4: LOL...have to check this out...
5: Dan Brown's Angels & Demons
6: Computer Issue
7: Status Report

Enter the number you want to use: 7

Enter who you want to send email to: davek@fakeaddress.com

What option do you want to use?

1. Use a GMAIL Account for your email attack.
2. Use your own server or open relay

Enter your choice: 1
Enter your GMAIL email address: davek@fakeaddress.com
Enter your password for gmail (it will not be displayed back to you):

RED SIFT

Just scratching the surface
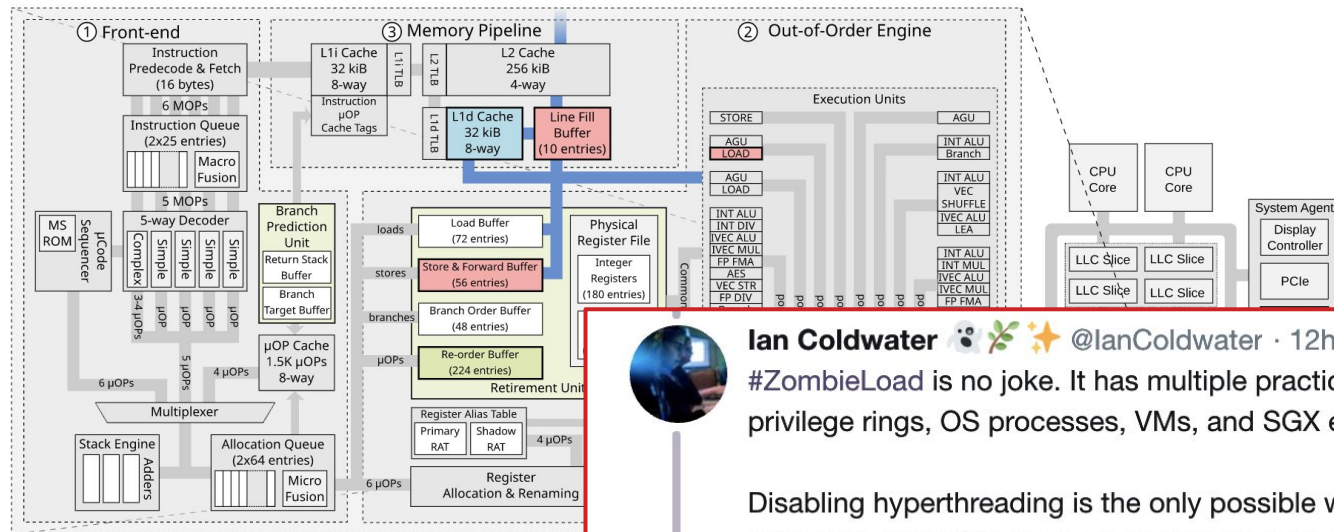
The business of security

Fundamental Economics

$1 to attack

$400 to defend

RED SIFT
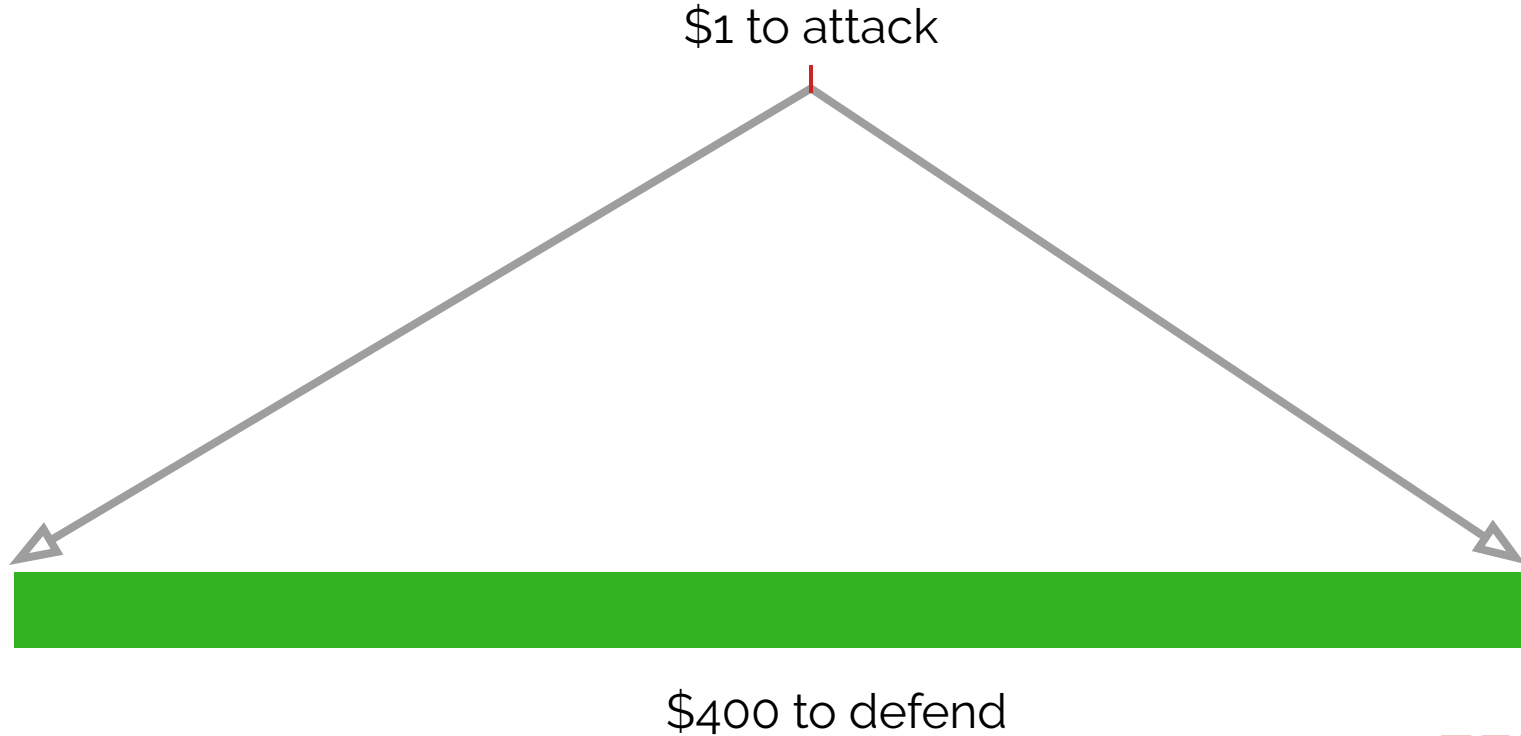
"They were still discussing pricing, when the Saudis said they wanted it immediately," says the businessman, who estimates the Saudi government paid $55m for the ability to track 150 targets simultaneously.*

What is a Proof of Concept Worth?

ZERODIUM Payouts for Mobiles*

RJB: Remote Jailbreak with Persistence
RCE: Remote Code Execution
LPE: Local Privilege Escalation
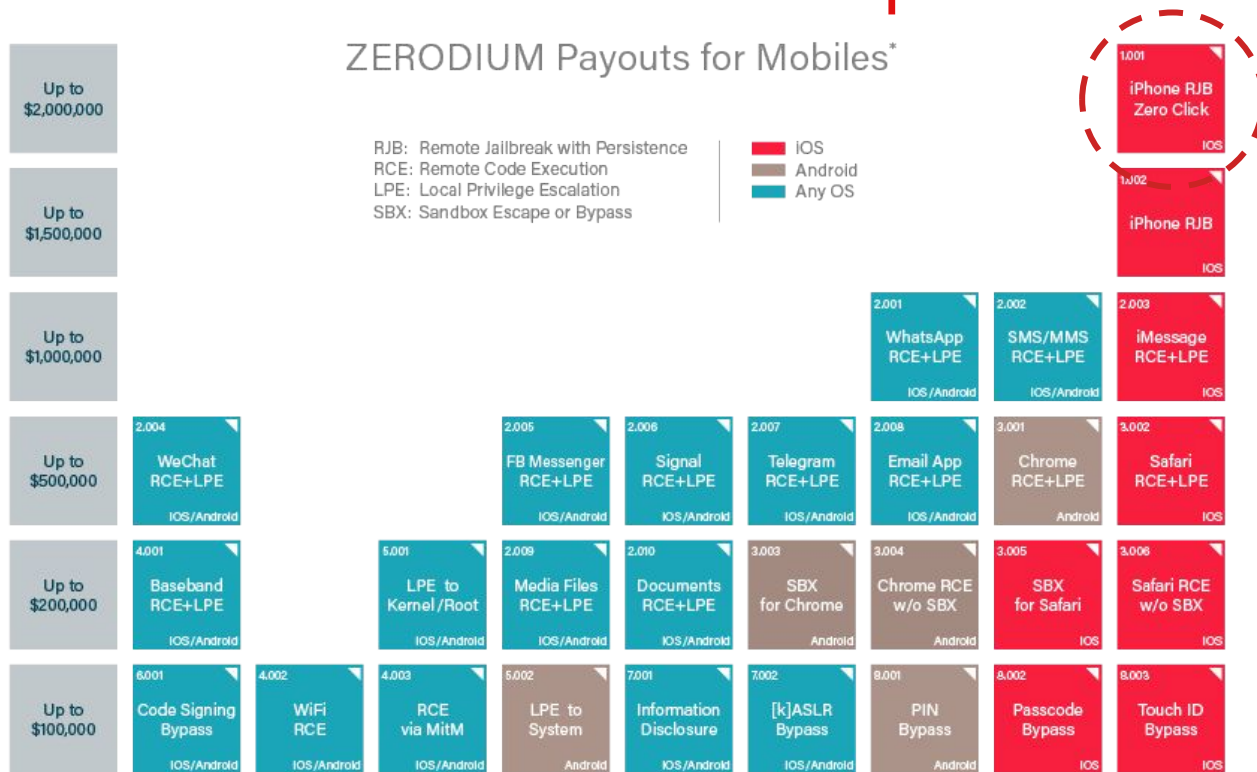SBX: Sandbox Escape or Bypass

- iOS
- Android
- Any OS

Up to $2,000,000								1.001 **iPhone RJB Zero Click** iOS
Up to $1,500,000								1.002 **iPhone RJB** iOS
Up to $1,000,000					2.001 **WhatsApp RCE+LPE** iOS/Android	2.002 **SMS/MMS RCE+LPE** iOS/Android	2.003 **iMessage RCE+LPE** iOS	
Up to $500,000	2.004 **WeChat RCE+LPE** iOS/Android		2.005 **FB Messenger RCE+LPE** iOS/Android	2.006 **Signal RCE+LPE** iOS/Android	2.007 **Telegram RCE+LPE** iOS/Android	2.008 **Email App RCE+LPE** iOS/Android	3.001 **Chrome RCE+LPE** Android	3.002 **Safari RCE+LPE** iOS
Up to $200,000	4.001 **Baseband RCE+LPE** iOS/Android	5.001 **LPE to Kernel/Root** iOS/Android	2.009 **Media Files RCE+LPE** iOS/Android	2.010 **Documents RCE+LPE** iOS/Android	3.003 **SBX for Chrome** Android	3.004 **Chrome RCE w/o SBX** Android	3.005 **SBX for Safari** iOS	3.006 **Safari RCE w/o SBX** iOS
Up to $100,000	6.001 **Code Signing Bypass** iOS/Android	4.002 **WiFi RCE** iOS/Android	4.003 **RCE via MitM** iOS/Android	5.002 **LPE to System** Android	7.001 **Information Disclosure** iOS/Android	7.002 **[k]ASLR Bypass** iOS/Android	8.001 **PIN Bypass** Android	8.002 **Passcode Bypass** iOS / 8.003 **Touch ID Bypass** iOS

* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

2019/01 © zerodium.com

RED SIFT

Enterprise is the growing target

Cost of breach to the company

Avg $3.6 million
IBM estimate, pre GDPR

$7.3 million in the USA
Not 'mega' breaches

$141 to $282 per data record

RED SIFT

The "hidden" costs can amount to 90 percent of the total business impact on an organization, and will most likely be experienced two years or more after the event.*

What Next?

@rahulpowar