Hacking the 0day Market
• Director of Crowdfense Limited
• Most recently, Head of Cyber Security for KPMG
• Working in the ICT security field since the XX century 😊
• Member of the National Security Observatory (Italy) --> contributed to write Italy’s “National Cyber Strategy”
• Author of many cyber-security guidelines and best practices:
  • Italy's “Cybersecurity Framework”
  • ENISA's “Cybersecurity and Resilience for Smart Hospitals”
  • ....
The 0day Market Today

Historically, it’s unsafe, chaotic and inefficient from a business pov.

This hampers the (now strategic) ability of law enforcement and intelligence agencies to fight crime / terrorism / hostile geopolitical actors in the cyber domain.

Researchers are often underpaid for their exponentially complicated efforts.

There is a talent vacuum as underpaid researchers seek more lucrative fields / do research as a second job.
To combat the inefficiencies in the current market, we need to “normalize” and streamline this business:

- Protect and pay researchers more
- Reduce unnecessary middle men
- Dedicate more economic resources
- Develop and adopt best practices

Come on... It’s not 2003 anymore.
Hacking the 0day Market

Step #1: Launched the largest Public Bug Bounty Program in History
Seeking single exploits and full / partial exploit chains to support our customers in their targeted information gathering activities (LE and Intel).
Highest payouts in our industry.

Step #2: Launched the Vulnerability Research Hub
An innovative web-based collaboration platform that allows vulnerability researchers to safely submit, discuss and quickly sell single 0day exploits and chains of exploits.
Legal, safe and easy to use.
In April 2018 we launched our 10M USD Public Bug Bounty program, which offers the highest bounties ever paid for these classes of exploits. Thanks to this program, we were able to purchase top quality capabilities, and are in the process of buying more.

In 2019 we added more bounties (15M USD) and include more classes of exploits in our program.

<table>
<thead>
<tr>
<th>OS</th>
<th>Chain components</th>
<th>Persistence</th>
<th>Partial or Full chain Payouts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>Chrome RCE ➔ Sandbox Escape</td>
<td></td>
<td>1 click - Up to 1.5M USD</td>
</tr>
<tr>
<td>MacOS</td>
<td>Safari RCE ➔ Sandbox Escape</td>
<td></td>
<td>1 click - Up to 500k USD</td>
</tr>
<tr>
<td>iOS</td>
<td>Safari RCE ➔ iOS PE</td>
<td>✓</td>
<td>1 click - Up to 1.5M - 2.5M USD</td>
</tr>
<tr>
<td></td>
<td>Zero-interaction RCE ➔ iOS PE</td>
<td>✓</td>
<td>0 click - Up to 1.5M - 3M USD</td>
</tr>
<tr>
<td>Android</td>
<td>Chrome RCE ➔ Android PE</td>
<td>✓</td>
<td>1 click - Up to 1.5M - 2M USD</td>
</tr>
<tr>
<td></td>
<td>Zero-interaction RCE ➔ Android PE</td>
<td>✓</td>
<td>0 click - Up to 1.5M - 3M USD</td>
</tr>
<tr>
<td>Various</td>
<td>Instant Messengers or SMS/MMS RCE</td>
<td>✓</td>
<td>0 click up to 1.5M USD</td>
</tr>
<tr>
<td></td>
<td>Routers RCE ➔</td>
<td></td>
<td>1 click up to 1M USD</td>
</tr>
<tr>
<td></td>
<td>WiFi / Baseband RCE ➔ LPE</td>
<td></td>
<td>up to 100k USD</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>up to 500k USD</td>
</tr>
</tbody>
</table>
The Vulnerability Research Hub (VRH)

Step by step, user friendly workflows manage submission, discussion, testing, evaluation, contracting and payment.

Findings can be both within the scope of the Bug Bounty Program or freely proposed by researchers (within our Code of Conduct).

Based on a zero-trust model with maximum OpSec for all participants.
Some VRH stats from Q1 2019
## List of Submissions

<table>
<thead>
<tr>
<th>Type</th>
<th>Title</th>
<th>Creation Date</th>
<th>Update Date</th>
<th>Seller</th>
<th>Account</th>
<th>Status</th>
<th>Action Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Claim</td>
<td>Remote code execution for Android 6</td>
<td>29 Dec 2017 4:32PM</td>
<td>29 Dec 2017 4:32PM</td>
<td>Seller0001</td>
<td></td>
<td>Pending</td>
<td>Action Required</td>
</tr>
<tr>
<td>Public Bug Bounty</td>
<td>Sandbox escape for Chrome 59+</td>
<td>29 Dec 2017 4:32PM</td>
<td>29 Dec 2017 4:32PM</td>
<td>Seller0002</td>
<td>Account033</td>
<td>In evaluation</td>
<td></td>
</tr>
</tbody>
</table>
VRH Goals

A faster time-to-market for sellers.

Higher quality products for customers.
How to join the VRH
Thank you!

To learn more about or to discuss ways to partner with Crowdfense come speak to us after this presentation or visit our website: crowdfense.com

To join the VRH: vrh.crowdfense.com

For inquiries:
Researchers and customer: info@crowdfense.com
Media: press@crowdfense.com