Gaza cybergang, where’s your IR team?

securelist.com/gaza-cybergang-wheres-your-ir-team/72283/

APT reports

APT reports

28 Sep 2015

minute read

Authors

-  Mohamad Amin Hasbini

- 

Ghareeb Saad

Summary information:

Gaza cybergang is a politically motivated Arabic cybercriminal group operating in the MENA (Middle East North Africa) region, targeting mainly **Egypt, United Arab Emirates and Yemen**. The group has been operating since 2012 and became particularly active in Q2 2015.

One interesting new fact about Gaza cybergang activities is that they are actively sending malware files to **IT (Information Technology)** and **IR (Incident Response)** staff; this is also obvious from the file names they are sending to victims, which reflect the IT functions or IR tools used in cyber attack investigations.

IT people are known for having more access and permissions inside their organizations than other employees, mainly because they need to manage and operate the infrastructure. This is why getting access to their devices could be worth a lot more than for a normal user.

IR people are also known for having access to sensitive data related to ongoing cyber investigations in their organizations, in addition to special access and permissions enabling them to hunt for malicious or suspicious activities on the network…

The main infection modules used by this group are pretty common RATs: XtremeRAT and PoisonIvy

Some more interesting facts about Gaza cybergang:

- Attackers take an interest in government entities, especially embassies, where security measures and IT operations might not be well established and reliable
- Use of special file names, content and domain names (e.g. gov.uae.kim), has helped the group perform better social engineering to infect targets
- Increasing interest in targeting IT and IR people, which is clear from most of the recent malware file names used

Other operation names:

- DownExecute
- MoleRATs

Kaspersky Lab products and services successfully detect and block attacks by Gaza team.

Political file names targeting Arabic countries

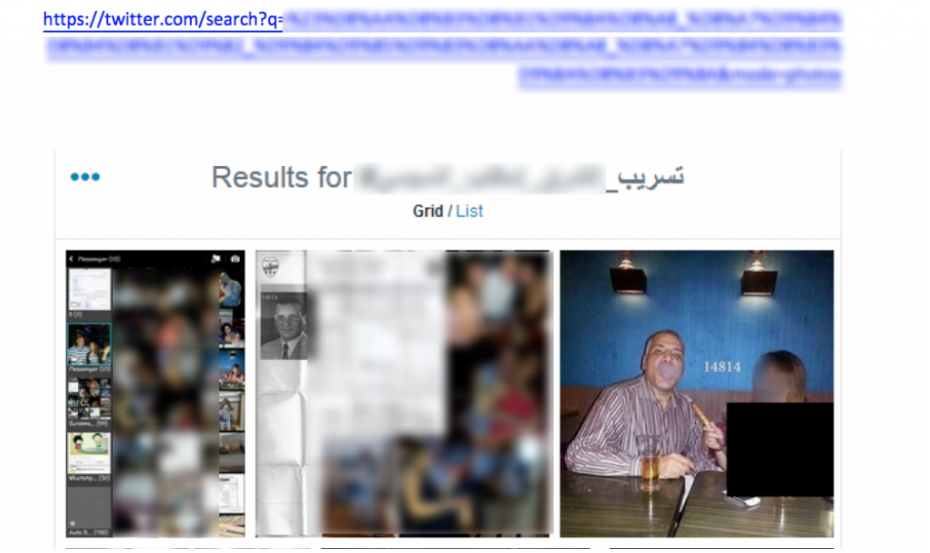
File name: بوادر خلاف جديد بين الامارات والسعودية.exe

Translation: Indications of disagreement between Saudi Arabia and UAE.exe

Filename: “Wikileaks documents on Sheikh ******* *** *****.exe”

File name: صور فاضحـــــة جدا لبعض العسكريين والقضاة والمستشاريين المصريين**.exe**

Translation: Scandalous pictures of Egyptian militants, judges and consultants



File name: Majed-Abaas.zip -> الرئيس الفلسطيني محمود عباس يشتم ماجد فرج.**exe**

Translation: President Mahmoud Abbas cursing Majed Faraj.exe

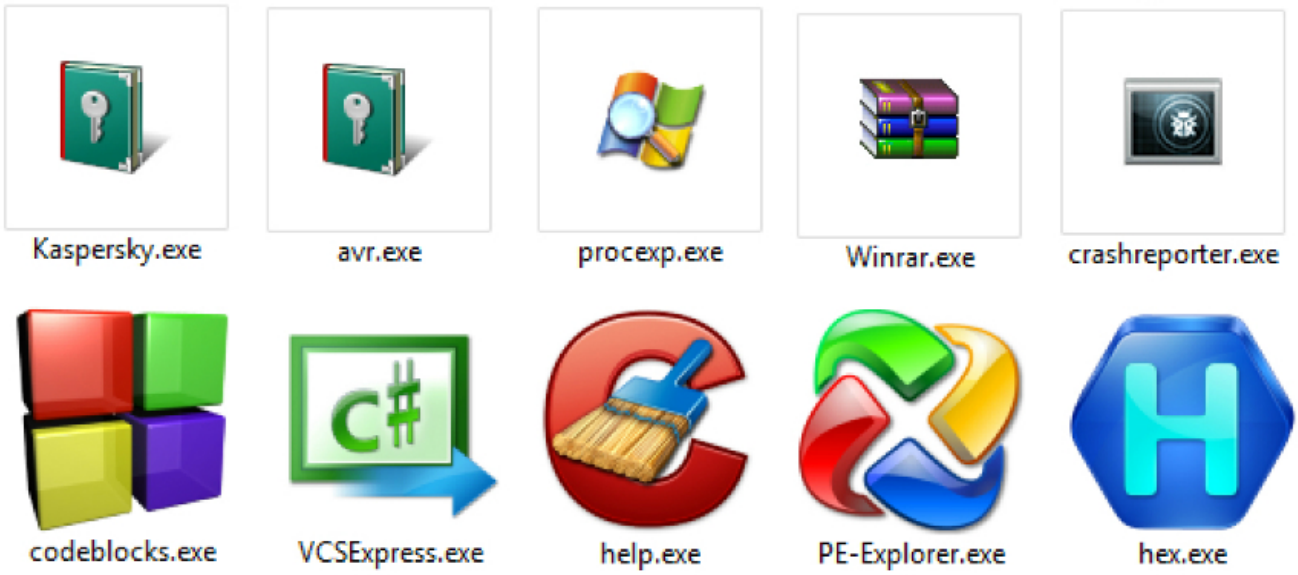
File name: "مكالمة مسربة بين القائد العام للقوات المسلحة المصرية صدقي صبحي.**exe"**

Translation: Leaked conversation with the Egyptian leader of military forces Sodqi Sobhi.exe

File name: tasreb.rar

IT and IR Malware File Names

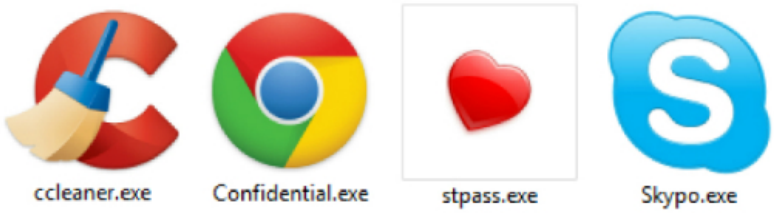
VCSExpress.exe	Hex.exe
Microsoft Log.exe	IMP.exe
Win.exe	Corss.exe
WinRAR.exe	AVR.exe
ccleaner.exe	codeblocks.exe
HelpPane.exe	Hex_Workshop_Hex_Editor-o.exe
Help.exe	Decoded.exe
vmplayer.exe	Decrypted.exe
procexp.exe	crashreporter.exe
RE.exe	WindowsUpdate.exe
PE.exe	AVP.exe
PE-Explorr.exe	Kaspersky.exe
PE-Explorr.exe	Kaspersky.exe
hworks32.exe	Kaspersky Password Manager.exe



Other malware file names

abc.exe
News.exe
Sky.exe
SkyC.exe
Skype.exe
Skypo.exe
وصية وصور الوالد أتمنى الدعاء له بالرحمة والمغفرة.exe
Secret_Report.exe

Military Police less military sexual offenses, drug offenses more.exe



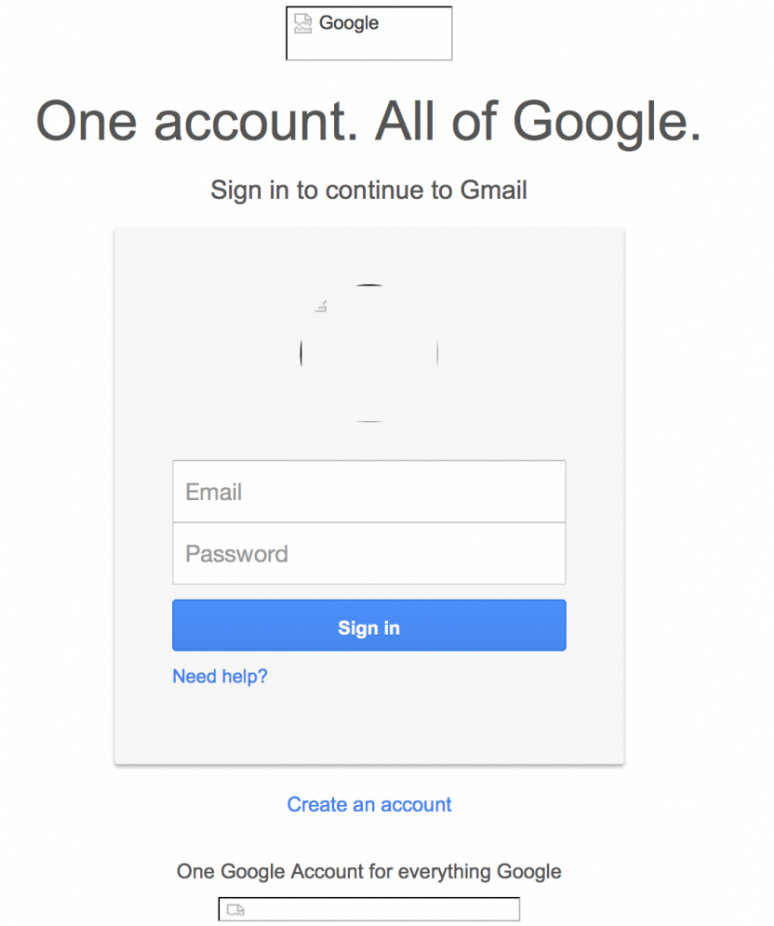
Phishing

http://google.com.*****/new/index.php?Email=FL1-08-2015@gmail.com

http://google.com.*****/new/g.htm?Email=sharq-2014-12-31@gmail.com

http://google.com.*****/new/index.php?Email=2014-12-04@gmail.com

http://googlecom*****/new/index.php?Email=yemen-22-01-2015@hotmail.com



IP addresses and domain names used in the attacks

Domains

uae.kim	natco1.no-ip.net
gov.uae.kim	natco3.no-ip.net
up.uae.kim	natco5.no-ip.net
uptime.uae.kim	nazer.zapto.org
google.com.r3irv2ykn0qnd7vr7sqv7kg2qho3ab5tngl5avxi5iimz1jxw9pa9.uae.kim	noredirecto.redirectme.net
ajaxo.zapto.org	nrehcnthrtfmyi.strangled.net
backjadwer.bounceme.net	ns2.negociosdesucesso.info
backop.mooo.com	offeline.webhop.net
bandao.publicvm.com	orango.redirectme.net
bypasstesting.servehalflife.com	redirectlnk.redirectme.net
cbbnews.tk	removalmalware.servecounterstrike.com
cccam.serveblog.net	mailchat.zapto.org
chromeupdt.tk	mp4.servemp3.com

cnaci8gyolttkgmguzog.ignorelist.com	rgoyfuadvkebxhjm.ddns.net
cyber18.no-ip.net	rotter2.publicvm.com
deapka.sytes.net	rotter2.sytes.net
depka.sytes.net	safar.selfip.com
dnsfor.dnsfor.me	safara.sytes.net
download.likescandy.com	safari.linkpc.net
downloadlog.linkpc.net	spreng.vizvaz.com
downloadmyhost.zapto.org	store-legal.biz
downloadskype.cf	su.noip.us
duntat.zapto.org	tango.zapto.org
fastbingcom.sytes.net	test.cable-modem.org
fatihah.zapto.org	test.ns01.info
gaonsmom.redirectme.net	testcom.strangled.net
goodday.zapto.org	thenewupdate.chickenkiller.com
googlecombq6xx.ddns.net	thenewupdatee.redirectme.net
gq4bp1baxfiblzqk.mrbasic.com	tvnew.otzo.com
haartezenglish.redirectme.net	update.ciscofreak.com
haartezenglish.strangled.net	updatee.hopto.org
help2014.linkpc.net	updatee.serveblog.net
httpo.sytes.net	updato.ns01.info
internetdownloadr.publicvm.com	use.mooo.com
justded.justdied.com	wallanews.publicvm.com
kaliob.selfip.org	wallanews.sytes.net
kaswer12.strangled.net	Wcf6f0nqvjtUP4uN.mooo.com
kolabdown.sytes.net	webfile.myq-see.com
ksm5sksm5sksm5s.zzux.com	webfile.myq-see.com
lastmoon.mooo.com	ynet.ignorelist.com
lilian.redirectme.net	ynet.sytes.net
live.isasecret.com	

IP addresses

192.52.166.115	131.72.136.28
109.200.23.207	131.72.136.124
66.155.23.36	172.227.95.162
162.220.246.117	162.220.246.117

192.253.246.169	192.99.111.228
192.52.167.125	185.33.168.150
198.105.117.37	185.45.193.4
198.105.122.96	131.72.136.11
131.72.136.171	84.200.17.147

Malware Hashes

302565aec2cd47bb6b62fa398144e0ad	f94385be79ed56ef77c961aa6d9eafbf
f6e8e1b239b66632fd77ac5edef7598d	a347d25ed2ee07cbfe4baaabc6ff768b
8921bf7c4ff825cb89099ddaa22c8cfd	674dec356cd9d8f24ef0f2ec73aaec88
3bb319214d83dfb8dc1f3c944fb06e3b	e20b5b300424fb1ea3c07a31f1279bde
826ab586b412d174b6abb78faa1f3737	42fca7968f6de3904225445312e4e985
5e255a512dd38ffc86a2a4f95c62c13f	3dcb43a83a53a965b40de316c1593bca
058368ede8f3b487768e1beb0070a4b8	e540076f48d7069bacb6d607f2d389d9
62b1e795a10bcd4412483a176df6bc77	699067ce203ab9893943905e5b76f106
39758da17265a07f2370cd04057ea749	11a00d29d583b66bedd8dfe728144850
f54c8a235c5cce30884f07b4a8351ebf	d5b63862b8328fb45c3dabdcdf070d0d
9ea2f8acddcd5ac32cfb45d5708b1e1e	bc42a09888de8b311f2e9ab0fc966c8c
948d32f3f12b8c7e47a6102ab968f705	c48cba5e50a58dcec3c57c5f7cc3332d
868781bcb4a4dcb1ed493cd353c9e9ab	658f47b30d545498e3895c5aa333ecb1
3c73f34e9119de7789f2c2b9d0ed0440	2b473f1f7c2b2b97f928c1fc497c0650
9dccb01facfbbb69429ef0faf4bc1bda	46cf06848e4d97fb3caa47c17cdd7a9e
4e8cbe3f2cf11d35827194fd016dbd7b	6eb17961e6b06f2472e4518589f66ab9
b4c8ff21441e99f8199b3a8d7e0a61b9	b0f49c2c29d3966125dd322a504799c6
4d0cbb45b47eb95a9d00aba9b0f7daad	ca78b173218ad8be863c7e00fec61f2f
18259503e5dfdf9f5c3fc98cdfac6b78	23108c347282ff101a2104bcf54204a8
0b074367862e1b0ae461900c8f8b81b6	76f9443edc9b71b2f2494cff6d4a26a8
89f2213a9a839af098e664aaa671111b	

Phishing Hashes

1d18df7ac9184fea0afe26981e57c6a7
57ab5f60198d311226cdc246598729ea

Additional references

http://cyber-peace.org/wp-content/uploads/2014/01/Cyberattack_against_Israeli_and_Palestinian_targets.pdf
https://www.fireeye.com/blog/threat-research/2013/08/operation-molerats-middle-east-cyber-attacks-using-poison-ivy.html
https://github.com/kbandla/APTnotes/blob/master/2012/Cyberattack_against_Israeli_and_Palestinian_targets.pdf
http://pwc.blogs.com/cyber_security_updates/2015/04/attacks-against-israeli-palestinian-interests.html

- APT
- Arabic Malware
- Cybercrime
- Fake AV
- Targeted attacks
- Thematic phishing

Authors

-  Mohamad Amin Hasbini
- Expert Ghareeb Saad

Gaza cybergang, where’s your IR team?

Your email address will not be published. Required fields are marked *

Table of Contents

GReAT webinars

Subscribe to our weekly e-mails

The hottest research right in your inbox

Reports

APT trends report Q1 2022

This is our latest summary of advanced persistent threat (APT) activity, focusing on events that we observed during Q1 2022.

Lazarus Trojanized DeFi app for delivering malware

We recently discovered a Trojanized DeFi application that was compiled in November 2021. This application contains a legitimate program called DeFi Wallet that saves and manages a cryptocurrency wallet, but also implants a full-featured backdoor.

MoonBounce: the dark side of UEFI firmware

At the end of 2021, we inspected UEFI firmware that was tampered with to embed a malicious code we dub MoonBounce. In this report we describe how the MoonBounce implant works and how it is connected to APT41.

The BlueNoroff cryptocurrency hunt is still on

It appears that BlueNoroff shifted focus from hitting banks and SWIFT-connected servers to solely cryptocurrency businesses as the main source of the group's illegal income.