Cyber Analytics

JANAKIRAM PULIPATI
KOWSIK KRISHNAN
PARAMA DUTTA
SHRIRAM CHANDRA ANBALAGAN

Section # 1
Introduction

- Cyber-attacks claim 1.5 million victims per day

- Malware, or malicious software attacks, increased 30 percent in 2012

- Malware on mobile devices grew by 139 percent. 15 percent of the world’s internet traffic is mobile

- Amount of sensitive information available in an organization is increasing exponentially

- Between December 23, 2013 and January 6, 2014 Proofpoint researchers detected a botnet that was aggressively mailing malicious spam three times each day. Proofpoint believes the 450,000 IP-address strong spam botnet included over 100,000 “Internet of Things” devices
Research Questions

- Who are the significant contributors to the Hacker Web forum? (slide 8-16)
- What are the most trending topics being discussed in Hacker Web? (slide 17)
- Analyze the organization and the Operating Systems that have installed the network products from various networking products companies and that are exposed by Shodan. (slide 21-22)
- Analysis on the ISP, cities and countries, that were most exposed by Shodan (slide 23-25)
Research Design

Hacker Web

- Perform text visualization on the hacker web database
- Determine the list of words with high frequency from the visuals
- Use list of words to
  a) Identify and analyze demographic information and temporal behavior of hacker
  b) Perform trend analysis of the hacker web data
Research design

- Shodan
  - Created an R library to retrieve data from Shodan API
  - Performed data analysis and visualization – bar plot and map plot
  - Expanded R libraries to perform statistical operations and better visualizations
  - Future work involves creating a custom JSON parser code that will effectively parse the Shodan results to make the entire process more automated.
## Tools Used

<table>
<thead>
<tr>
<th>Hacker Web</th>
<th>Shodan</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM Many Eyes</td>
<td>R programming</td>
</tr>
<tr>
<td>Microstrategy Analytic Express</td>
<td>Rapid Miner</td>
</tr>
<tr>
<td>Google Fusion</td>
<td>Google Fusion</td>
</tr>
<tr>
<td>Heidi SQL</td>
<td></td>
</tr>
<tr>
<td>Microsoft Excel</td>
<td></td>
</tr>
</tbody>
</table>
Hacker web
Hacker 1 Demographics:

- Name: Moh3eN (alias Moheen)
- Hacker-web ID: 21127
- Country: Tehran, Iran.
- Age: Mid-thirties
- Likes a page called ‘Group born in 60s and 70s’
- One of the most active in www.mihandownloadforum
Temporal behavior
Temporal behavior analysis

- Most active on weekends, non-working hours
- Probably an employee
- Hacking activity must be his passion
Hacker 1 statistics

- Total Posts: 14258
- Average number of posts per day: 8.16
- Joined date: 2009
- Last activity date: 2013
Hacker 1 activity

- Posted downloads links for paid softwares, games, TV series
- Posted keys, cracks, serials

Consequences
a) Huge loss for organizations
b) Encouraged illegal activity
Hacker-2 Demographics

- **Name**: Shahroze Rashid
- **Hacker-web ID**: 4512
- **Location details**
  - (a) **Native Country**: Pakistan
  - (b) **City**: Near Haripur
  - (c) **Northern part of Pakistan**
  - (d) **Current City**: California

**Food for thought:**

Likes the page “Cycling across Haripur” and “Northern Part of Pakistan”. We infer that he comes from Haripur, a town in northern part of Pakistan.
Email ID: shahrozerasheed007@gmail.com

Facebook ID: fb.com/sahrozeecute

Education: University of Central Punjab/Lahore Central university
Hacker 2 in pictures

EliteHackForums

Full Version: need hacker quick!!

You're currently viewing a stripped down version of our content. View the full version with proper layout.

duchess

in need of hacker to change grades ASAP willing to pay..

l4info

hello i can do it,, email me at shahrozerashid007@gmail.com

---

Assalam o alaikum everyone.. its shahroze here

today i will show u my ultimate all in one email hacker..

with the help of this software u can hack any account :)

ok lets start :p

my victim id is: cheerybelle@yahoo.com

lets hack this id

I am gonna hack fb id :p

---

To see what he shares with friends, send him a friend request.

Studied Ethical Hacking and Countermeasures at Histo.org

Lives in California City, California

Followed by 190 people

Admin at Histo.org

About: Student and well educated CA.
Temporal behavior of Hacker 2 - Shahroze

Most busy during non-working hours
Hackers like discussing about...

- PHP, Java
- DDoS, DNS Attacks, Social engineering, SQL injection
- Talking about Social Media (Facebook, skype etc)
- Browsers: Google chrome, Firefox
- Post viruses, softwares, games etc
- USA, Korea, Taiwan, Canada, Seoul
SHODAN
“Shodan Search API” - retrieves the Shodan search result from SHODAN API
Features of R-script

Our R-script…

- retrieves data from Shodan’s
  - search API
  - location API
  - host API
- auto-exports
  - visualization of analysis as PNG file
  - the results as CSV to facilitate additional visualizations
- is simple and efficient
Organization wise analysis

List of Top –10 Vulnerable Organizations exposed by Shodan

Graphical representation of ‘org’ field in Shodan Search API
<table>
<thead>
<tr>
<th>Affected OS</th>
<th>Graphical Representation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux 2.4-2.5</td>
<td>![Graph for Linux 2.4-2.5]</td>
</tr>
<tr>
<td>Linux 2.5x</td>
<td>![Graph for Linux 2.5x]</td>
</tr>
<tr>
<td>Linux 3.0x</td>
<td>![Graph for Linux 3.0x]</td>
</tr>
<tr>
<td>Windows 7 or 8</td>
<td>![Graph for Windows 7 or 8]</td>
</tr>
<tr>
<td>Windows XP</td>
<td>![Graph for Windows XP]</td>
</tr>
<tr>
<td>N/A</td>
<td>![Graph for N/A]</td>
</tr>
</tbody>
</table>

Graphical representation of ‘OS’ field in Shodan Search API
ISP wise Analysis

List of Top – 20 Vulnerable ISP exposed by Shodan

Graphical representation of ‘ISP’ field in Shodan Search API
ITC Analysis - Worldwide

Vulnerable devices from ITC Organization
Worldwide Shodan Exposures

Heat-map of vulnerable cities
Conclusion – Hacker Web

- Most talked about...
  - Languages: PHP, Java
  - Types of Attacks: DDoS, DNS Attacks, Social engineering, SQL injection
  - Social Media: Facebook, YouTube, Skype
  - Browsers: Google Chrome, Firefox

- Hacker Behavior
  - Doing mostly out of self interest
  - Damaging organization’s revenue (Moheen)
  - Threat to user’s security (Shahroze)
  - Active mostly during non-working hours
Conclusion - Shodan

- Most Vulnerable Organization: Information Technology Company (ITC)
- Most Vulnerable ISP: Information Technology Company (ITC)
- Most Vulnerable OS: Windows 7 and 8
- Most vulnerable countries: USA, South East countries
Interesting Correlation

- Most talked about countries in hacker web - US, Southeast countries (Korea, Taiwan)
- Most vulnerable countries for shodan - US, Southeast countries
- Major network product manufacturers - US, Taiwan

Conclusion – Major network product manufacturing countries are most interesting to hackers and are most vulnerable
References

- http://www.r-bloggers.com/shodan-api-in-r-with-examples/
- http://www.bloomberg.com/markets/companies/networking-products/
Thank you