June
2016

Operation DustySky Part 2

ClearSky Cybersecurity

www.clearskysec.com/dustysky2

TLP:White
For public distribution

Contents

Foreword

This report is a follow-up on our DustySky operation report from January 2016[1]. It analyses new attacks by Molerats against targets in Israel, The United States, Egypt, Saudi Arabia, United Arab Emirates and The Palestinian Authority.

We elaborate on the scope and targeting of the DustySky campaign and expose new infrastructure and incidents. In addition, we expose the identity of an individual who is behind the DustySky campaign. Following the previous report, this individual has contacted us trying to learn what we know about him.

Attacks against all targets in the Middle East stopped at once, after we published our first report. However, the attacks against targets in the Middle East (except Israel) were renewed in less than 20 days. In the beginning of April 2016, we found evidence that the attacks against Israel have been renewed as well[2].

Based on the type of targets, on Gaza being the source of the attacks, and on the type of information the attackers are after - we estimate with medium-high certainty that the **Hamas terrorist organization[3] is behind these attacks**.

Acknowledgments

This research was facilitated by the PassiveTotal for threat infrastructure analysis.
We would like to thank the security researchers and organizations who shared information and provided feedback, which have been crucial for this research.

[1] clearskysec.com/dustysky

[2] The report seems to have indeed disrupted the attacker for several months. In a PDB found in a sample from the April wave, there is an indication that the attacker saw that wave as “part 2” of the attacks (part 1 being the attacks before the public report): Name D:\IL\Working Tools\2016-04-23 NeD Ver 9 **Ran II** - 192.52.167.118\NeD Download and execute Version 1 - Doc\bin\Release\Obfuscated\News.pdb

[3] https://www.nctc.gov/site/groups/hamas.html

Background

DustySky is a multi-stage malware written in .NET (recently ported to C++). It is composed of a DustySky dropper, DustySky core, and the DustySky keylogging component. It has been developed and used since May 2015 by Molerats (aka "Gaza cybergang"), a terrorist group whose main objective in this campaign is intelligence gathering.

A wave of malicious email messages has been sent on a weekly basis to hundreds of targets. The email message and the lure documents are written in Hebrew, Arabic or English. The attackers would send a malicious email message that either links to an archive file (RAR or ZIP compressed) or has one attached to it. The archive contains an .exe file, sometimes disguised as a Microsoft Word file, a video, or another file format, using the corresponding icon. We have also found samples that use Microsoft Word files embeded with a malicious macro, which would infect the victim if enabled. In all cases the attackers rely on social engineering - convincing the victim to open the file (and enabling content if it is disabled) - and not on software vulnerabilities

In addition to DustySky, the attackers use publicly available tools such as the following Remote Administration Tools (RAT): Poison ivy, Nano Core, XtremeRAT, DarkComet and Spy-Net. These tools have been used either following an initial DustySky infection, or by themselves.

Targeted sectors are mostly governmental and diplomatic institutions including embassies; companies from the aerospace and defense Industries; financial institutions; journalists; software developers.

Most targets are from the Middle East, some are in the United States and Europe.

In January 2016 we've published an extensive report about the campaign and malware - “Operation DustySky” - which is available here: clearskysec.com/dustysky

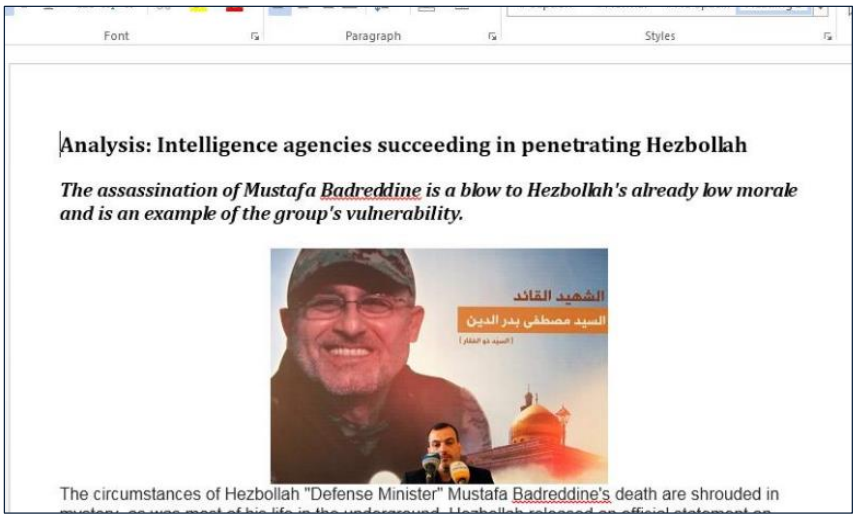
Targeting and Incidents

Who are they after?

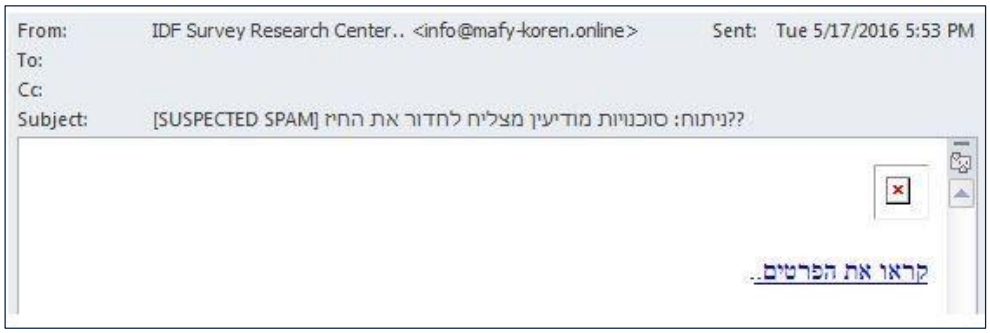
Targeting in Hebrew and English

Below are examples of lure documents presented to the victim while the malware infects the computer. The content of the document is always copied from an online public source. The subject usually revolves around defense and security or current affairs. Once in a while other topics or content are used - such as a public corporate responsibility document published by Egged, an Israeli bus company; a part of an online Novel published as a doc file; or pornographic materials.

Intelligence agencies succeeding in penetrating Hezbollah.exe

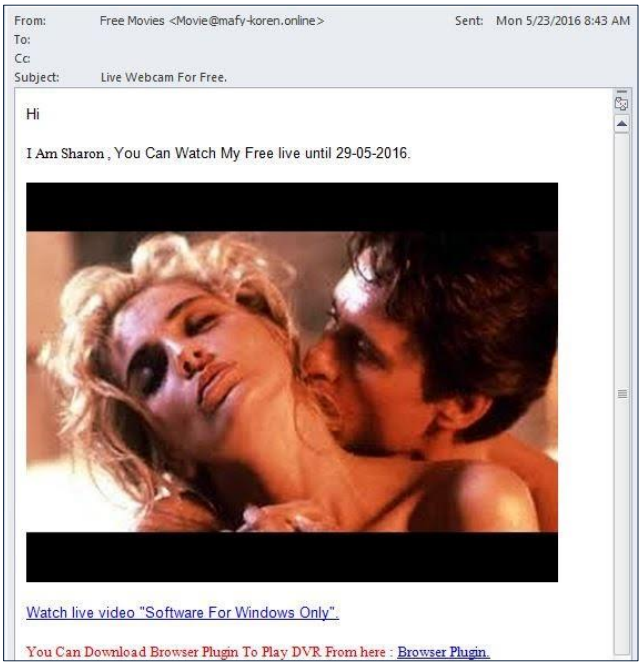


IDF survey Research Center



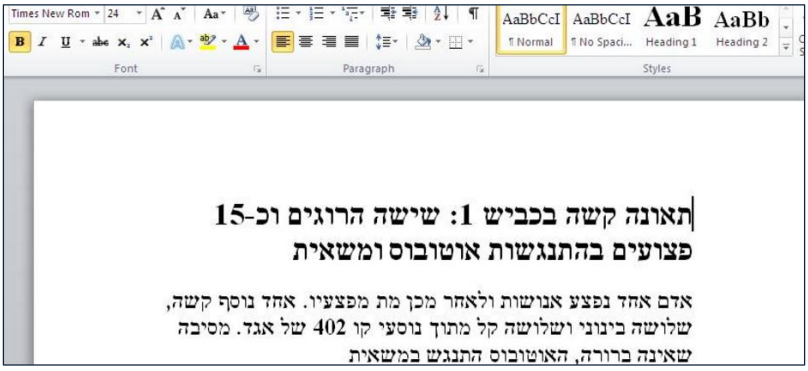
קונדום לא משומש (unused condom)

Live Webcam For Free

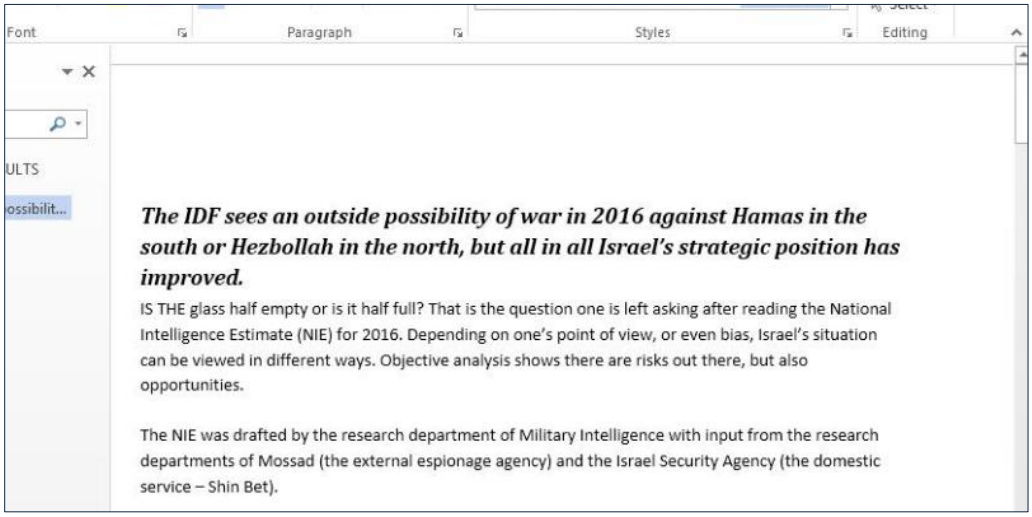


שישה הרוגים וכ-15 פצועים בהתנגשות אוטובוס ומשאית.exe

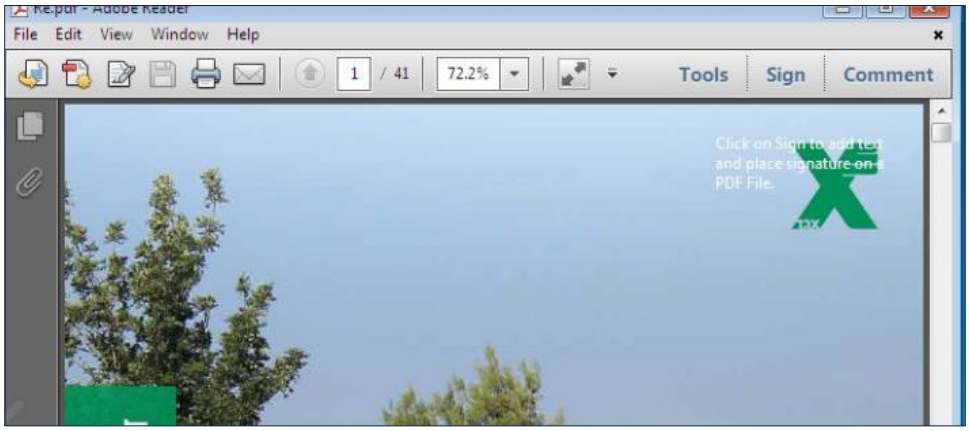
(Six killed and 15 wounded in an collision between bus and tractor trailer)



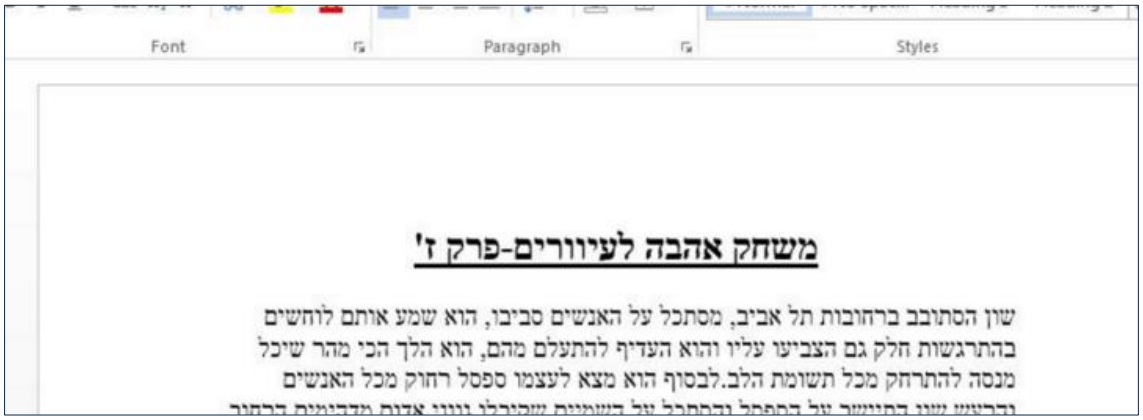
Intelligence Report: Israel's strategic position has improved.exe



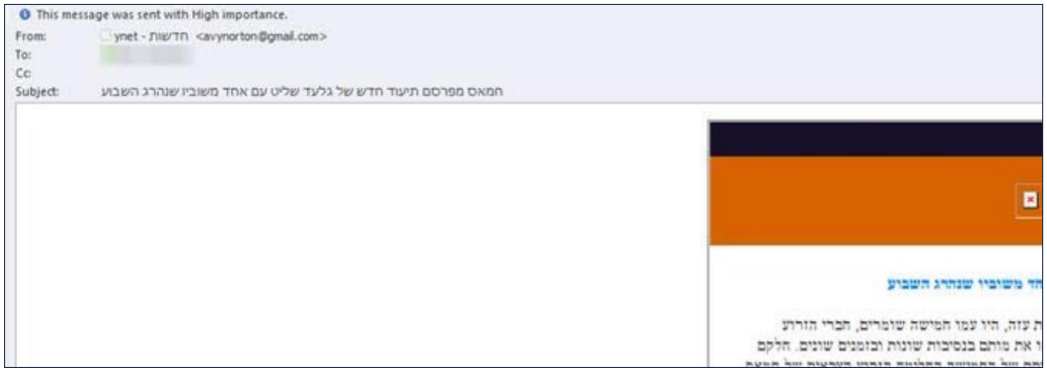
דוח אחריות תאגידית וקיימות - אגד.exe
(corporate responsibility and sustainability report - Egged)



משחק אהבה לעיוורים-פרק ז'.exe
(blind love game – chapter G)



Ynet news



In a recent wave, a bit.ly link (https://bitly[.]com/1YRoIPX) was used instead of a direct link to the malware (bit.ly is a legitimate URL shortening service). The shortened link statistics page enables us to learn about the scope and the targeting of this threat actor.

We can see that the link was clicked 210 times, out of which 130 were in **Israel**, 32 in the **United States**, 9 in the **Palestinian authority**, and 39 from 12 other countries (1-5 each).

Top Countries (clicks / % of total)

Israel	136	65%
United States	32	15%
Palestinian Territo...	9	4%
Anonymous Proxy	8	4%
France	5	2%
Lithuania	3	1%
Turkey	3	1%
Netherlands	3	1%
Germany	2	1.0%
Austria	2	1.0%
United Kingdom	2	1.0%
Korea, Republic of	1	0.5%
Lebanon	1	0.5%
Russian Federation	1	0.5%
Hong Kong	1	0.5%
Belgium	1	0.5%

The statistics do not necessarily reflect the exact distribution of targets: one target may click more than one time; a proxy or VPN may skew the country count; and security researchers and bots may also comprise part of the clicks. However, they do roughly represent the scope of the campaign: tens to few hundreds of recipients - mostly in Israel, the United States and the Palestinian Territories.

This corresponds to the distribution we know of based on other sources such as direct reports from targets, cases we have investigated, and open source intelligence.

Targeting in arabic

Below are examples of a document and a malicious email, targeting Arabic speaking victims.

ملخص تقرير المخابرات اليومي .

(Summary daily intelligence report)


From: الهيئة العامة للإستعلامات <ladysalmeen@gmail.com>
Date: 2016-01-27 9:33 GMT+00:00
Subject: ملخص تقرير المخابرات اليومي .
To:

مرفق تقرير مدعم بالصور يلخص ما جاء في تقرير المخابرات العامة والمخابرات الحربية والإستطلاع حول أحداث اليوم.
يمكنك تحميل المرفق من الموقع الرسمي من هنا

Download Here

الهيئة العامة للإستعلامات

3 شارع الاستاد البحرى - مدينة نصر

القاهرة - جمهورية مصرالعربية

ت : 22617345 - 22617344 - 22617358 - 22617308 - 22617304

القصة الحقيقية لموت القيادي فريد إسماعيل في سجن العقرب .exe

(The true story behind the death of the leader Farid Ismail in Scorpio prison)


بمحبسه بسجن العقرب وفاة القيادي الإخواني فريد إسماعيل وفاة
القيادي الإخواني فريد إسماعيل الأربعاء, 13 مايو 2015 20:03
توفى منذ قليل الدكتور فريد إسماعيل، البرلماني السابق وعضو

When targeting Arab-speaking counties, most targets are in **Egypt, Saudi Arabia, The Palestinian authority and United Arab Emirates.**

We have learned of more than 150 targets in these countries when investigating a breached email account used by the attackers to send further malicious emails.

About 60% of targeted the email addresses where Gmail, Hotmail and Yahoo accounts. The rest of the email accounts were in organizations - both private and governmental.

We searched for information about the targets in order to learn the interests of the attackers. **Below are examples of targeted individuals and organizations:**

- Several diplomats and employees of the ministry of foreign affairs in **Egypt** (20 emails addresses at mfa.gov.eg, investment.gov.eg and other offices).
- **Egypt**'s Ambassador in the Ukraine, Counsellor of Permanent Mission of Egypt to the United Nations, the Egyptian Embassy in New Zealand, and Egyptian Embassy in Pakistan.
- An individual at the prime minister's office at the **Palestinian Authority** (both his Gmail account and an account under pmo.pna.ps).
- A senior official at the Birzeit University in the **Palestinian Authority.**
- A consultant at West Bank and Gaza Group, **The World Bank** (worldbank.org).
- **Israeli** banks.
- **Israeli** military and defense companies.
- Ministry of Foreign Affairs of **Saudi Arabia** (2 email addresses at mofa.gov.ae).
- Ministry of Foreign Affairs of **United Arab Emirates** (2 email addresses at mofa.gov.sa).
- A banks in Dubai and Abu Dhabi, **United Arab Emirates**.
- A Lobbying organizations in the **UK.**
- Former politician in the **UK**.
- A diplomat the **European Commission** (ec.europa.eu).
- The Royal Hashemite Court in **Jordan** (rhc.jo).
- An employee at the **U.S.** Department of State (state.gov).

What are they after?

The malware scans the computer for files that contain certain keywords. The list of keywords, in base64 format, is retrieved from the command and control server as a text file. For example:

```
Y3YuZG9j
Y3YucGRm
c2VjcmV0IA==
INiz2LHZiiA=
2KPZhdmG2Yog
2LnYs9mD2LHZiiA=
2YXYrtin2KjYsdin2Kog
INeh15PXqNeUIA==
157XodeV15XXkiA=
15DXkdeY15fXlCA=
INem15HXkCA=
157Xktei15nXnSA=
INee15XXodeTIA==
16HXmdeh157XkNeV16o=
16HXmdeh157XkA==
cGFzc3dvcmQg
cGFzc3dvcmRz
157XmdeV15fXkyA=
cHJpdmF0ZSA=
INiu2KfYtSA=
INmF2K3YttixIA==
INiz2YrYqtinIA==
INiq2K3ZgtmK2YIg
Lm92cG4=
LnBmeA==
dXB3b3Jr
```

These words indicate what information the attackers are after - information pertaining to homeland security and military issues; personal documents; credentials, certificates and private keys.

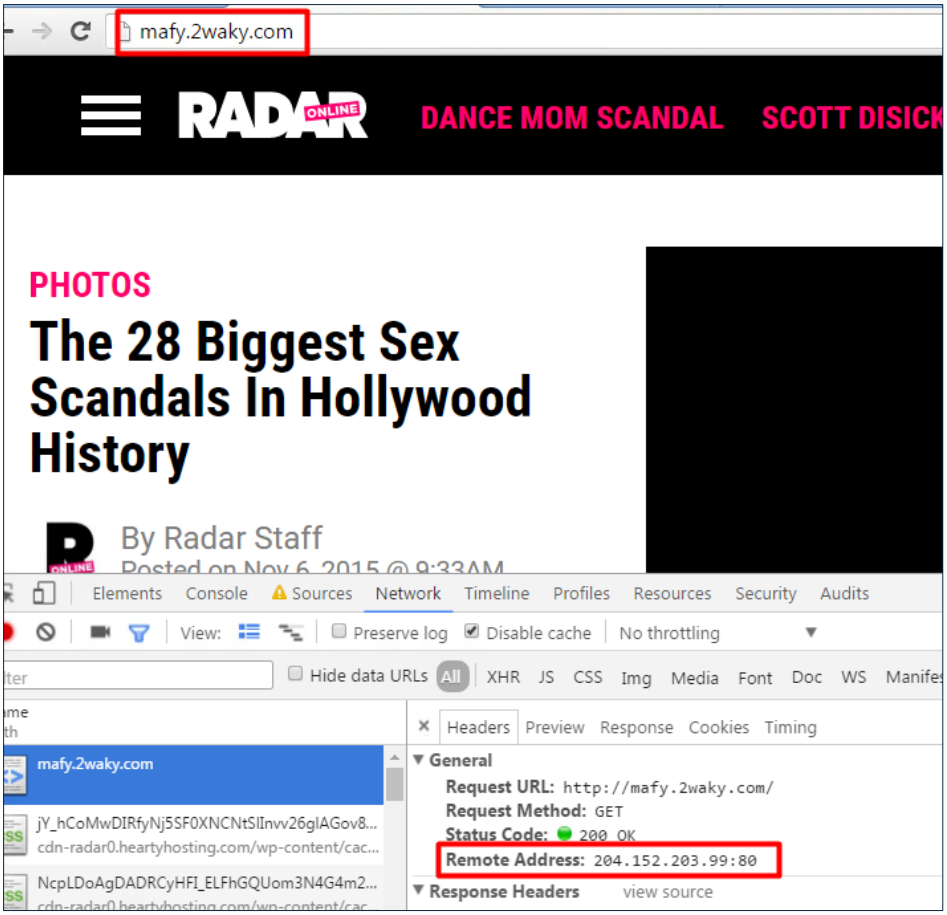
Below are keywords that have been used in the recent campaigns:

Baste64	Decoded	English translation
ZW1haWxz	Emails	
YWNjb3VudHM=	Accounts	
YmI0Y29pbg==	Bitcoin	
Y3YuZG9j	cv.doc	
Y3YucGRm	cv.pdf	
TG9naW4gRGF0YQ==	Login Data	
S2V5V29yZA==	KeyWord	
LndhbGxldA==	.wallet	
LnBmeA==	.pfx	
Lm92cG4=	.ovpn	
dXNlcnMgbmFtZSBhbmQgcGFzc3dvcmQ=	users name and password	
dG9yLmRvYw==	tor.doc	
cGFzc3dvcmRz	passwords	
cGF5cGFs	paypal	
bG9naW5zLg==	logins.	
bG9naW5z	logins	
aWQucGRm	id.pdf	
aWQuanBn	id.jpg	

2YXYrtin2KjYsdin2Kog	مخابرات	Intelligence
2YXYrdi22LEg2KfYrNiq2YXYp9i5	محضر اجتماع	meeting protocol
2YPZhNmF2KfYqiDZhdix2YjYsQ==	كلمات مرور	passwords
2YPZhNmF2KfYqiDYs9ix	كلمات سر	passwords
2YPZhNmF2KfYqiDYp9mE2YXYsdml2LE=	كلمات المرور	the passwords
2YPZhNmF2KfYqiDYp9mE2LPYsQ==	كلمات السر	the passwords
2YPZhNmF2KfYqiDYp9mE2LPYsQ==	كلمات السر	the passwords
2YLYp9i52K/YqSDYqNmK2KfZhtin2Ko=	قاعدة بيانات	Database
2YjYq9mK2YLYqQ==	وثيقة	document
2LPZitix2Kkg2LDYp9iq2YrYqQ==	سيرة ذاتية	CV
2LPZitiq2Kcg	سيتا	SITA (www.sita.aero)
2LnYs9mD2LHZiiA=	عسكري	military
2KPZhdmG2Yog	أمني	defense or security related
2KfZhNil2YrZhdmK2YTYp9iq	الإيميلات	the emails
2KfYs9iq2K7YqNin2LHYp9iq	استخبارات	intelligence
16rXldeb16DXmdeV16og16bXkdeQ15nXldeq	תוכניות צבאיות	military plans
16rXldeb16DXmdeV16o=	תוכניות	plans
16nXkScn15s=	שב"כ	Shabak (Israel Security Agency)
16jXkNepINeU157Xntep15zXlA==	ראש הממשלה	prime minister
16HXmdeh157XkNeV16o=	סיסמאות	passwords
16HXmdeh157XkA==	סיסמא	password
16HXldeTLg==	סוד	secret
16DXntec15nXnSDXp9eo15HXmded	נמלים קרבים	combat sea ports
16bXkdeQ15nXldeq	צבאיות	military related
16bXkdeQ15k=	צבאי	military related
15TXldeT16LXldeq	הודעות	messages
15nXl9eZ15PXlCAg157XmdeV15fXk9eq	יחידה מיוחדת	special forces unit
15jXmdeh15nXnQ==	טיסים	pilots
15HXmdeY15fXldeg15nXnQ==	ביטחונים	Defense and security related
15DXkdeY15fXlA==	אבטחה	security
157XqdeqJyfXpA==	משת"פ	collaborator (a person who cooperates with the enemy)
157Xqdeo15Mg15TXpNeg15nXnQ==	משרד הפנים	ministry of internal affairs
157XoNeU16jXldeq	מנהרות	tunnels
157XoNeU16jXlA==	מנהרה	tunnel
157Xlicn15zXmA==	מזל"ט	drone
157XldeT16LXmdef	מודעין	intelligence
157XldeT15nXoteZ158=	מודיעין	intelligence
157Xldeh15Mg	מוסד	Mossad

Infrastructure

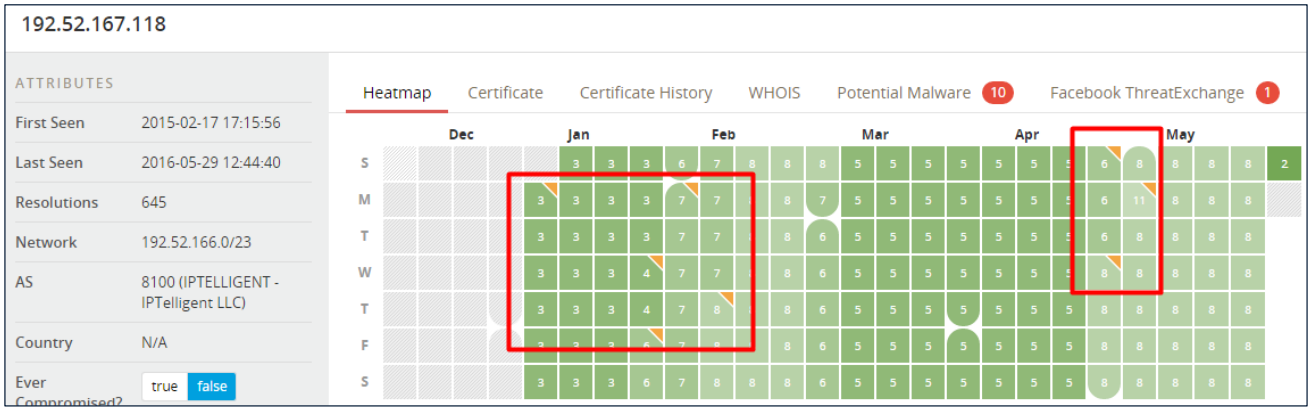
As in previous cases, the attackers still serve copied content on IPs, domains and hosts they control. For example, one of the command and control servers, mafy.2waky[.]com, serves content copied from a legitimate unrelated website - radaronline.com. The copied content is probably there just to confuse suspecting targets and security researchers.



In other cases, the visitor was redirected via HTTP 301 response to a legitimate unrelated website - www.onlinepcsupport.co.uk.

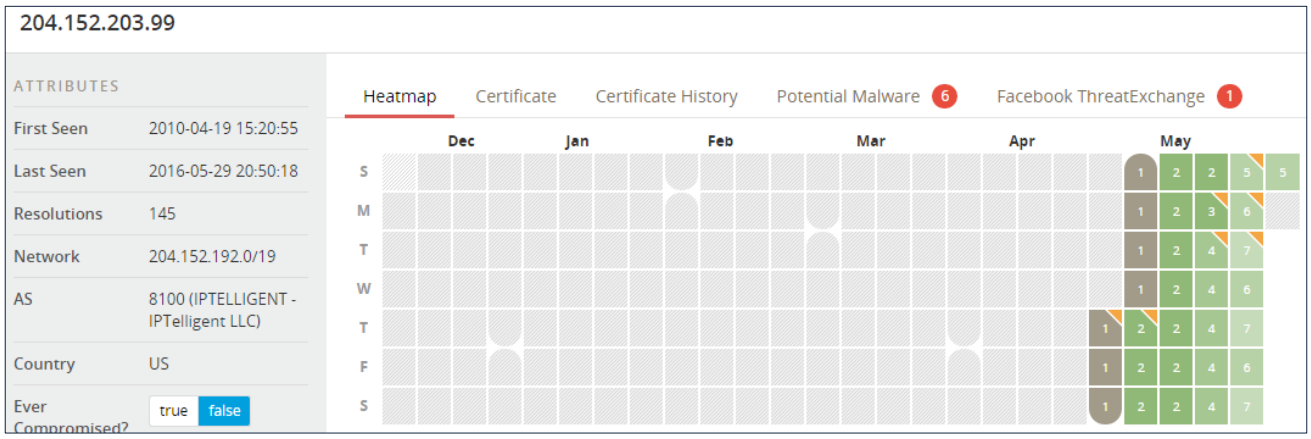
Key C2 and delivery servers

The attackers have been using IP address 192.52.167.118 since the beginning of January. In the Heat map below, we can see that new hosts/domains (marked by orange triangle) have pointed to it during January-February and again in May.



Source: https://www.passivetotal.org/passive/192.52.167.118

IP address 204.152.203.99 is newer and has been in use since May:



Source: https://www.passivetotal.org/passive/204.152.203.99

Below are the active IPs used for command and control or for delivery:

IP	ASN and Hosting provider
204.152.203.99	United States Los Angeles Graeme Tee, QuadraNet
192.161.48.59	United States Los Angeles Graeme Tee, QuadraNet
192.52.167.118	United States Burns Crowncloud Us Llc, Crowncloud US LLC
185.82.202.207	Netherlands Amsterdam Host Sailor Ltd.
173.254.236.130	United States Los Angeles Graeme Tee, QuadraNet, Inc
168.235.86.156	United States Macon Ramnode Llc
167.160.36.101	United States Lewes Gwy It Pty Ltd, Web2Objects LLC
107.191.47.42	United States Tampa Vultr Holdings Llc, Choopa, LLC
84.200.68.163	Germany Freinsheim Ip Projects, IP-Projects GmbH & Co. KG
72.11.148.147	United States Los Angeles QuadraNet Inc
23.229.3.70	Turkey Istanbul Turkrdns.com, B2 Net Solutions Inc

Further indicators are provided in Appendix A.

Threat Actor and Attribution

The DustySky campaign has been going on for over a year, with more than 120 command and control hostnames, and dozens of known unique malware samples. However, it has not been technologically advanced, and the infrastructure and attacks have not been operated professionally.

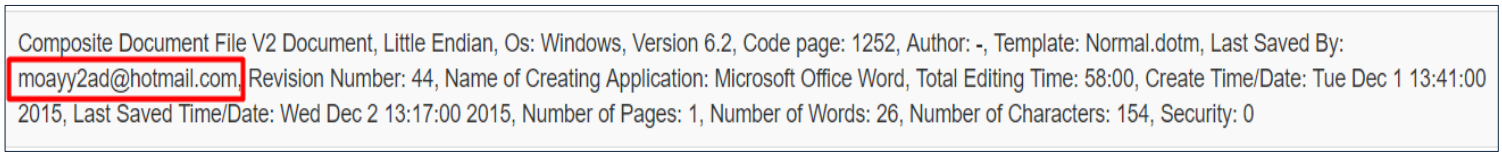
Open directories were often left on delivery servers. Traces were left on infected systems and abused email accounts. Malware delivery was often predictable, contained spelling mistakes or even irrelevant lure documents, and were easy to identify. Most importantly, the attacker forgot to cover his trails, enabling us to learn his identity.

Threat actor

In the beginning of December 2015, three samples were submitted to online malware detection and analysis platforms malwr.com and Virus Total. The samples were Word documents with a macro version of DustySky. They were submitted on the same date they were last saved.

The person who last saved the documents (after weaponizing them with the malicious macro) forgot to clear the file metadata. Thus, the "Last Saved By" properties of the documents contained his username: **moayy2ad@hotmail.com**

The images below display this username in the samples metadata:



Invoice details.doc (b1071ab4c3ef255c6ec95628744cfd3d), uploaded on 3 December 2015[4]
and Invoice-Complete.doc (77d6e2068bb3367b1a46472b56063f10) uploaded on 2 December 2015[5]

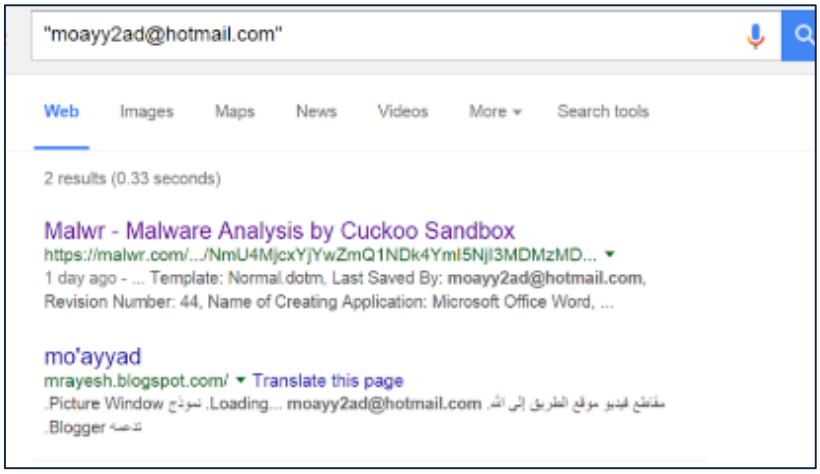
[4] https://malwr.com/analysis/Yjc4YjVjYmNjYzVjNGE2MzhkMTc1OWJjMjdjNjExNWU/
[5] https://malwr.com/analysis/NmU4MjcxYjYwZmQ1NDk4YmI5NjI3MDMzMDM2N2E1ZTY/

ExifTool file metadata	
SharedDoc	No
Author	-
CodePage	Windows Latin 1 (Western European)
LinksUpToDate	No
LastModifiedBy	moayy2ad@hotmail.com
HeadingPairs	Title, 1
Template	Normal.dotm
CharCountWithSpaces	5752
CreateDate	2015:12:01 13:41:00
CompObjUserType	Microsoft Word 97-2003 Document
ModifyDate	2015:12:03 10:24:00

Google-Privacy.doc (9c60fadece6ea770e2c1814ac4b3ae74) uploaded to VirusTotal on 3 December 2015[6]

Who is moayy2ad@hotmail.com

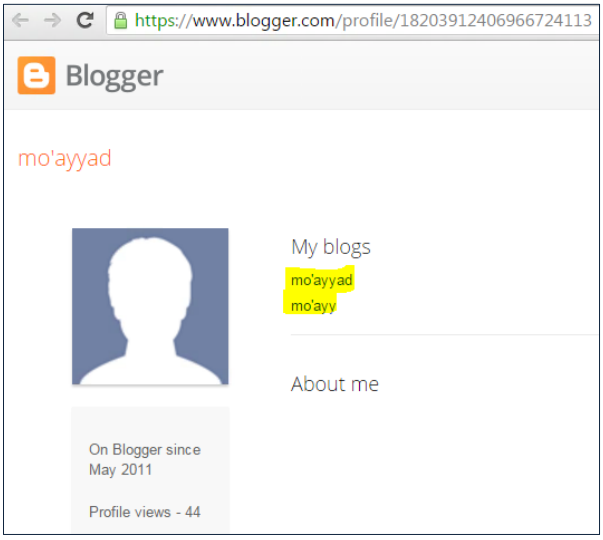
The unique username *moayy2ad* enabled us to find plenty of information on the attacker. Googling for moayy2ad@hotmail.com led the following blog[7], which has been removed in the months after we published the first report:



[6] https://www.virustotal.com/en/file/f96f07288039ebabb8d837043f06f8f1445ed4484023353e1111a40ac4f25fd8/analysis/

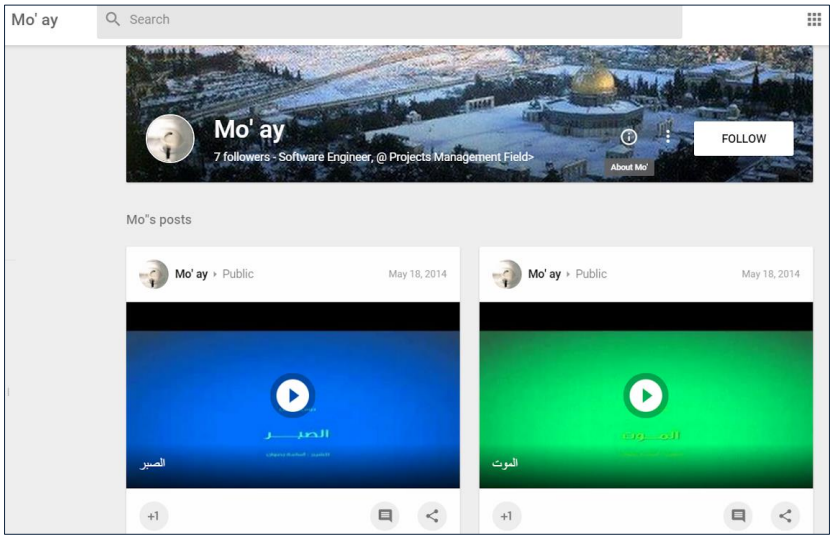
[7] mrayesh.blogspot[.]com

The blog was created by *mo'ayyad* on Blogger, who is also using the name *mo'ayy*. This profile has been made private following our publication.

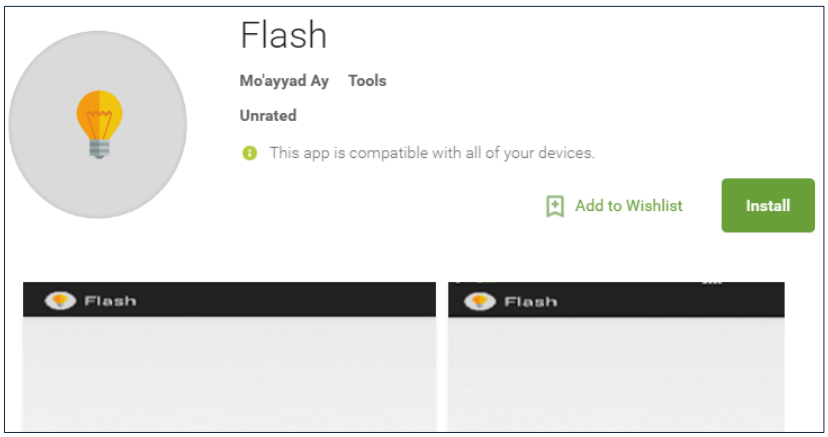


Searching for the same username in Gmail (**moayy2ad@gmail**.com) yielded further results. A Google+ profile[8] with a similar nickname – *Mo'ay* - was connected to this address. The profile has also been disabled in the months after we published the first report.

[8] https://plus.google.com/u/1/115033746922297164649



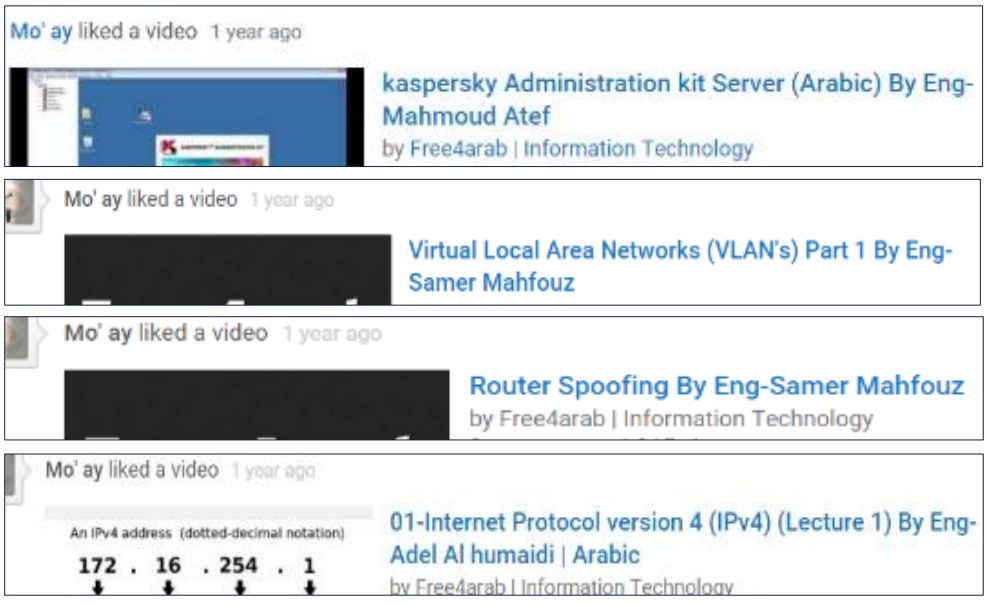
The owner of the Gmail account has developed a flashlight app[9]. In the app's page we learn that he uses the name *Mo'ayyad Ay* and that he is from Gaza"

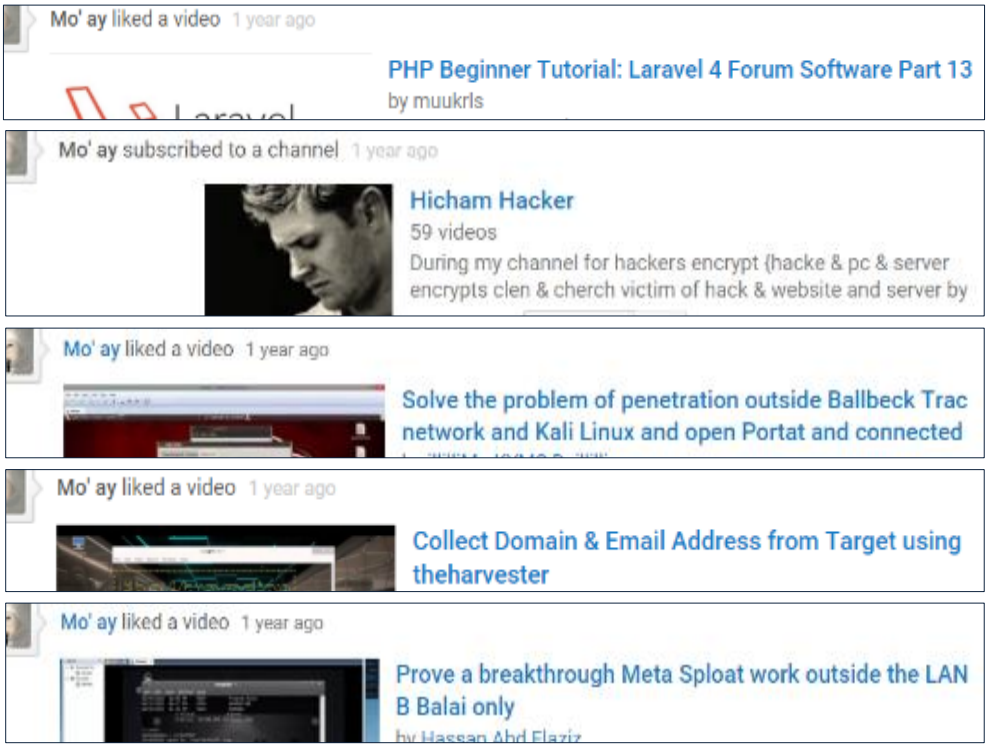


In the YouTube channel[10] linked to moayy2ad@gmail.com (which, like the other accounts, has been made private later), the individual has uploaded anti-Israeli propaganda videos:

[9] https://play.google.com/store/apps/details?id=org.moayyad.aye.flash.app&hl=en
[10] https://www.youtube.com/user/1quds/feed

According to the videos he watched it seems that he was learning development and hacking skills over the past few years:

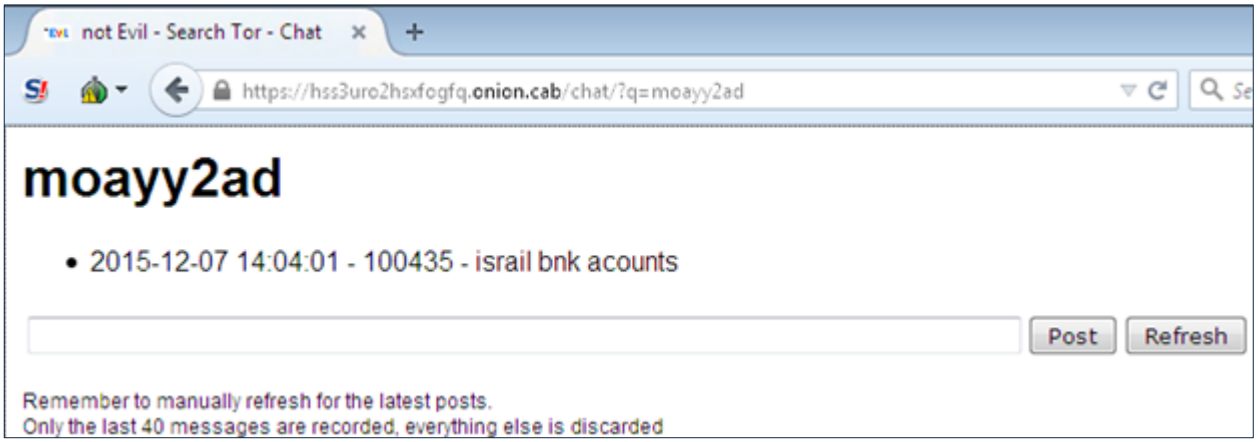




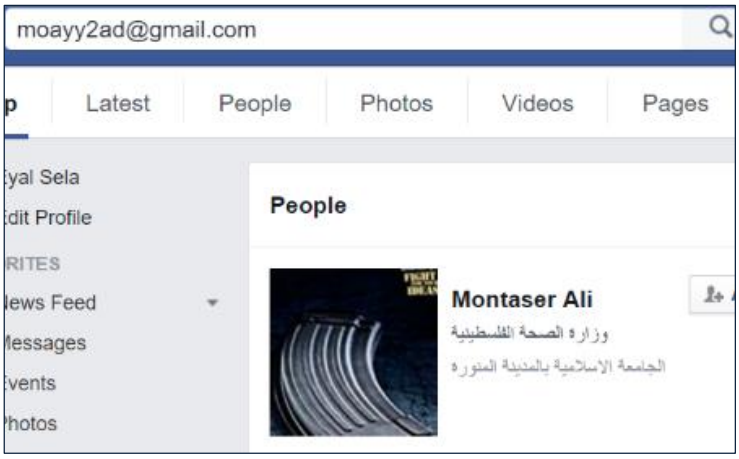
Similarly, we found his Twitter account[11] (also disabled) full name *Moayyad Ayesh* and Facebook account[12]

[11] https://twitter.com/MoayyadAyesh
[12] https://www.facebook.com/profile.php?id=100012034095150

We also found this cached chat in Tor based chat service in which moayy2ad is talking about “israil bnk acounts" (we do not have the rest of the conversation).



The Gmail address is connected to a Facebook account, probably of a fake identity - **Montaser Ali** (https://www.facebook[.]com/montaser.ali.338).



The profile says that the actor resides in Nablus, and that he is a member of a group called “Rebellion – West-Bank”[13].

Contacting ClearSky

In the first DustySky report, we mentioned we know the identity of the attacker, but have decided not to reveal it. Consequently, the attacker contacted us, trying to learn what we know about him.

By Email

Eleven days after we publicly published “Operation DustySky”, we received the following email

From: **IDF Cyber Team** <idf.cyber@gmail.com>
Date: Mon, Jan 18, 2016 at 3:09 AM
Subject: Operation DustySky.
To: info@clearskysec.com

Hi,
Please send any private information for the Operation Dusty Sky.

"we have decided not to disclose this individual's name in the public report".

Thanks

Israel Defense Forces.

[13] https://www.facebook.com/%D8%AA%D9%85%D8%B1%D8%AF-%D8%A7%D9%84%D8%B6%D9%81%D8%A9-%D8%A7%D9%84%D8%BA%D8%B1%D8%A8%D9%8A%D8%A9-542062199177072/

We immediately recognized the email as a fake – coming from an unofficial address - idf.cyber@gmail.com – and written in English.

The email, allegedly sent by the "Israeli Defense Force cyber team", asked for undisclosed information we had about the culprit behind DustySky (the email referred to a statement in the first report in which we wrote that "we have decided not to disclose this individual's name in the public report").

By phone

Few days later, we were contacted again, this time by phone. The caller pretended to be an official in one of the effected countries mentioned in the report. Similarly, he asked for further information about the identity of the attacker. We asked the caller to send his request via email. Corroborating the provided contact information, we learned that this was also a fake.

In both cases, we did not send any information to the attackers. However, we used the new leads to deepen the investigation.

Below is the email we received:

From: [redacted]
Date: Sat, Jan 23, 2016 at 4:20 PM
Subject: Operation DustySky
To: "info@clearskysec.com" <info@clearskysec.com>

Dear Mr. [redacted]

as per our phone call, i'd really like to thank you for your great report regarding the mentioned above subject

i'm interested to know more about the Social media account linked to this attack and other reports

Best Regards,

[redacted]

Appendix A – Indicators

Type	indicator	comments
AV detection	Win.Trojan.DustySky	
AV detection	Trojan.Dustky	
AV detection	Trojan.MSIL.Musik	
domain	education-support.space	
domain	falcondefender.com	
domain	support-update.ml	
domain	such.market	
hostname	support.mafy-koren.online	
hostname	mafy.2waky.com	
hostname	smail.otzo.com	delivery
hostname	ad.education-support.space	
hostname	info.education-support.space	
hostname	support.servecounterstrike.com	
hostname	reme.otzo.com	
hostname	supports.esmtp.biz	
hostname	news.cloudns.cc	
hostname	speed.ns01.biz	
hostname	space.support-reg.space	
hostname	mo.mefound.com	
hostname	support.read-books.org	
hostname	supports.3utilities.com	
IP	84.200.68.163	
IP	23.229.3.70	
IP	204.152.203.99	
IP	192.52.167.118	
IP	168.235.86.156	email source address
IP	167.160.36.101	
sender	"Free Movies" <Movie@mafy-koren.online>	
sender	"IDF Survey Research Center.." <info@mafy-koren.online>	
sender	avynorton@gmail.com	
md5	59bab785127418972dda9da5571b73fd	
md5	07dae7dada9ec3fa22507dfa5921c993	
md5	4bd6a959cce13d1f5b5511a428e88c9c	
md5	2ba0e52b885cabfbcd88866ab4072f54	
md5	1d922e183418ac087933c526f7bd06c1	
md5	3ce39f8afce9463c6d90c00ce72edb86	
md5	77fd78042407a7318dba388da00700cc	

md5	a5b3fb5119fad72ac321d8d6416b6b92	
md5	30b843343590518e7b62c5f6db394bc2	
md5	2a654ecb26664013d8e2369fe9c0b565	
md5	b11b7b7b5bd80779dd885628d65e02e5	Folder.exe
md5	cc24cd17fa93fce7ea1128edeb9ee40b	Drops b11b7b7b5bd80779dd885628d65e02e5
md5	5e906ccb3b67131e4771ca72609c0648	
md5	ad5531b085ef005ee12319e88fb8f674	
md5	2f5397ad6205ab4463e6e3be9aba4efe	drops ad5531b085ef005ee12319e88fb8f674
md5	0ae4345213cad388dbe38e2acda1a489	Updata.exe
md5	28a5e9b2ef5cfd2edb7f31d3da9a5a15	
md5	8655af063090ef192a7f1e0c05c7883f	
md5	6e66ed5d8c7d4ca9c2e96f2cc045eb94	
md5	d01848a20e0f5c4a7a7243bb98a7b26c	
md5	923844dfc3d5b21f288df9beaa958baf	
md5	639d768d575c45372ea707ed89423f36	
md5	b4ab538f592082373e9ab96373561713	cleaned.exe
md5	b85c17f92629fec41502b44cf86ba859	1.exe
md5	6f08808d0be510698563d3b0443fe5a4	New.exe
md5	b8c6c8eeb9a18b1d4632bc8191db5517	Folder.exe
md5	ddff0a7643f4ff2fe777e768e7bae004	log file.exe
md5	2395c798ca8628e735ac2d8d274cd230	
md5	bc6baf7a1d420d226a7a157b412a51d9	
md5	8ba38899a6446366724d98761dd10d46	
md5	d538e50df25e30f3c4252ce523507d23	
md5	a50da199db97abb2dfd6fd62b5a00f02	
md5	2a1884bdab940ea66b28599245e79fa9	
md5	2f30034885045bae4a201bf6b3913b54	
md5	23c3f3e93ea2ffe704abb602d04588c0	
md5	b8c6c8eeb9a18b1d4632bc8191db5517	
md5	e5500274853f77be6ffba610dac2cae4	
md5	ffa1bdc105013e1cbb00483b412b98b8	
md5	0264076c190af6e1176e1abff47d1ae8	
md5	02ef03bd5e6dbf9c03e8504c9e797abd	
pdb	Name D:\IL\Working Tools\2016-04-23 NeD Ver 9 Ran Il - 192.52.167.118\NeD Download and execute Version 1 - Doc\bin\Release\Obfuscated\News.pdb	
url	http://bit[.]ly/1YRoIPX	
url	http://smail.otzo[.]com/W/Gfsdfsdfsrydkfpsdmfpsadsdfsdfsdfsdfdfsp.php	
url	http://smail.otzo[.]com/y/analysis--hezbollah.rar	
url	https://drive.google[.]com/uc?export=download&id=0B7XzN8DNbJKiQlFNRHdVTmpCd0U	
url	https://drive.google[.]com/uc?export=download&id=0BxaUrWGCqlWLMTQzMVFNOENIUFk	

url	https://drive.google[.]com/uc?export=download&id=0B7n4BFDObRocdm1uS2J4SWVUNWc	
url	http://drive.google[.]com/uc?export=download&id=0ByjYVMTYJB0saHlTalJ6ZWlWWGM	
	support.mafy-koren[.]online/reg-update	
url	support.mafy-koren[.]online/UFeed.php	
filename	Israel's Cellebrite linked to FBI's iPhone hack attempt.exe	
filename	Report-Photos.rar	
filename	Analysis--Hezbollah.rar	
filename	Report.rar	
filename	דוח אחריות תאגידית וקיימות - אגד.exe	
filename	Logs.exe	
filename	Analysis and estimates (Dahlan) heads of state next Palestine.exe	
filename	Report-Palestinian-President.rar	
filename	Folder.lnk	in \Startup\
filename	Folder.exe	
filename	גלעד שליט פציעה בפיגוע טרור.exe	
filename	Intelligence Report Israelג€™s strategic position has improved.exe	
filename	Updata.lnk	in \Startup\
filename	تحليل وتقديرات (محمد دحلان) رئيس دولة فلسطين القادم.exe	
filename	Office 2016.exe	
filename	edikvlxhprg.lnk	in \Startup\
filename	edikvlxhprg.exe	in \Startup\
filename	plugin.exe	
filename	Fared-Ismael.rar	
filename	القصة الحقيقية لموت القيادي فريد إسماعيل في سجن العقرب .exe	
filename	cleaned.exe	
filename	cbkp1vpsv1y.exe	
filename	jnpqmri1aus.exe	
filename	gzch5y2cyne.exe	
filename	retn0gzbksd.lnk	in \Startup\
filename	pktkvkgj4bl.lnk	in \Startup\
filename	Intelligence agencies succeeding in penetrating Hezbollah.exe	
filename	בוחרות בכל חודש את מהלך התוכן המוצלח ביותר. והחודש, מהלך התוכן של דורקס סקר הסקס הגדול.exe	
filename	Intelligence Report Israel's strategic position has improved.exe	
filename	تحليل وتقديرات (محمد دحلان) رئيس دولة فلسطين القادم.exe	
x509 fingerprint	cadd3141e42227c0a30aa58ab3ca9fa91384f4c7	SSL communication with C2
x509 fingerprint	9fb60ae410cf8e7739535aaa9771edd781f766d3	SSL communication with C2
x509 fingerprint	0387ac82a3eabd3ffc48a73cc440e02ce3018bc8	SSL communication with C2
x509 fingerprint	9fb60ae410cf8e7739535aaa9771edd781f766d3	SSL communication with C2