Indicators of Compromise (IoCs)
for the Attack Group APT-C-23

Symantec

SHA256

90236bcdd71611256642ea4e76cf8fdccb2af8fd37da1a4bc7f0844d0fc6be7d
e431aa55ad197aa027ab51c22c2afa01454fb7cb9a4e4d4cec8f5a9c2ad735e8
823f66c8d27294e54d0fdc91629bd8487af9b9ee034d06cc8dacc6ca5ac32926
b09f657063d254e4ce73d35a9da1aee9e1662ad8d8458a19f08cc32de53035e1
541583f20ec349ea3ce921c2a54194559bbd90bbd0b954f1f8562ae88bbffc6e
96ab58d8ffb99f4b3b87afb48ceed3be01e9f8de333be0b91efd39fc7a99eeb3
6307bee86c07f0d24a4708a2265aebf44126389da4649e83d38d3d76a4a18a57
3b22e84e7edb9b7277672a1341f8a347094797beb8e8ee80e09fdb9a9230fc76
5dd46064501235c0d02ae9155d6d5f0b526703a8244da5d8299f590b427a3c2e
c5f576339f5389518d9cf7ed8efe2727b5685ccdd55f5f862411b17138b44c73
9db025bb854b4d9cd9d9bb29a626501e89c6f4704953b852f3b7c4fae5389f13
5c4733a5dabeda2dcd8602b12a86460bca6ed33ac1197045536ed8e7afbe9244
79af9a040c633914b911be45ef4301979e2c54bd65f47391432bf9cdecb797a9
453437ea43a67536b5724bb0e6bf576fb510ff1d6ea5307cfa7ec8ee46c0dc8f
885fcf646972f40a775388f29a51fbb9232a9e000a2cc53eeb3125ba6e696020
d209352b6814660ccfc95c5ff7f780d395cdca18d793db8bd3004fd8ba9b6922
dd43001cfdbfe1cdade2f8a969580b4e134dbb66d0517518afc773f22e9f97e0
46f5df76f723e67a42ef49cce8d84a0f9af869b170f730df01d29138b36d3f24
d756387e7becead2ff2d035d94282741f5d6c04129cb0a1dceefd71eefabcb35
9d567bf55bce66ae9419f90c59570f51df54cb5fc1d6d360e3e13c42aa74c2bb
8d5f5be15c93f57a6349dd9ce1637c5a8913523745f502f37cd1a0691db30693
ac8ecb7190b7c3c7a2f45ddc26040dae5e048b8c6c657c78007412e7ee56d50e
99dbcf0200ec3d046c92f32e4494590c18667f163f97cc9f5a2fb8f4a5c83da5
46c5bec32c558b9c4aa0775759568a730211baf8807e797b4bd21707dd40dee4
66bd32489206fdbb8b5d15f589e999db1b8e67c9102244735ac154123f2e9495
dac29a5e7f19b51c9cff249b8e930d15913a92907f96bcc20f7de8ef3d0185f3
a9ba4e59e1d4bc3757d276c9c083e0a1c13843ff32c0cb45b29b60cb6586e022
e14f99608a8d16cdd17786d218e173b44bbf9d5e30387d949a72604ec29cc4c6
c417cacb2fc6160e3754e552f6ac9006350a1fa016c987a885d3e4e1c33c84b6
b806eaa463d6da64caf3e04f6344ce113a2b12c5107e37cd0ddaa382a7932a36
7d7d554e84deae2c46bc2a9bf747207303deb50dc5996b018336035ac7a80059
cbf9a0737e27fafafaff5c73825bb96907a976b230bf18843badd7b10d475eb2
1f015490141eca78f98a0dc32089ed7430819e763e909007ab97dc76fcf9803a
f047aefc87d9d5bdcb507db857b5e16cb7e7177452480ac18d8e34069f289174
28f2686345338587255 00b1e05d85174d29f58f51d9b2af3f75daabdc9a4f32b
e2cb9140c47492e7931e0b6629caf5c03cbc4e7a28c7976a28e3158b5d1c67fb
0fe9facdb01a4836036eaccaafd386721095b18c890d676e8d387647153fa927
8da31d3102524d6a2906d1ffa1118edf39cf54d72456937bfbae5546e09a3c32
6befd9dac5286f72516bba531371dc7769d9efecf56c8a44ce0c8de164662c6b
313ae27ec66e533f7224d99c1a0c254272818d031456359d3dc85f02f21fd992
7dea246c7f97f0526f622e03ee6a56cf11681338d30b2a0a4d30c00821ccfa72

Indicators of Compromise (IoCs)
for the Attack Group APT-C-23

Symantec

SHA256

1aa881100698621fab59ebe8caf0a7b422bee42137c3dcf0edd5e6608286e1da
566385bff532d1eb26b49363b8d91ed6881f860ffa4b5ddb2bb5fe068bb6c87e
59689c7112d94170e669fd692dfa807a064ecce2f1e505ddda7cd6874dbc351c
815f3fd9353ad54dbec0cc1f3cf86477f2f812f995385ac701759959c444a7f1
a841b71431e19df7e925d10a6e43a965fc68ccbb6523b447de82c516cfba93a8
ec1ed9b064ffbd237e1808d4e156d011b8b77402042b7a6fee92923b69ba65d4
4e681d242bebf64bbba3f0da91ad109dd14f26e97cd62f306e9fca1603a0009e
bea4915454933db54ddc1d41c9e5d06dc7c4abdf5ae4a768239b32733498e10f
1c0e3895f264ac51e185045aa2bf38102da5b340eb3c3c3f6aacb7476c294d62
14c846939641eb575f78fc8f1ecb2dc76979a5e08366e1809be24fad240f6ad6
ca8d892a616feaf240bd9e05a250db8ed4d56b7db6348bbaa415dec1e0c626f3
be809f5442aa5a60cbb07556ea25e7730078f1d44d5b0e7bb31b14193cfe9ba2
9cff78daf29290514b088272db4f0502c5f969905c6bebfdf5a022ddbb69b248
d17308fb06760de1b06d03448a01f3762f2712c1a66b50c8d5f4ac061d6deb27
b7007d2039abaf8b8b0db77241d400a8c4d3b48c6fece5d80dc69905d4d272c3
377716c6a2b73c94d3307e9f2ea1a5b3774fa42df452c0867e7384eb45422e4f
b6326e17ec8307edf63e731c635fbfa8469d9264cb414592e2d2a5c71093d809
28a9a97927e76c5c9228ef465f78feea51f0d47e6e0c1440f38f2bc1230ae437
58ddd057ec7f2420ce94cf3fc52794d0f62603ca7eaf8c5911f55b8b100ac493
8a7f8ab2bd774ce6861d1e86f52ad8ae2df2a2ac84e86a1f2e362b73c7f077f7
66d1d6f099a1aadd8d747a4b3cefeb72d835eaa55ec5392ff55fd6e892d90344
964be0420d65b6581d970a7b330f8c0b85fe735d1f7fbfc21dafbc3bf8b4db39
597d362a1206b0d69e3c69a0a2f1725589af239c56d5de781622d317602b1f11
ed6c375e86fb5670bb23fe060399bf2232099197a3e226f318d54cdf9b1b946a
6ab11df57111af5c4965d3d39a3e8fe710c3eb7a1ba013e74551c14f42c5bb67
80c6995426581878262 66a4aab84edc1fef5fde53281168806efb3e0e77e82b1
961ec09537004445b85ab79c0ff69fea08d619da97344a792b689223ca1d5b43
f11cdfdad004425780dfed26a604f9b1f0738598180f34204073e6dcb16fc4d0
1f18aac7c04725c934f6cfbbcdc1e170c80ca8bd51a722a462fa2fd2ef549923
56007b32b896991527fbc3fa806418ecd954518758ed04e4b03a4079b754061b
455c5bbcc9b90a2799d4a5477950bbcc102757a4216cbcbb749a6fe74de4bb15
76e0e770d2abbf7ea63b0221ef0b0f799f54792004f15a2a9e1e7844cf8b1965
3a6ce795b393cf05daa2fcb82eb7c0fee5b1b0b7cd268d6432aace0e8ca42e27
e59dfdb9da28e2d8016e40f09f1744b45379eebe02d3244a9dd7327b787923b8
7daa98b750217a72e6e1e33878e9ec737c871563d3bd98e20610926607d9a05d
6c53feb4b6cac4ac7c17227b076ff3248bfae37d21802646db7540d3748029bf
91b3eeb8ba6853cab5f2669267cf9bccdba389149cc8b2c32656af62bd016b04
5de5b948aeca6e0811f9625dec48601133913c24e419ce99f75596cb04503141
93da08ced346b9958e34bda4fe41062572253472c762a3a837e0dd368fffec8b
dfbd6e916ab1660f4fd87552fd392e43122e797ca8d66aa3123623cd70b78d0c
9d629d20fdb0d4650a3c1a308028c7c51d673770a988d78cccb4bb819ffc08a8
65495e63799a0e919937d83dee6f059a1cd2affe5411ba7d6fc454e36c0571e8

Indicators of Compromise (IoCs) for the Attack Group APT-C-23

SHA256

9a8bb68564c8cd38e47a91c816776a84d78dfe5bd35cd014400e87cb76ca9440
cf2d7545b1f5ec57142727f795e07e85b84cbfe9a8b9f75aa5219495c746d853
e7d7f110369a67dd1129c5fbd38daeadcc01c2ab3ced98e2a3135283678e1914
461e9c8fb2b0a049df3b5fccd9c453c65d30ee02699f715da09796a5bb236f7c
0537cdd971843545ce569415226dfabd1053a149a2586f163b58f7cb46e80ac5
16327e5fbb60bc8f57ba2bbfe02c0464ce0755312a10f566cd7123cf978160d3
2240c56c98c90acc0cbc58ba0ea6f7d78bb2f80d97f5c23e2a6e0ba5e2db4960
46976081c1bcec4daa9701fbe373010c0bcb17463359a91556f09339522b6a13
1995f315d0431141b25dd2962a2b517bc27d0ba694fddf982d970f512f784945
e0e1addc23a032b538a344498e862b808e767ce8bed9412dd8990d00b1d64b34
79947899241dde6bb6c3b82d8a0841928fa25333909907ddafeddcc987d37fb9
d6a7c537a3101c38d0bafdcde685ad97ebc15ecac6bfa6eacba80b933ae8a151
fe074e77cf64227b6f79d08cae573dd8d48e32e72abf8482a1a4d7a6e42b4f2d
56f13b40f115af5114445d6ea04e5c00b19302ec4425e1995e423f0cd4cc3cf0
14b739028e1e85a95cd2efc4019fdae9a49622afe07d8ef542634b1908baedee
51e2630f942578d81ed000aa8a7b5ff7e19608a53323092ba72bc3b686614e25
adcc3186e92f9ffe6277443b918cef997f2debbd84f7ccba974ab89bedfe90a3
76962d334b894349a512d8e533c8373b71389f1d20fd814cd8e7ecc89ed8530a
7e4a5c61a6d7718381884ac7675f3352821696415183 79ea921731cf08c95b49
4b5dafd98fdffe2736787281db233f8f1e904b05e70acbfa2358cb901269d039
1702b7038a1a1dc514054d3070939b4c1fabf3b51a0192d64dcd4f934c27b3ca
c38d2a739d9a4e7df51176c95abc43ba606928c5d88b3ebcd7202dbaa0499e35
86e453b251707eb2b73a3f547d7ed34af2b850fd9d319143c22778dd73066901
91cbeb6b02575423621e0a0871efca3b6d25004ce9c1700b97748e2d330b60fb
2ff47bb5ce6baacba85047c43afe1f3a7f034f1dd547c385394055afa4ba64bc
4ebb385b0bf460d8561c39af8b69144bfe8c7a4d8607b157784674de653b9a05
6bdf6f1d5a8a4c94589ab9f1d40db7e7710bae82f143209f058b6e0b8f25884d
6665a99e53b2d28497e4edba4c67b8e587b9291d524c737235c69379a00190ae
183ec1960e40b0831fbc47bbd87de530a1f92de02b1a60eb91771ef5d7dd016b
4842cff6fc7a7a413ceed132f735eee3121ffb03f98453dae966f900e341dd52
cc40a67b3844116c594fd192055d62498f9907d46cc84afd6bfaefa3b6b665a9
27d89d88db6fe1365e2c1ded2e8af805c353d741bfd45023e9f67e2cc8c4d28e
1a9d5717622111e73cd11617bf29b9e8e9c50a83b90c85dee909faad24684585
7752f5662d904a261eb57a948278d0804efef827c1bec6337e6b210a00635a27
ddfe29e690f8ecd08c6efd304ac89283967b63e9e0ea508d8b69ab4a5365f038
bdea751c2e106a4f83d8ba32b1f193a3aa65bf3aba4405e025887bb66cb7a0c3
371f13e4dacb0a740752a2352f09804bae99887b833c6989feb211702b3679cb
93a21428286602cfe02380a33411cb9d25004f627c685b4363e9ffb3baa5f201
dd21373738175567c92de2031e9efce761ba8d1fe6c6e04e69648e7528eed309
d16b235d931d4eecb38365af538be023bebdb547f8aadf69de4aadfabc65620a
8d184f24277ace3dd55811c3ed5b810eaa34a1c9bff0de2a15eb996134e9e241
1b3fddc07f524b22559a6c6688ff90fd0e7f035a5ac36237be5e28a10887e928

Indicators of Compromise (IoCs) for the Attack Group APT-C-23

Symantec

Domains

1jve.com	clarke-taylor.life	hcttmail.com	mail-presidency.com
aamir-khan.site	daario-naharis.info	help-live.club	margaery-tyrell.info
accaunts-googlc.com	dachfunny.club	help-sec.club	maria-bouchard.website
account-gocgle.com	dachfunny.us	heyapp.website	marklavi.com
account-googlc.com	dardash.club	hitmesanjjoy.pro	mary-crawley.com
accountforuser.website	dardash.fun	hoopoechat.com	masuka.club
accountforusers.website	dardash.info	hotimael.com	matthew-stevens.club
accounts-gocgle.com	dardash.live	hotmailme.website	mauricefischer.club
accounts-googlc.com	david-mclean.club	italk-chat.com	max-eleanor.info
accountusers.website	david-moris.website	italk-chat.info	max-mayfield.com
accuant-googlc.com	davina-claire.xyz	jack-wagner.website	maxlight.us
activedardash.club	davos-seaworth.info	james-charles.club	mediauploader.info
alain.ps	debra-morgan.com	jimmykudo.online	meet-me.chat
alisonparker.club	donna-paulsen.info	john-brown.website	meetme.cam
android-settings.info	easyshow.fun	jon-snow.pro	men-ana.fun
apkapps.pro	eleanor-guthrie.info	jorah-mormont.info	michael-keaton.info
apkapps.site	eleanorguthrie.site	joycebyers.club	miranda-barlow.website
appchecker.us	engin-altan.website	juana.fun	miwakosato.club
appuree.info	esofiezo.website	kaniel-outis.info	mofa-help.site
arthursaito.club	everyservices.space	karenwheeler.club	moneymotion.club
aryastark.info	exvsnomy.club	kate-austen.info	myboon.website
aslaug-sigurd.info	ezofiezo.website	katesacker.club	mygift.site
assets-acc.club	face-book-support.email	katie.party	mygift.website
bbc-learning.com	fasebcck.com	kik-com.com	namybotter.info
bellamy-bob.life	fasebock.info	kristy-milligan.website	namyyeatop.club
bestbitloly.website	fasebook.cam	lagertha-lothbrok.info	natemunson.com
billy-bones.info	fasebookvideo.com	leonard-kim.website	new.filetea.me
bitgames.world	fatehmedia.site	leslie-barnes.website	nightchat.fun
black-honey.club	firesky.site	lets-see.site	nightchat.live
bob-turco.website	flirtymania.fun	lexi-branson.website	nissour-beton.com
buymicrosft.com	freya.miranda-barlow.website	lincoln-blake.website	octavia-blake.world
camilleoconnell.website	geny-wise.com	lindamullins.info	olivia-hartman.info
caroline-nina.com	gmailservice.us	liz-keen.website	oriential.website
cassy-gray.club	graceygretchen.info	login-yohoo.com	ososezo.club
cecilia-dobrev.com	hareyupnow.club	lord-varys.info	ososezo.site
cecilia-gilbert.com	harper-monty.site	lyanna-stark.info	parrotchat.co
cerseilannister.info	harrykane.online	mail-accout.club	pmi-pna.com
chat-often.com	harvey-ross.info	mail-goog1e.com	pml-help.site
christopher.fun	hayleymarshal.com	mail-mofa-pna.com	pml-sac.info
claire-browne.info	hazel-grace.info	mail-pmi-pna.com	pmo-gov.info
clarke-griffin.info	hctmial.com	mail-police-sec.com	police-sec.club

Indicators of Compromise (IoCs) for the Attack Group APT-C-23

Domains

police-sec.info	sec-outluck.com	tellme.site	whispers-talk.com
pure-talk.com	secureaccountes.com	top4up.website	white-hony.online
rachel-green.info	selin-yilmaz.info	tyrion-lannister.info	whowatchyou.com
ragnar-lothbrok.info	sendbird-chat.com	upload999.com	win-laive.com
ran-togomory.com	serv2.sandtengineers.info	useraccount.website	winlife.host
redirect-wa.com	shahrukh-khan.club	usr-accounts-validation.pw	world-cup-live-2018.stream
rexkatsugeki.info	shailene-hazel.life	victor-stewart.info	yahaoa.com
richard-hines.website	shailene-tris.xyz	wa-loading.com	yohoa-users.com
rocket-chat.com	sherlock-holmes.club	wab-watzapp.com	young-spencer.com
rose-sturat.info	shortupload.com	wab-whtsap.com	youngmija.club
ross-gellller.info	show-me.fun	web-wnatzapp.com	zachlieberman.club
sahem.pcanywhere.net	so-chat.org	web-wtsapp.com	zee-player.com
sahemnews.dynamicdns.co.uk	sophie-deverau.xyz	websetting.me	zee-player.website
sanblitch.club	sopotfile.website	wes-gibbins.com	
sanjynono.website	spgbotup.club	whatsaapp.us	
sapport-accounts.com	sportliner.website	whatsapps.cam	
saratancredi.info	sybil-parks.info	whatsusers.fun	
sec-acoaunt.com	tawjihi2018.site	whatzopp.com	