Point of Sale Threat Actor Attribution Through POS Honeypots

Kyle Wilhoit
Sr. Threat Researcher
Trend Micro
#whoami

• Spoke at many conferences worldwide, including Blackhat
• Specialize in threat intelligence, offensive security, and ICS
• Master’s in Computer Science
• Bachelor’s in Computer Science

@lowcalspam
Objective...

WHO IS BEHIND POS SYSTEM ATTACKS
Merchant. Goods and services provider that accepts credit card payments
Acquiring Bank: Bank that processes and settles a merchant’s credit card transactions with an issuer
ISSUING BANK: Bank or financial institution that issues credit cards to consumers
Payment Services Provider:
Third-party service provider that handles payment transactions between merchant’s bank and acquirers bank
“Regular” Merchant Transactions
Large Merchant Transactions

Store #1

Store #2

Store #3

Private WAN (MLPS)

Central location that houses payment switch

Internet
Why Attack POS Systems?

• Old operating systems
• Multiple components (Network, bot, kill switch)
• Multiple exfil methods supported
• Generally unpatched
POS RAM Scraping- Credit Card Data

<table>
<thead>
<tr>
<th>SS</th>
<th>FC</th>
<th>PAN</th>
<th>FS</th>
<th>CN</th>
<th>FS</th>
<th>ED</th>
<th>SC</th>
<th>DD</th>
<th>ES</th>
<th>LRC</th>
</tr>
</thead>
</table>

- **SS**: Start sentinel (%)
- **FC**: Format code (B or b)
- **PAN**: Primary account number (up to 19 digits long)
- **FS**: Field separator (*)
- **CN**: Cardholder’s name (up to 26 characters long)
- **ED**: Expiry date (in the form, "YYMM")
- **SC**: Service code
- **DD**: Discretionary date (may include the Card Verification Value [CVV]/Code, the PIN Verification Value, and the PIN Verification Key Indicator)
- **ES**: End sentinel (?)
- **LRC**: Longitudinal redundancy check
POS RAM Scraping- Quick Overview

<table>
<thead>
<tr>
<th>SS</th>
<th>PAN</th>
<th>FS</th>
<th>ED</th>
<th>SC</th>
<th>DD</th>
<th>ES</th>
<th>LRC</th>
</tr>
</thead>
<tbody>
<tr>
<td>SS:</td>
<td>Start sentinel (;)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PAN:</td>
<td>Primary account number (up to 19 digits long)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FS:</td>
<td>Field separator (=)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ED:</td>
<td>Expiry date (in the form, “YYMM”)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SC:</td>
<td>Service code</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DD:</td>
<td>Discretionary data (similar to that in Track 1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ES:</td>
<td>End sentinel (?)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LRC:</td>
<td>Longitudinal redundancy check</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
POS RAM Scraping Malware- A Family Affair
POS Honeypots for Intel

• To track actor movement, honeypot was created
• Fake credit card information was used
• Fake names/personas
• Fake companies
• “Embedded” documents
• Acting as a Merchant
POS Honeypots for Intel
Hardware/Software

• Radiant POS 1220C
  – Microsoft Embedded XP
  – Microsoft Embedded POSReady7
  – Windows Embedded Compact 2013
  – Aloha POS

• Additional virtualized environments

• Fake credit card generator
Legal Disclaimer!
Fake Company

• MLOT Coffee Company

• Created website to entice attackers
  – Primarily for use when facing POS system on Internet
Architecture
Honeypot Considerations

• Username:Password
  – Aloha:Password

• Kept default install
  – Default VNC credentials
  – Unencrypted VNC connection
  – Etc.

• Customized to come from MLOT Coffee Company
Fake Credit Card Generator

• Python script to generate fake credit numbers and dump into memory, generating fake transactions

• Multiple output methods to target many families
  – Luhn algorithm
  – Track 1 / Track 2 dumps
  – Credit card numbers between 13 and 19 digits
  – Track delimiter (^)

• Randomly generated to track on UG
Three Execution Locations

- Execute malware directly on POS system
- Execute malware directly on batch processor
- Hung off Internet and wait
Execution on PoS System
Sensitive & Confidential, Trend Micro 2015
Any Bites?

5103997799204658 | 0519 | 0175 | Charles Blue | Cupertino | 5953 Countess Dr | 95129 | CA | US

5529876429582855 | 0919 | 058 | Barbara Wafer | College Park | 2087 Flanigan Oaks Drive | 20741 | MD | US

5111387990819704 | 0521 | 585 | Laura D Griffin | Waco | 3160 Hill Haven Drive | 76706 | TX | US

5446387373227851 | 0321 | 244 | James Evans | Los Angeles | 2564 Kerry Way | 90017 | CA | US
250 CC's UNCHECKED

268,82 EUR (0.057338 BTC)
10 pcs in stock

Netherlands → Worldwide

pm (included) 3 1 Buy

This listing is for a data base of 250 CC’s unchecked, different countries on it (Don’t ask me countries it’s unchecked)

Card infos :
**** Card Numbers
**** Expiration
**** CVV/CVV2
**** Date
**** Name and Surname
**** Complete Address
**** Phone Number/Email (not always)

IMPORTANT FOR CC’s buyers [IMPORTANT FOR CC’s buyers]

I ask FE = Finalize Early, because many dishonest persons tried to scam me or newbs on carding burn cards because they don’t use it correctly. So if you buy CC’s on my store please ACCEPT THE RULES or DON’T BUY TO ME, I don’t force anyone to buy. I don’t know balances on cards can be 1 usd or 10 000 usd it’s the random games of CC’s. Before use a card use solid socks (not free proxy or only VPN because IP can be blacklisted). Use MAC ADDRESS CHANGER, flush your DNS, ... I DON T REPLACE CARDS IF YOU DON T USE IT CORRECTLY. Thank you for understanding and thank us to scammers for my rules...

Vendor requires finalizing early (FE) for this product.
Possible Scenarios Regarding Seller

• May be running POS malware and selling harvested numbers
• May be purchasing fullz from malware administrator/author
• May be trading for fullz from malware administrator/author
Execution on Batch Processor System
Batch Processor Configuration

- Merchants store an entire day’s authorized sales in a batch. At the end of the day, they send the batch via PSPs to acquirers in order to receive payment.
- Can be done remotely or locally on POS system
- For case of exercise, used a different POS system
  - Portuguese language setting
Retail Point of Sale POS System - NEW POS WITH REFURBISHED DELL PC WIN 7 PRO
NO HIDDEN FEES WARRANTY & REAL (LIVE) SUPPORT INCLUDED

Item condition: Seller refurbished
“Computer and monitor are refurbished and may have minor scuffs or blemishes that DO NOT have an”

Quantity: 1 More than 10 available / 216 sold

Price: US $399.99
Buy It Now
Add to cart

Best Offer:
Make Offer

294 watching
Add to watch list
Add to collection

216 sold More than 92% sold 7 inquiries

Seller information
techsigma (1255 ★)
99.5% Positive feedback

Follow this seller
Visit store: Inventak Point of.. See other items

LEARN HOW TO EARN $30 E
Possible Scenarios Regarding Seller

• Malware Author/Seller are likely not the same
  – Malware appears tied to FighterPOS
  – Seller appears to be unrelated, other than Brazilian connection

• Could be working together?

• Could have traded credit card numbers on UG
Hanging Off the Internet

• Unfortunately, there wasn’t much directly related to POS exploitation
  – Three logins with default Aloha username/password

• No PoS specific malware utilized

• Appears to be mostly skids

• Rest of the data was all garbage automated scans
<table>
<thead>
<tr>
<th><strong>City</strong></th>
<th>Scottsville</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Country</strong></td>
<td>United States</td>
</tr>
<tr>
<td><strong>Organization</strong></td>
<td>Time Warner Cable</td>
</tr>
<tr>
<td><strong>ISP</strong></td>
<td>Time Warner Cable</td>
</tr>
<tr>
<td><strong>Last Update</strong></td>
<td>2016-04-28T15:51:13.615195</td>
</tr>
<tr>
<td><strong>Hostnames</strong></td>
<td>rcs-24-105-186-82.rns.blc.rr.com</td>
</tr>
<tr>
<td><strong>ASN</strong></td>
<td>AS1351</td>
</tr>
</tbody>
</table>

### Ports
- 21
- 80
- 3389

### Services

220 Welcome to The Floral POS, FTP Server.
530 Login or password incorrect!

214-The following commands are recognized:

- ABO
- ADATE
- ALLO
- APPR
- AUTH
- CDUP
- CTYPE
- CWD
- DELE
- EPSV
- FTP
- HELP
- LIST
- NAME
- NCD
- NLST
- NOOP
- OPTS
- PASV
- PASV
- PBSZ
- PORT
- PROT
- QUIT
- REST
- RETR
- RND
- RNFR
- RNTO
- SITE
- SIZE
- STOR
- STRU
- SYST
- TYPE
- USER
- XCAP
- XMV
- XTR

214 Have a nice day.

211-Features:
- MDTM
- REST
- STREAM
- SITE
- MLST type=;size=;modify=
- MLSD
- UTF8
- CLNT
- MFTP
- EPSV
- EPRT

213 End
So Who Cares?

• Most criminals don’t pre-test before sale
• They may or may not be directly responsible for the sale and POS malware
• Correlation between POS actors and the sale of CC numbers
• Gather “intel” about actors/authors
Fin.

KYLEWILHOIT@GMAIL.COM

@LOWCALSPAM