The Real Life Story Behind Payment Card Hacks

Brian Hussey
Global Director of Incident Response and Readiness
Agenda

The Underground World of Cybercrime

Payment Card Hack Case Study – A Forensic Examiner’s Point of View

Monetization of Card Data & The Secret Economy
The Underground World of CyberCrime
Cybercrime Motivations
Why this problem is NOT going away

- Trustwave Global Security Report research shows 1,425% Return on Investment

- Estimated ROI for a one-month ransomware campaign

- Based on Trustwave SpiderLabs research into underground markets

- One example: $5,900 investment = $84,100 profit
Organized Cybercrime

A Sophisticated Underground Economy
Payment Card Hack Case Study –
A Forensic Examiner’s Point of View
Payment Card Hack Case Study

A Day in the Life of a Computer Forensic Examiner

Compromised POS Server Case Study:
- Over a million dollars lost in false credit card charges
- Brands track cards to a US-based hotel
- Trustwave gets the call to investigate

Victim POS Security Implementation:
- Antivirus installed and updated
- Firewalls active and configured intelligently
- Secure user accounts and passwords
- Network segregation properly isolates card data environment
- Credit card data never touches the hard drive, only exists in Random Access Memory (RAM)
Simple Phishing Email

*Step 1 – Identify the Attack Vector*

Employee used POS server to check personal email
Apparent LinkedIn phishing message sent to user’s personal email
Hyperlinks redirect to Italian webserver (ecodyger.com)
Redirected to Angler Exploit Kit

Exploit Kits

*Automation of Network Attacks*

Quickly scans for client-side vulnerabilities

Automates compromise of victims

Usually targets browsers and programs a website can invoke

- Adobe Reader,
- Java,
- Flash, etc...

POS and Ecommerce Web Servers now specifically targeted by Exploit Kits

---

### Overview

<table>
<thead>
<tr>
<th>Downloads</th>
<th>Exploits</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>1057591</td>
<td>397512</td>
<td>37.6%</td>
</tr>
</tbody>
</table>

---

### Exploits

<table>
<thead>
<tr>
<th>Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flash</td>
<td>115632</td>
</tr>
<tr>
<td>ie10</td>
<td></td>
</tr>
<tr>
<td>msi</td>
<td>96567</td>
</tr>
<tr>
<td>silver</td>
<td>6515</td>
</tr>
</tbody>
</table>

---

### Countries

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>BR</td>
<td>619728</td>
</tr>
<tr>
<td>NL</td>
<td>41124</td>
</tr>
<tr>
<td>NO</td>
<td>19553</td>
</tr>
<tr>
<td>DE</td>
<td>13566</td>
</tr>
<tr>
<td>TR</td>
<td>8771</td>
</tr>
</tbody>
</table>

---

### Browsers

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSIE 7.0</td>
<td>386945</td>
</tr>
<tr>
<td>MSIE 11.0</td>
<td>302240</td>
</tr>
<tr>
<td>Unknown</td>
<td>116038</td>
</tr>
<tr>
<td>MSIE 6.0</td>
<td>112598</td>
</tr>
<tr>
<td>MSIE 5.0</td>
<td>68871</td>
</tr>
</tbody>
</table>

---

### OS

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 7</td>
<td></td>
</tr>
<tr>
<td>Windows 8</td>
<td></td>
</tr>
<tr>
<td>Unknown</td>
<td></td>
</tr>
<tr>
<td>Windows 0.1</td>
<td></td>
</tr>
</tbody>
</table>
Angler Exploit Kit – Targeting POS

Step 2 – Identify the Payload Operation

• Angler exploit conducts automated reconnaissance, searching for POS systems, E-Commerce Web servers, or basic workstations

• Uses “Net View” command to identify list of computer names on network, searching for:
  • POS
  • STORE
  • SHOP
  • SALE

• Upon identification of POS or Ecom server, appropriate payload malware is selected and distributed
Step 3 – Identify the Malware

Expert at Hiding in Plain Sight

Challenges

- Antivirus turns out to be ineffective on this malware - studies show antivirus catches 30% of active malware
- Timeline analysis no good - malware alters its own timestamps
- Malware uses names similar to Windows system files

The Break

- Analysis showed an unusual file called Edcsrv-1916.dmp was created and deleted in C:\temp every 60 seconds
- Edcsrv-1916.dmp created by an unknown executable: sysmon16.exe
- MFT parsing extracted true creation dates, linking an additional 2 pieces of malware to the attack: syncsrv.exe and winsock32.exe
Step 4 – Malware Analysis

How do these nasty little programs get my card data?

winsock32.exe
- Installed itself as Windows Service, ensuring reboot survival
- Silently started the other two pieces of malware

sysmon16.exe
- Monitored system process lists for known credit card programs
- Extracted memory space for targeted processes and wrote it to a file on the hard drive called Edcsrv-1916.dmp

syncsrv.exe
-Parsed credit card data from the dump files and wrote them to a new file called winsrv.chm
- Occasionally collected all the winsrv.chm files in a password protected .rar file and emailed them to dimple@ziggy.ru
Step 5 – Identify Exfiltrated Data

What did they actually take?

Suspicious Factors

- Location: C:\Temp
- Windows System sounding name but not in a Windows System Folder
- No Extension
- Hidden Attribute Set
Decoding Data Exfiltration

First level of obfuscation: Base64

File appears to be Base64 encoded

Unusual and out of place... Possible data exfiltration file?

Used a simple decoder for first level of obfuscation
Decoding Data Exfiltration

Second level of obfuscation: WinRAR Compression

Recovered file has no extension

Signature analysis reveals a **Rar!** Header

Rar is a compression tool often used to package up multiple files for data transfer

Next step: Give a `.rar` extension to the exfil file and open with Winrar.exe
Decoding Data Exfiltration

Third level of obfuscation: WinRar encryption

Opening the file in WinRAR shows file contents
4 winsrv.chm files discovered
Remember - this is the file created by the syncsrv.exe malware
Name contains possible timestamp
Rar file encrypted and I don’t have the password
Decoding Data Exfiltration

Identifying the WinRar Password

Dynamic Malware analysis reveals malicious process behavior
Malware created a password protected Rar file
Analysis intercepted the password: HELLZHxr182
Decoding Data Exfiltration

Extracting the Encrypted Files

The password **HELLZHxrZ182** enabled successful decryption of `regsvr32.rar` and extraction of files.
Decoding Data Exfiltration

Extracted Winsrv.chm files still contain no comprehendible data
Decoding Data Exfiltration

Fourth level of obfuscation: XOR Encoding

Careful examination shows the repeating string “xANADU”

Inherent weakness in XOR obfuscation is hex 20 character (Space key) – it reveals the case-opposite XOR key

In this case, the key is: Xanadu
Decoding Data Exfiltration

Apply a reverse XOR function using the key: Xanadu
Decoding Data Exfiltration

Decrypted Contents of winsrv.chm reveal the stolen credit card data

```
memdump/MICROS.exe-2729.dmp found (track2):
7729272752992590=99059099909092977090

memdump/MICROS.exe-2729.dmp found (TRACK1):
B5728659005707994APARKER/EILL
ALLEN^9909909000000000000792000

memdump/MICROS.exe-2729.dmp found (track2):
572805090570799=99099090000079200000

memdump/MICROS.exe-2729.dmp found (TRACK1):
B7029220209270202A^JAMES T FRANKLIN/^9999990900799000000

memdump/MICROS.exe-2729.dmp found (track2):
7029220209270202=999999099827097990

memdump/MICROS.exe-2729.dmp found (TRACK1):
B7977279028778972^WATERS
ZACHARY^920929090000000000000000000000278009000

memdump/MICROS.exe-2729.dmp found (TRACK1):
B5779285755099050^SMITH/JULIE^990790990000900097000000
```
Pursuit of a cyber criminal
*Following the trail of breadcrumbs back to the attacker*

Remember the email address that regsrv32 was sent to?

Open Source Internet Research
- Dimple@ziggy.ru used to register a number of Internet domains
- Dimple@ziggy.ru comments on a number of software development blogs

Both blogs and domain registrant information identify a well known Russian Hacker, with his physical address in Moscow

Leading to an FBI investigation focused on this individual
Prosecution and Expert Witness Testimony

Chasing Down International Cyber Criminals

Briefings for Special Agents, AUSAs, Department of State, Russian Police

MLAT (Mutual Legal Assistance Treaty) creation

Extradition delayed – Moved forward with ex-parte prosecution

Testimony in Federal Court

Bad guy goes to jail!
Monetization of Card Data & The Secret Economy
Online Cyber Intelligence Operations

How do the bad guys turn this into real cash?

• Online cyber Intelligence Gathering

• Some Tips:
  • Use an isolated Virtual Machine
  • Use virtual snapshots frequently to revert to in case of infection
  • Always use a VPN – I use an anonymous VPN and TOR browser concurrently
  • Create a completely separate identity that cannot be linked back to yourself

• We will look deeper into a few popular sites:
  • Sky-fraud.ru
  • www.mastercvv.ru
  • Swiped.su

• Live Demonstration – Pending Conference Internet
Conclusions

Greed + Basic Hacking Ability + Lax Security = Massive Data Loss

• As long as cybercriminals can convert hacking into money, then the looming threat remains
• Not all cybercriminals are as dumb as Dimple – They usually get rich and are rarely caught
• The only way to prepare for this threat is to:
  • Maximize the protection of your security infrastructure
  • Sophisticated 24x7 security monitoring
  • Frequent security testing via vulnerability scanning and penetration tests
  • Have an Incident Response Plan in place and a top notch incident response team ready to take action on your behalf
Thank You