An Insight into Symbiotic APT Groups

Thoufique Haq, Sr. Malware Research Scientist
FireEye

Outline

- Threat landscape
- DragonOK and Moafee group
- NJQ8, MoDis, Houdini, BlackMafia, BlackHacker
- Sunshop campaign
- Shared weponization tools
Threat Landscape

Specimen A

Moafee & DragonOK
Moafee Group

• One of their HTRAN command control infrastructure at 58.64.201.229
• Many domains resolving to this IP between January – March 2014
• We also monitored their HTRAN command control server at 58.64.201.229 from January - March 2014.
• Consistent connections to HTRAN backend from Guangdong

<table>
<thead>
<tr>
<th>DATE</th>
<th>CNC</th>
<th>HTRAN Backend</th>
<th>HTRAN Backend Geolocation</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014-03-10</td>
<td>58.64.201.229</td>
<td>189.251.163.19</td>
<td>LIRR LOCAL</td>
</tr>
<tr>
<td>2014-03-12</td>
<td>58.64.201.229</td>
<td>189.251.163.19</td>
<td>LIRR LOCAL</td>
</tr>
<tr>
<td>2014-02-18</td>
<td>58.64.201.229</td>
<td>113.68.111.111</td>
<td>CHINESE GUANGDONG PROVINCE NETWORK</td>
</tr>
<tr>
<td>2014-02-15</td>
<td>58.64.201.229</td>
<td>113.68.108.62</td>
<td>CHINESE GUANGDONG PROVINCE NETWORK</td>
</tr>
<tr>
<td>2014-02-12</td>
<td>58.64.201.229</td>
<td>113.68.168.73</td>
<td>CHINESE GUANGDONG PROVINCE NETWORK</td>
</tr>
<tr>
<td>2014-02-05</td>
<td>58.64.201.229</td>
<td>189.251.163.25</td>
<td>LIRR LOCAL</td>
</tr>
<tr>
<td>2014-01-19</td>
<td>58.64.201.229</td>
<td>113.68.112.12</td>
<td>CHINESE GUANGDONG PROVINCE NETWORK</td>
</tr>
<tr>
<td>2014-01-25</td>
<td>58.64.201.229</td>
<td>113.68.41.28</td>
<td>CHINESE GUANGDONG PROVINCE NETWORK</td>
</tr>
<tr>
<td>2014-01-20</td>
<td>58.64.201.229</td>
<td>113.68.171.67</td>
<td>CHINESE GUANGDONG PROVINCE NETWORK</td>
</tr>
<tr>
<td>2014-01-15</td>
<td>58.64.201.229</td>
<td>113.68.171.339</td>
<td>CHINESE GUANGDONG PROVINCE NETWORK</td>
</tr>
</tbody>
</table>

DragonOK Group

• One of their HTRAN command and control infrastructure at www.ndbssh[.]com (206.161.216.219)
• Many domains resolving to this IP between between 2013-09-28 and 2013-10-04
• We monitored their HTRAN command control server for one week, between July 31, 2013 and August 8, 2013
• Consistent Connections to HTRAN backend from Jiangsu

<table>
<thead>
<tr>
<th>First Seen</th>
<th>CNC Domain</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013-08-20</td>
<td><a href="http://www.ghostalef%5B.%5Dcom">www.ghostalef[.]com</a></td>
<td>2013-05-09</td>
</tr>
<tr>
<td>2013-09-09</td>
<td><a href="http://www.cbeastapi%5B.%5Dcom">www.cbeastapi[.]com</a></td>
<td>2013-08-20</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DATE</th>
<th>CNC</th>
<th>HTRAN Backend</th>
<th>HTRAN Backend Geolocation</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013-08-30</td>
<td><a href="http://www.ndbssh%5B.%5Dcom">www.ndbssh[.]com</a> 58.217.488.209</td>
<td>CHINESE JIANGSU PROVINCE NETWORK</td>
<td></td>
</tr>
<tr>
<td>2013-08-30</td>
<td><a href="http://www.ndbssh%5B.%5Dcom">www.ndbssh[.]com</a> 222.35.172.170</td>
<td>CHINESE JIANGSU PROVINCE NETWORK</td>
<td></td>
</tr>
<tr>
<td>2013-09-21</td>
<td><a href="http://www.ndbssh%5B.%5Dcom">www.ndbssh[.]com</a> 58.217.149.99</td>
<td>CHINESE JIANGSU PROVINCE NETWORK</td>
<td></td>
</tr>
<tr>
<td>2013-09-23</td>
<td><a href="http://www.jiagouanjing%5B.%5Dcom">www.jiagouanjing[.]com</a></td>
<td>2013-12-20</td>
<td></td>
</tr>
<tr>
<td>2013-12-20</td>
<td>bbs.pxtedins[.]com</td>
<td>2013-12-20</td>
<td></td>
</tr>
</tbody>
</table>
Moafee and DragonOK – Not one entity

- Geographical separation
  - Over 700 miles between them
  - Moafee – Guangdong
  - DragonOK – Jiangsu

Moafee & DragonOK – Not one entity

- Different Industry verticals
  - Moafee – Regional conflicts and US Defense
  - DragonOK – Regional High Tech and Manufacturing
Moafee & DragonOK – Tradecraft

NewCT/CT Rat

- Used by both DragonOK and Moafee group
- Embedded within a dropper with a fake header
- Embedded string table with language origins
- Found older versions going as far back as 2012

NewCT/CT Rat

- POST stub encrypted with a rolling byte XOR scheme and byte negation
- Campaign codes embedded within the implant
Moafee & DragonOK – Tradecraft

Code level similarity V1 & V2

V1
POST /NtLog/Ntfile.asp HTTP/1.1
Accept: */*
User-Agent: Mozilla/5.0 (compatible; MSIE 7.0; Windows NT 5.1)
Host:
Content-Length: 0
Cache-Control: no-cache

POST /NtLog/Ntfile.asp?ClientId=[LocalIp]%4D%65%73%69%6C%65&Ic
kel=[Identifier]&Version=[1.0.5.53] HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0;
.NET CLR 1.1.4322)
Host:
Content-Length: 36
Cache-Control: no-cache
Cookie: ASPSESSIONID124ACMCDG-GRSPOCGLEKEHSMIOLCND

V2
POST /windows/Reports.asp?Host=16-16-16-16 HTTP/1.1
Accept: */*
Cache-Control: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0;
.NET CLR 1.1.4322)
Host:
Content-Length: 126
Connection: Close
Cookie: ASPSESSIONID124ACMCDG-GRSPOCGLEKEHSMIOLCND

Moafee & DragonOK – Tradecraft

PoisonIvy
- Off the shelf RAT
- Used by a large number of actors
- Distinct configurations used by Moafee and DragonOK groups

Moafee
ID: Domains: afp.mozilla.com
Password: 741526
Mutex: )\afpA.l4

DragonOK
ID: ftp
Domains: ftp.skydnastwm.com:15836
Password: Ecp982*@Me2
Mutex: ftp
Moafee & DragonOK – Evasion techniques

- CPU core evasion

- Password protected documents
Moafee & DragonOK – Evasion techniques

- Large overlays

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
<th>Start</th>
<th>Size</th>
<th>Color</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNV Overlays</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SNV Overlay(0)</td>
<td>0</td>
<td>6789h</td>
<td></td>
<td>F0</td>
</tr>
<tr>
<td>SNV Overlay(1)</td>
<td>0</td>
<td>6789h</td>
<td></td>
<td>F0</td>
</tr>
<tr>
<td>SNV Overlay(2)</td>
<td>0</td>
<td>6789h</td>
<td></td>
<td>F0</td>
</tr>
<tr>
<td>SNV Overlay(3)</td>
<td>0</td>
<td>6789h</td>
<td></td>
<td>F0</td>
</tr>
<tr>
<td>SNV Overlay(4)</td>
<td>0</td>
<td>6789h</td>
<td></td>
<td>F0</td>
</tr>
<tr>
<td>SNV Overlay(5)</td>
<td>0</td>
<td>6789h</td>
<td></td>
<td>F0</td>
</tr>
<tr>
<td>SNV Overlay(6)</td>
<td>0</td>
<td>6789h</td>
<td></td>
<td>F0</td>
</tr>
<tr>
<td>SNV Overlay(7)</td>
<td>0</td>
<td>6789h</td>
<td></td>
<td>F0</td>
</tr>
<tr>
<td>SNV Overlay(8)</td>
<td>0</td>
<td>6789h</td>
<td></td>
<td>F0</td>
</tr>
<tr>
<td>SNV Overlay(9)</td>
<td>0</td>
<td>6789h</td>
<td></td>
<td>F0</td>
</tr>
<tr>
<td>SNV Overlays</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Moafee & DragonOK – Conclusion

Actors are either

- Collaborating on attack methodologies
- Have a common training regimen
- Have a common supply chain
Specimen B

NJQ8 Enterprise

NJQ8

• ‘Nasser Al Mutairi’ based out of Kuwait goes by the moniker njq8
• Developer of .NET based njRat/LV and VB based njW0rm
• Active on twitter, blogs and forums
• Code forks/collaboration with multiple individuals
• Both targeted and widespread activity employing these tools
NJQ8 Tools – C&C Infrastructure

Command and Control Infrastructure Heatmap

NJQ8 Tools – Campaign Codes
NJQ8 Tools – Network Telemetry Similarity

NJQ8 Collaboration - Houdini

- **H-worm** – Houdini and njq8
- Houdini aka ‘Mohamed Binadbellah’ from Algeria
NJQ8 Collaboration – BlackMafia, BlackHacker

Blackworm – njq8, BlackMafia and BlackHacker

NJQ8 Collaboration – Spygate, Fallaga

Spygate and Fallaga Rat reuse njq8 code

```
public SocketClient()
{
    this.IsBusy = false;
    this.SPL = njq8;
}
```
NJQ8 and Posse – Conclusion

Authors/actors are either

- Collaborating by creating development forks on code
- Stealing code techniques

Specimen C

Sunshop Campaign
Sunshop Campaign – Overview

- Campaign first observed May 20, 2013
- Additional waves observed August 19 and 28, 2013
- We found 110 samples linked to 11 different campaigns that utilized common infrastructure.

<table>
<thead>
<tr>
<th>Detection</th>
<th>Number of Samples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trojan.APT.9002</td>
<td>70</td>
</tr>
<tr>
<td>Trojan.APT.PoisonIvy</td>
<td>26</td>
</tr>
<tr>
<td>Trojan.APT.Gh0st</td>
<td>12</td>
</tr>
<tr>
<td>Trojan.APT.Kaba</td>
<td>1</td>
</tr>
<tr>
<td>Trojan.APT.Briba</td>
<td>1</td>
</tr>
</tbody>
</table>

Sunshop Campaign - Overview

- Deeper analysis revealed that 11 different campaigns utilized parts of the same infrastructure.
  - 13 unique c2 domains
  - C2s hosted in 58.64.205.0/24
  - Reuse of unique PE resource
  - Reuse of unique import table
  - Common compile times
  - Common builder tool
Sunshop Campaign – 9002 Builder

- Builds 9002 RAT
- Allows user to configure C2 details, campaign ID, proxy details
- Private builder, not publicly available

Sunshop Campaign – Supply chain

Its all connected!
Sunshop Campaign– Conclusion

Either

- A ‘digital quartermaster’ exists and supports separate APT campaigns
- A singular ‘digital quartermaster’ does not exist, and APT actors informally share among each other
- The ‘digital quartermaster’ exists and supports a single APT actor responsible for all of the campaigns discussed
Shared Weaponization Tools

- Metadata artifacts seen within exploit documents employed in targeted attacks
- These artifacts are seen across multiple campaigns and APT groups
- These artifacts are seen in exploit documents with different document file formats

Specimen D

Shared Weaponization Tools
Shared Weaponization Tools – Web Archive DOC

Shared Weaponization Tools – Decoy mismatches
Shared Weaponization Tools - Builders

- How are these weaponized documents created?
- Private builders not widely available
- Used in many campaigns and by many actors
- Likely supply chain supporting attackers

Overall Conclusion

Analysis points to evidence of

- Attackers evolving and adapting
- Likely digital quartermasters driving the supply chain
- Cross collaboration in development phases
- Cross collaboration in attack phases
- Formal or informal sharing channels

Continued research is required to unravel attackers ecosystems and operations in order to develop better defensive measures
Additional Resources

- Operation Quantum Entanglement
- njW0rm, njq8 [http://www.fireeye.com/blog/technical/malware-research/2013/08/njw0rm-brother-from-the-same-mother.html](http://www.fireeye.com/blog/technical/malware-research/2013/08/njw0rm-brother-from-the-same-mother.html)

Questions?