Anatomy of a Crime:
Secure DevOps or Darknet Early Breach Detection

October 30, 2018
Large Installation System Administration (LISA) USENIX 2018 Conference Keynote
Nashville, TN
Dr. Sarah Lewis Cortes, PhD, IAPP/E, CISA, CRISC
Agenda

- Convicted: Roman Seleznev; Crimes: Carding, Skimming, Financial & High-Tech Fraud
- Breach Technical Deep Dive: Retailer Hack
  - Password Cracking
  - Darknet Acquisition
  - POS RAM Malware/Skimmers
- Prevention/Solutions
Convicted!
Roman Seleznev

- aka Track2, “нCuХ” псих, "psycho"
- Bankrupted businesses
- Hacked into point-of-sale (POS) computers
- 2014: Arrested in Maldives with > 1.7m credit card numbers
- 2016: Convicted, 38 counts: wire fraud, intentional damage to a protected computer, aggravated identity theft, > $169m damages
- 2017: Sentenced to 27 + 14 years
Roman Seleznev

- Helped grow market for stolen credit card data
- Top point-of-sale hacker, criminal underworld
- Son of Valery Seleznev, Russian Parliament member, Putin ally
Roman Seleznev: Innovator

You can buy dumps in online shop called 2pac.cc, the only one real shop who is legit and they have from almost all the world countries. More than 10000 of stolen dumps.

METHOD #1:

When you login to a shop, you can see “Dumps” in navigation menu, click There.

Then you can see BIN(is first 6 digit of credit card) information on what bank is it and which type card is it like GOLD, PLATINUM, CLASSIC)

Writing dumps on Plastic

We need software to connect our MSR206 with computer. Write on Magnetic stripe of our Gift Card.

DOWNLOAD IT HERE - THEJERM

MSR206 Utility Program v1.8 by TheJerm

What is this program? It's a utility program I wrote interface with the MSR206 magstripe reader/writer.
Roman Seleznev: Inmate
<table>
<thead>
<tr>
<th>AutoIncId</th>
<th>UTC TimeStamp</th>
<th>AppId</th>
<th>UserId</th>
<th>ForegroundCycleTime</th>
</tr>
</thead>
<tbody>
<tr>
<td>114124</td>
<td>07/05/2014 02:24:00</td>
<td>Device\Harddisk\Volume5\Users\smaus\Desktop\Tor Browser\Browser\firefox.exe</td>
<td>S-1-5-21-872295761-2623846239-3737112615-1001</td>
<td>9813130135</td>
</tr>
<tr>
<td>114125</td>
<td>07/05/2014 02:24:00</td>
<td>Device\Harddisk\Volume5\Users\smaus\Desktop\Tor Browser\Tor\tor.exe</td>
<td>S-1-5-21-872295761-2623846239-3737112615-1001</td>
<td>12665306444</td>
</tr>
<tr>
<td>114126</td>
<td>07/05/2014 18:00:00</td>
<td>System</td>
<td>S-1-5-18</td>
<td>39925098676</td>
</tr>
<tr>
<td>114127</td>
<td>07/05/2014 18:00:00</td>
<td>Device\Harddisk\Volume5\Windows\System32\smss.exe</td>
<td>S-1-5-18</td>
<td>6248861</td>
</tr>
<tr>
<td>114128</td>
<td>07/05/2014 18:00:00</td>
<td>Device\Harddisk\Volume5\Windows\System32\csrss.exe</td>
<td>S-1-5-18</td>
<td>1481443719</td>
</tr>
</tbody>
</table>
### Forensic Evidence

#### Response October 29, 2010

<table>
<thead>
<tr>
<th>Name</th>
<th>Url Name</th>
<th>Internet Artifact Type</th>
<th>Last Modification Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>REGISTRY_USER_NTUSER_5-1-5-21-3344409597-1S8R80585-2984941884-1005</td>
<td><a href="http://schnitt.fyde.re/wdt2.exe">http://schnitt.fyde.re/wdt2.exe</a></td>
<td>History/Typed URL</td>
<td>10/22/10 10:29:07</td>
</tr>
<tr>
<td>REGISTRY_USER_NTUSER_5-1-5-21-3344409597-1S8R80585-2984941884-1005</td>
<td><a href="http://sendspace.com/">http://sendspace.com/</a></td>
<td>History/Typed URL</td>
<td>10/22/10 10:29:07</td>
</tr>
</tbody>
</table>

#### Response January 20, 2011

<table>
<thead>
<tr>
<th>Name</th>
<th>Url Name</th>
<th>Internet Artifact Type</th>
<th>Last Modification Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>_REGISTRY_USER_NTUSER_5-1-5-21-7538628-179605362-725345543-1003</td>
<td><a href="http://188.120.225.66/slitnak.exe">http://188.120.225.66/slitnak.exe</a></td>
<td>History/Typed URL</td>
<td>01/04/10 17:38:17</td>
</tr>
</tbody>
</table>

#### HOP ONE, MCLEAN, VA

<table>
<thead>
<tr>
<th>Start</th>
<th>Value</th>
<th>Start</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>r委会</td>
<td>40h</td>
<td>100h</td>
</tr>
<tr>
<td></td>
<td>doscode[64]</td>
<td>40h</td>
<td>40h</td>
</tr>
<tr>
<td></td>
<td>IMAGE_NT_HEADERS nt_headers</td>
<td>80h</td>
<td>F8h</td>
</tr>
<tr>
<td></td>
<td>IMAGE_SECTION_HEADER sections...</td>
<td>178h</td>
<td>A0h</td>
</tr>
<tr>
<td></td>
<td>textsection[8192]</td>
<td>3000h</td>
<td>1000h</td>
</tr>
<tr>
<td></td>
<td>_BITLIST 4096</td>
<td>4000h</td>
<td>1000h</td>
</tr>
<tr>
<td></td>
<td>_BITLIST 4096</td>
<td>5000h</td>
<td>1000h</td>
</tr>
</tbody>
</table>
Criminal Carding

- Buy, sell, trade online credit card data stolen from large retailer data breaches
- ~$10-$25/stolen card#
- Use purchased stolen card#s to buy pre-paid credit cards
- Buy gift cards, electronics at retail stores
- Resell fraudulently purchased goods on the internet
- Items shipped to a “reshipper”
Breach Technical Deep Dive
Data Breach Events

<table>
<thead>
<tr>
<th>Year</th>
<th>Company</th>
<th>Breach Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018</td>
<td>Manufacturer</td>
<td>150 million</td>
</tr>
<tr>
<td>2017</td>
<td>Online financial svc provider</td>
<td>143m</td>
</tr>
<tr>
<td>2016</td>
<td>Online social network</td>
<td>4m</td>
</tr>
<tr>
<td>2015</td>
<td>Online financial svc provider</td>
<td>15m</td>
</tr>
<tr>
<td>2014</td>
<td>Retailer</td>
<td>56m</td>
</tr>
<tr>
<td>2013</td>
<td>Online mail/news aggregator</td>
<td>3 billion</td>
</tr>
<tr>
<td></td>
<td>Many others…</td>
<td></td>
</tr>
</tbody>
</table>

Source: CSO online
Breached Data on the Darknet: Retailer

- Settlement includes mandatory darknet monitoring

**Source: Dark Owl**
Breached Private Data on the Darknet: Credit Cards

Source: Dark Owl
Retailer Hack: Skimmers

Image: Skimmers

Photo Credit: Sarah Lewis Cortes, 2018
Retailer Hack: How they did it

Password Cracking (e.g. Burp Suite)

Even easier: Account acquisition from the darknet

Event starts with attacker gaining credentials from outside vendor
Background
Darknet Privacy Breach Technical Review:

Retailer Hack

Overview
Retailer Hack: Profile of most frequent targets

- Large retailers
- Many locations
- Large number of customer credit/debit card accounts
- Millions of customer email addresses

*You probably shopped at one of these in the last week!*
Retailer Hack: Cost: 2017 Settlement

$136m- Visa, MasterCard

$ 27m- banks: fraudulent charges

$ 19m- consumers

$ 16m- legal fees

$198m- Total
Retailer Hack: Timeline

April 2013

● Password Cracking; Account acquisition from the darknet

July 2013

● Zero-day Attack: Exploit vulnerability
● Jump the barriers between vendor and retailer system
Retailer Hack: Timeline

April 2014

Malware on self-checkout terminals:

- Reads cleartext payment card data in RAM on POS terminal
- Uses regex (regular expressions) to grab payment card information (PCI)
- Sends to attacker's servers

Image: Tor Dark Market via Brian Krebs
Retailer Hack: Timeline

June-November 2014- Carding on dark markets

September 2014- Breach publicly detected, reported by a journalist: cards seen for sale on the darknet

November 2014- Phishing

October 2017- Breached customer PII still on the darknet
Retailer Hack: How they did it

- Event starts with a target’s vendor: Attacker gains vendor’s credentials
- Password Cracking (e.g. Burp Suite)
- Account acquisition from the darknet
Retailer Hack: Skimmers
3. The Company shall monitor and periodically assess key indicators of compromise on computer network endpoints;

4. The Company shall maintain and periodically assess partnership with a dark web mining service to search for [REDACTED] information;

Source: *In re: Retailer, Shareholder Derivative Litigation, US District Court for the Northern District of Georgia, 2017*
Darknet Privacy Breach Technical Review:
Retailer Hack
Password Cracking
Retailer Hack: Password Crack Demo
Retailer Hack: Brute Force w/DVWA

1) Target: DVWA Web login: [http://www.dvwa.co.uk](http://www.dvwa.co.uk)

   (D*** Vulnerable Web App)
Retailer Hack: Brute Force w/DVWA

2) Burpsuite: web history
Retailer Hack: Brute Force w/DVWA

3) Review session captures so far
1) Select session we want
Retailer Hack: Brute Force w/DVWA

2) Send to intruder
3) Upload a wordlist for passwords-payload
Retailer Hack: Brute Force w/DVWA

4) Attacker starts their attack
Darknet Privacy Breach Technical Review:
Retailer Hack
Darknet Credential Acquisition
2011 Egypt- Mubarak shuts down Internet (Tor)

Photo: Jafria News
2013: Snowden uses Tor

Photo: Barton Gellman—Getty Images
Darknet Fundamentals
Anonymous Communications Systems

Image: Tor Project, Inc.
What is the darknet?

- Definition
- What is it used for
- How does it work?
Congratulations!
This browser is configured to use Tor.

You are now free to browse the Internet anonymously.

Test Tor Network Settings

Search securely with Disconnect.me.

What Next?
Tor is NOT all you need to browse anonymously!
You may need to change some of your browsing habits to ensure your identity stays safe.

Tips On Staying Anonymous »

You Can Help!
There are many ways you can help make the Tor Network faster and stronger:
- Run a Tor Relay Node »
- Volunteer Your Services »
- Make a Donation »

The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. Learn more about The Tor Project »
A breakdown of the content found in our darknet database by category over time.

Source: Dark Owl
A Darknet Market: Tor “Hidden Services”

Overview
1. HS establishes Intro Points (IPs)
2. HS publishes Descriptors, IPs to HSDirs
3. Client requests IPs
4. Client establishes RendezVous Point (RP)
5. Client provides RP to IP
6. IP provides RP to HS
7. HS establishes circuit

Introduction Point (IP): “I have a line on those tarts”

Rendezvous Point (RP): order tarts here

Client: “I want to order tarts”

Circuit Relays
A-1st Tor Relay
B-2nd Tor Relay
C-3rd Tor Relay
G Guard Relay
M Middle Relay
E Exit Relay

Yellow: Tor relay
Pink: non-Tor relay

Tor Hidden Services
Explained Intuitively
By @SarahCortes

HSDir: “Tarts for sale @ tarts.onion. Go to Bob’s bakery for more info”

Hidden Service: tarts.onion
“Darknet” is...

- Internet “Overlay” network
- Alternative internet addressing scheme to DNS
- Cannot be traced to IP address

Source: The Tor Project, Inc.
“Tor” is...

- Online Network
- Software
- Network of People
- Nonprofit Organization
- Research Project
- Cryptographic Routing Protocol
- What Tor is NOT

Photo and Image: US Navy: Dr. Paul Syverson, US Navy, Inventor of Tor, Onion Routing
“Tor” timeline...

● 1990s: US Navy Project

● 2001: Syverson: US Navy patent

● 2002: Alpha version

● 2004: Public

● 2006: “The Tor Project,” incorporated by Dingledine, Mathewson, Lewman et al.

● 2018: 6,300 Tor relays, ~2 m sessions daily network traffic, > 275 Gbits/second
Darknet Privacy Breach Technical Review

Retailer Hack
POS Ram Scraper Malware
Retailer Hack: POS RAM scrapers

Features

• Multi-component
• Single binary
• Networking functionality
• Bot functionality
• Kill switch
• Encryption
• Development kits
• Multi-exfiltration techniques

Source: US v. Seleznev, W. District of WA, Bench Warrant
Retailer Hack: POS RAM Scraper Malware

Malware on self-checkout terminals:

- Reads clear text payment card data RAM on POS terminal
- Uses regex (regular expressions)- grabs payment card info (PCI)

\[
([0-9]{15-16} \text{ D=} [0 (7-9)] | 1[0-5])

((0 [1-9]) | [1 (0-2))] ))[0-9]{8-30})
\]

- Predominantly Windows OS
- Captured data: sent to attacker's servers

http://www.badguysserver.co.cc/
api/process.php?xy=BadGuyBadGuyBadGuyBadGuyBadGuyBadGuy##
Retailer Hack: BlackPOS v2 a/k/a FrameworkPOS malware

- Pretends to be a component of antivirus
- Enumerates all of the processes running on the infected system using the `EnumProcesses` method and scans the process memory for Tracks 1 and 2 credit card data

---

**Source:** Ars Technica

**FIXER-UPPER** — ignored security warnings for years, employees say

Old antivirus, infrequent scans, and a security architect who pled guilty to sabotage.
Retailer Hack: BlackPOS malware

Sample BlackPOS credit card data output

Source: Trend Micro
Retailer Hack:
Similar example: Decebal POS RAM scraper

1) Coded in VBScript, compiled into an executable file
2) Coded in C, C++, or Delphi
3) Source code leaked online
4) Data-exfiltration method: HTTP POST requests
   a) not cached
   b) not saved in history
   c) no restrictions on data-sending length

Source: Trend Micro
Retailer Hack: Decebal POS RAM scraper

1) Infects systems via drive-by-download attacks

2) Startup: checks for installed sandboxing/reverse-engineering tools on infected systems. To evade detection, if any is discovered, it will terminate its process. (1)

3) Installs itself in %USERPROFILE% as iexplorer.exe. It then audits infected systems in order to determine their OS, computer name, and username (2)

4) Decebal also retrieves the name of any anti-malware solution installed on infected systems. This information is exfiltrated to a remote server, along with the stolen Tracks 1 and 2 credit card data. (3)

Source: Trend Micro
1) Decebal checks for the presence of debugging tools

Source: Trend Micro
Retailer Hack: Decebal malware example

2) Decebal audits infected systems
Retailer Hack: Decebal malware example

3) Decebal checks for anti-malware solutions

Source: Trend Micro
Retailer Hack: POS RAM scrapers
Decebal malware example

5) Inspects all of the running processes by calling `CreateToolhelp32Snapshot` to take a snapshot of all of the running processes on infected systems, along with the heaps, modules & threads. (4)

6) Then calls `Process32Next` inside a do-while loop. (4) Maintains blacklist of processes (e.g., `svchost.exe`, `csrss.exe`, `wininit.exe`, etc.) to skip because finding credit card data in the memory of these processes is highly unlikely.

7) If a current process being inspected is not in the blacklist, it opens the process object using `OpenProcess` and reads the memory content via `ReadProcessMemory`. (4)

Source: Trend Micro
Retailer Hack: Decebal malware example

4) Uses `CreateToolhelp32Snapshot` method to search for Track 2 credit card data. Calls `Process32Next` inside a do-while loop
8) Regexes to match Tracks 1 and 2 credit card data are run on the process memory content that Decebal reads. (4)

9) Decebal has a built-in Luhn-validation mechanism. (5) The results returned by regex matching are validated to make sure that the Track data that it scrapes from the process memory contains valid credit card numbers.

10) Exfiltrates stolen data by making connection requests to a remote server via InternetOpenUrl. Data is exfiltrated in HTTP header sent to the remote server. SendPHP() subroutine constructs a special URL that contains hexadecimal-encoded values (6)

Source: Trend Micro
Retailer Hack: Decebal malware

5) Built-in Luhn-validation
Retailer Hack: Decebal malware

6) Uses HTTP headers to exfiltrate stolen data
Prevention and Solutions
How it Happened: POS Technical Review

POS Security Weaknesses

- Inadequate network segregation between corporate and POS networks
- Practice of entering credit card numbers directly into computers at each department, rather than using POS credit card terminals directly
- Weak third-party vendor identity/access mgt/compliance oversight
- Attackers initially broke in using credentials stolen from a third-party vendor

Source: Trend Micro
Basic Problem

● Tradeoff: Speed, Ease-of-Use vs. Security

● Speed & Ease-of-Use gain more $ than is lost by security vulnerabilities

● All proposed solutions cost time or money
Prevention: Top Impactful POS Security Ideas

- Hardware: Restrict physical POS device access
- Software: Encrypt POS apps->POS data comms
- Policy: Delete stored cardholder data
Prevention: Policy-Based

- Enforce strict policies regarding physical PoS system repairs and upgrades.
- Routinely delete stored cardholder data.
- Restrict access to the Internet on PoS systems.
- Implement POS logs/audit trails.
Prevention: Impactful ideas

- Set up PoS systems to automatically reimage every 24h.
- Restrict Internet access on PoS systems.
- Disable remote access if not required.
- Whitelisting: only allow approved apps to run on POS devices.
- Communication in and out of POS environments: Restrict to minimum required.
- Encrypt comms between POS applications ->POS data.
- Change default passwords, configurations, and encryption keys. Use strong passwords.
Prevention: Impactful ideas

- Deploy the latest version of POS OSs; regularly apply POS patches.
- Eliminate unnecessary POS ports, accounts, services, scripts, drivers, features, subsystems, file systems, web servers, protocols.
- Regularly apply updates to installed POS software.
- Identify when POS system components change.
- Install and regularly update POS anti-malware solutions to protect against POS malware and malicious URLs.
- Vulnerability scanner: scan systems, apps, web apps.
Prevention: Hardware-based

- Multitier hardware firewalls: protect POS networks.
- Breach detection systems (BDSs): detect POS-targeted attacks.
- Intrusion detection/prevention systems (IDPSs): scan inbound/outbound POS traffic.
- 2FA for remote POS network access by employees, administrators, third parties.
- POS point-to-point encryption.
References/Resources

BurpSuite- password crack
https://www.youtube.com/watch?v=SCHEBIzZkdo

Sample RAM Scraper malware:
https://github.com/warewolf/fireeye/blob/master/Alert_Details_example.com_20131025_181223.xml
https://www.shellntel.com/blog/2015/9/16/powershell-cc-memory-scraper

POS Malware

Numaan Huq, Trend Micro
Questions?