

# Mobile Cyberespionage Campaign 'Bouncing Golf' Affects Middle East

Appendix

## Indicators of Compromise (IoCs)

SHA-256	Package Name	Label	Version	App Internal Name
00e82927b20d2db5bdfc6bff77f6841d0e59af80adce3f86f90277669159e5f3	com.iran.sunni.time	نسيم حق	1.1	Azaan N-2
01cebc3a542b08c7f818540d826c7717b7354552c20ff897e9cddbdeaaabe962f	com.whatsapp.w4b	WhatsApp Business	2.18.122	00024-USER17-WAB-01
0593167d6e7f63c8401c4393f999de2b889078ddaa3713a0d0277b953b7b41c9	com.andromo.dev791306.app895682	موطني	1	00064-USER12-MAWTANI_AHAM MED
0801d88fa8a3cf0569e2b388ec74ed3ff71e1edaf173e99c78edf86cf3aba6f6	com.andromo.dev785707.app891043	مارب برس	1	00055-USER12-MAREBPRESS-12000
09649ca5ea3efb312b6fde47fb3e0e260f762caec2c81f663fb5489eb630ae15	com.geektoro.assramaja7l7ayat	النجاح فى الحياة	1	00038-USER17-NAJAHINHIAH-00
0ad4930bbbf510a4b71379a5415a22dc15f2210c872494e128b875fa114d5918	com.dianxinos.optimizer.duplay	DU Speed Booster	2.4.6	00058-USER17-DU.Speed.Booster-17000
1024c9bc5bb77c274aa28502f280470a25d27d99657a4cc9b15e194a677fb5cc	com.andromo.dev791306.app895677	موطني	1	00065-USER12-MAWTANI_KAMAL
10e7ef263a62b3bde0047bc5870f1791781d32f399dc0e15f1fac8076d52d9f7	com.andromo.dev789740.app892709	صحيفة البيان	1	00060-USER12-AL-BIANEMARAT.1.0-12000
146fd6f27df73bcdf9a245ed429047c8d279fd635cf8db63f3039a9b47fd5363	com.devhd.feedly	feedly	38.0.0	00026-USER12-feedly_38
18b9f74dba23030272ae87a4612813317fe3c8ab8bef8ca643c7fd8b0c2ce7dd	com.andromo.dev785707.app890246	عكاظ	1	00054-USER12-AKAZMAIN.1.0-12000
1abd66b4b608735e760537103849b64aaa56a118b80bdc02c2d23ef20087ee57	com.andromo.dev789740.app892698	صحيفة الاتحاد	1	00061-USER13-ETHADEMARAT-13000
208d3af2924585fae89228705bb5e1a0695ab3ad9ccedc4fa5f5234c38b36bba	org.telegram.plus	Plus	4.9.1.5	00031-USER17-Plus_Tele.4.9.1.2
22df35ef54e8381ab7be67dfd4f781c8b9eef3a80499e5261d0b9f2d4e7b8e91	com.zico.shalt_2	شيلات ابو حنظلة السوداني 2018	1.4	00063-USER12-SHILAT_ABO_HANTHALAH
24c3c9c8d4174da861ca852af2de65d72c8f63e5d8f70c88e10c170256743da1	zozo.android.riddle	لغز وكلمة	4.1	00043-USER12-PUZZLEANDWORD-12000
2a1d539d08826b36f3e1dcad174c9693401ab94dd22cf315fb2af9b37d3e9d0f	com.maher4web.hisn	حصن المسلم	4	000154-USER12-Hisn Al Muslim Azkar_v4.0

2d76d929c6e9a2e45caaca7706ff3a0cfefbcac4a8c711d44d586eb4bc121eed	com.andromo.dev800523.app906043	يوميات الجيش	1	00071-USER13-SITENEWS
30287e48b23b6098d7cebafb3b14c6a2167de214c46553ca1a995a83fe934ef5	com.ag4apps.drawfuture	ارسم مستقبلك بنفسك	1	00059-USER17-MOSTAQBEL_RA SEM-17000
306db737da630c68957a3f9c200f7cc3f5d16d2aa2e1719cc5445dd126a27249	org.thoughtcrime.securesms	Signal	4.6.1	00036-USER13-Signal
319c499932badf0b51fa4401d6cdc97b3a677299ebb2c80e53078ae1b5ca236f	com.dianxinos.optimizer.duplay	DU Speed Booster	2.4.6	193-DSB-51201
34d750ec2c208982d37d8fb3fea30d41fa0c681464f5f477fc20ed3c75499bd4	com.okaz.okaz_yemen	Okaz-Yemen	1	00161-USER12-okaz
36be3e5f866a2b80ebe8e2f16b2d52a6109b27e703302ea763f923a160bbebd6	org.telegram.messenger	Telegram	3.2.5	00019-USER13-TELEGRAM2.3.5-130000
371f80e2cddb0a37280b03b006fd7756b3e07b2e264f7f5b56a277b99ccae406a	com.andromo.dev798323.app903534	اخر اخبار اليمن	1	00068-USER12-APPSAHEL-01
3787bfd64c6092407a9e46d6a444ea1ea7380ac87a5576f8222a6db8c502ad03	com.andromo.dev783746.app883584	صفحتي	1	00049-USER12-Mareb-1.0-12000
3984c25dba94309a89f911ecd65df2e182e6430f3b0aec1efa11b6a9e58932b4	ding.com.android.messages	DingDing	3.4.0	364-ding-71225
3dd8ddce3d5d8ba028227b2aba2edd7646be8d8cae4db8e7a40015c31c8c39b5	com.andromo.dev798323.app923901	اخبار الوطن	1	00078-USER12-WAFA-SA-0.2.1
403f8e773d57c5b9247c089a11a96edd9260bc3a616a5a3cf70f17fe8fd37fe4	org.telegram.messenger	Telegram	3.2.5	00037-USER12-TELEGRAM2.3.5-12000
428c851322095fb1c737966a843c325575779b0d2c1ef3581bf517ea8a2a5ea	org.telegram.plus	Plus	3.18.0.3	00034-USER13-plus-messenger-3-18-0-3
4590333a279c91e95a2f05426cde11321727d6d474644775413efb99c494516a	com.andromo.dev798323.app934321	موطني	1	00081-USER12-WMOTANI.1.0.3
4b3a60464fa67162faf533d458acf4095c204a67f44ecb4e2ad70b989aca7861	com.andromo.dev786391.app887683	الصدائة	1	00053-USER13-FRINDSHIP.1.0-13000
4c230a591f1ed15f447105ae5b351f3cb93e355cb2ccf158e52f0e1f1ddb7121	com.andromo.dev798838.app904084	اخر اخبار اليمن	1	00069-USER12-APPMAREBL-01
4cf86f63aef17ae5ce6e8f7f705e773a08cb89bd81a7137597bd255736ac01f6	org.telegram.plus	Plus	4.9.1.5	00053-USER12-TELEGRAM-PLUSE_4.9-12000

4da793d6391c122e3c7b1a3581a7aff2c322f02d3297840a4c72beda3c3ec2e1	org.telegram.messenger	Telegram	3.2.5	00014-USER17-TELEGRAM2.3-17000
55123ed4982fa135dbeda49969ab68444125143e36930fe1612d367f2fa615fc	kik.android	Kik	8.7.0.1643	00016-USER12-KIK8.7-12000
5671ec93761abf62036560b418b069a8a8065cff1725389a2a21623555576ef	com.ag4apps.drawfuture	ارسم مستقبلك بنفسك	1	00041-USER12-MOSTAQBEL_RA SEM-12000
59215d0ee868df7561b4bbeccb152a378119d452d1435cb1531f635b98b5ced	com.duolingo	Duolingo	3.104.2	00074-USER12-Duolingo_3.104.2
5be6ccd78074458159e286bb2cb9024728581ebdb071f3d1d4fc88ac48d21e15	org.telegram.messenger	Telegram	4.8.10	00033-USER13-Telegram.4.8.10
609142d17ff473adab484915f1ee799f69685da77421a51421369c42fbac077e	com.jrzheng.supervpnfree	SuperVPN	2.1.0	000151-USER12-SuperVPN Free_v2.1.0_
6095c5cef13067ebb8d8a521bc633a626839ba8b25af70113ad42cc638a9744a	com.skyray.fekky_hekam	100 حكمة تتفكك في حياتك	1	00017-USER17-HEKAM1.0-17000
61c4ee1b0ad5a0457a04c78eb0516986e8b5846f4dc4109520bfc4950cd3b0ac	ir.ahadis.bokhari	مختصر صحيح بخارى 2	2	Sahih
62d74126525e5323c07d5f103dc2cdd1f36b53b36f371032360570f3c6cebb1e	kik.android	Kik	8.7.0.1643	00018-USER13-KIK8.7-13000
6774af8daf50c8f8be205285ed69b3f9169ec6150774ef5f6469706cbc113b49f	com.aymsou.wasaya.rasol	تجميع لأروع وصايا الرسول	1	00042-USER12-WASAYA-RASWOL-12000
6791d66557ae34ab78d7376cabb4ac2166d20f02ea93202ebe1720b262248799	com.andromo.dev818085.app925502	نبأ الإخبارية	1	00079-USER17-NABA-V1
73a5509351bb789af6a997c955d70f06455c77485c0a9349ac62b24ebae9b6e9	com.pdfreder.pdfreder	الصدافة	1	00168-USER13-Frinds
75a231d6026a4d0155710c76055b065dfa083d127ad001a8abd1fdf7e39cc8f6	com.andromo.dev798323.app950103	ارسم مستقبلك بنفسك	1	00163-USER12-AI-Shaif-FUTURE
76332cd87db67c15f536a911a4a58d5bf4e1130655dcfa00f2a6273ad315626d	com.dianxinos.dxbs	DU Battery Saver	3.7.1	188-DBS-51201
7c7551acf443070ad728f8e197b46bda020085325c248c26fb6696b434a9cafb	com.andromo.dev801338.app906994	اخر اخبار اليمن	1	00072-USER12-ALHODIDA_NEWS
821379d30653b6b6e9dd9010bd3d0282503284a7dac77af896d63bd6ce785e7	org.telegram.messenger	Telegram	3.2.5	00015-USER12-TELEGRAM2.3-12000

8388d12d8dd3375c6fa2341d9de5f7d15a0fc37306496cdfa9cfe266da66318f	com.ag4apps.drawfuture	ارسم مستقبلك بنفسك	1	0001-USER14-mostgbalrasme.1.0-14000
860ac70a8374c1851fe1d968686db7638bf3d337805ff3c64293c41fecd0522	com.andromo.dev798323.app950110	الوطن	1	00164-USER12-AI-Shaif-Waten
88256d9f3e047a04560834ed7a9cc19a4216122f8210272342ce1b4449364e4a	com.andromo.dev819383.app941989	الصداقه والمحبة والاخاء	1	00160-USER13-app_941989_819383
8835a5a686382786f4067d0eefaff585eef9714bee13cd853f9504b9985017ca	org.telegram.plus	Plus	4.9.1.2	00031-USER17-Plus_4.9.1.2
953c2ce6cc1f013cb9de527a28f8068f4a5c6dabab07701b139dfa661904a8db	com.dianxinos.dxls	DU Battery Saver	3.7.1	192-DBS-51201
969ccee7cff3cc789767108d0e72a5a082d7a3ea562ef0a262c47cebdac171ae	com.andromo.dev783746.app883596	صفحتي	1	00048-USER12-Okaz-1.0-12000
9ba57ad172212923e65b77bbc8714f9584b061342985ae9289f2df9101399159	com.mzdhr.quicktodo	Quick ToDos	2.1	000149-USER12-Quick ToDos_v2
9d70b9d3cc1b6ee692cce6bd96a78a953a15344e9ba8c788ff114e3c169958cd	com.akhbar.yemen.news	أخبار اليمن	1.0.1	00039-USER12-YEMENNEWS-12000
a064c89eda2de4404fd33989eb7dc46534b8dc551ebaca5de40537715b3a95a7	com.apps.medamine.hobfizaman	HobFiZaman	1	00075-USER17-HobFiZaman_1.0
a080bb6b44cb4b776c001c5381e600cde4f4c2aaa3bf75087a204f901e803bd9	com.application.service.googleoogleservice	Google Service	4.1.455.4896	240-GooPho-61112
a54e93c8c9efeadb63f888746c4bbef53bdba2ed1339ed7468c6241555240895	com.mobeg.content.zoelhega	عشر ذى الحجة	1.0.1	00022-USER12-BOOK-ASHER-ALHAJEH01
aa66752539f420bbf49701fd2912605fcbf6693cf55b12972b8f7fe2ed1809af	kik.android	Kik	8.7.0.1643	00013-USER17-KIK8.7-17000
ab757f7fd4b8b082ce406f14559c795097b31989bb9a0e3968ee99e53d972666	ae.albayan	البيان	2.3.23	00040-USER12-UAE-Bian_2.3.23-12000
acfa1ac90a2145987d27c30aa7d31a2077513ce507350919d6e521806fde1d44	org.telegram.plus	Plus	3.18.0.3	00032-USER17-plus-messenger-3-18-0-3
b5a12b5ab55528582faac103591ca72fe79c24dbf2453e8196715aa94f909a3a	com.wahid.muqbel	فتاوى العلامة مقبل الوادعي	1	56-USER12-fatawa_muqbelwa dai02
b5dab5c1a72909b5fb14e8855d1bf4e6981aac98e226f63cc676f1de3a32959a	com.pdfreder.pdfreder	موطني الحبيب	1	00165-USER12Mawtani Sherouq

c55427800e3f6b96453eeaabbac8e58d2bdfea9e4324d969f0c99a436adc7eaf	com.andromo.dev798323.app922825	اخر الاخبار	1	00077-USER12-BUSHRA_SA-0.1
c59b2edc4c07ab7f93861dde7575e27a6607f9ebf287c4b1f8bee93424e78b7b	com.juphoon.justalk	JusTalk	7.2.42	00052-USER20-JusTalk_7.2.42-20000
c62422b607084024b3544481a465a3c3a7444ef6ab37b4ed7868167aede0c072	com.andromo.dev780997.app879040	Make_your_own_future	1	00046-USER12-DRAW-YOUR-FUTURE-1.0-12000
c6be8f1890d1ba512bdf257770d64e38c08b378f0c92acc6b1d3bfbcb6e45de3	org.telegram.messenger	Telegram	5.1.0	00070-USER13-TELEGRAM-5.1.0
c6f35bf8a95717b3dadcd1dcace90d81adfee278c59d643fa92ef67c506147210	com.okaz.okaz_yemen	الوطن الاخبارية	1	00175-USER12-Oatan.1.0.1
cdd32b243bc5e6f172cd4c8340ca9de2d320942afaf9a582a41b4d4bc60d89ed	com.najeeb.watnanh	شيلات سعودية وطنية	8	00062-USER12-SHILAT_WATAN
cf4422494ba059b07407f14d438d148ac3bdbcc06047731d82d878ab3a6f9930	com.wahid.muqbel	فتاوى العلامة مقبل الوادعي	1	00020-USER12-FatawaMoqbel-12000
d0515f2ff687e5ca32bc1c0f2fb84878caea7f56378cec94f79b70fb366a8b30	org.thoughtcrime.securesms	Signal	4.6.1	00028-USER12-Signal
d605e7061266468a71a8f3abaa0c3bf1a323a5caef45755835cffe835002a047	com.std.hosting.remindme	تكرني	2.0.5	000150-USER12-Remind Me_v2
d6945f30a2a27959c47f79df0436e685075ac34d6337f21ba07f7eae317cb29b	com.okaz.okaz_yemen	الجيش الوطني	1	00167-USER13-jesh_watani
dbeea2747e0818bea0b7cbe03923b41a7bbb3a92cb70b4e069f3b323ac418a75	ibadat.chahr.ramadan.new	عبادات شهر رمضان	1.2	00174-USER17-abadtRamazn
dd688ab9c7f7048cbfc7fe3f4816b84298d6c1b51b58167074b1a63aa8290a67	com.pdfreder.pdfreder	ارسم مستقبلك بنفسك	1	00166-USER12-Afaf AI - Aqili
e3648fa09b8136222f254588ebe4df0857e2689721d6b88b70c0554e6634230a	com.okaz.okaz_yemen	نبا الاخبارية	1	00169-USER17-NabaNewa.0.1
e6686671c0b97e9c1ec69fefeef22e8519bd4df7a5129ca46bac2eda7f06bb09	com.aymsou.wasaya.rasol	تجميع لأروع وصايا الرسول	1	0004-USER14-WasayaRaswol.1.0-14000
e9fbb42061c63bb3f93c00297c081924d725df6283b4eaf650011c760ed961dd	com.andromo.dev780997.app879040	Make_your_own_future	1	00057-USER17-DRAW-YOUR-FUTURE-1.0
ea2b03abc503f3c87e625ce07871c899e55f68930e60070dcea00368dfd2aedf	com.mohamed.management	ادارة الوقت د.ابراهيم الفقي	2.1	000155-USER12-Management_time_abraham_alfqih

ec9930cd52c6a6e1fe07ecb1cc7e90757ae31071358cf9f5ff28cdf11fbee3ed	com.andromo.dev819383.app926986	الساحل الغربي	1	00080-USER13-SAHELNEWS.1.0.2
eda3f3b2ee8e186be56b613f6fe0f2a58467081fca10651a01743741ac91fddb	com.imo.android.imoim	imo	9.8.00000003051	00035-USER12-IMO-9.8-12000
ee3bd9e9a18b4d044c43e1e4e452593b39e6dde55f6691b4ff46dfbb2db96224	com.andromo.dev805111.app911811	صحيفة الاتحاد	1	00073-USER13-ATHAD_NEWS
ee812debadc056b8cad6dd637ced3c296e2fc60db007e643d27a1f0a888fae	com.dianxinos.optimizer.duplay	DU Speed Booster	2.4.6	00044-USER12-DU.Speed.Booster
f41aa669f77a3aeebcb6cfa06bcc6a75523dfbed4288be3674f5d1ae114377d7	com.andromo.dev793597.app897553	موطني	1	00065-USER12-MAWTANI_RABA B-1200
f5eee8a332c7088afd51dbaa792daa49a19fe423ea0b543622378e47d99b8b32	com.abdulapp.sana	السنة الجديدة 2019	1.4	00066-USER12-message_happyn ewyear
f7424fd05e3ea2823c7498f79302032deecaa51334eac0444216566c81913a12	com.geektoro.assramaja7l7ayat	النجاح في الحياة	1	00038-USER17-NAJAHINHIAH-17000
fdd0df40778b203af4f744e9a41e267ead67be13de9c33539aa351e1def0762c	com.okaz.okaz_yemen	Okaz-Yemen	1	00162-USER12-okaz-02
fea34718aa1f0c292bf1669717e1281122b94317e3f673cf0a814bf5ddcae52e	org.telegram.messenger	Telegram	5.3.1	00076-USER17-TELEGRAM-5-3-1

## C&C IP Addresses and Domains Related to Bouncing Golf

- 185[.]183[.]99[.]116
- 190[.]2[.]130[.]53
- 194[.]187[.]249[.]134
- 212[.]8[.]248[.]179
- 54[.]38[.]51[.]159
- 82[.]211[.]31[.]181
- 84[.]234[.]96[.]167
- androidsmedia[.]com
- androidssystem[.]com
- mediadownload[.]space
- mediamobilereg[.]com
- secandroid[.]com
- sharpion[.]org
- shileyfetwell[.]com



## TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threats techniques. We continually work to anticipate new threats and deliver thought-provoking research.

[www.trendmicro.com](http://www.trendmicro.com)



©2019 by Trend Micro, Incorporated. All rights reserved. Trend Micro and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.