RESEARCH QUESTION 1

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?

Introduction:

In 2009, it was discovered that Russian hackers employed the assistance of an insider at Diebold to inject the Skimmer-A Trojan onto their Automatic Teller Machines (ATMs) throughout eastern Europe. This malware enabled the Russian hackers to remotely capture card data and PINs. While they hackers needed to employ an insider to get physical access to the machines, the ability to remote access ATM machines - not just card skimmers – had become a reality.

In 2013, cells of an international cyber gang successfully perpetrated what has been ranked as the second largest bank heist in New York City history. Within the span of approximately 10 hours, gang members withdrew $44.7 million from ATMs around the world. The New York City cell is responsible for $2.8 million of the total amount. Although the final event took place over a 10 hour period, planning and organizing everything took over seven months. The group executed various measures to acquire the resources necessary to access the ATMs as well as distribution of those resources to cells around the world. It is theorized that the hackers used social engineering (such as phishing) to gain access to bank databases.

ARTICLES/NEWS/URLS:

My research into Automatic Teller Machine (ATM) security involved searches into the following:

Triton ATMs https://www.tritonatm.com/products/triton_connect

I also consulted some articles and web sites:


SCRIPTS AND DATA

The data I used for my analysis was obtained from Shodan via a python script that automatically entered the data into a MySQL database.

A sample of my python script:

```
import MySQLdb
from shodan import WebAPI

SHODAN_API_KEY = "IT3whkyVHH7iAtP28iNlq7hVNIK638vR"
api = WebAPI(SHODAN_API_KEY)

try:
    # Search Shodan
    shodansearch = raw_input( 'Enter Search Parameter' )

    Sample SQL queries:
    SELECT ip, port, country, devicedata FROM dv_ip_atm WHERE country = "United States";
    SELECT ip, port, country, devicedata FROM dv_ip_atm WHERE country = "United Kingdom";
```

1
FINDINGS AND DISCUSSION

The industry has made attempts to increase ATM security. One attempt includes increased monitoring utilizing video capture with embedded transaction data. Dedicated Micros produces the DV-IP ATM to accomplish this task.

However, the human factor still remains a problem as I was easily able to locate an unprotected remote login for this device:

To determine a subset of data that would represent the worldwide distribution of the DV-IP devices, I used my Python script with Shodan and MySql. The results indicated a concentration in the United Kingdom and the United States:
The industry isn’t standing still on the issue though, there is continued research and development into improving the security of the ATM systems. One possible future includes mobile applications for ATMs as discussed in the atm marketplace article “Could mobile be the future for the ATMs and FI brands?” by Rebecca Hellman. In this article she describes the trend toward mobility in all financial industries such as Square point of sale devices and e-wallet technologies. The scope of this project, however, limits the depth of research and expanding into the developing technologies is not possible at this time.

RESEARCH QUESTION 2

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

Introduction

Aircrack is a tool used to obtain packets with a wireless connection. It is a network software suite consisting of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless LANs. It works with any wireless network interface controller whose driver supports raw monitoring mode and can sniff 802.11a, 802.11b and 802.11g traffic. It is used for obtaining information mostly from networks that have WEP encryption. It captures various packets from the reporting network. It can be used to obtain user name and passwords from poorly encrypted networks.

Aircrack-ng is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured. It implements the standard FMS attack along with some optimizations like KoreK attacks, as well as the PTW attack, thus making the attack much faster compared to other WEP cracking tools.

Research Question Hypothesis

Cracking WEP is very easy with Aircrack. To hack a Wireless Network with a WEP encrypted password, you must have a Linux compatible wireless card. In order to crack a WEP key you must have a large number of encrypted packets to work with. The best way to get a large number of packets is to perform an ARP request re injection. In order to do this attack and get results there must be a client already authenticated with the AP, or connecting to the AP.

Aircrack can be used to perform a variety of operations. Some of them include –

- Cracking WEP and WPA (Dictionary attack) keys.
- Decrypting WEP or WPA encrypted capture files with known key.
• Packet injector (Linux, and Windows with CommView drivers).
• 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.

Research design

Collective methods

SQL

```sql
select * from anonposts a, elitehackposts b, hackhoundposts c, icodeposts d, vctoolposts e
where a.flatcontent like '%aircrack%' OR b.flatcontent like '%aircrack%' OR c.flatcontent like '%aircrack%'
OR d.flatcontent like '%aircrack%' OR e.flatcontent like '%aircrack%';
```

```sql
select * from vctoolposts where flatcontent like '%aircrack%' and postrank = 1;
```

```sql
select * from anonposts where flatcontent like '%aircrack%' order by postdate desc;
```

Analytics methods

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>

Database posts

![Database posts chart](chart.png)
Findings and discussions

- For cracking the key, you need at least 5,000 Data/IV’s for 64 bit encryption and at least 10,000 Data/IV’s for 128 bit encryption.
- 128 bit WEP key can be cracked in less than 2 minutes you just need to injecting packets for speed-up the process and get a lot of IV’S.
- 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 but at least 1 hour and it’s done.
- For WEP, you need to collect IV packets, once you have a sufficient amount, Aircrack will do the rest.
- WPA, PSK and AES can both be cracked with Aircrack.
- If you really want a WPA passphrase cracked, it’s easier to build a rig or pay for a service, a CPU alone is not enough.
- It does take some time to crack WEP, but it goes faster if there is a lot of traffic on the network.
- WI Fi AP discovery tools - Airodump-ng and Wi-Fi raw packet capture tools - Aircrack-ng suite.
- Spy on other network users and collect sensitive information such as login details or users cookies (depending on any content encryption methods that may be in use)

Steps for Hacking a WEP network -

1) The first thing you should do is get the 'BSSID' & 'Channel' of the network.
2) Now you get a list of networks with there [BSSID], [CHANNEL], [ENCRYPTION] First of all we need a WEP encrypted network (ex. wifi_98) The 2 things we need: the ‘BSSID’ and the ‘CHANNEL’.
3) Create a new 'Shell'. Now you have to watch the ACKs. If there over 30,000 you can try to crack the password.
RESEARCH QUESTION 3

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

Introduction:

Zeus, ZeuS, or Zbot is a trojan horse computer malware which runs on computers running under versions of the Microsoft Windows operating system. It is most often used to steal banking information by 2 methods namely: man-in-the-browser keystroke logging and form grabbing. It is also used to install the CryptoLocker ransomware on the systems. Zeus is spread mainly through drive-by downloads and phishing schemes available online.

ARTICLES/NEWS/URLS:

The Zeus Trojan has been spotted being put to yet another devious use: swiping business data from Salesforce.com. It was detected targeting an individual's Windows-based computer in order to get into Salesforce.com as the victim logged in, and then quickly gathered up a large amount of Salesforce business data through a kind of web-crawling action. It grabbed 2 gigabytes of data in less than 10 minutes.


The notorious info-stealing Zeus/Zbot variants are re-emerging with a vengeance, with increased activity and a different version of the malware. It is more dangerous as it uses more advanced infection and avoidance techniques. Unlike earlier versions, the mutex name is randomly generated in these. Both variants send DNS queries to randomized domain names.


SQL SCRIPTS USED TO OBTAIN DATA:

```sql
select * from anonposts where flatContent like '%zeus%';
sel ect * from elitehackposts where flatContent like '%zeus%';
sel ect * from hackhoundposts where flatContent like '%zeus%';
sel ect * from icodeposts where flatContent like '%zeus%';
sel ect * from vctoolposts where flatContent like '%zeus%';
```

ANALYTICS AND METHODS FOR DATA MINING:

![Number of posts by table](image-url)
FINDINGS AND DISCUSSIONS:

From the findings it was observed that discussion going on about **how to setup Zeus Bot** and a user supplied the tutorial about Zeus Bot Setup.

Steps to setup Zeus Bot are given below:

1. The user needs to have offshore hosting, preferably bulletproof on his system. As per the post owner, Addon Hosting with cPanel is the best offshore hosting option. The user should use a domain that cannot be tracked easily. Get all the files and mirrors from the link provided.
2. Upload the files, login to CPanelX. Then, go to file manager and create a directory.
3. Upload the upload.zip to the directory created and extract the files.
4. Chmod the directory /install/ and /system/ to 777. Also the whole directory.
5. Go to MySQL database in the CPanel and add a new user. Then, add the user to the created database and select all privileges.
6. To install the panel, go to the directory created before and go to /directory/install/. A Panel installer should appear. Enter data as given below:

   ```
   Code:
   Username: Enter the default username which you will use when logging in.
   Password: Your password when logging in. Make it strong.
   MySQL server:
   Host: "localhost"
   User: Your database user created before.
   Password: Your database password created for the user.
   Database: The database name.
   ```

   7. Provide the data in Control Panel 1.2.10.1 Installer GUI and click Install.
8. To make the bot, navigate to the Zeus files and open config.txt. Replace the link where it prompts to with your link. Also, use the encryption key used before. Then open Open the zsb.exe. The builder also has a remover so if you test your server on your own pc you can just remove it with a mouse click. Click on Builder. Then click on Build Config. Save the file. Click Build Loader. Save the file.
9. Now go and upload cfg.bin and bt.exe to the same directory as the panel. In final the directory with Zeus installed should look like this:
There was another forum hackers are having discussions on **how to avoid Zeus Tracker (a tracker that tracks Zeus Botnets)**. It is suggested that a user can use the following code to avoid Zeus Tracker:

```bash
#Anti ZS Tracker .htaccess
RewriteEngine on
RewriteCond %{HTTP_REFERER} ^http://.*google.com [NC]
RewriteRule .* - [F]
order allow,deny
deny from dclient.hispeed.ch #84.74.14?.*
deny from 84.74.14
allow from al
```

**Research Question 4**  
**How can we use Keylogger to “hack” information?**

**Introduction**

What is Keylogger? A keylogger also known as a keystroke logger is software or hardware device which monitors each and every key typed by you on your keyboard. It can be used in a good way, for instance, the parents can keep eye on their children playing computers or the company owner spy to their employees during the work. At the same time, the 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 realize that if they are using a computer with a keylogger software. For this research, I will mainly address how we can use the Keylogger hacking the information.

**Articles/ News**

- **How does keylogger work**
  - See what you type through the keyboard and sends it to a hacker
  - Hackers use keyloggers to steal passwords, credit card numbers and other confidential data.
  - Runs hidden from a user in background and logs/records all the keystrokes of a user
- **Trojans**
  - Programs which are often known as backdoors, which are similar to keyloggers but they can execute certain commands sent by the hacker
- **How to protect from the Keylogger**
  - Have a good AntiVirus
    - Zemana Antilogger, NoAdware, Keyscrambler,

Reference: [http://vctools.net/forum/Thread-tutorial-setup-zeus-bot-with-pictures-tutorial#axzz2uOBW2z1X](http://vctools.net/forum/Thread-tutorial-setup-zeus-bot-with-pictures-tutorial#axzz2uOBW2z1X)
**Research Design**

SELECT * FROM elitehack WHERE flatContent like "%keylogger%";
(also use these SQL for searching anon, hackhound, icode, vctoll, unpack and cnhonkerarmy tables)

SELECT * FROM elitehack WHERE flatContent like "%keylogger%"
AND postrank = "1";
(also use these SQL for searching anon, hackhound, icode, vctoll, unpack and cnhonkerarmy tables)

**Finding and discussions**

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.

<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>
### No. of related results for Keylogger

<table>
<thead>
<tr>
<th>Platform</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>cnhonkerarmy</td>
<td>21</td>
</tr>
<tr>
<td>unpack</td>
<td>141</td>
</tr>
<tr>
<td>vctool</td>
<td>186</td>
</tr>
<tr>
<td>icode</td>
<td>66</td>
</tr>
<tr>
<td>hackhound</td>
<td>57</td>
</tr>
<tr>
<td>elitehack</td>
<td>111</td>
</tr>
<tr>
<td>anonposts</td>
<td>34</td>
</tr>
</tbody>
</table>

### References

- [https://www.tritonatm.com/products/triton_connect/](https://www.tritonatm.com/products/triton_connect/)
- [www.elitehack.net/showthread.php?mode=threaded&tid=455](http://www.elitehack.net/showthread.php?mode=threaded&tid=455)
- [http://vctools.net/forum/Thread-how-to-avoid-zeustracker?pid=19561#pid19561](http://vctools.net/forum/Thread-how-to-avoid-zeustracker?pid=19561#pid19561)
- [http://vctools.net/forum/Thread-tutorial-setup-zeus-bot-with-pictures-tutorial#axzz2uOBW2z1X](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-how-to-avoid-zeustracker#axzz2uOBW2z1X)