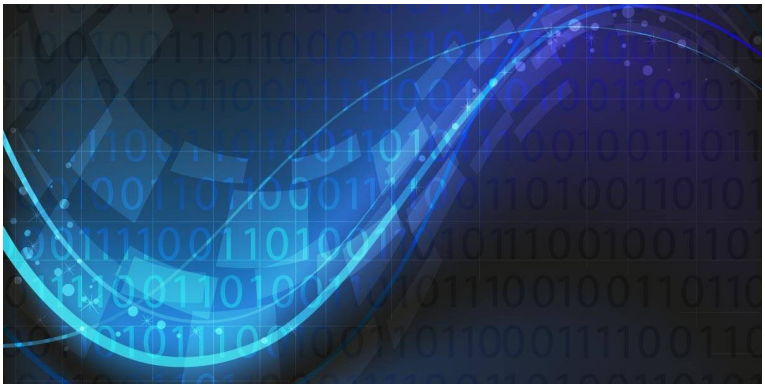
Gaza cybergang, where's your IR team?

APT REPORTS 28 SEP 2015 2 minute read



// AUTHORS

MOHAMAD AMIN HASBINI Expert 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

Table of Contents

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

FROM THE SAME AUTHORS

5G technology predictions 2020

5G security and privacy for smart cities

Gaza Cybergang – updated activity in 2017:

Operation Ghoul: targeted attacks on industrial and engineering organizations

The Desert Falcons targeted attacks

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
gov.uae.kim
up.uae.kim
uptime.uae.kim
google.com.r3irv2ykn0qnd7vr7sqv7kg2qho3ab5tngl5avxi5iimz1jxw9pa9
ajaxo.zapto.org
backjadwer.bounceme.net
backop.mooo.com
bandao.publicvm.com

bypasstesting.servehalflife.com

cbbnews.tk

cccam.serveblog.net

chromeupdt.tk

cnaci8gyolttkgmguzog.ignorelist.com

cyber18.no-ip.net

deapka.sytes.net

depka.sytes.net

dnsfor.dnsfor.me

download.likescandy.com

downloadlog.linkpc.net

downloadmyhost.zapto.org

downloadskype.cf

duntat.zapto.org

fastbingcom.sytes.net

fatihah.zapto.org

gaonsmom.redirectme.net

goodday.zapto.org

googlecombq6xx.ddns.net

gq4bp1baxfiblzqk.mrbasic.com

haartezenglish.redirectme.net

haartezenglish.strangled.net

help2014.linkpc.net

httpo.sytes.net

internetdownloadr.publicvm.com

justded.justdied.com
kaliob.selfip.org
kaswer12.strangled.net
kolabdown.sytes.net
ksm5sksm5sksm5s.zzux.com
lastmoon.mooo.com
lilian.redirectme.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	f94385be79ed56ef77c961aa
f6e8e1b239b66632fd77ac5edef7598d	a347d25ed2ee07cbfe4baaa

IN THE SAME CATEGORY

HrServ – Previously unknown web shell used in APT attack

Modern Asian APT groups' tactics, techniques and procedures (TTPs)

A cascade of compromise: unveiling Lazarus' new campaign

8921bf7c4ff825cb89099ddaa22c8cfd	674dec356cd9d8f24ef0f2e
3bb319214d83dfb8dc1f3c944fb06e3b	e20b5b300424fb1ea3c07a3
826ab586b412d174b6abb78faa1f3737	42fca7968f6de3904225445
5e255a512dd38ffc86a2a4f95c62c13f	3dcb43a83a53a965b40de3
058368ede8f3b487768e1beb0070a4b8	e540076f48d7069bacb6d6(
62b1e795a10bcd4412483a176df6bc77	699067ce203ab9893943905
39758da17265a07f2370cd04057ea749	11a00d29d583b66bedd8dfe
f54c8a235c5cce30884f07b4a8351ebf	d5b63862b8328fb45c3dab(
9ea2f8acddcd5ac32cfb45d5708b1e1e	bc42a09888de8b311f2e9ab(
948d32f3f12b8c7e47a6102ab968f705	c48cba5e50a58dcec3c57c
868781bcb4a4dcb1ed493cd353c9e9ab	658f47b30d545498e3895c5
3c73f34e9119de7789f2c2b9d0ed0440	2b473f1f7c2b2b97f928c1fc4
9dccb01facfbbb69429ef0faf4bc1bda	46cf06848e4d97fb3caa47c
4e8cbe3f2cf11d35827194fd016dbd7b	6eb17961e6b06f2472e45185
b4c8ff21441e99f8199b3a8d7e0a61b9	b0f49c2c29d3966125dd322
4d0cbb45b47eb95a9d00aba9b0f7daad	ca78b173218ad8be863c7e0(
18259503e5dfdf9f5c3fc98cdfac6b78	23108c347282ff101a2104bcf
0b074367862e1b0ae461900c8f8b81b6	76f9443edc9b71b2f2494cff
89f2213a9a839af098e664aaa671111b	

Phishing Hashes

1d18df7ac9184fea0afe26981e57c6a7
57ab5f60198d311226cdc246598729ea

Additional references

How to catch a wild triangle

StripedFly: Perennially flying under the radar

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

Gaza cybergang, where's your IR team?

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

Type your comment here

Name * Email *

Comment

AYMAN HASHEM
Posted on September 28, 2015. 4:33 pm

good

Reply

// LATEST POSTS

MALWARE REPORTS

Android malware, Android malware and more Android malware

GREAT

SOC, TI AND IR POSTS

A patched Windows attack surface is still exploitable

ELSAYED ELREFAEI, ASHRAF REFAAT, KASPERSKY GERT

MALWARE DESCRIPTIONS

What's in your notepad? Infected text editors target Chinese users

SERGEY PUZAN

RESEARCH

Top 10 web application vulnerabilities in 2021–2023

OXANA ANDREEVA, KASPERSKY SECURITY SERVICES

// LATEST WEBINARS

TECHNOLOGIES AND SERVICES

11 DEC 2023, 4:00PM 60 MIN

The Future of AI in cybersecurity: what to expect in 2024

VLADIMIR DASHCHENKO, VICTOR SERGEEV, VLADISLAV TUSHKANOV, DENNIS KIPKER

THREAT INTELLIGENCE AND IR

30 NOV 2023, 4:00PM 70 MIN

Responding to a data breach: a step-by-step guide

ANNA PAVLOVSKAYA

CYBERTHREAT TALKS

14 NOV 2023, 4:00PM 60 MIN

2024 Advanced persistent threat predictions

IGOR KUZNETSOV, DAVID EMM, MARC RIVERO, DAN DEMETER, SHERIF MAGDY

CYBERTHREAT TALKS

09 NOV 2023, 5:00PM 60 MIN

Overview of modern car compromise techniques and methods of protection

ALEXANDER KOZLOV, SERGEY ANUFRIENKO

// REPORTS

HrServ – Previously unknown web shell used in APT attack

In this report Kaspersky researchers provide an analysis of the previously unknown HrServ web shell, which exhibits both APT and crimeware features and has likely been active since 2021.

Modern Asian APT groups' tactics, techniques and procedures (TTPs)

Asian APT groups target various organizations from a multitude of regions and industries. We created this report to provide the cybersecurity community with the best-prepared intelligence data to effectively counteract Asian APT groups.

A cascade of compromise: unveiling Lazarus' new campaign

We unveil a Lazarus campaign exploiting security company products and examine its intricate connections with other campaigns

How to catch a wild triangle

How Kaspersky researchers obtained all stages of the Operation Triangulation campaign targeting iPhones and iPads, including zero-day exploits, validators, TriangleDB implant and additional modules.

THREATS

APT (Targeted attacks)
Secure environment (IoT)
Mobile threats
Financial threats
Spam and phishing
Industrial threats
Web threats
Vulnerabilities and exploits

CATEGORIES

APT reports
Malware descriptions
Security Bulletin
Malware reports
Spam and phishing reports
Security technologies
Research
Publications

OTHER SECTIONS

Archive
All tags
Webinars
APT Logbook
Statistics
Encyclopedia
Threats descriptions
KSB 2023