How to hack, earn money and stay out of jail.

IOANNIS CHALKIADIS

CERN IT SECURITY TEAM

IT LIGHTNING TALK 04.12.15

CERN
Hacking started about curiosity and knowledge, now it is just business.
How much is the global spending in IT Security?

- Up to 77$ Billion in 2015*. 
- Is it enough?

*http://cybersecurityventures.com/cybersecurity-market-report/
I ask you again is it enough?
Biggest data breaches in the last decade *

<table>
<thead>
<tr>
<th>Company</th>
<th>Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>JP Morgan Chase</td>
<td>76.000.000</td>
</tr>
<tr>
<td>Sony</td>
<td>77.000.000</td>
</tr>
<tr>
<td>Ebay</td>
<td>145.000.000</td>
</tr>
<tr>
<td>Adobe</td>
<td>36.000.000</td>
</tr>
<tr>
<td>Apple</td>
<td>12.400.000</td>
</tr>
<tr>
<td>US Military</td>
<td>76.000.000</td>
</tr>
<tr>
<td>Yahoo</td>
<td>22.000.000</td>
</tr>
</tbody>
</table>

*http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
24 year old Algerian
- ZEUS BOTNET-
3.600.000 million infected machines
70 million $$ loss
27 year old Russian
- BLACKHOLE EXPLOIT KIT-

97% of 2014 browser threats was from blackhole. (AVG)

Was making 70.000$ per month selling his kit

←------ He was smart huh?

You know how he got arrested?

He posted this picture in his Facebook profile.. Meh..
What is bug bounty, terms/rules

You report -> They reply -> Fix or will not fix -> Reward/Thank you
99% of the companies have this list of rules:

- Do not cause DOS (Denial of service) to their services.
- The vulnerability should not affect the user data or critical information.
- Responsible and ethical disclosure to the company.
- Do not share it with any third parties.
<table>
<thead>
<tr>
<th>Company</th>
<th>Description</th>
<th>Bug Bounty Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dropbox</td>
<td>A free service that lets you bring your photos, docs, and videos anywhere and share them easily.</td>
<td>$216 - $4,913 Per Bug</td>
</tr>
<tr>
<td>AVG Technologies</td>
<td>The online security company</td>
<td>$50 - $1,000 Per Bug</td>
</tr>
<tr>
<td>Tesla Motors</td>
<td>Accelerating the world’s transition to electric mobility</td>
<td>$25 - $10,000 Per Bug</td>
</tr>
<tr>
<td>Pinterest</td>
<td>Discover ideas for any project or interest, hand-picked by people like you.</td>
<td>$50 - $1,500 Per Bug</td>
</tr>
<tr>
<td>LastPass</td>
<td>LastPass is a password manager and form filler which locally encrypts your sensitive data with a key that is not sent to LastPass</td>
<td>$50 - $1,000 Per Bug</td>
</tr>
<tr>
<td>ProtonMail</td>
<td>Email Privacy For All</td>
<td>$50 - $500 Per Bug</td>
</tr>
<tr>
<td>Socrata</td>
<td>Put your skills to the test!</td>
<td>$25 - $1,500 Per Bug</td>
</tr>
<tr>
<td>Jet.com</td>
<td>The most brilliant way to shop.</td>
<td>$25 - $2,500 Per Bug</td>
</tr>
<tr>
<td>Category</td>
<td>Examples</td>
<td>Applications that permit taking over a Google account [1]</td>
</tr>
<tr>
<td>--------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td>Vulnerabilities giving direct access to Google servers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote code execution</td>
<td>Command injection, deserialization bugs, sandbox escapes</td>
<td>$20,000</td>
</tr>
<tr>
<td>Unrestricted file system or database access</td>
<td>Unsandboxed XXE, SQL Injection</td>
<td>$10,000</td>
</tr>
<tr>
<td>Logic flaw bugs leaking or bypassing significant security controls</td>
<td>Direct object reference, remote user impersonation</td>
<td>$10,000</td>
</tr>
<tr>
<td>Vulnerabilities giving access to client or authenticated session of the logged-in victim</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Execute code on the client                                  | Web: Cross-site scripting  
Mobile: Code execution                      | $7,500                                                   | $5,000                                   | $3,133.7                  | $100                                                                |
| Other valid security vulnerabilities                          | Web: CSRF, Clickjacking  
Mobile: Information leak, privilege escalation | $500 - $7,500                                            | $500 - $5,000                            | $500 - $3,133.7           | $100                                                                |
My Personal Adventures

**Google**

- Contacted them 17.10.14
- Got Response 18.10.14
- Triaged Situation (implementing fix) 19.10.14
- Fixed Reward $$ and thank you email. 21.10.14
My Personal Adventures

**Western union:**

- Contacted them 11.05.15
- Got Response 16.05.15
- Triaged Situation (implementing fix) 24.05.15
- Fixed Reward $$ and thank you email. 03.06.15
Western Union tại Việt Nam

- Trang chủ
- Giới thiệu về chúng tôi

Xác Định Vị Trí

Có một đại lý gần chỗ bạn!

Tìm điểm Western Union gần nhất tại Việt Nam

Chọn Tỉnh/Thành phố

Tìm kiếm nâng cao

Thêm nhiều trang web của Western Union!

Quý vị có thể gửi tiền qua mạng internet tại các quốc gia sau:

Chọn quốc gia

Các trang web khác của Western Union:

Chọn trang web

GIỚI THIỆU VỀ CHÚNG TÔI

- Tổng quan
Sites that host bug bounty programs

https://bugcrowd.com/programs

https://hackerone.com/directory
Want to learn more and improve?

Become a pen-tester:
white-hats@cern.ch
Any Questions?