A Primer in Credit Card Theft

Point of Sale Malware

Agenda

- Michael Robinson, pinch hitting
  Material developed by CyTech Services!
  Smart folks: www.cytechservices.com

- Classes of malware
- Threat landscape
- Recent breach examples
- Survey of POS malware
- What now?

Different Types of Malware

- **Virus** – attach to other files, spread on their own
- **Trojan** – stand-alone, generally will try to look not evil
- **Worm** – spread via a network exploit
- **Spyware** – steals information about the user
- **Adware** – displays ads to user, generates $ for author
- **Ransomware** – restricts access unless user pays
- **RAT** – Remote Admin Toolkit, provides attacker with access
- **Rootkit** –conceals malware and provides persistent access

Threat Landscape

- Espionage
  - State Sponsored Intelligence Operations
  - Corporate Espionage

Google Hack Attack Was Ultra Sophisticated, New Details Show

By Kim Zetter | January 14, 2010 | 8:01 pm | Categories: Breaches, Cybersecurity,

McAfee Calls Operation Aurora A "Watershed Moment In Cybersecurity", Offers Guidance

ROBIN WAUTERS

Report: Stuxnet Worm Was Planted By an Iranian Secret Agent

1 Comment

g for Israel planted the Stuxnet computer worm into
lant through a USB stick, according to a fascinating

Russians Seem To Be Hacking Into Pentagon

Sensitive information taken -- but nothing top secret

Bob Drogin, Los Angeles Times
Thursday, October 7, 1999

PRINT E-MAIL SHARE COMMENTS (0) FONT | SIZE:

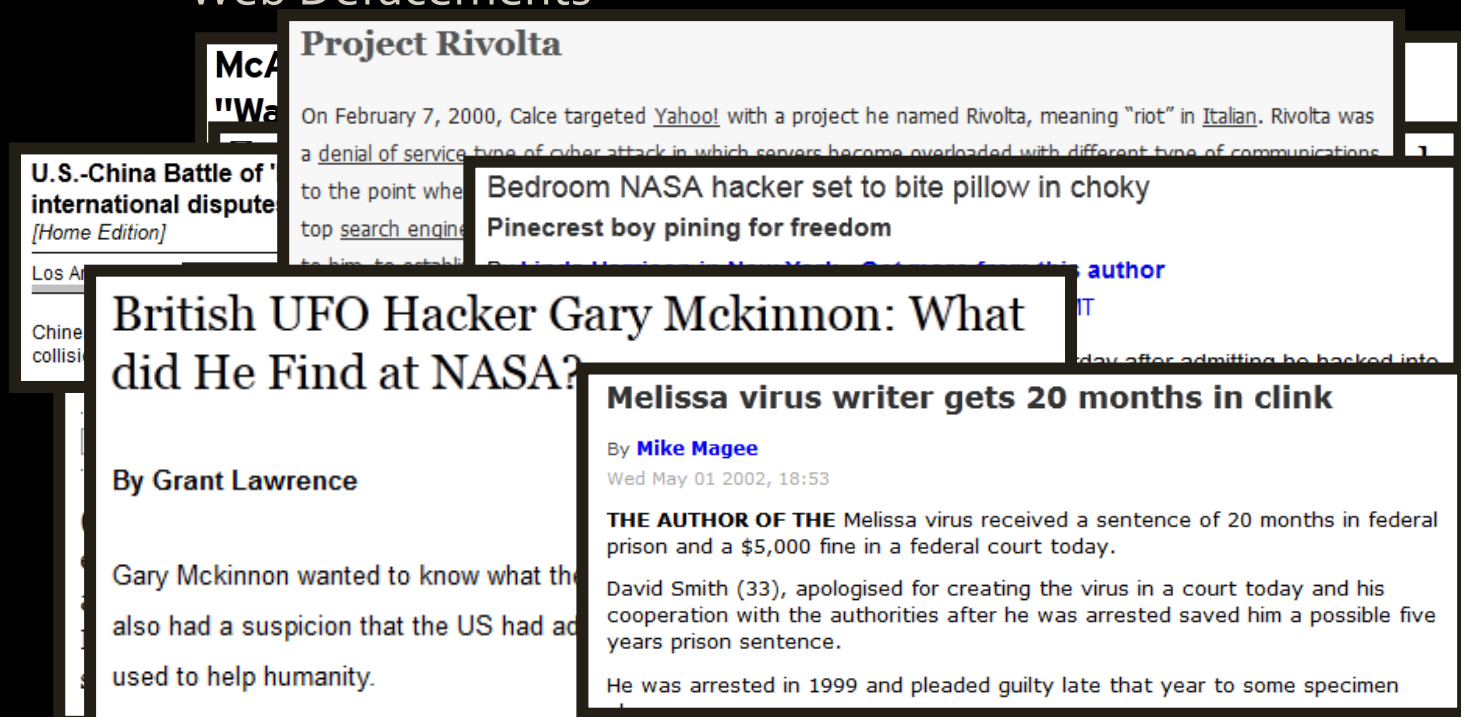
(10-07) 04:00 PDT Washington -- In what appears to be the most extensive cyber-attack ever aimed at the U.S. government, covert hackers apparently working from Russia have systematically broken into Defense Department computers for more than a year and plundered vast amounts sensitive information, U.S. officials said yesterday.

Threat Landscape

- Criminal
  - Organized Crime
  - Click Fraud
  - Spam
  - Credit Card Theft

Threat Landscape

- Activist
  - "Anonymous"
  - Hactivism
  - Web Defacements



Threat Landscape

- Thrill Seekers
  - "Because it's there"

Some Recent Breaches

According to the government's indictment, other high-profile heists tied to this gang include compromises at:

Hannaford Brothers Co: 2007, 4.2 million card numbers

Carrefour S.A.: 2007, 2 million card numbers

Commidea Ltd.: 2008, 30 million card numbers

Euronet: 2010, 2 million card numbers

Visa, Inc.: 2011, 800,000 card numbers

Discover Financial Services: 500,000 Diners card numbers

In addition, the group is being blamed for breaking into and planting malware on the networks of **NASDAQ**, **7-Eleven**, **JetBlue**, **JCPenny**, **Wet Seal**, **Dexia**, **Dow Jones**, and **Ingenicard**.

Credi
Marri

160 Million C

On Thursday 25th
and one Ukrainian
States."

The 5 hackers used
databases of some c
160 million credit c
million.

The group sought t
depending on the n

"The defendants are
Commidea, Dexia, Jetblue, Dow Jones, Euronet, Visa Jordan, Global Payment, Diners Singapore and Ingenicard. It is
not alleged that the NASDAQ hack affected its trading platform." the indictment states.

the agency

Anatomy of a Breach

- Penetration
  - Could be drive-by or could be targeted
  - Web exploits and phishing emails common
  - Computers within retailer become bots

Anatomy of a Breach

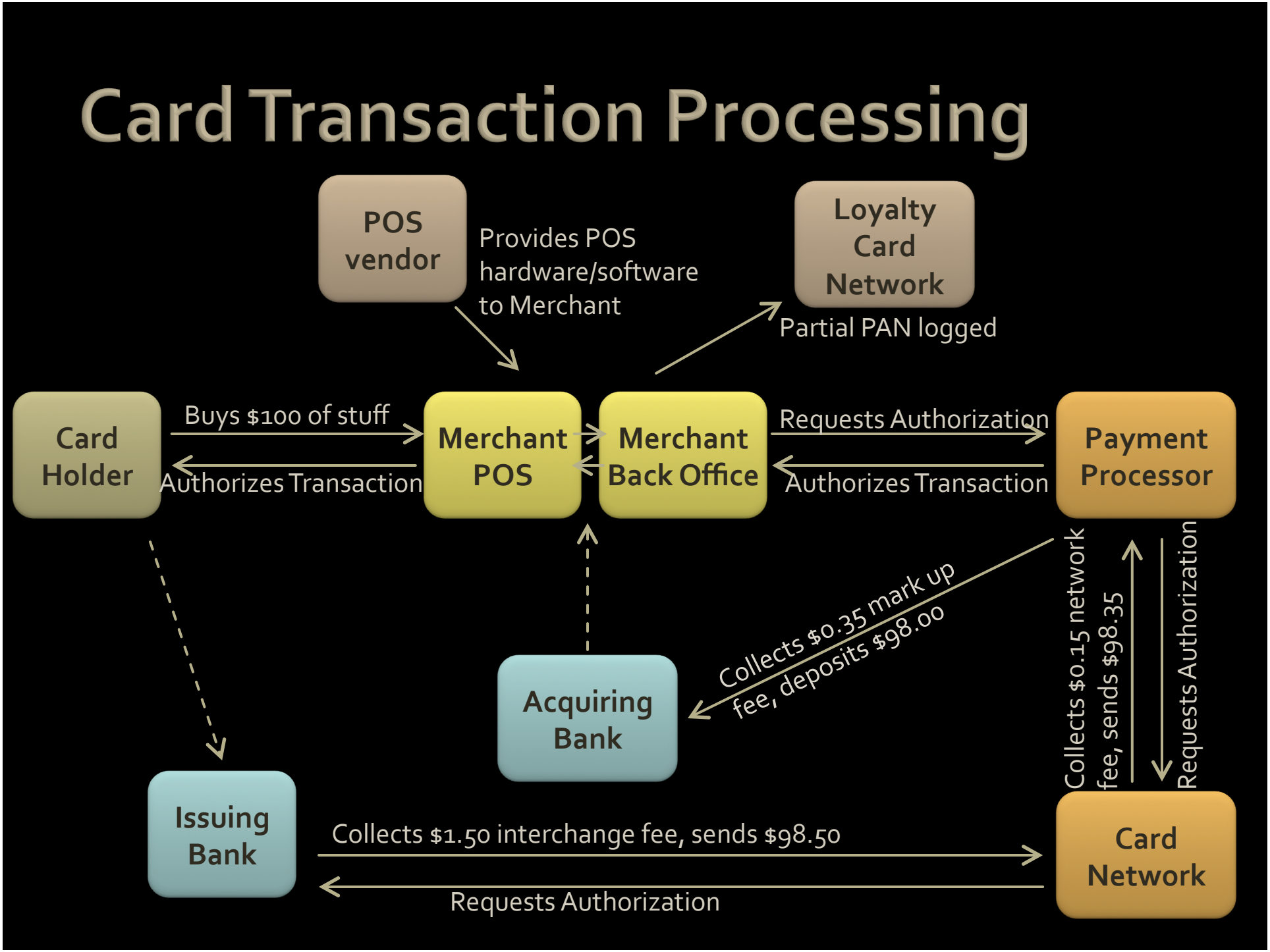
- Scan and Spread
  - Initial entry point isn't target, so must spread
  - Use some other malware to keep access

Anatomy of a Breach

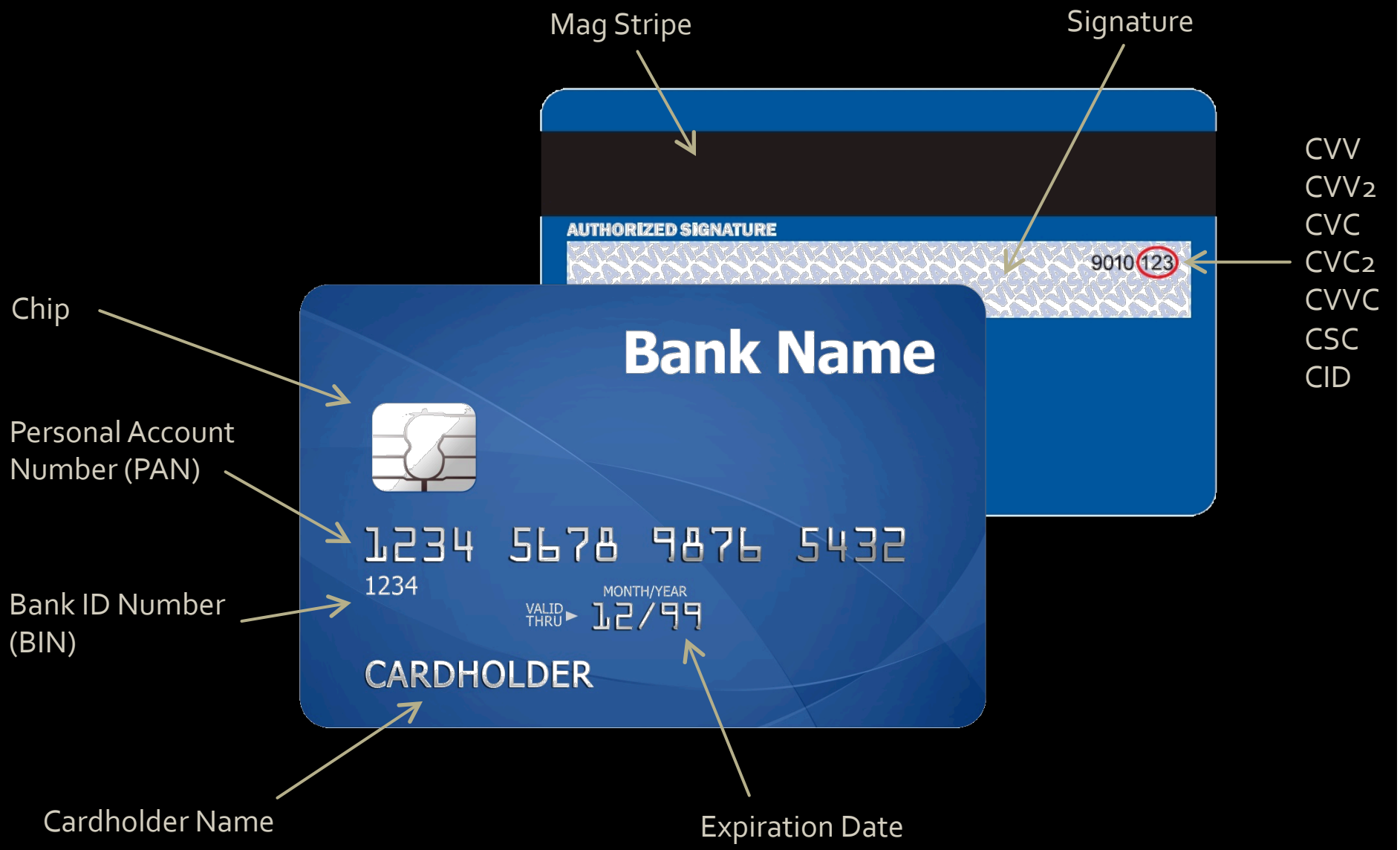
- Install Skimmer
  - Skimmer usually separate from backdoor
  - Often written specifically for targeted POS
  - Most operate as memory scrapers
    - Regex through RAM until finds card data

Anatomy of a Breach

- Exfil Card #s
  - Malware has to get data out somehow
  - Usually encrypted payload
  - Most send out through HTTP or FTP direct from POS to Internet (no reason for that)


Card Transaction Processing
POS vendor
Provides POS hardware/software to Merchant
Loyalty Card Network
Partial PAN logged
Card Holder
Buys $100 of stuff
Authorizes Transaction
Merchant POS
Merchant Back Office
Requests Authorization
Authorizes Transaction
Payment Processor
Collects $0.35 mark up fee, deposits $98.00
Acquiring Bank
Collects $0.15 network fee, sends $98.35
Requests Authorization
Issuing Bank
Collects $1.50 interchange fee, sends $98.50
Requests Authorization
Card Network

Payment Card Anatomy



Card Skimming Malware

- Dexter
- VSkimmer
- POSCardStealer
- Alina
- ChewBacca
- Project Hook
- BlackPOS
- JackPOS
- And others

Card Skimming Malware

- Dexter
- VSkimmer
- POSCardStealer
- Alina
- ChewBacca
- Project Hook
- BlackPOS
- JackPOS
- And others

- First seen Dec 2012
- Steals full Track 1 & 2
- Appears as two "iexplorer.exe" processes
- Persists via values in "run" registry key
- Iterates over every running process in a loop reading in their memory space looking for track data
- Outputs track data as encrypted HTTP traffic, generally to set domains or IPs (changes in each variant)

- NOT ALLOWING POS TO CONNECT TO INTERNET WOULD HAVE MITIGATED THIS

Card Skimming Malware

- Dexter
- VSkimmer
- POSCardStealer
- Alina
- ChewBacca
- Project Hook
- BlackPOS
- JackPOS
- And others

- First seen Jan 2013
- Steals full Track 1 & 2
- Small exe injected with other malware
- Persists with "run" registry key
- Auto adds itself to windows firewall allow rule
- Whitelists windows process and checks others
- Loops over memory space grep'ing for track
- Exfils encrypted HTTP traffic to set domain/IP
- If it can't reach internet, it writes to a local log
- If thumb drive with set volume name appears, log is moved to thumb drive

Card Skimming Malware

- Dexter
- VSkimmer
- POSCardStealer
- Alina
- ChewBacca
- Project Hook
- BlackPOS
- JackPOS
- And others

- First seen Jan 2013
- Steals full Track 1 & 2
- Generic name with no better name comes up
- The .O variant:
- Hides in %appdata%\Micorsoft\Windows \System\Hidden
- Persists with "svchost-windows-redquired" value in "run" key
- Open processes one at a time in loop, grep'ing for track data
- Dumps out to sys.dll
- Periodically sends a HTTP POST to a .php forum to upload the contents of dump file.

- WOULD HAVE BEEN NO EXFIL IF POS COULDN'T CONNECT TO INTERNET

Card Skimming Malware

- Dexter
- VSkimmer
- POSCardStealer
- Alina
- ChewBacca
- Project Hook
- BlackPOS
- JackPOS
- And others

- First seen Feb 2013
- Steals full Track 1 & 2
- Creates itself in %appdata%\ as java.exe, jusched.exe, jucheck.exe, dwm.exe, or others
- Persists with "java" entry in "Run" key
- Calls out to C&C using HTTP POST traffic to a series of hard coded IPs
- Numerous versions of Alina, based on internal version numbers – 1.0, 2.1, 3.3, 3.4, 4.0, 5.0 etc
- Can be updated to newer versions via command from C&C server

- COULD NOT HAVE CONNECTED TO C&C IF POS COULD NOT CONNECT TO INTERNET

Card Skimming Malware

- Dexter
- VSkimmer
- POSCardStealer
- Alina
- ChewBacca
- Project Hook
- BlackPOS
- JackPOS
- And others

- First seen Dec 2013
- Steals full Track 1 & 2
- Contains both a keystroke logger and a grep through memory for track data skimmer
- When run, copies itself to the following folder All Users\Start Menu\Programs\Startup
- Writes its output to %temp%\"system.log"
- Uses TOR to hide the C&C server
- Written in Pascal

- COULD NOT HAVE CONNECTED TO C&C IF POS COULD NOT CONNECT TO INTERNET

Card Skimming Malware

- Dexter
- VSkimmer
- POSCardStealer
- Alina
- ChewBacca
- Project Hook
- BlackPOS
- JackPOS
- And others

- First seen Dec 2013
- Steals full Track 1 & 2
- Related to Dexter malware
- In %appdata%\Resourcing or \Resourcing
- When it pulls track it checks service code
  - Tells malware if this is US card or chip'ed
- Hooks API calls and watches for track data instead of just skimming through RAM – this actually increases likelihood of getting results
- Some variants are very specific to specific POS software, while others are more generic
- Exfils via HTTP GET

- WOULD HAVE BEEN NO EXFIL IF POS COULDN'T CONNECT TO INTERNET

Card Skimming Malware

- Dexter
- VSkimmer
- POSCardStealer
- Alina
- ChewBacca
- Project Hook
- BlackPOS
- JackPOS
- And others

- First seen Jan 2014
- Steals full Track 1 & 2
- aka Kartoxa
- Persists via "Run" key
- Newer version runs as a Service (POSWDS)
- Modifies Windows firewall to allow itself
- Has other RAM scraper embedded inside it
  - Executes that, then catches output
  - No grep pattern – has its own pattern match routine
- Writes output, encrypted, to file
- SMB to move files within victim's network
- FTPs file out

Card Skimming Malware

- Dexter
- VSkimmer
- POSCardStealer
- Alina
- ChewBacca
- Project Hook
- BlackPOS
- JackPOS
- And others

- First seen Feb 2014
- Steals full Track 1 & 2
- Based on the Alina code
- Installs to %appdata%\Java SE Updater
- Uses .exe names like java.exe, jucheck.exe, jusched.exe, jse.exe, and other java related
- Persists through "Run" key
- Persistent process – if killed, it respawns
  - %temp%\svchost.exe is watchdog
- Persistent persistence – if the reg key is deleted, it recreates it
- Ignores white list of windows core processes
- Once it finds a process that contains track data, focuses on that
- Exfil via HTTP POST

Card Skimming Malware

- Dexter
- VSkimmer
- POSCardStealer
- Alina
- ChewBacca
- Project Hook
- BlackPOS
- JackPOS
- And others

- Common themes:

- POS being able to talk to Internet enabled easy exfiltration of data
- Most just iterate over all/most processes running a regex against their RAM space
- Use very easy to spot persistence mechanisms
- Execute from %appdata% or %temp%, which should raise huge, glaring red flags
- Most appear to come from Eastern Europe – Russia, Ukraine, and one from France

Stolen Credit Card Marketplace

- Malware Authors
  - Write the malware, but often don't use it
  - Offer support, SLAs, guarantees

Stolen Credit Card Marketplace

- Card # Collectors
  - Hacker groups that breach retailers
  - Sell their stolen numbers in bulk

Stolen Credit Card Marketplace

- Wholesale Sellers
  - Operate carder forums – black market shops
  - Like amazon or ebay, but for stolen card #s
  - Keep a cut of whatever sales occur

Stolen Credit Card Marketplace

- Card Makers
  - Create clones of cards using stolen numbers
  - Or use the cards for online purchases
  - Sell their cards or have their own team

Stolen Credit Card Marketplace

- Mules
  - People who make the purchases
  - Bring merchandise back to their bosses and get paid for it
  - Sometimes unwitting – "work from home earning $$$$ by making online purchases!"

What do you do about it?

- DSS compliance is a must
  - But, compliant does not mean secure
  - But, DSS is a decent base to start
  - Good perimeter security
- No direct access from POS to Internet
- 2-factor auth for any access to CDE
- Application whitelisting works
- Monitor your own network!

What do you do about it?

- Watch your credit card statements
- You are not responsible for fraudulent charges
  - Hacked retailer is; credit company will refund you
- Credit is safer than debit
  - If PIN is compromised, attackers can hit ATM
  - Credit company usually won't refund lost cash

الأسئلة

Preguntas?

Fragen?

пытанні?

Spørsmål?

Questions?

Küsimused?

вопросы?

Frågor?

問題?

Otázky?

질문?

Spørgsmål?