Cyber Analytics Project

Team
- Akhil Ashok Kanakkasserry
- Allan Babu Kurian
- Maninderjit Singh
- Tom Thomas
Content

- Introduction
- Data collection and analysis techniques.
- Is our personal data in right hands?
  - Social Engineering
  - Data Mining and Spamming
- Mobile Malware getting smarter?
- Economic impacts of piracy.
- Security analysis of NTP.
Introduction

- Cyber security deals with safeguarding the user information on the web

- Cybercrimes have ever been rampant since the explosion of most modern internet technologies.

- Though there are measures to contain and prevent them, new ways of exploiting the security measures adopted are being found out by hackers
Research Tool Design for HackerWeb

- Web tool in Visual Studio 2013, using the MVC architecture to query data from the hacker web.

- A search engine to HackerWeb database.

- Generates MySQL query for the database dynamically.

- The capability to query all the tables together and also the multilingual information.
### Research Tool Design for HackerWeb

#### Key Word Search

Enter Keywords with space:

<table>
<thead>
<tr>
<th>Keyword</th>
<th>ThreadID</th>
<th>NumOfPosts</th>
<th>ForumName</th>
</tr>
</thead>
<tbody>
<tr>
<td>hack web</td>
<td>1322</td>
<td>0</td>
<td>anon</td>
</tr>
<tr>
<td>Met A Webmaster Telling Me His Wp Sites Are Unhackable</td>
<td>996</td>
<td>1</td>
<td>anon</td>
</tr>
<tr>
<td>Hacking specific websites</td>
<td>72</td>
<td>0</td>
<td>anon</td>
</tr>
<tr>
<td>How Did My Website Get Hacked? how To Hack A Website</td>
<td>378</td>
<td>0</td>
<td>anon</td>
</tr>
<tr>
<td>I Want To Hack This Websites:</td>
<td>1028</td>
<td>0</td>
<td>anon</td>
</tr>
<tr>
<td>Learn The Basics To Website And Server Hacking</td>
<td>936</td>
<td>3</td>
<td>anon</td>
</tr>
<tr>
<td>Hacking Tools Website</td>
<td>651</td>
<td>12</td>
<td>anon</td>
</tr>
<tr>
<td>For All Those Who Want To &quot;hack&quot; facebook Or Any Website Like Facebook</td>
<td>742</td>
<td>20</td>
<td>anon</td>
</tr>
<tr>
<td>Portal Hacking (Dm) - Website Hacking Technique Explained !</td>
<td>372</td>
<td>0</td>
<td>anon</td>
</tr>
<tr>
<td>10 reasons websites get hacked</td>
<td>50964</td>
<td>0</td>
<td>antichat</td>
</tr>
<tr>
<td>Web-Hack</td>
<td>4579</td>
<td>27</td>
<td>antichat</td>
</tr>
<tr>
<td>BackTrack website Hacked</td>
<td>116317</td>
<td>12</td>
<td>antichat</td>
</tr>
<tr>
<td>Hacked websites for sale at Russian underground store</td>
<td>390712</td>
<td>0</td>
<td>antichat</td>
</tr>
<tr>
<td>Russian hacked thousands of WebMoney accounts</td>
<td>92687</td>
<td>19</td>
<td>antichat</td>
</tr>
<tr>
<td>Website for computer security experts hacked</td>
<td>53482</td>
<td>0</td>
<td>antichat</td>
</tr>
<tr>
<td>Web-Hack - trovamento =)</td>
<td>5439</td>
<td>n/a</td>
<td>antichat</td>
</tr>
<tr>
<td>The_web_Application_Hackers_Handbook</td>
<td>69531</td>
<td>2</td>
<td>arhack</td>
</tr>
<tr>
<td>hack by 1h1hack dz-hack italien web site</td>
<td>13786</td>
<td>4</td>
<td>arhack</td>
</tr>
<tr>
<td>22 Website HackED</td>
<td>66063</td>
<td>3</td>
<td>arhack</td>
</tr>
<tr>
<td>Hacked 4 Websites</td>
<td>46514</td>
<td>7</td>
<td>arhack</td>
</tr>
<tr>
<td>hacked 2 webs system windows xp by 70p-h4ck3r</td>
<td>26854</td>
<td>5</td>
<td>arhack</td>
</tr>
<tr>
<td>jossor.org Hacked by mr.crazyweb</td>
<td>32331</td>
<td>5</td>
<td>arhack</td>
</tr>
</tbody>
</table>
Research Tool Design for HackerWeb

Keyword Search for HackerWeb

Key Word Search

Enter Keywords with space

Search Results for 黑客网站 || Results Found: 20

<table>
<thead>
<tr>
<th>Post</th>
<th>ThreadID</th>
<th>NumOfPosts</th>
<th>ForumName</th>
</tr>
</thead>
<tbody>
<tr>
<td>献给红盟的所有兄弟姐妹----全球顶级黑客网站大集合</td>
<td>107309</td>
<td>479</td>
<td>enbunkerarmy</td>
</tr>
<tr>
<td>各大黑客网站VIP--学完你就是大牛(转)</td>
<td>140924</td>
<td>13</td>
<td>enbunkerarmy</td>
</tr>
<tr>
<td>入 侵黑客网站之旅【转】求黑客网站邀请码啊</td>
<td>91565</td>
<td>44</td>
<td>enbunkerarmy</td>
</tr>
<tr>
<td>部分国际黑客网站站点</td>
<td>146552</td>
<td>3</td>
<td>enbunkerarmy</td>
</tr>
<tr>
<td>公布几个各大黑客网站的网盘!</td>
<td>136938</td>
<td>5</td>
<td>enbunkerarmy</td>
</tr>
<tr>
<td>浙江嘉兴某男做钓鱼站及黑客网站圈钱被判半年</td>
<td>113649</td>
<td>39</td>
<td>enbunkerarmy</td>
</tr>
<tr>
<td>国外黑客网站！！！！！</td>
<td>40397</td>
<td>1</td>
<td>enbunkerarmy</td>
</tr>
<tr>
<td>某黑客网站教程（1-50）（大家顶下，第一次发贴）</td>
<td>23374</td>
<td>29</td>
<td>enbunkerarmy</td>
</tr>
<tr>
<td>2013年黑客网站大全 亲自整理!所以网站都能打开,史上最全。</td>
<td>59362</td>
<td>15</td>
<td>enbunkerarmy</td>
</tr>
<tr>
<td>最近诸多黑客网站被黑的幕后黑客资料曝光</td>
<td>151871</td>
<td>14</td>
<td>enbunkerarmy</td>
</tr>
<tr>
<td>国内最大黑客网站被查 对会员暂不能定罪</td>
<td>6896</td>
<td>3</td>
<td>hackdark</td>
</tr>
<tr>
<td>黑客基地被黑客国内最大的黑客网站被黑hackbase.com</td>
<td>1284</td>
<td>1</td>
<td>hackdark</td>
</tr>
<tr>
<td>各大黑客网站VIP--学完你就是大牛了！！！！！</td>
<td>277365</td>
<td>8</td>
<td>hackdark</td>
</tr>
<tr>
<td>黑客网站负责人因培训黑客技术入狱</td>
<td>72492</td>
<td>4</td>
<td>unpack</td>
</tr>
<tr>
<td>中国100强黑客网站网址</td>
<td>62262</td>
<td>17</td>
<td>unpack</td>
</tr>
<tr>
<td>内部最大黑客网站&amp;quot;黑客安全网&amp;quot;负责人被抓!</td>
<td>11253</td>
<td>3</td>
<td>unpack</td>
</tr>
<tr>
<td>CCTV达拾在线警方揭开黑客网站真相[图]</td>
<td>45788</td>
<td>31</td>
<td>unpack</td>
</tr>
<tr>
<td>中国第一家黑客网站被抄袭</td>
<td>19272</td>
<td>0</td>
<td>unpack</td>
</tr>
<tr>
<td>一个帖子已经出问题了的&amp;quot;黑客网站关门不找我&amp;quot;</td>
<td>38252</td>
<td>47</td>
<td>unpack</td>
</tr>
<tr>
<td>Waiting for localhost...</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Research Tool Design for Shodan

- Shodan API was used to gather data for the analysis of the NTP ports
- A basic python program using the shodan API was used to collect the count of NTP ports in various US cities.

**Code Snippets**

```python
# for cities is US
results = api.search('port:123 city:"X" country:US')

    # Show the results
    print results['total']

# for countries
results = api.search('port:123 country:Y')

    # Show the results
    print results['total']
```
Question 1: Is our personal data is in right hands?

- The rapid growth of social media is giving rise to new types of cyber threats.
- These threats affect the psychological, social and cultural aspect of social media users.
- Social Network sites act as a platform for Phishers and Spammers for carrying out their fraudulent activities.
- Even the governments and organizations are finding it difficult to curb the cybercrimes related to social media.
Sophos 2013 Security threat report

- Facebook is the most targeted place for cybercrime

Threats percentage-pose on social network
Social Media Suspicious Posts distribution

Suspicious Post Distribution

TOTAL

Fourm
- anon
- antichat
- arhack
- ashiyane
- cnhonkerarmy
- elitehack
- exploit
Classification of cyber crimes

- **Social Engineering**: Social engineering techniques are mostly used for identity thefts, it includes the theft of users' account credentials.

- **Data Mining & Spamming**: Cyber criminals use data mining techniques to extract the user information by using data collections methods like survey and questionnaire.
Social Engineering posts trend

Count of Post

Total

anon | antichat | arhack | ashiyane | cthonkerarmy | elitehack | hackhound | icode | shabgard | v4team | vctool
---|---|---|---|---|---|---|---|---|---|---
3  | 1  | 1  | 1  | 1  | 10 | 2  | 1  | 3  | 8  | 10
Social Media spammer posts distribution

Source: Hacker Web
Question 2: Mobile malware getting smarter?

- As the web landscape is now inclined towards the internet of things, it is highly vulnerable to the mobile based malwares.

- As the landscape is changing, malware author has learned to build the malware which cannot be identify by the cutting edge technology of detecting the virus.
Things which helps cyber criminals to have an edge over mobile developer:

- The mobile devices are becoming more efficient in handling traditional desktop task.

- Second is the growth of mobile apps market. More users are downloading the apps regularly without doing any verification regarding the apps.
Mobile Malware Trends

Source: Hacker Web
Mobile Vulnerability Distribution

- Iphone: 51%
- android: 48%
- Windows: 1%

Source: Hacker Web
Findings

- IPhone and Android are mobile devices which are more vulnerable to malware.

- Even though the number of posts pertaining to Iphone are more, but the number of malware suspicious posts are more for Android devices.

- We can infer that Android platform is more vulnerable to cyber criminals as predicted by Cisco 2014 security annual report.
Research Question 3: Analysis of Piracy Activity in Forums

- Software Piracy is the unauthorized usage or copying of software.
- Though copying for backup purposes is allowed, sharing is considered illegal.
- The illegal sharing and copying of software causes losses to the count of millions of dollars to the software industry annually.
Literature Review

- **Software crack** is the modification of software to disable or remove features which are used to protect it from being used without the license.

- **Serial number** is a license code issued to the authorized user to validate his use of the software/application.

- **Keygen** is the another way to circumvent the authentication of the software.
Data Analysis - Serial Number Activity

Serial Number Activity in HackerWeb Forums

[Bar chart showing the activity levels for different usernames, with 'total' on the right side of the chart.]
Keygen Activity

Keygen Activity in HackerWeb Forums

- antichat
- ahref
- ashbyne
- elitehack
- hackdark
- hackhound
- icode
- mhtdownload
- shagard
- unpack
- v4team
- vcool
- xakepok

Total
Crack Activity

Crack Activity in HackerWeb Forums

- Total
Findings

- The forum Unpack is highly active in distributing cracks, keygens and serial numbers
- arhack, ashiyane, elitehack, myhandownload and vctool have a lot of discussions going on about serial numbers.
Network Time Protocol (NTP) is an internet protocol used for time synchronization of clocks of computers to some time interface.

Security Concerns

- Run replay attacks using captured OTP and Kerberos tickets before they expire.
- Stop security-related cron jobs from running or cause them to run at incorrect times.
- Make system and audit logs unreliable since time is alterable.
Research Design & Data Obtained

- Shodan API used to gather data for analysis of the NTP ports

- A basic python program using the shodan API was used to collect the count of NTP ports in various US cities. The sample code is given below:

```python
# for cities is US
results = api.search('port:123 city:"X" country:US')

    # Show the results
    print results['total']

# for countries
results = api.search('port:123 country:"Y"')

    # Show the results
    print results['total']
```
NTP Distribution In Major US Cities
NTP Devices Distribution Across the World

- US: 25.00%
- China: 4.00%
- India: 0.80%
- Russia: 6.00%
- Japan: 10.00%
- Germany: 2.00%
Findings

- The major finding is that US has about 25% of the total NTP vulnerabilities in the world.
- Houston, New York and Dallas are most vulnerable in that order. But the distribution we found is all over the country.
THANK YOU