Cybersecurity: From State Actors to Bedroom Hackers

BCS, May ‘19
Rahul

- **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
- **Today**: Red Sift - CEO
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
Cybersecurity: Why now?
“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.”

*washingtonpost.com 25th July 2012*
“After shutting down the network, the attackers played the song *Thunderstruck* by the hard rock band AC/DC at maximum volume.”*
Hacking goes OSS

The Social-Engineer Toolkit (SET) repository from TrustedSec - All new versions of SET will be deployed here.

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

Choose 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.

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):
Just scratching the surface

Ian Coldwater 🌱 ⭐ ⭐ @IanColdwater · 12h

#ZombieLoad is no joke. It has multiple practical attack scenarios across CPU privilege rings, OS processes, VMs, and SGX enclaves.

Disabling hyperthreading is the only possible workaround to prevent this extremely powerful attack on current processors.
The business of security
Fundamental Economics

$1 to attack

$400 to defend
“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*

<table>
<thead>
<tr>
<th>Payout</th>
<th>RCE</th>
<th>LPE</th>
<th>SBX</th>
<th>RJB</th>
<th>RCE+LPE</th>
<th>LPE+RCE</th>
<th>Any OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to $2,000,000</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Up to $1,500,000</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Up to $1,000,000</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Up to $500,000</td>
<td>2,001</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Up to $200,000</td>
<td>4,001</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Up to $100,000</td>
<td>6,001</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

2019/01 © zerodium.com
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
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