Point of Sale Threat Actor Attribution Through POS Honeypots

Kyle Wilhoit

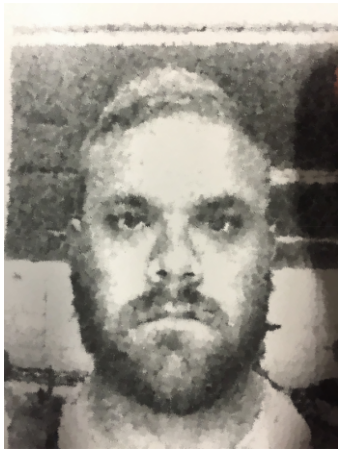
Sr. Threat Researcher

Trend Micro

28th ANNUAL FIRST CONFERENCE SEOUL JUNE 12 - 17, 2016

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

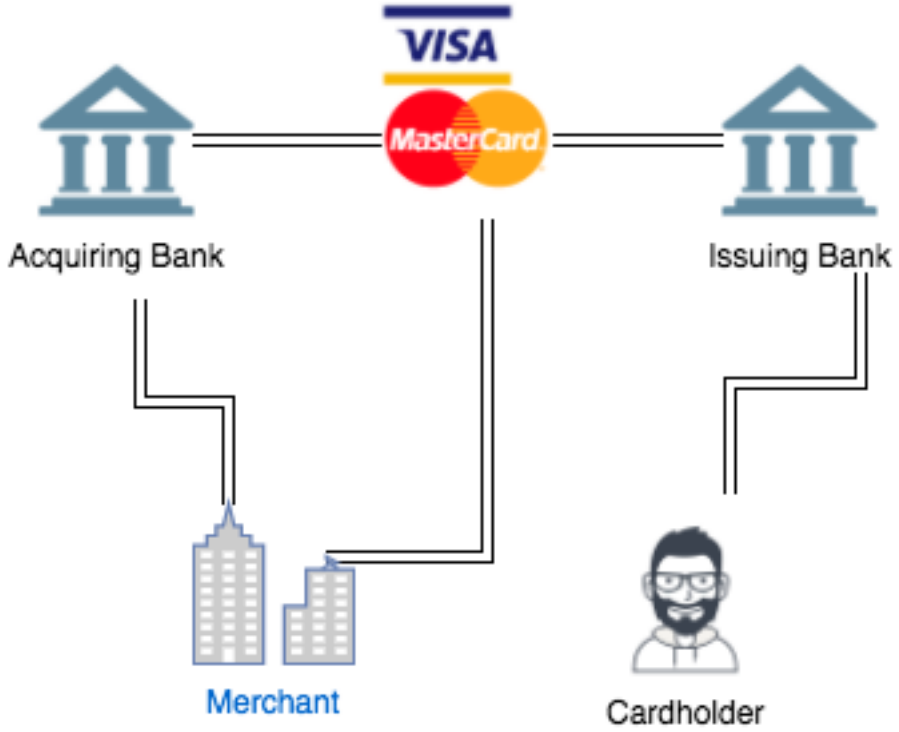
Merchant. Goods and services provider that accepts credit card payments

Acquiring Bank: Bank that processes and settles a merchant's credit card transactions with an issuer

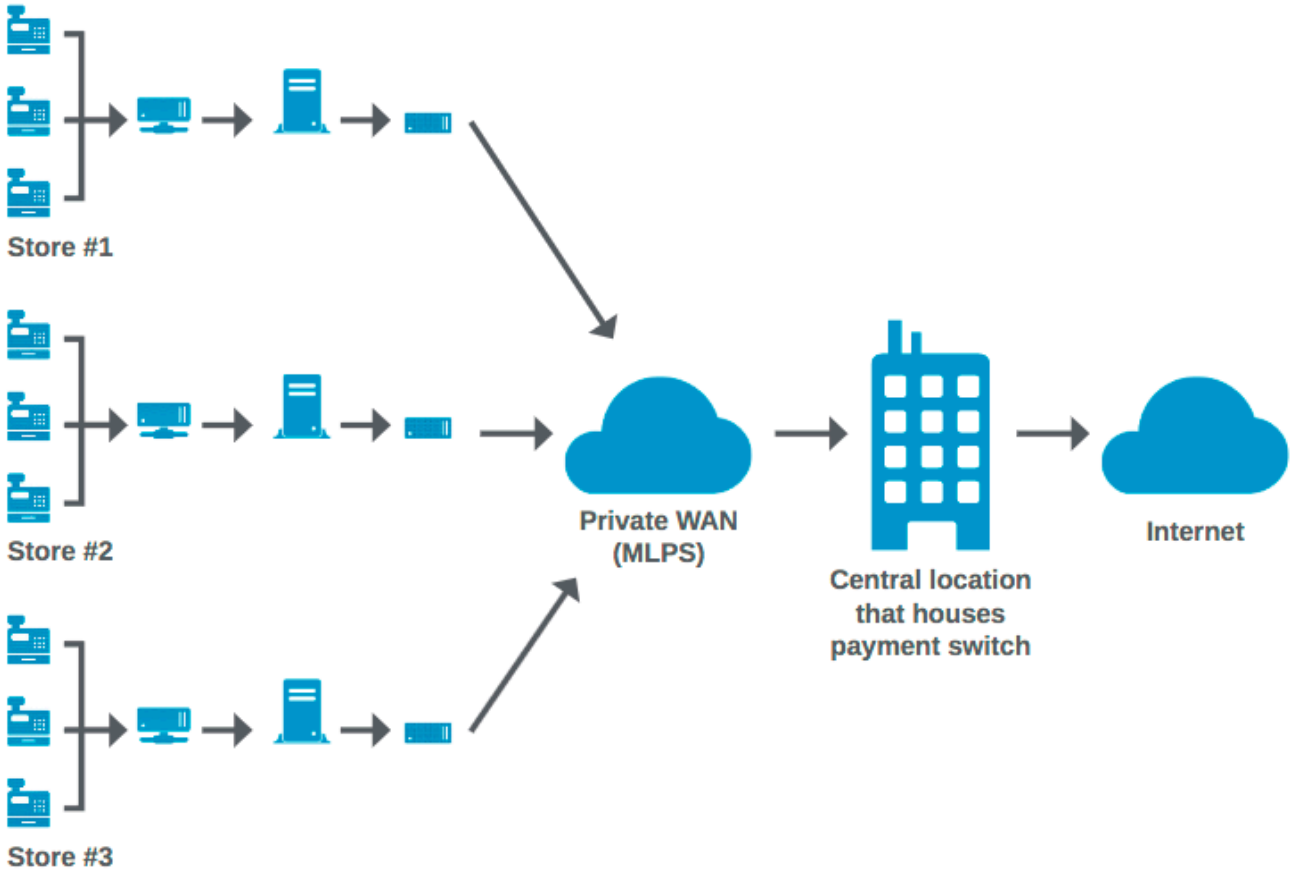
Issuing Bank: Bank or financial institution that issues credit cards to consumers

Payment Services Provider: Third-party service provider that handles payment transactions between merchant's bank and acquirers bank

“Regular” Merchant Transactions



Large Merchant Transactions



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

Track 1 Standard										
SS	FC	PAN	FS	CN	FS	ED	SC	DD	ES	LRC

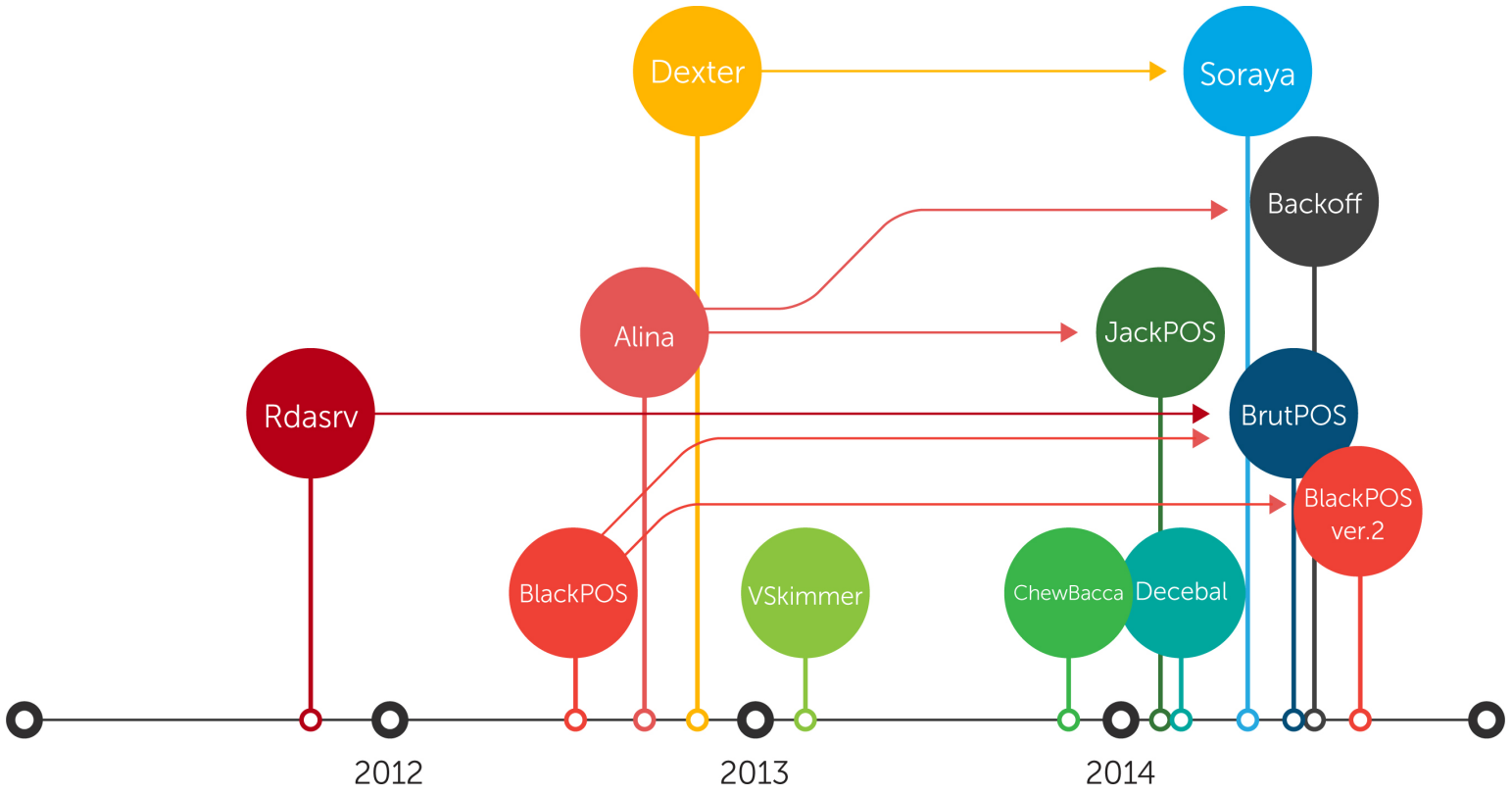
SS: Start sentinel (%)
FC: Format code (*B* or *b*)
PAN: Primary account number (up to 19 digits long)
FS: Field separator (^)
CN: Cardholder's name (up to 26 characters long)
ED: Expiry date (in the form, "YYMM")
SC: Service code
DD: Discretionary date (may include the Card Verification Value [CVV]/Code,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

POS RAM Scraping- Quick Overview

Track 2 Standard							
SS	PAN	FS	ED	SC	DD	ES	LRC

SS: Start sentinel (;)
PAN: Primary account number (up to 19 digits long)
FS: Field separator (=)
ED: Expiry date (in the form, "YYMM")
SC: Service code
DD: Discretionary data (similar to that in Track 1)
ES: End sentinel (?)
LRC: Longitudinal redundancy check

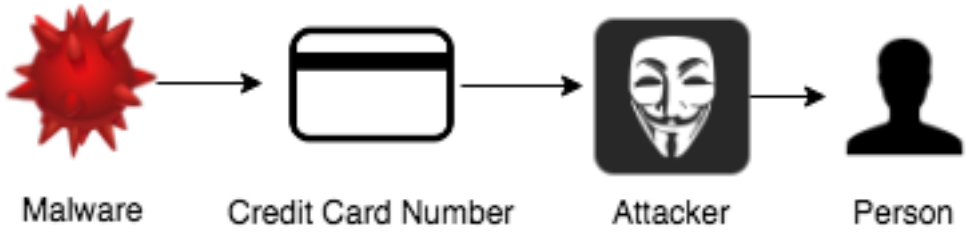
POS RAM Scraping Malware- A Family Affair



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

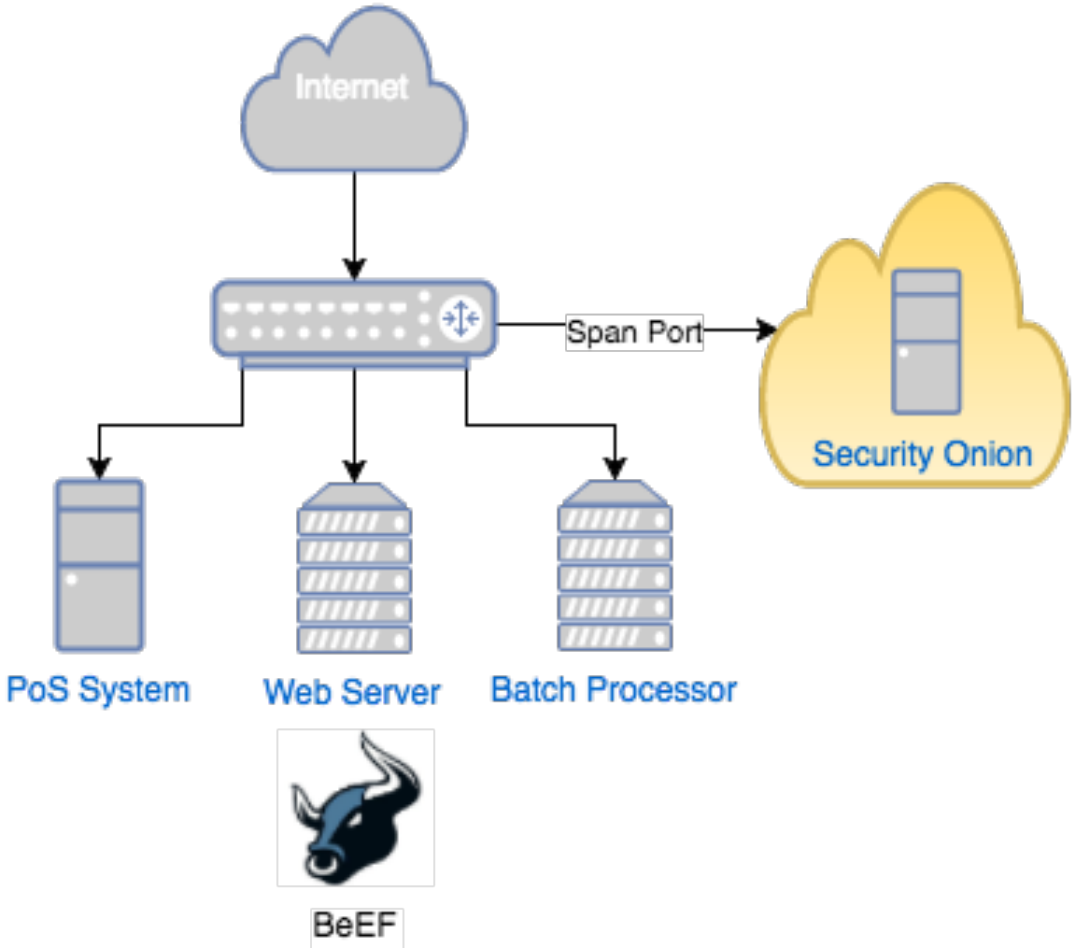
Legal Disclaimer!

TREND MICRO

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

```
Mastercard
----------
5476616730972988
5415731251977961
5591922454792838
5474678095660287
5510933188357390
5470079723258772
5106650289404133
5342663094411874
5334297564243614
5289317879912755

VISA 16 digit
-------------
4716015327243478
4539710105376566
4716647534751990
4556955079916792
4486114907980787
4486529687676901
4716504038880710
4539136894446024
4532699459332332
4539275873644256

VISA 13 digit
-------------
4916931112869
4486505388451
4929203869884
4956601874083
4532524303995
```

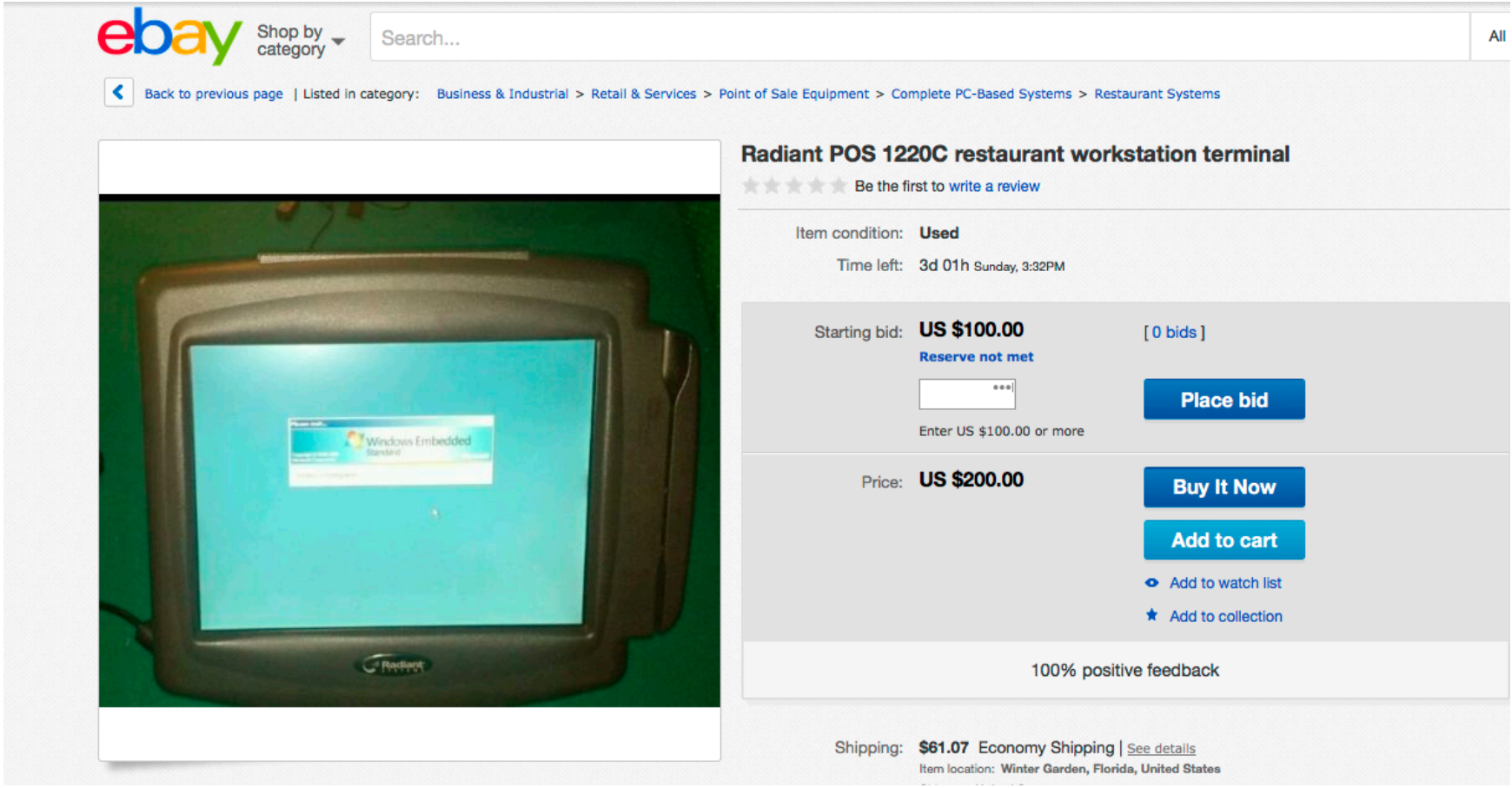
FAKE NAME GENERATOR™

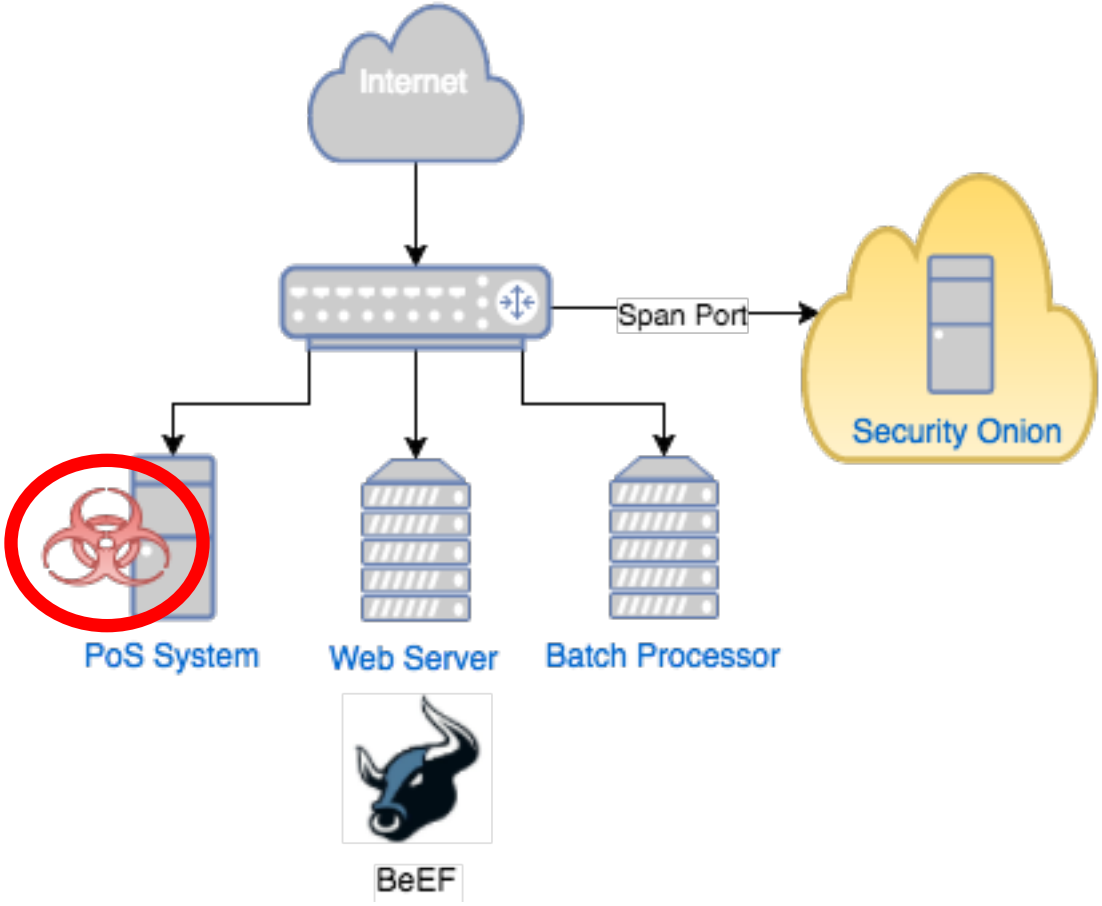
TREND MICRO

Three Execution Locations

- Execute malware directly on POS system
- Execute malware directly on batch processor
- Hung off Internet and wait

Execution on PoS System


ebay
Shop by category
Search...
All
Back to previous page | Listed in category: Business & Industrial > Retail & Services > Point of Sale Equipment > Complete PC-Based Systems > Restaurant Systems
Radiant POS 1220C restaurant workstation terminal
Be the first to write a review
Item condition: Used
Time left: 3d 01h Sunday, 3:32PM
Starting bid: US $100.00
[0 bids]
Reserve not met
Place bid
Enter US $100.00 or more
Price: US $200.00
Buy It Now
Add to cart
Add to watch list
Add to collection
100% positive feedback
Shipping: $61.07 Economy Shipping | See details
Item location: Winter Garden, Florida, United States


Internet
Span Port
Security Onion
PoS System
Web Server
Batch Processor
BeEF

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

valhallaxmn3fydu.onion/products/35253

Search

valhallaxmn3fydu.onion | All products | My purchases | Messages | [redacted]

[redacted]

250 CC's UNCHECKED

268.82 EUR *(0.557393 BTC)*

10 pcs in stock

[redacted] (285 / -2)

Netherlands → Worldwide

pm (included) | 1 | Buy

This listing is for a data base of 250 CC's unchecked, differents 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 □□□□□□□□□□□□

I ask FE = Finalize Early, because many dishonnest personn 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 socks5 (not free proxy or only VPN because IP can be blacklisted), use MAC ADRESS 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.

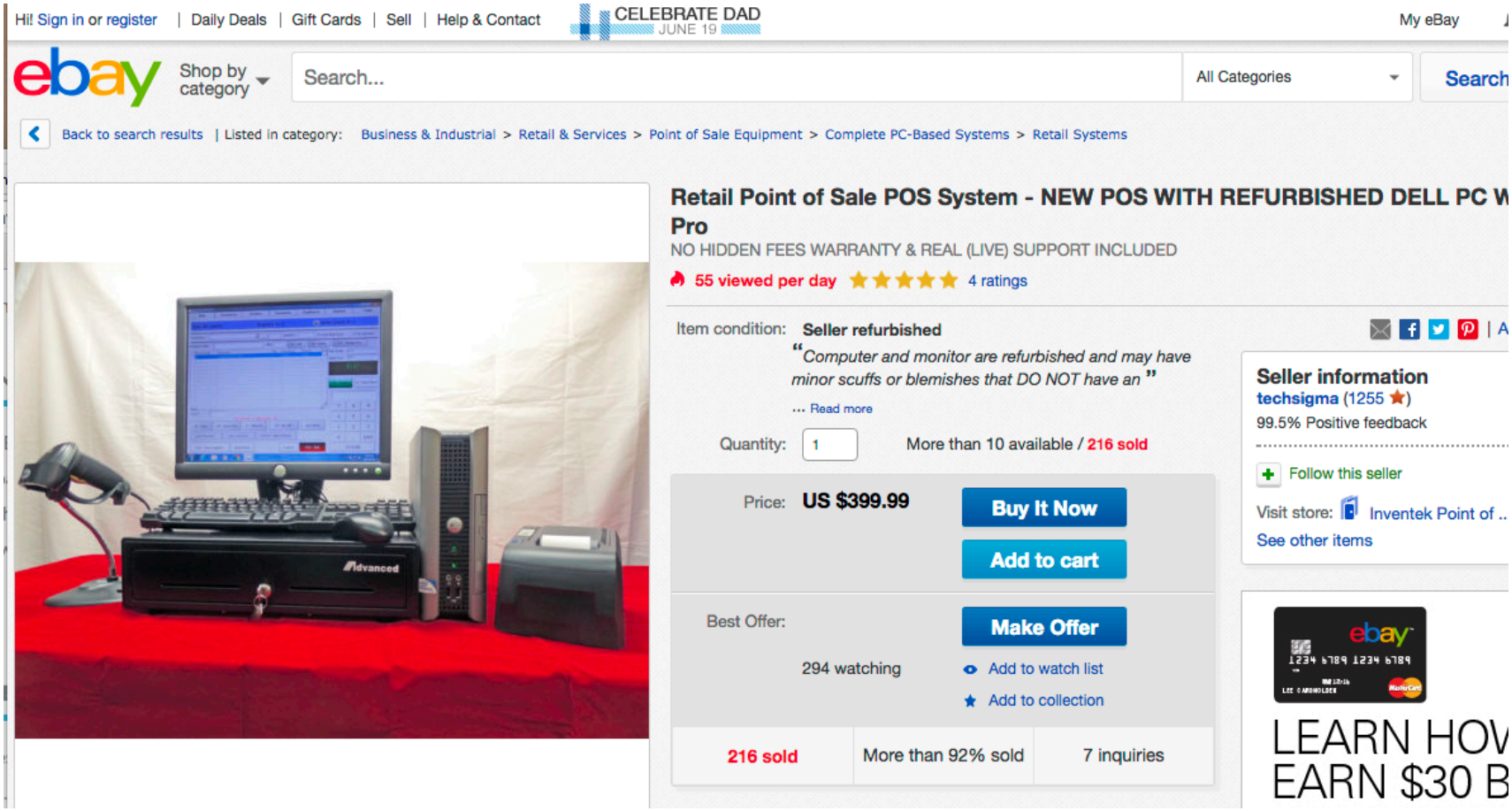
Possible Scenarios Regarding Seller

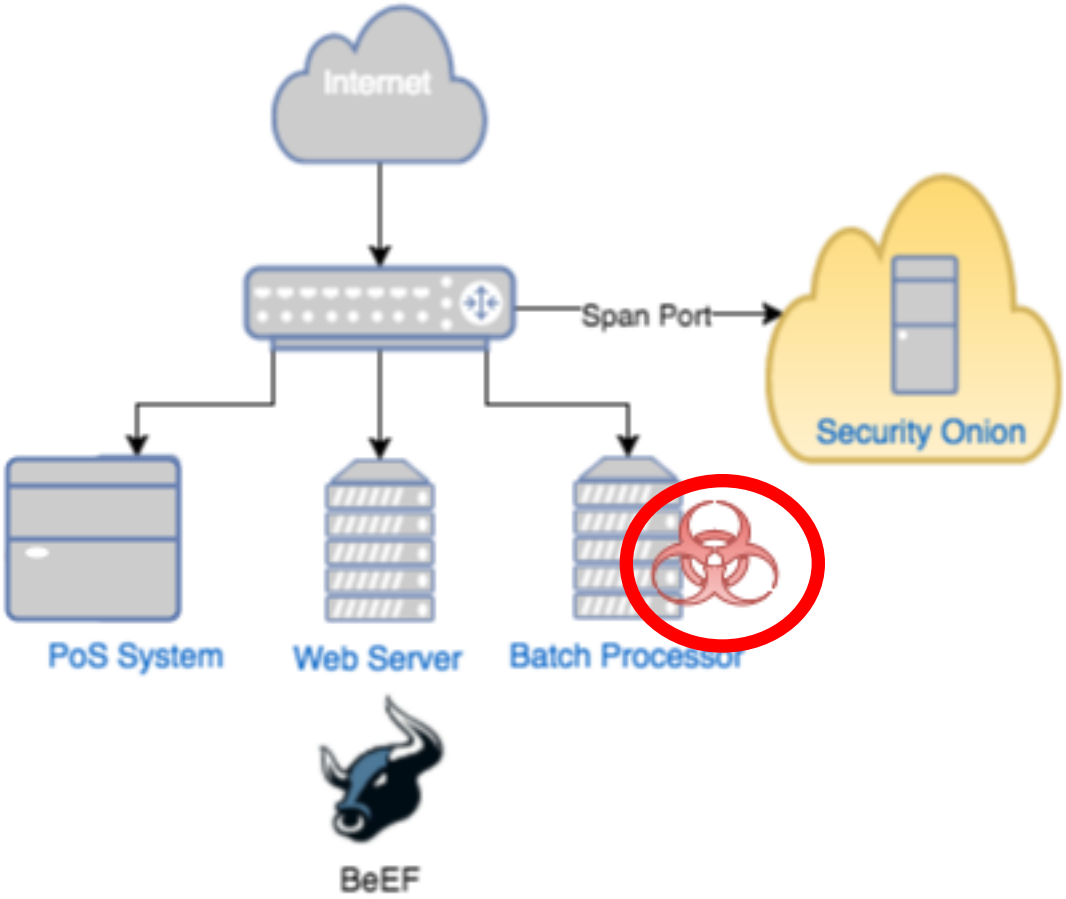
- May be running POS malware and selling harvested numbers
- May be purchasing fullz from malware administrator/author
- May be trading for fullz from malware administrator/author

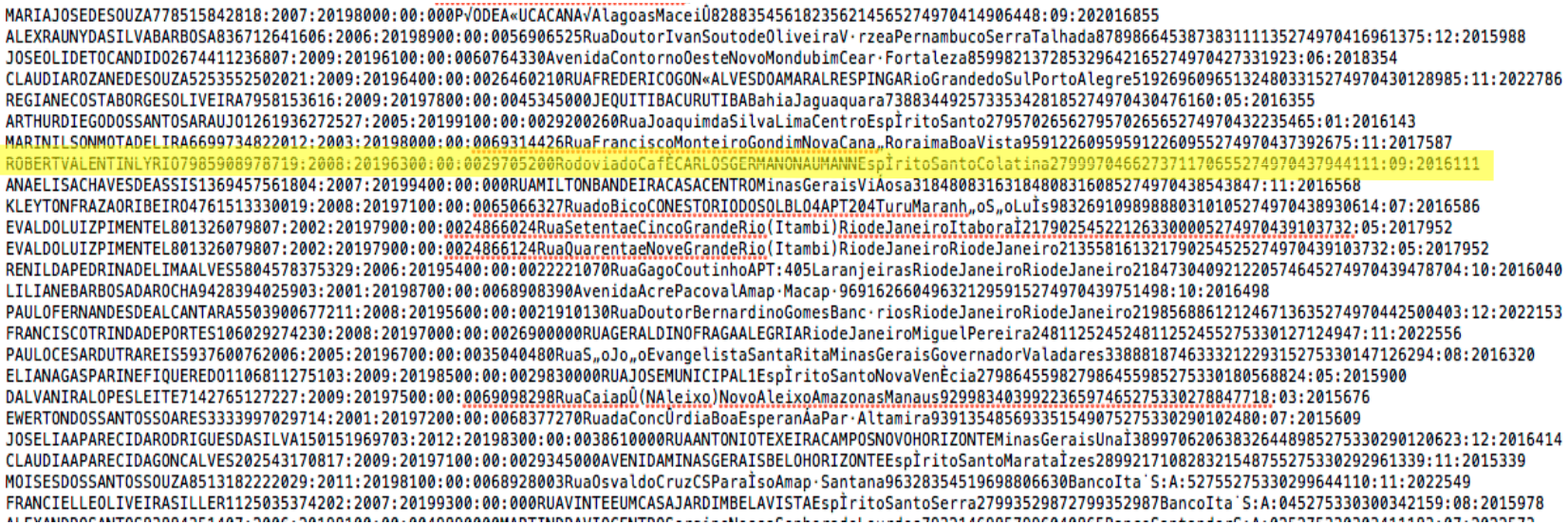
Execution on Batch Processor System

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


Hi! Sign in or register | Daily Deals | Gift Cards | Sell | Help & Contact
CELEBRATE DAD
JUNE 19
My eBay
ebay
Shop by category
Search...
All Categories
Search
Back to search results | Listed in category: Business & Industrial > Retail & Services > Point of Sale Equipment > Complete PC-Based Systems > Retail Systems
Retail Point of Sale POS System - NEW POS WITH REFURBISHED DELL PC W
Pro
NO HIDDEN FEES WARRANTY & REAL (LIVE) SUPPORT INCLUDED
55 viewed per day
4 ratings
Item condition: Seller refurbished
"Computer and monitor are refurbished and may have minor scuffs or blemishes that DO NOT have an"
... Read more
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: Inventek Point of ..
See other items
LEARN HOV
EARN $30 B


Internet
Span Port
Security Onion
PoS System
Web Server
Batch Processor
BeEF


MARIAJOSEDESOUZA778515842818:2007:20198000:00:000PvODEA«UCACANAvAlagoasMaceiÛ828835456182356214565274970414906448:09:202016855
ALEXRAUNYDASILVABARBOSA836712641606:2006:20198900:00:0056906525RuaDoutorIvanSoutodeOliveiraV·rzeaPernambucoSerraTalhada878986645387383111135274970416961375:12:2015988
JOSEOLIDETOCANDIDO2674411236807:2009:20196100:00:0060764330AvenidaContornoOesteNovoMondubimCear·Fortaleza859982137285329642165274970427331923:06:2018354
CLAUDIAROZANEDESOUZA5253552502021:2009:20196400:00:0026460210RUAFREDERICOGON«ALVESDOAMARALRESPINGARioGrandedoSulPortoAlegre519269609651324803315274970430128985:11:2022786
REGIANECOSTABORGESOLIVEIRA7958153616:2009:20197800:00:0045345000JEQUITIBACURUTIBABahiaJaguaquara738834492573353428185274970430476160:05:2016355
ARTHURDIEGODOSSANTOSARAUJO1261936272527:2005:20199100:00:0029200260RuaJoaquimdaSilvaLimaCentroEspÍritoSanto279570265627957026565274970432235465:01:2016143
MARINILSONMOTADELIRA6699734822012:2003:20198000:00:0069314426RuaFranciscoMonteiroGondimNovaCana„RoraimaBoaVista959122609595912260955274970437392675:11:2017587
ROBERTVALENTINLYRI07985908978719:2008:20196300:00:0029705200RodoviadoCafÉCARLOSGERMANONAUMANNEspÍritoSantoColatina279997046627371170655274970437944111:09:2016111
ANAELISACHAVESDEASSIS1369457561804:2007:20199400:00:000RUAMILTONBANDEIRACASACENTROMinasGeraisViAosa31848083163184808316085274970438543847:11:2016568
KLEYTONFRAZAORIBEIRO4761513330019:2008:20197100:00:0065066327RuadoBicoCONESTORIODOSOLBLO4APT204TuruMaranh„oS„oLuÍs983269109898880310105274970438930614:07:2016586
EVALDOLUIZPIMENTEL801326079807:2002:20197900:00:0024866024RuaSetentaeCincoGrandeRio(Itambi)RiodeJaneiroItaboraÍ217902545221263300005274970439103732:05:2017952
EVALDOLUIZPIMENTEL801326079807:2002:20197900:00:0024866124RuaQuarentaeNoveGrandeRio(Itambi)RiodeJaneiroRiodeJaneiro213558161321790254525274970439103732:05:2017952
RENILDAPEDRINADELIMAALVES5804578375329:2006:20195400:00:0022221070RuaGagoCoutinhoAPT:405LaranjeirasRiodeJaneiroRiodeJaneiro218473040921220574645274970439478704:10:2016040
LILIANEBARBOSADAROCHA9428394025903:2001:20198700:00:0068908390AvenidaAcrePacovalAmap·Macap·969162660496321295915274970439751498:10:2016498
PAULOFERNANDESDEALCANTARA5503900677211:2008:20195600:00:0021910130RuaDoutorBernardinoGomesBanc·riosRiodeJaneiroRiodeJaneiro219856886121246713635274970442500403:12:2022153
FRANCISCOTRINDADEPORTES106029274230:2008:20197000:00:0026900000RUAGERALDINOFRAGAALEGRIARiodeJaneiroMiguelPereira248112524524811252455275330127124947:11:2022556
PAULOCESARDUTRAREIS5937600762006:2005:20196700:00:0035040480RuaS„oJo„oEvangelistaSantaRitaMinasGeraisGovernadorValadares338881874633321229315275330147126294:08:2016320
ELIANAGASPARINEFIQUEREDO1106811275103:2009:20198500:00:0029830000RUAJOSEMUNICIPAL1EspÍritoSantoNovaVenÈcia279864559827986455985275330180568824:05:2015900
DALVANIRALOPESLEITE7142765127227:2009:20197500:00:0069098298RuaCaiapÚ(NAleixo)NovoAleixoAmazonasManaus92998340399223659746527533027887718:03:2015676
EWERTONDOSSANTOSSOARES3333997029714:2001:20197200:00:0068377270RuadaConcÚrdiaBoaEsperanÀaPar·Altamira939135485693351549075275330290102480:07:2015609
JOSELIAAPARECIDARODRIGUESDASILVA150151969703:2012:20198300:00:0038610000RUAANTONIOTEXEIRACAMPOSNOVOHORIZONTEMinasGeraisUnaÍ389970620638326448985275330290120623:12:2016414
CLAUDIAAPARECIDAGONCALVES202543170817:2009:20197100:00:0029345000AVENIDAMINASGERAISBELOHORIZONTEEspÍritoSantoMarataÍzes2899217108283215487552753302929613 39:11:2015339
MOISESDOSSANTOSSOUZA8513182222029:2011:20198100:00:0068928003RuaOsvaldoCruzCSParaÍsoAmap·Santana96328354519698806630BancoIta´S:A:527552753302996441 10:11:2022549
FRANCIELLEOLIVEIRASILLER1125035374202:2007:20199300:00:000RUAVINTEEUMCASAJARDIMBELAVISTAEspÍritoSantoSerra279935298727993529878BancoIta´S:A:045275330300342159:08:2015978

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 connetion
- Could be working together?
- Could have traded credit card numbers on UG


But wait

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

City	**Scottsville**
Country	**United States**
Organization	**Time Warner Cable**
ISP	**Time Warner Cable**
Last Update	**2016-04-28T15:51:13.615195**
Hostnames	**rrcs-24-105-186-82.nys.biz.rr.com**
ASN	**AS11351**

Ports

21 80 3389

Services

21
tcp
ftp

```
220 Welcome to The Floral POS, FTP Server.
530 Login or password incorrect!
214-The following commands are recognized:
   ABOR   ADAT   ALLO   APPE   AUTH   CDUP   CLNT   CWD
   DELE   EPRT   EPSV   FEAT   HASH   HELP   LIST   MDTM
   MFMT   MKD    MLSD   MLST   MODE   NLST   NOOP   NOP
   OPTS   P@SW   PASS   PASV   PBSZ   PORT   PROT   PWD
   QUIT   REST   RETR   RMD    RNFR   RNTO   SITE   SIZE
   STOR   STRU   SYST   TYPE   USER   XCUP   XCWD   XMKD
   XPWD   XRMD
214 Have a nice day.
211-Features:
 MDTM
 REST STREAM
 SIZE
 MLST type*;size*;modify*;
 MLSD
 UTF8
 CLNT
 MFMT
 EPSV
 EPRT
211 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