INTRODUCTION

The purpose of this project is to research different cyberspace vulnerabilities and opportunities.

Cyber analytics offers a better understanding of organizations’ infrastructure and its vulnerabilities.

In this project we have researched different vulnerabilities such as –

- The state of Automatic Teller Machine security in the wake of the 2009 Russian ATM hack
- Cracking WEP/WPA wireless networks
- Trojan malware and its impact
- Use of keylogger to hack information
RESEARCH QUESTIONS

- What is the state of Automatic Teller Machine security in the wake of the 2009 Russian ATM hack using the Troj/Skimmer-A malware and the 2013 $44.7 million worldwide ATM cyberheist?

- How can I crack a WEP or WPA wireless network and analyze packet exchange in a network?

- How is Zeus Bot setup in the system, the links where it can be hosted and how to avoid Zeus Tracker?

- How can we use Keylogger to “hack” information?
Automatic Teller Machines

**BACKGROUND**

- **2009** – Russian hackers use Skimmer-A Trojan to hack ATMs
  - Required the employment of an insider to inject the Trojan in person
  - Diebold ATMs
- **2013** – Worldwide cyber gang employs 2 part scheme resulting in $44.7 million cyber heist
  - Social Engineering for database access (phishing)
  - International cooperation of multiple cells of the cyber gang
import MySQLdb
from shodan import WebAPI

SHODAN_API_KEY = "T3whkyVHH7AlP28INq7hVNIK638vR"
api = WebAPI(SHODAN_API_KEY)

try:
    # Search Shodan
    shodansearch = raw_input( 'Enter Search Parameter' )
    results = api.search(shodansearch, page=1, limit=3000, offset=None)

    # Show the results
    print 'Results found: %s' % results['total']
    for result in results['matches']:
        # searchid = '0'
        ip = result['ip']
        port = result['port']
        # server = result['names']
        # mac = result['mac']
        city = result['city']
        country = result['country_name']
        # operatesys = result['os']
        updatedt = str(result['updated'])

        lat = str(result['latitude'])
        lon = str(result['longitude'])
        devicedata = result['data']
        portnum = int(port)
        strip = str(ip)
        # strhost = ('\n'.join((host)))

        # Open database connection
db = MySQLdb.connect(host='127.0.0.1',
                             user='shodan',
                             passwd='shodan',
                             db='ShodanDB')

        # prepare a cursor object using cursor() method
cursor = db.cursor()

        null = None

        sql = "INSERT INTO dv_ip_atm (ip, port, city, country, updated, lat, lon, devicedata) VALUES ("%s",%s,%s,%s,%s,%s,%s,%s)"
        try:
            # Execute the SQL command
            cursor.execute(sql)
            # Commit your changes in the database
db.commit()
            print "Successfully inserted 1 row"
        except:
            # Rollback in case there is any error
db.rollback()
            print "Error inserting Data: rollback"
            print "Error on IP '%s'" % strip
            # disconnect from server
db.close()

except Exception, e:

United States Devices

SELECT ip, port, country, devicedata
FROM dv_ip_atm
WHERE country="United States";

United Kingdom devices

SELECT ip, port, country, devicedata
FROM dv_ip_atm
WHERE country="United Kingdom";
ATM Protections

- DV-IP ATM device
- Video and embedded transaction logging
- Available web interface

- Human factor remains weakest link
- Unprotected web interface accessible
ATM Findings

Distribution of DV-IP ATM Device

**DV-IP ATM DISTRIBUTION**
- United Kingdom: 47%
- United States: 23%
- Sweden: 8%
- Germany: 9%
- France: 8%

**DV-IT ATM Dist - Tail End**
- Turkey: 17%
- Australia: 13%
- India: 8%
- Ireland: 8%
- Ireland: 8%
- Australia: 8%
- Malta: 4%
- Norway: 4%
- Czech Republic: 4%
- Spain: 4%
- Switzerland: 4%
Aircrack

- Cracking WEP and WPA (Dictionary attack) keys
- Decrypting WEP or WPA encrypted capture files with known key
- Packet sniffer: Places air traffic into PCAP or IVS files and shows information about networks
- Creating encrypted packets for injection
- Allows you to access the wireless card from other computers
Aircrack – Database posts

Database posts

- anonposts: 5
- elitehackposts: 17
- hackhoundposts: 16
- vctoolposts: 12
Aircrack - Statistics

<table>
<thead>
<tr>
<th>Title</th>
<th>Stats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database posts</td>
<td>50</td>
</tr>
<tr>
<td>First post</td>
<td>27-Jan-10</td>
</tr>
<tr>
<td>Last post</td>
<td>10-Sep-13</td>
</tr>
<tr>
<td>Post rank of 1</td>
<td>29</td>
</tr>
<tr>
<td>Unique authors</td>
<td>24</td>
</tr>
<tr>
<td>Threads</td>
<td>15</td>
</tr>
<tr>
<td>Posts with attachments</td>
<td>4</td>
</tr>
</tbody>
</table>
Aircrack - Findings

- For cracking, 5,000 Data/IV's for 64 bit encryption and 10,000 Data/IV's for 128 bit encryption
- 128 bit WEP key can be cracked in less than 2 minutes
- It is less efficient on UNIX systems
- It's a little bit longer when it's a WPA protection because of the handshake and dictionary attack for cracking process
- For WEP, you need to collect IV packets, once you have a sufficient amount
- WPA, PSK and AES can be cracked
Zeus BotNet:

- A toolkit providing a malware creator with all tools required to build and administer a botnet

- Some of the features of this botnet:
  - Captures credentials over HTTP, HTTPS, FTP, POP3 and Steals/deletes HTTP and flash cookies
  - Steals client-side X.509 public key infrastructure certificates
  - Captures screenshots and scrapes HTML from target sites
  - Modifies the local hosts file
  - Groups the infected user systems into different botnets to distribute command and control
  - Has a major function to kill the operating system
  - Sends a lot of information to C&C server, such as the version of the bot, operating system, local time, geographic locations, etc.
Zeus Botnet – Database posts

![Number of posts](image)
Zeus and its variant account for half of total known banking malware.
Zeus Botnet - Findings

- Mirage Anti-Bot: a software that blocks all known bots site including:
  - Zeus Bot, Palevo Bot and Spyeye Bot
- The code to avoid Zeus Tracker, a software that tracks Zeus Botnet
- Latest Version: Zeus 3.0 (upgrade to GameOver Zeus)
- Setup of Zeus Botnet
- Links to host Zeus Botnet
Keylogger:

- A keylogger also know as keystroke logger is software or hardware device which monitors each and every key typed by you on your keyboard.

- Keylogger can also harm you by storing all the sensitive information such as your username and password, bank credit card details etc.

- There are two types of keylogger hardware keylogger and software keylogger.

- Software keylogger is installed in your computer where as a Hardware keylogger is attached to your keyboard.

- For the hardware, it is easy to discover, however, it is hard for people to realized that if they are using a computer with a keylogger software.
Keylogger – Database posts

# of related results

- U.S.: 454
- China: 162
# Keylogger - Statistics

<table>
<thead>
<tr>
<th>Name of Table</th>
<th># of 1st postrank</th>
</tr>
</thead>
<tbody>
<tr>
<td>anonposts</td>
<td>17</td>
</tr>
<tr>
<td>elitehack</td>
<td>53</td>
</tr>
<tr>
<td>hackhound</td>
<td>16</td>
</tr>
<tr>
<td>icode</td>
<td>33</td>
</tr>
<tr>
<td>vctool</td>
<td>106</td>
</tr>
<tr>
<td>unpack</td>
<td>129</td>
</tr>
<tr>
<td>cnhonkerarmy</td>
<td>14</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>368</strong></td>
</tr>
<tr>
<td><strong>Percentage</strong></td>
<td><strong>59.74%</strong></td>
</tr>
</tbody>
</table>
Keylogger - Findings

- Based on the data from Hacker Web, there are total seven tables who is talking about the Keylogger.

- Two of them are Chinese forums and rest of them are U.S. From the Pie Chart we can see the partition of these two countries' discussion results of Keylogger.

- From the Table we can see that the Keylogger is a very hot topic in the world wide.

- There are above 50% of the posts are ranking the 1st in the forums that is discussing about the Keylogger.
REFERENCES

- http://www.aircrack-ng.org/
- http://hackhound.org/forums/topic/1303-wifi-cracker/
- http://vctools.net/forum/Thread-tutorial-setup-zeus-bot-with-pictures-tutorial#axzz2uOBW2z1X
- http://vctools.net/forum/Thread-how-to-avoid-zeustracker#axzz2uOBW2z1X
- http://vctools.net/forum/Thread-where-to-host-your-istealer-zeus#axzz2uOBW2z1X
- https://www.tritonatm.com/products/triton_connect/