GRU close access cyber operation against OPCW

Genmaj. O. Eichelsheim

Defence Intelligence & Security Service

4 October 2018
Tuesday 10 April 2018

- Arrival from Moscow at Amsterdam Schiphol Airport
Tuesday 10 April 2018

• Accompanied by embassy personnel
Overview of Russian persons

- Diplomatic passports
Aleksei MORENETS

Name: Aleksei Sergeyvich MORENETS
Date of birth: 31-07-1977
Place of birth: Moermanskaya Oblast
Passport nr: 100135556
Role: Cyber operator
Evgenii SEREBRIAKOV

Name: Evgenii Mikhaylovich SEREBRIAKOV (a.k.a. SEREBRYAKOV)
Date of birth: 26-07-1981
Place of birth: Kursk
Passport nr: 100135555
Role: cyber operator
Oleg SOTNIKOV

Name: Oleg Mikhaylovich SOTNIKOV
Date of birth: 24-08-1972
Place of birth: Ulyanovsk
Passport nr: 120018866
Role: HUMINT support
Alexey MININ

Name: Alexey Valeryevich MININ
Date of birth: 27-05-1972
Place of birth: Perm Oblast
Passport nr: 120017582

Role: HUMINT support
Car rental agreement
Citroën C3, PF-934-R

Naam: O.M Sotnikov
Adres: Podmoscowskaya Street 10 211
Postcode / plaats: 112220 RUSSIA
Land: Russia
Telefoon: 0617671589

verklaren dat zij een overeenkomst hebben gesloten tot huur en verhuur van

Bestuurder 2: Minin, 27-05-1972
Car rental agreement
Citroën C3, PF-934-R

Huurder: Aleksey Minin
Adres: Michajlovskiy str 8
Plaats: 1735 MOSCOW
Rusland
Bestuurder: Aleksey Minin
Telefoon: 3456

Huurauto: CITROEN C3
Kenteken: PF-934-R (NX-508-T)
Sublocatie: 

ACCESSORIES

INNAME / CHECK-IN

DAMAGE:
YES / NO

Handtekening en naam huurder
Handtekening en naam verhuurder

[Formalities and other details]

[Return policy and additional information]
Reconnaissance of OPCW and surroundings

• Photos taken on 11 April, found on MININ’s camera
Reconnaissance of OPCW and surroundings

- Photo taken on 12 April, found on MININ’s camera
Reconnaissance of OPCW and surroundings

- Photo taken on 13 April, found on MININ’s camera
Situation map

- Location of rental vehicle on Friday 13 April
Connected to:
- Smartphone (4G)
- WiFi panel antenna

Specialist equipment in vehicle
- Setup for hacking WiFi connections

- WiFi panel antenna (covered)
- Bag with battery
- Transformer
Schematische weergave
WiFi panel antenna

• Hidden under coat
Battery

- Power supply for equipment
- Purchased in The Hague
Operational modus operandi

- Security awareness
- Tried to destroy smartphone during disruption operation
Operational modus operandi

• Security awareness
• GRU intelligence officers took their trash out of their hotel rooms
Operational modus operandi

- Cash money: 20,000 Euro’s and 20,000 dollars
Online searches from SEREBRIAKOV’s laptop

- Indicating interest in OPCW headquarters building and immediate surroundings
**Additional specialist equipment**

- Carried by SEREBRIAKOV
- Intended for hacking WiFi networks
The world's largest Open Database of Cell Towers

Locate devices without GPS, explore Mobile Operator coverage and more!

Sony Xperia F3311
- Activated on 9 April, through cell tower in Moscow (GSM MCC: 250 MNC: 20 LAC: 27813 CID: 197679381)
CID: 197679381
- Nearest cell tower to known GRU barracks at Komsomolsky Prospekt 20, Moscow
MORENETS’ taxi receipt

- From Nesvizhskiy Pereulok to Moscow Shermetyevo airport
- Date: 10 April 2018
Rear entrance of GRU barracks

- Opening onto Nesvizhskiy Pereulok
Previous operations: photo on SEREBRIAKOV’s laptop

- 14 August 2016: Olympic Games in Brazil (picture above taken on 16.39, 14-08-2016 with LG-K350ds)
<table>
<thead>
<tr>
<th>Network Name</th>
<th>Name Type</th>
<th>First Connect</th>
<th>Last Connected</th>
<th>Managed</th>
<th>DNS Suffix</th>
<th>Gateway Mac Address</th>
<th>Profile GUID</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sheremetyevo Wi-Fi</td>
<td>Wireless</td>
<td>2016-09-17 19:10:57 +00:00</td>
<td>2016-09-17 19:10:57 +00:00</td>
<td>Unchecked</td>
<td>&lt;отсутствует&gt;</td>
<td>B4-E9-B0-C9-1E-40</td>
<td>(7D30FD49-1E32-4618-8278-AFF127C2F288)</td>
<td>Airport, Khimki, Russia</td>
</tr>
<tr>
<td>LP Public</td>
<td>Wireless</td>
<td>2016-09-20 20:17:39 +00:00</td>
<td>2016-09-20 20:29:12 +00:00</td>
<td>Unchecked</td>
<td>lausanne-palace.net</td>
<td>00-90-0B-29-02-D7</td>
<td>(FC1F8A2C-7959-4C0A-AE0D-6ACAAA049420)</td>
<td>Lausanne, Switzerland</td>
</tr>
<tr>
<td>Hotel Alpha-Palmiers</td>
<td>Wireless</td>
<td>2016-09-20 21:26:51 +00:00</td>
<td>2016-09-22 08:59:34 +00:00</td>
<td>Unchecked</td>
<td>monzoon.net</td>
<td>00-1A-A2-9F-9C-AE</td>
<td>(7E6EC1D0-6B1A-467E-A81D-DFFFF2375E69)</td>
<td>Lausanne, Switzerland</td>
</tr>
<tr>
<td>GMKL hotel</td>
<td>Wireless</td>
<td>2017-12-16 03:21:01 +00:00</td>
<td>2017-12-22 12:39:21 +00:00</td>
<td>Unchecked</td>
<td>localdomain</td>
<td>90-E2-BA-58-ED-FB</td>
<td>(64746B9B-1E16-4366-AE08-38596037B691)</td>
<td>Kuala Lumpur, Malaysia</td>
</tr>
<tr>
<td>Palace-Hotel-Guests</td>
<td>Wireless</td>
<td>2018-04-10 22:58:44 +00:00</td>
<td>2018-04-12 09:53:14 +00:00</td>
<td>Unchecked</td>
<td>hotspot.internet-for-guests.com</td>
<td>D0-BF-9C-3A-66-B5</td>
<td>(2B8E00FF-9942-4818-A5B9-B0FC6DB52D2)</td>
<td>Noordwijk, Netherlands</td>
</tr>
<tr>
<td>Marriott GUEST</td>
<td>Wireless</td>
<td>2018-04-12 19:08:00 +00:00</td>
<td>2018-04-13 14:12:52 +00:00</td>
<td>Unchecked</td>
<td>&lt;отсутствует&gt;</td>
<td>50-9A-4C-6A-F0-E5</td>
<td>(01E8FAC9-4419-4B38-80B9-9A9F896A5415)</td>
<td>The Hague, Netherlands</td>
</tr>
</tbody>
</table>

**Previous operations: WiFi connections made by SEREBRIAKOV’s laptop**

- Grand Millenium Hotel (Kuala Lumpur, Malaysia) from 16 to 22 December 2017;
- Alpha Palmiers Hotel (Lausanne, Switzerland) from 20 to 22 September 2016;
- Palace Hotel (Lausanne, Switzerland) on 20 September 2016.
Target: Spiez Laboratory

- Train tickets to Bern
- Online searches for Spiez laboratory
- Google-maps print-outs of Russian diplomatic facilities in Bern
Google Maps print-outs

- Russian diplomatic facilities in Bern and Geneva
Train tickets to Switzerland

- Departure from Utrecht for Bern via Basel
- Planned date: 17 April 2018