Hacking the 0day Market
#WhoAmI -- Andrea Zapparoli Manzoni

- 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 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”
  - ….
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.
The 0day Market Today

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.
The Public Bug Bounty Program

In April 2018 we launched our 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 will add more bounties and include more classes of exploits in our program.
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.
The VRH

<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</td>
<td>29 Dec 2017</td>
<td>Seller0001</td>
<td>Account033</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</td>
<td>29 Dec 2017</td>
<td>Seller0002</td>
<td>Account033</td>
<td>In evaluation</td>
<td>Action Required</td>
</tr>
<tr>
<td>Public Bug Bounty</td>
<td>Remote code execution for Android 8</td>
<td>29 Dec 2017</td>
<td>29 Dec 2017</td>
<td>Seller0009</td>
<td>Account033</td>
<td>Code Evaluation</td>
<td>Action Required</td>
</tr>
<tr>
<td>Claim</td>
<td>Remote code execution for Android 9</td>
<td>29 Dec 2017</td>
<td>29 Dec 2017</td>
<td>Seller0044</td>
<td>Account033</td>
<td>Pending</td>
<td>Action Required</td>
</tr>
</tbody>
</table>
VRH Goals

A faster time-to-market for sellers.

Higher quality products for customers.
How to join the VRH

**Username**

**Email**

**PGP Key**

For security reasons, all communication from the VRH are PGP encrypted. We strongly suggest you to create a dedicated email address and to generate new keys for it. Please paste here the public key associated to the email address you provided above, without removing the ASCII Armor encoding tags.

**Private key passphrase**

The VRH is based on end-to-end encryption. To protect your data, we are going to generate a 4096-bit RSA keypair in your browser. Please choose a strong passphrase strong to be used to encrypt your private key.

Keep in mind that if this passphrase is lost all your data will become recoverable.

**Submission Details**

**Item title**

Android AAA Authentication Bypass

**Auction price (in dollars)**

- $10000

**Availability for exclusive acquisitions**

- Available
- Not Available

**Targets Information**

- Android 6.0
- Android 6.1
- Android 7.0
- Android 7.1

**Systems against which this is tested and functional**

- Monochrome tablet and blackberry android.
- Monochrome tablet and blackberry android.
- Monochrome tablet and blackberry android.
- Monochrome tablet and blackberry android.

**Reliability of the item against the specified versions**

- Monochrome tablet and blackberry android.
- Monochrome tablet and blackberry android.
- Monochrome tablet and blackberry android.
- Monochrome tablet and blackberry android.
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