



TRAILS OF WINDSHIFT

TAHA KARIM – MALWARE SPECIALIST

A little bit about me

- Currently I'm founder and CTO of tephraCore Technologies
- Malware Analysis for more than a decade.
- Previously worked at : Dark Matter, FireEye, Symantec ...
- Most known for:
 - *Uncovering LatentBot In 2015*
 - *A major carding investigation in 2016*
 - *Multiple intelligence reports 2011-2019*
 - *Uncovering WindShift APT in 2018*

A little bit about my company

- In 2019, tephraCore Technologies a cyber security startup was established in Dubai
- With the purpose of raising the bar very high against threat actors (their job wont be easy anymore)
- We are specialized in malware analysis, Incident Response, Vulnerability analysis, security testing, building APT deception frameworks, and red team assessments and malware analysis training courses.
- We communicate via our technical blog see: <https://tephracore.com/blog>



Contents

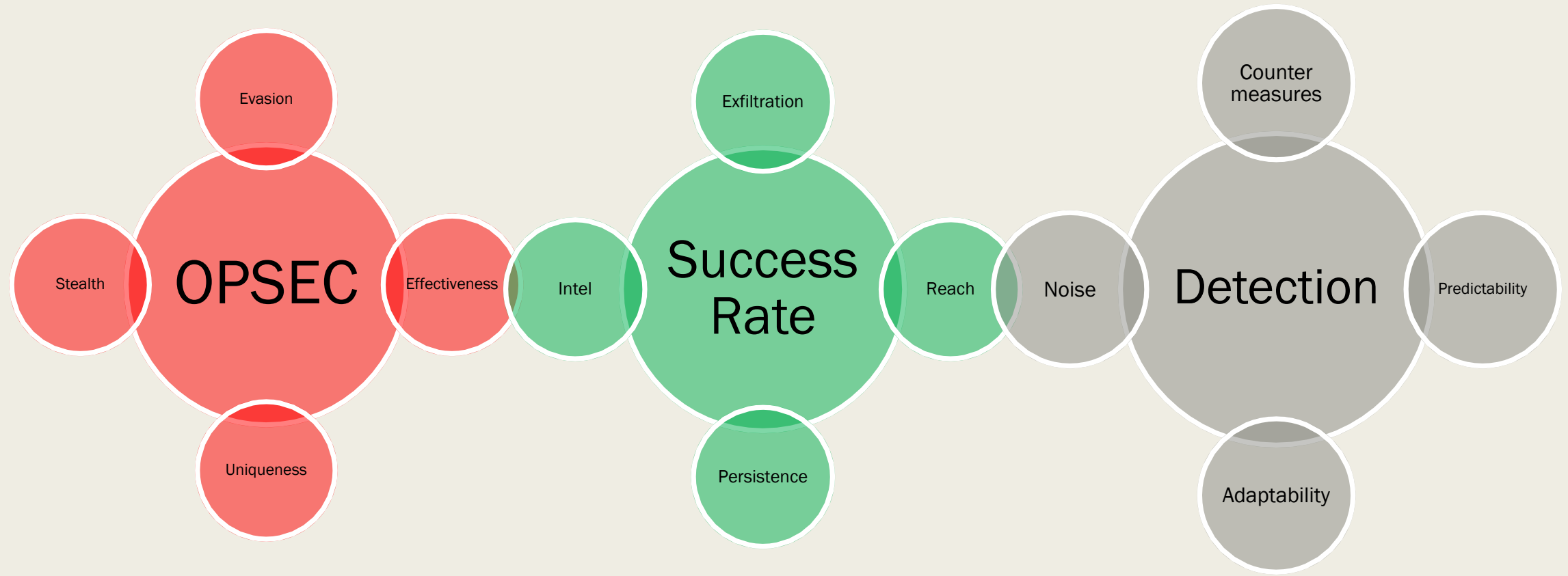
- Part 1: APT Myths and Definitions
- Part 2: WINDSHIFT Modus Operandi
- Part 3: WINDSHIFT Attribution

Part 1: 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 1: APT Myths and Definitions

How to measure an APT skill level



Part 1: APT Myths and Definitions

- Public and most known “Middle-East” APT’s, based on public feeds:
 - *GREENBUG*
 - *OILRIG*
 - *MUDDYWATER*
 - *APT 33*
 - *APT 34*
 - **Kittens*
 - *Private ones ... non disclosed yet..*

Part 1: APT Myths and Definitions

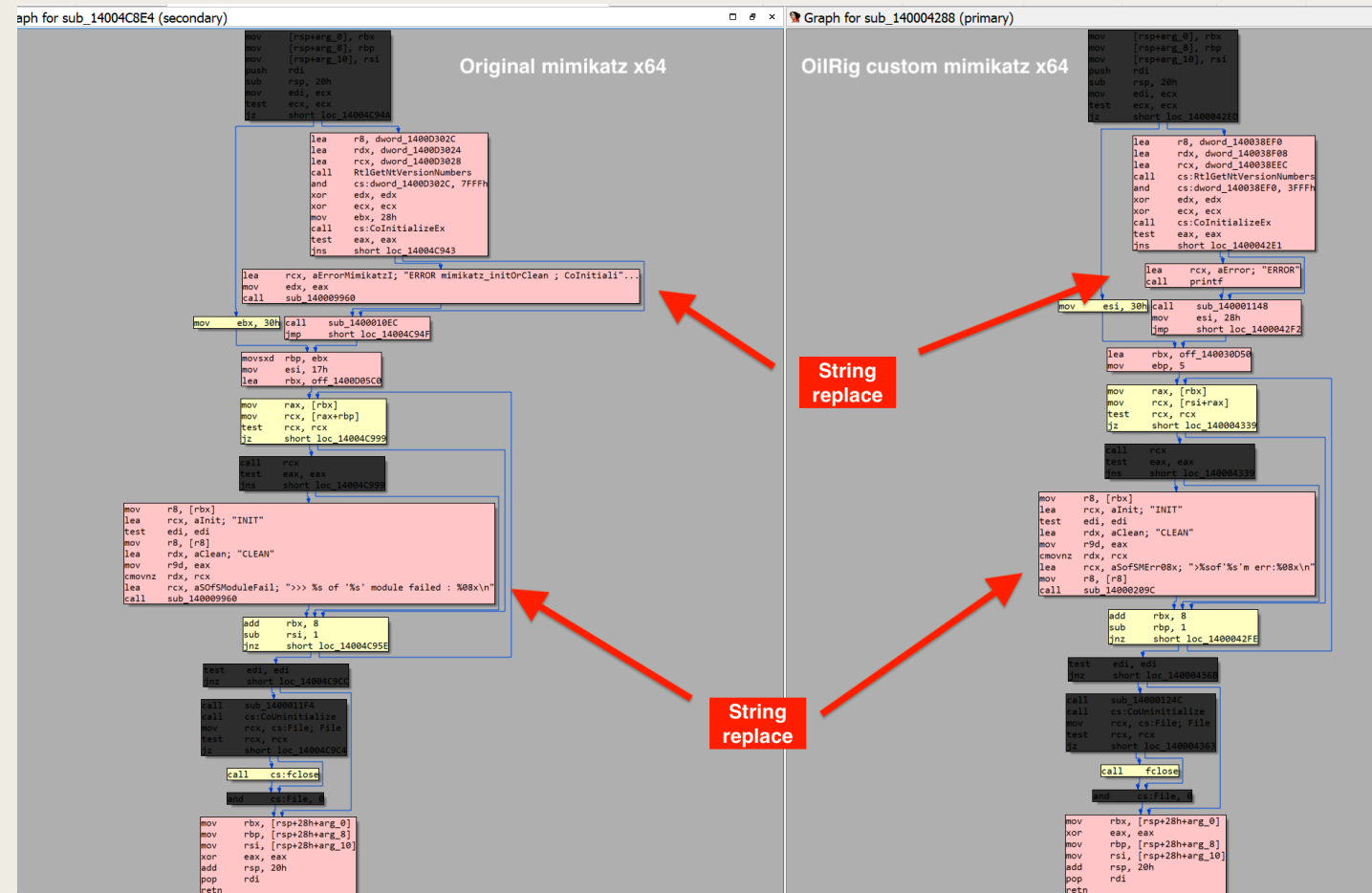
- Most of them rely on open-source tools:
 - *Empire, Metasploit, Mimikatz, invoke-obfuscation, PsExec...*
 - *Minor some customization: strings replacements, code refractoring, customizing open source code obfuscators (ConfuserEX), etc..*
- Sometimes relying and re-using low commodity malware:
 - *RATs: NANOCORE, NETWIRE, njRAT, ...*
 - *OR build copy-pasta Android malware (decompiling/recoding previous 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 1: 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*

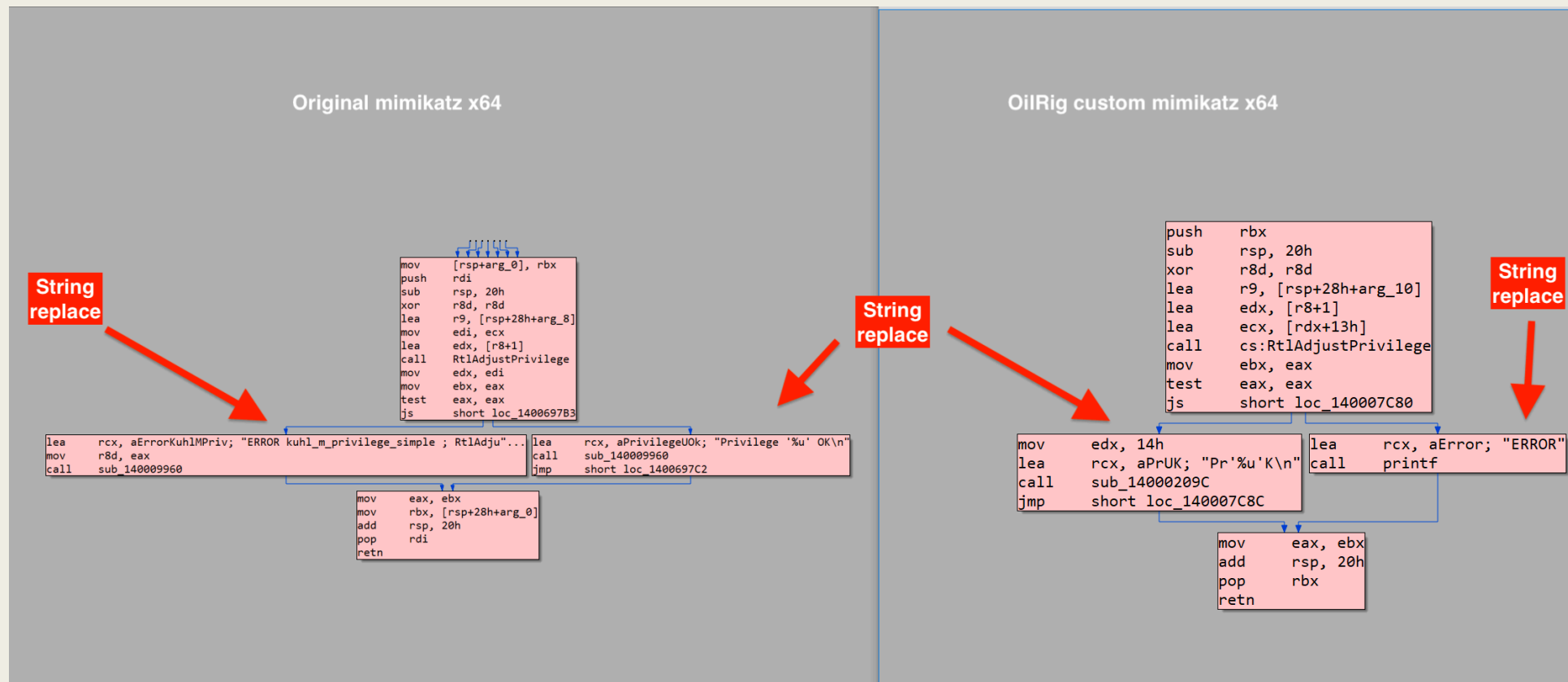
Part 1: APT Myths and Definitions

- String changes for the OilRig custom x64 Mimikatz:



Part 1: APT Myths and Definitions

- String changes for the OilRig custom x64 Mimikatz:



WINDSHIFT APT Profile



Attribution: work in progress



Confidence: Medium



A.K.A: BAHAMUT



Industries:
Government



Targets: **UAE**, Jordan,
UK, EGYPT



Toolset: WINDTAIL,
WINDTAPE,
repurpose malware..



Part 2: WINDSHIFT Modus Operandi

- 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 repurposing malware*
- 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.

Part 2: WINDSHIFT Modus Operandi

■ 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*

PS: Turn-on Privacy setting in your LinkedIn. ("you might also be interested in")

Part 2: WINDSHIFT Modus Operandi

- Phase 1: RECON – phase 1 duration 1-2 years
 - Example of fake online persona Asalah (أصالة آل سمیحة) Al Sameeha

The image displays three screenshots of social media profiles for a persona named Asalah Al Sameeha (أصالة آل سمیحة).

Facebook Profile: The profile is for "Asalah Al Sameeha" (asalahalsameeha@). The cover photo is an aerial view of a city. The profile picture is a woman's face with a blacked-out area. The bio lists "Dubai Airports", "University of Dubai", and "United Arab Emirates". The page shows 414 likes and 415 posts. The interface is in Arabic.

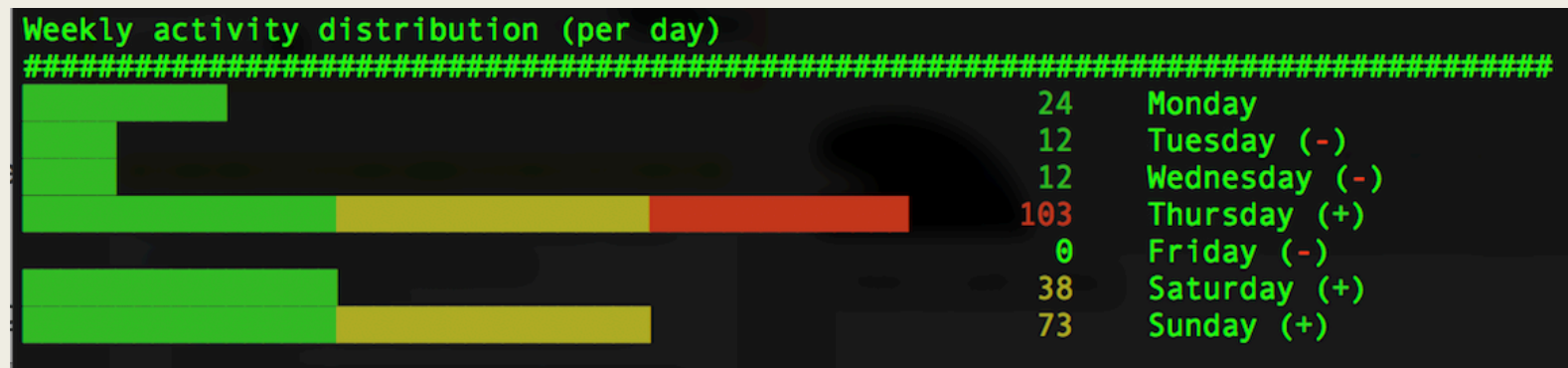
Instagram Profile: The profile is for "asalahalsameeha". The profile picture is a woman's face with a blacked-out area. The bio lists "7 publications", "59 abonnés", and "71 suivis". The page shows "Asalah Al Sameeha" as the name.

Twitter Profile: The profile is for "Asalah Al Sameeha" (@aheernastalahalasa). The profile picture is a woman's face with a blacked-out area. The bio lists "Abu Dhabi", "abudhabi.ae", and "Joined June 2014". The page shows 262 tweets, 539 following, 81 followers, and 76 likes. The interface is in Arabic.

Part 2: WINDSHIFT Modus Operandi

■ Twitter OSINT 101:

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



APT maintained Twitter account: @aheemaslahalasa

Part 2: WINDSHIFT Modus Operandi

- 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 2: WINDSHIFT Modus Operandi

- 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

Khaleej Times

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](#)

■ Phase 2: RECON – phase 2 – duration 6 months – 1 year

- ```
<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. =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>
```
- email tracking**

Hi,

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

[http://www.ifread.com/trackreport?k=\[REDACTED\]](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



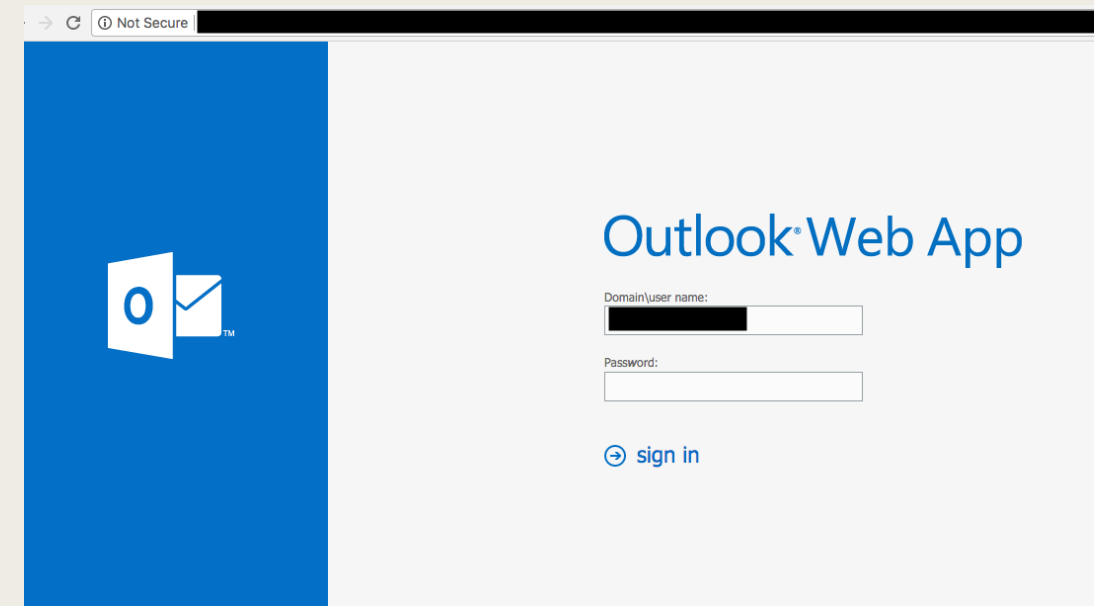
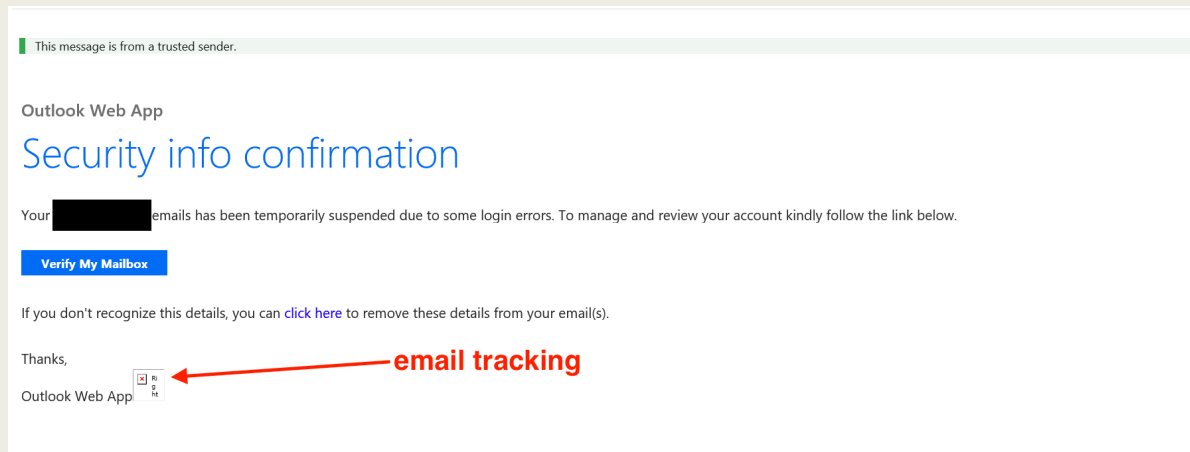
# Part 2: WINDSHIFT Modus Operandi

- 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 2: WINDSHIFT Modus Operandi

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



# Part 2: WINDSHIFT Modus Operandi

- 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://\[REDACTED\].ml/payment](https://[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

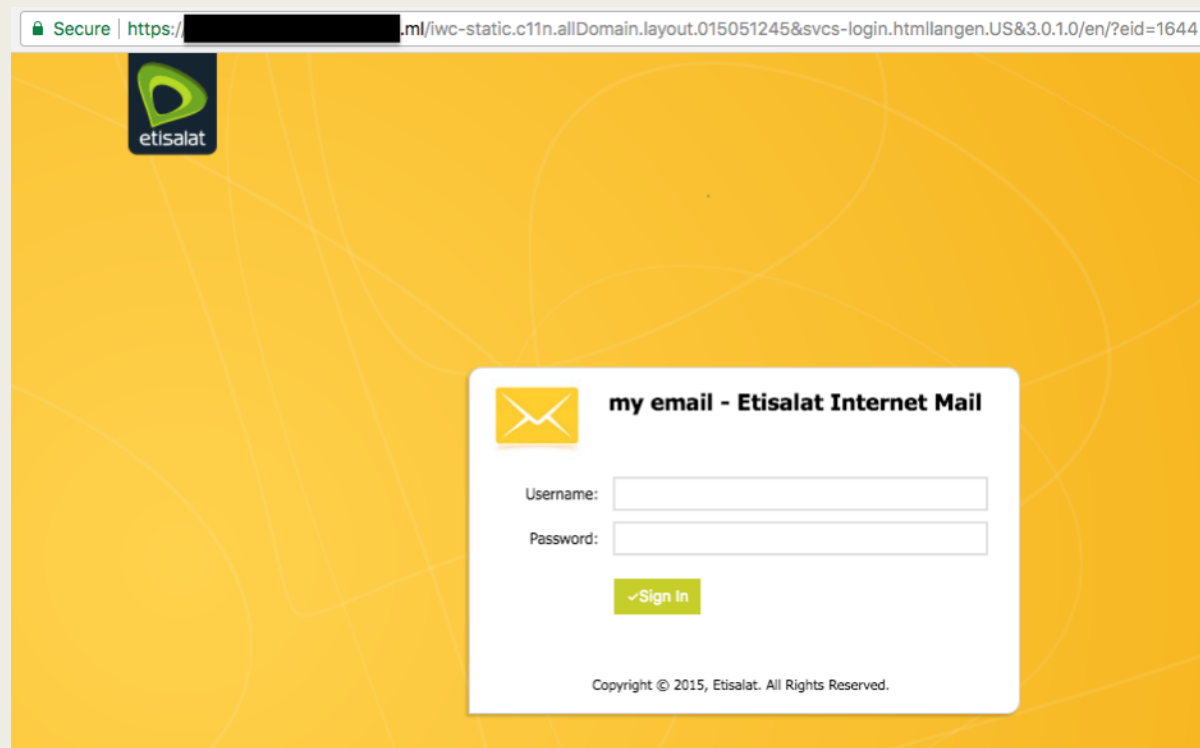
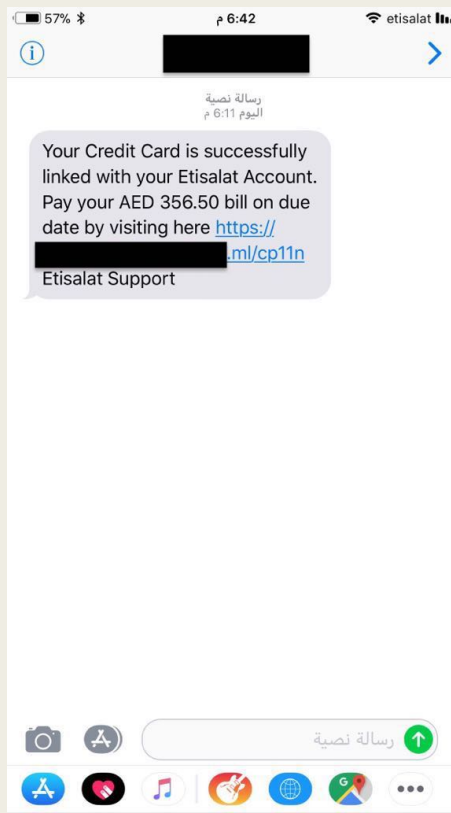
[Apple ID](#) | [Support](#) | [Privacy Policy](#)

Copyright © 2017 Apple Inc. 1 Infinite Loop, Cupertino, CA 95014, United States. All rights reserved.

# Part 2: WINDSHIFT Modus Operandi

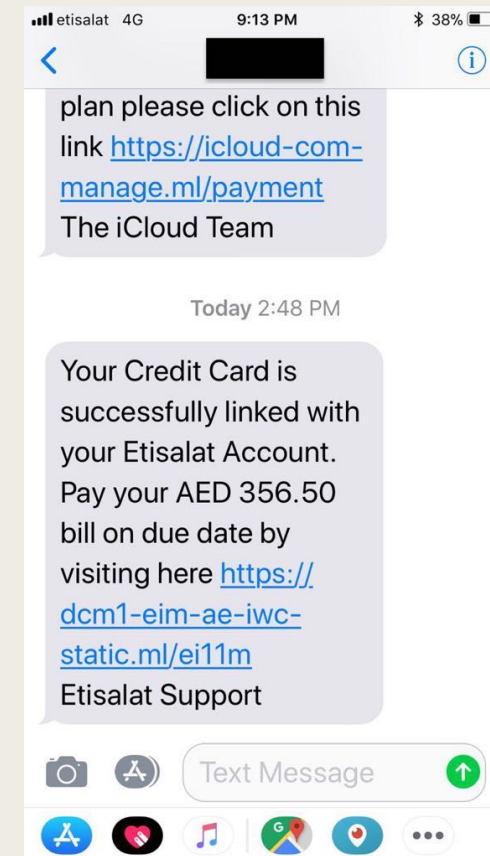
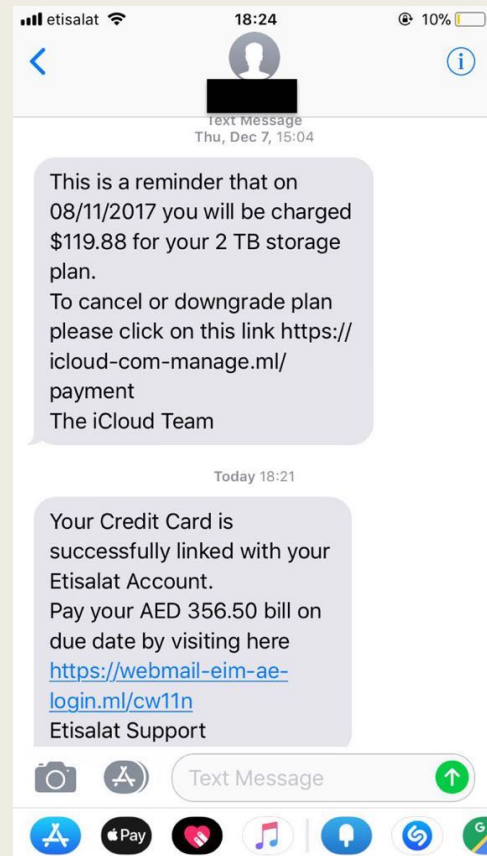
## ■ Phase 3: Credential harvesting, **duration 1 day**

– *SMS targeting Etisalat Users:*



# Part 2: WINDSHIFT Modus Operandi

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



# Part 2: WINDSHIFT Modus Operandi

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



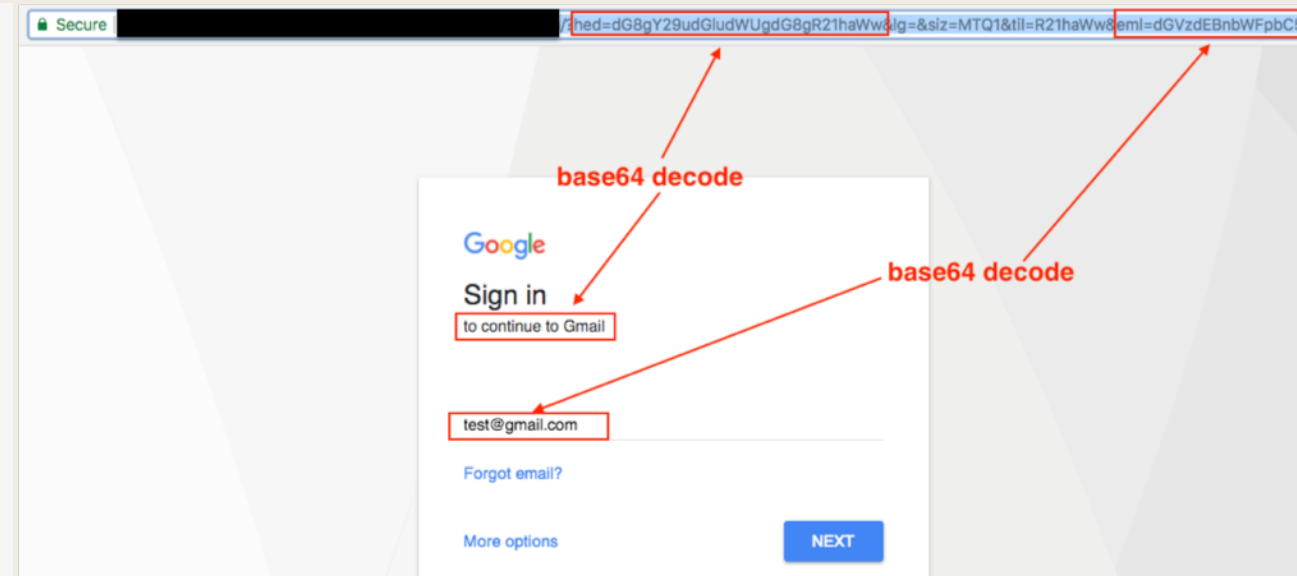
Hi [REDACTED]  
Someone just try to signin to your Googlemail [REDACTED]@gmail.com recently. To protect your account please change your password now by following the link below:

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

[CHANGE YOUR PASSWORD NOW](#)

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.



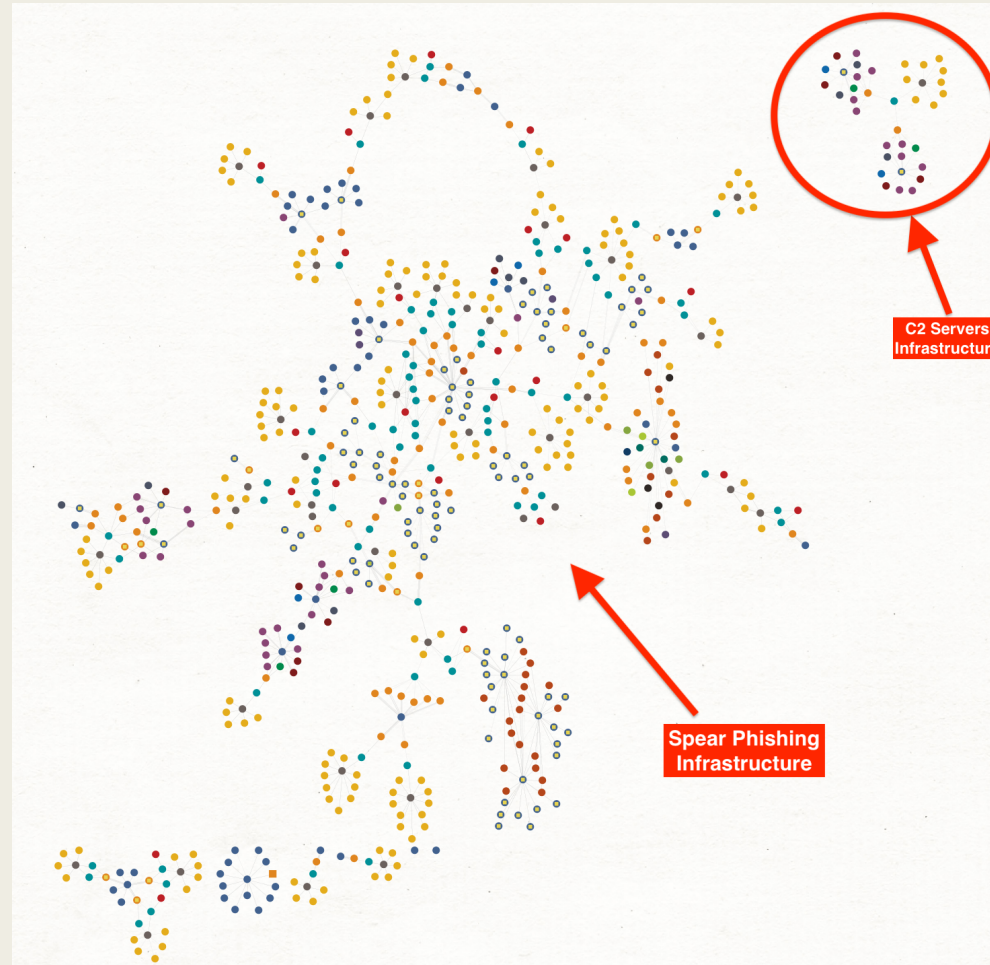
# Part 2: WINDSHIFT Modus Operandi

## ■ 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.*
- *Repurposing malware of other APT actors.*
- *Re-use command and control infrastructure from other APT actors*
- *Real separation between spear phishing infrastructure and malware C2 infrastructure, to avoid attribution, suspicions and takedowns..*

# Part 2: WINDSHIFT Modus Operandi

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



# Part 2: WINDSHIFT Modus Operandi

## ■ Phase 5 : Evasion/ Disappearance

- *Shutting the domain names*
- *Switching to other spear phishing infrastructures*
- *Continuously getting more access to new infrastructures:*
  - Hacking
  - purchasing new access from VPS resellers (bitcoin), bullet proof hosting providers.
  - Renting infrastructures from other cyber crime groups
- *Repointing domains to new infrastructures*
- *Getting access to more malware, and more C2 infrastructures and maintain access*



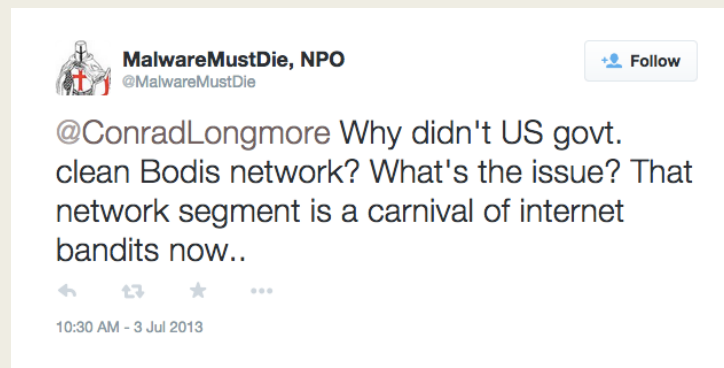
# Part 2: WINDSHIFT Modus Operandi

## ■ 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
<input type="checkbox"/> 199.59. [REDACTED] 📁	US	199.59. [REDACTED]	395082	2018-01-12	2018-06-08	kaspersky, pingly	<a href="#">Bodis</a> <a href="#">Routable</a>

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



# Part 2: WINDSHIFT Modus Operandi

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

Malware ID	First seen	Target OS	Purpose
WINDTAIL.A	Jan 2017	macOS	Backdoor exfiltrating files
WINDTAIL.B	Jan 2018	macOS	Downloader of WINDTAPE
WINDTAIL.C	Jan 2018	macOS	Variant of WINDTAIL.B
WINDTAPE	Jan 2018	macOS	Backdoor taking screenshots
WINDDROP	May 2018	Windows	Downloader of an unknown windows malware

# Part 2: WINDSHIFT Modus Operandi

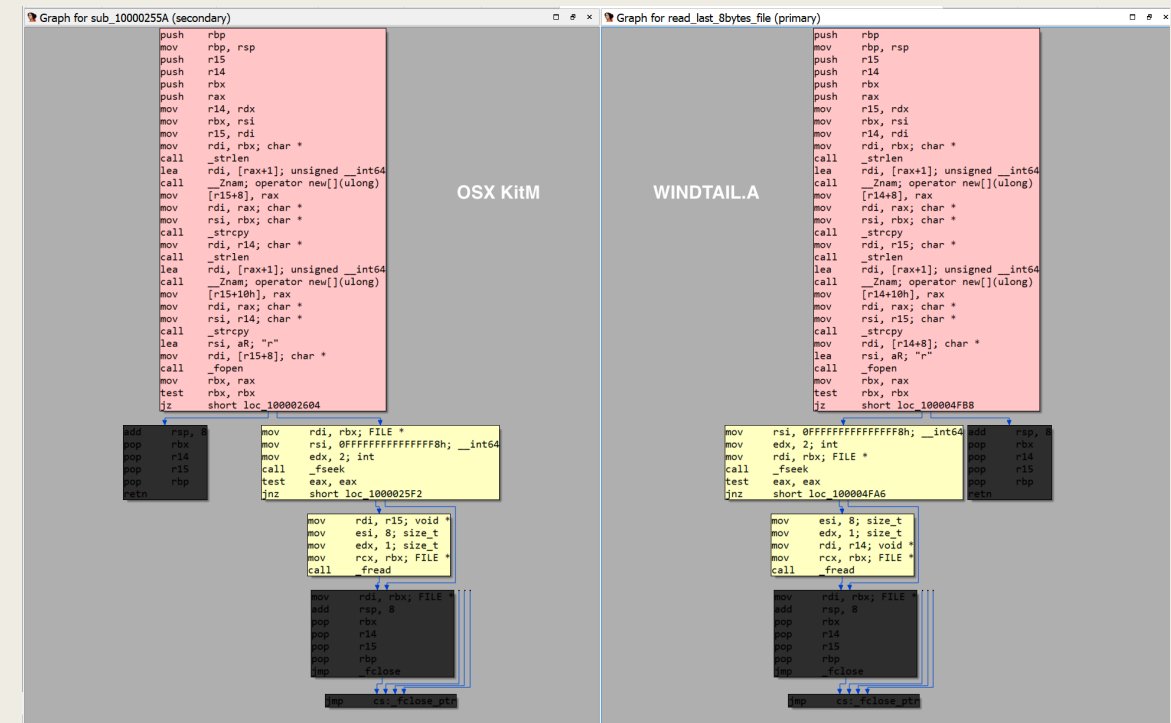
- MacOS malware was signed, below are the signing developer certificates :

Developer name	Developer ID	Email
Warren Portman	9S442G74FH	warren82port@mail.com
Caren Van	4F9G49SUXB	N/A
Andrew wilson	CXNRU596HQ	N/A

- We sent the malicious samples to Apple along with detailed technical analysis.
- Apple revoked the developer ID certificates. This mean all malware signed with these certificates won't be able to run and will be blocked by OSX Gatekeeper.

# Part 3: WINDSHIFT Attribution

- WINDTAIL is 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



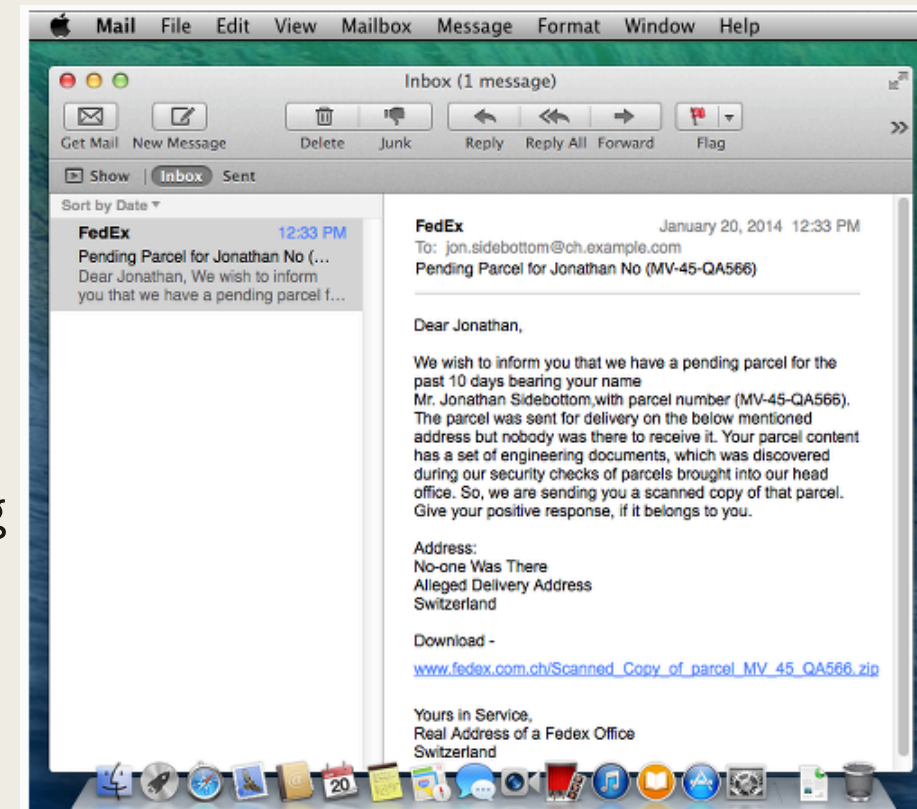
# Part 3: WINDSHIFT Attribution

- A very similar malware, dubbed **LaoShu**, similar to “Hack Back” aka “KitM OSX”, was used in 2014 targeting individual using “undeliverable item” phishing scam:
- Malware communicated to floracrunch[.]com
- In 2014 (during the attack) it was resolving to a Russian server : **93.189.43.236**

Resolve	Location	Network	ASN	First	Last
<a href="#">209.99.40.223</a>	US	<a href="#">209.99.40.0/24</a>	40034	2016-07-26	2016-07-26
<a href="#">93.189.43.236</a>	RU	<a href="#">93.189.40.0/21</a>	41853	2013-11-09	2014-02-01

- A very recent WindShift attack we found, was resolving to **209.99.40.223**, the same IP address used 3 years ago By LaoShu:

Resolve	Location	Network	ASN	First	Last
<a href="#">209.99.40.223</a>	US	<a href="#">209.99.40.0/24</a>	40034	2019-01-27	2019-03-04
<a href="#">209.99.40.222</a>	US	<a href="#">209.99.40.0/24</a>	40034	2019-01-26	2019-03-01
<a href="#">185.25.50.189</a>	LT	<a href="#">185.25.48.0/22</a>	61272	2018-01-25	2018-06-04

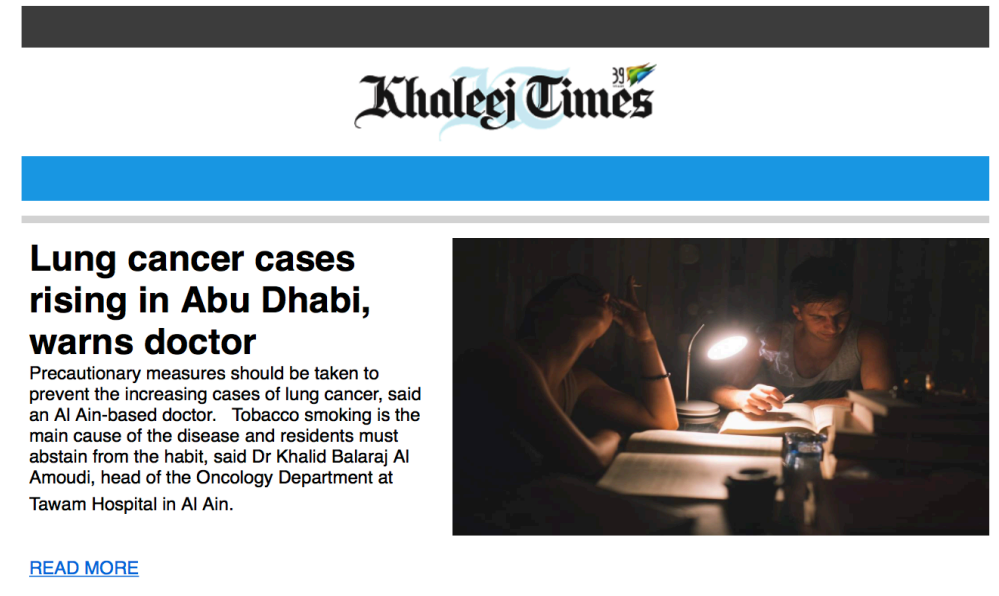


# Part 3: WINDSHIFT Attribution



BAHAMUT 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



WINDSHIFT APT



# Part 3: WINDSHIFT Attribution



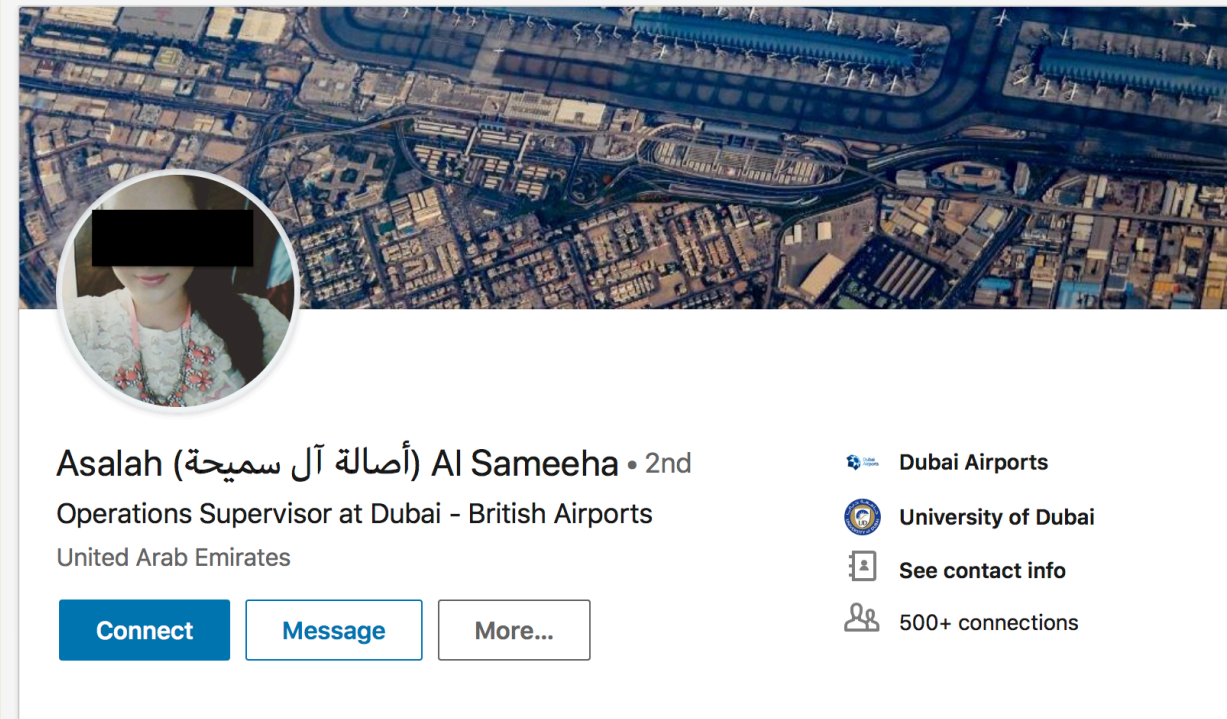
ForexClub

**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

Send InMail

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

BAHAMUT APT



**Asalah (أصالة آل سميحة) Al Sameeha • 2nd**  
Operations Supervisor at Dubai - British Airports  
United Arab Emirates

Connect Message More...

Dubai Airports  
University of Dubai  
See contact info  
500+ connections

WINDSHIFT APT

# Conclusion

- 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.
- 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,*
- We will be releasing technical details of analysis next week. Please monitor <https://tephracore.com/blog>



# WINDSHIFT APT Indicators of compromise

domain	string2me.com
domain	domforworld.com
domain	floracrunch.com
FileHash-SHA1	4613f5b1e172cb08d6a2e7f2186e2fdd875b24e5
FileHash-SHA1	6d1614617732f106d5ab01125cb8e57119f29d91
FileHash-SHA1	da342c4ca1b2ab31483c6f2d43cdcc195dfe481b
FileHash-SHA1	df2a83dc0ae09c970e7318b93d95041395976da7
FileHash-SHA256	3085c2ad23f35a2ac0a3a87631991eeb9497dbe68d19c8dd2869578a33ecba0d
FileHash-SHA256	34561763c4c43a8811d7eb404f5dee72a17d2fff3e20f458fc6a9247043ecbb6
FileHash-SHA256	38dd6b0e7ed513fa9f8947680aa3cc76f31187f726d26c780b2e7eafa3f9879d
FileHash-SHA256	5443ad1db119b599232b91bbf0ac3d0e1e4f4894f7f4ba191e7b9f7a27acea0d
FileHash-SHA256	69504c5b18f4c6347b5921d2a676abf841aecbefad67cafa2ea4d97960d10614
FileHash-SHA256	ad282e5ba2bc06a128eb20da753350278a2e47ab545fdab808e94a2ff7b4061e
FileHash-SHA256	ceebf77899d2676193dbb79e660ad62d97220fd0a54380804bc3737c77407d2f
FileHash-SHA256	d3baa6af5bbb9318126dc62a7dcab19d1dd5592c30ea552c21361d0cc0ebe2f5
FileHash-SHA256	dde5d98f6ee472f3779ece1cc44e18243c0eb4d12f8abc4b56f559da50d896db
FileHash-SHA256	ebba0fd56ad6f861e7103b9dcbbb21353a9d48fa40d23eb83efd78523b5b40d3
FileHash-SHA256	f38f490d7a132c847ac71ee5f4d4b290b9f5592e6b436d68ca0a4be7cee918d3
FileHash-SHA256	0c0fce879c8ca00a6f9feeaccf6cba64374e508cacd664682e794a4a4cc64ffb
FileHash-SHA256	1de218e45cdf069c10d1a8735d82688b8964261a5efe3b6560e0fdcfa3c44c1d
FileHash-SHA256	1fbfbaefd50627796e7f16b8cc2b81ffbc5effcb33b64cc8e349e44b5d5d3ee8
FileHash-SHA256	8c8b53f4d4836bd7d4574fe80039caf9f2bd4d75740f2e8e22619064c830c6d9
FileHash-SHA256	cb3068ee887fc2f66d3df886421d5e5fa5e31ec4ee0079a7dcf9628bd2730de0
FileHash-SHA256	ce8e01373499b539f4746c0e68c850357476abe36b12834f507f9ba19af3d4f9
FileHash-SHA256	dd0e0883392ffe8c72c4b13f58e5861fc2f4bc518a6abea4f81ae3a44b2eda1c
FileHash-SHA256	e0fdbcb5e0215f9fae485fbfcd615c79b85806827e461bca2e1c00c82e83281dc
FileHash-SHA256	e2a5663584727efa396c319f7f99a12205bb05c9c678ffae130e9f86667505a6
FileHash-SHA256	ffae55894f0f31d99105b5b7bbbca79e9c1019b37b7a5a20368f50c173352fd1
URL	<a href="http://flux2key.com/skdfhwsdkfksgfuisiseifgygffiw.php">http://flux2key.com/skdfhwsdkfksgfuisiseifgygffiw.php</a>