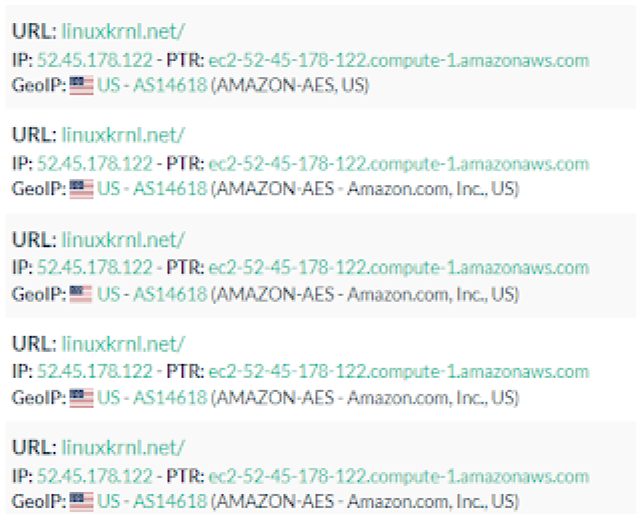
Exposing GRU's Unit 74455 "NotPetya" Malware Gang - An OSINT Analysis



Brace yourselves!

In this in-depth technical and qualitative OSINT analysis Dancho Danchev decided to publicly provide an in-depth peek inside the Internet-connected fraudulent and malicious infrastructure of GRU's "NotPetya" malware with the purpose of assisting U.S Law Enforcement on its way to track down monitor and prosecute the cybercriminals behind these campaigns.

Sample Cyber Attack campaign names: Sandworm Team, Telebots, Voodoo Bear, Iron Viking.

Sample malicious attachment: Qui_peut_parler_aux_journalists.docx

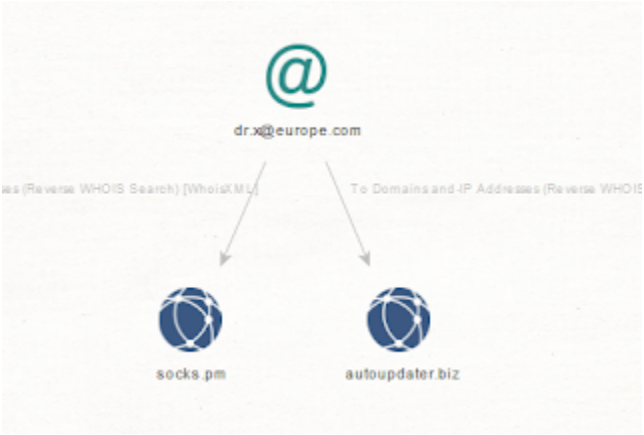
Sample personal email address accounts known to have been involved in the campaign:

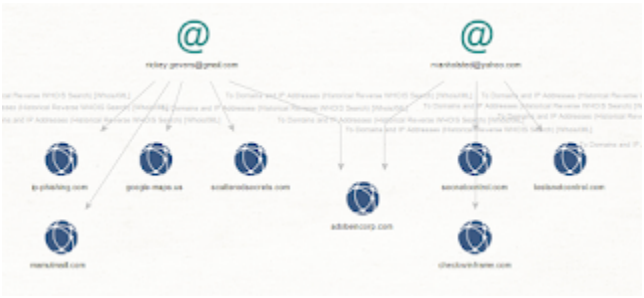
olympicgameinfo@gmail.com
alert.safekorea@gmail.com
nctc.go@gmail.com

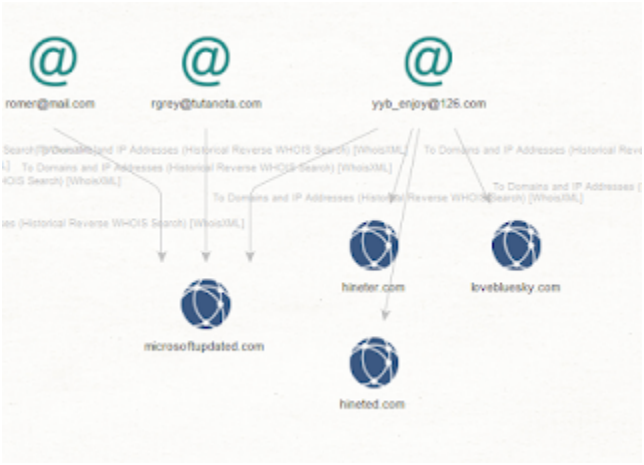
Sample C&C (Command and Control) server domain known to have been involved in the campaign:
hxxp://msrole.com - 52.45.178.122 -
hxxp://acledit.com/3gJw/2eH1eL/cQ6.zip/?4ft=XcF3DnwktjA4IrcxT2I=

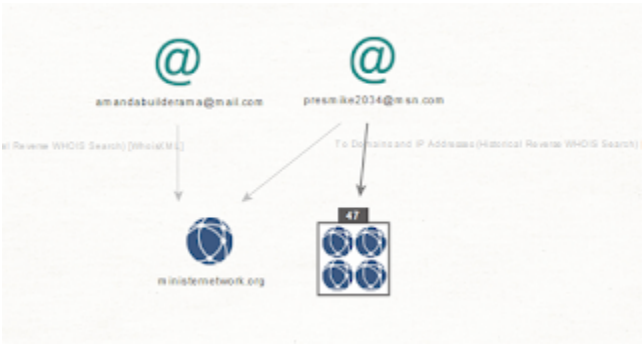
Sample malicious MD5 known to have been involved in the campaign:
MD5: 77089c094c0f2c15898ff0f021945148
Sample name servers known to have been involved in the campaign:
hxxp://ns1.msrole.com - 27.102.102.30
hxxp://ns2.msrole.com

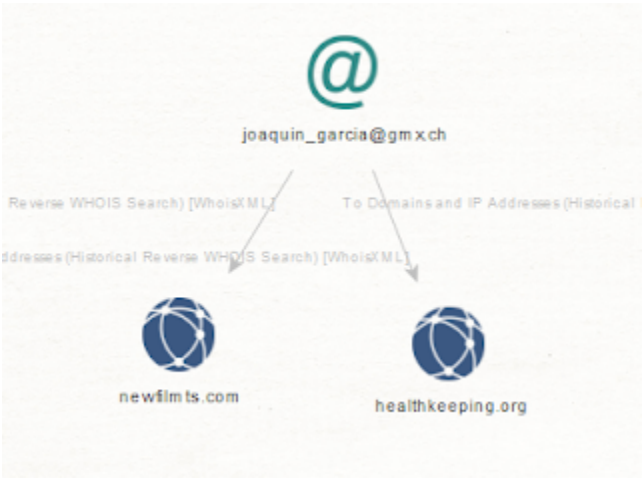
Sample Maltego graphs:





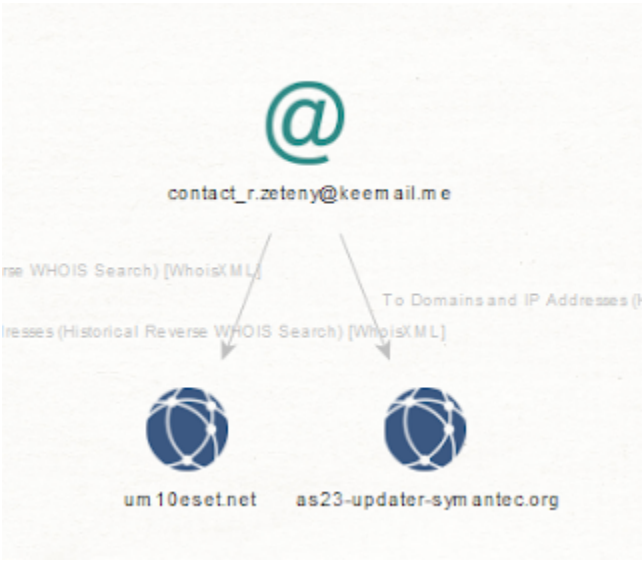

romer@mail.com
rgrey@tutanota.com
yyb_enjoy@126.com
hineter.com
lovebluesky.com
microsoftupdated.com
hineted.com

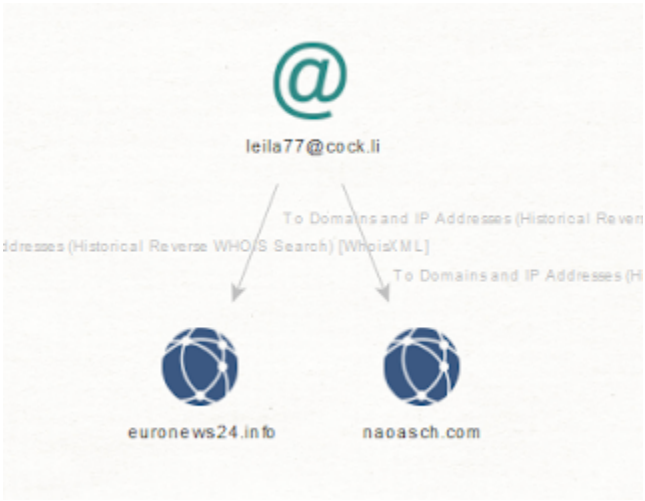

amandabuilderama@mail.com
presmike2034@msn.com
ministernetwork.org
47


joaquin_garcia@gmx.ch
Reverse WHOIS Search) [WhoisXML]
To Domains and IP Addresses (Historical
ddresses (Historical Reverse WHOIS Search) [WhoisXML]
newfilmts.com
healthkeeping.org


iflatley@openmailbox.org
al Reverse WHOIS Search) [WhoisXML]
To Domains and IP Addresses (Historical Reverse W
To Domains and IP Addresses (Historical Rev
mvsband.com
rndversion.net


jada.okeefe15@mail.com
generalsecuritycorp.org
reservecorpind.com


contact_r.zeteny@keemail.me
um10eset.net
as23-updater-symantec.org



Related malicious and fraudulent domains known to have been involved in the campaign:

hxxp://abs.twitter.com.webapp.workbench.run
hxxp://abv.bg.login-site.online
hxxp://accounts-updates.club
hxxp://accounts.ukr.net.checklogin.fbapp.info
hxxp://accounts.ukr.net.checklogin.updatenote.net
hxxp://accounts.ukr.net.checklogin.userarea.click
hxxp://accounts.ukr.net.fbapp.info
hxxp://accounts.ukr.net.updatenote.net
hxxp://accounts.ukr.net.userarea.click
hxxp://algemene-controle.online
hxxp://beststreammusic.com
hxxp://bg.fbapp.info
hxxp://bg.login-site.online
hxxp://bg.userarea.click
hxxp://center.cmdswitch.xyz
hxxp://checklogin.login-site.online
hxxp://cn.beststreammusic.com
hxxp://com.webapp.workbench.run
hxxp://cpanel.fairfieldsch.org
hxxp://dns.thehomeofbaseball.com
hxxp://e.mail.ru.settings.fbapp.info
hxxp://escochartzone.com
hxxp://facebook.com.webapp.workbench.run
hxxp://fastfilmsbucket.com

hxxp://fbapp.info
hxxp://fontdrvstore.com
hxxp://free24player.com
hxxp://georgia-travel.org
hxxp://google-account-settings.spdup.art
hxxp://google-moogle.spdup.info
hxxp://google-settingsapi.fbapp.link
hxxp://hostmaster.fbapp.info
hxxp://hostmaster.jazzradiostream.com
hxxp://hs126.tamsimail.com
hxxp://hs157.tamsimail.com
hxxp://jazzradiostream.com
hxxp://laerka.supplrald.com
hxxp://liveserviceonedrive.com
hxxp://login-site.online
hxxp://login-yahoo.fbapp.link
hxxp://loungecinemaclub.com
hxxp://luxefighting.net
hxxp://m.facebook.com.webapp.workbench.run
hxxp://mail.algemene-controle.online
hxxp://mail.bg.fbapp.info
hxxp://mail.bg.login-site.online
hxxp://mail.bg.login.photography
hxxp://mail.bg.userarea.click
hxxp://mail.eservicesystems.net
hxxp://mail.fairfieldsch.org
hxxp://mail.linuxkrnl.net
hxxp://mail.liveserviceonedrive.com
hxxp://mail.regvirt.com
hxxp://mail.suncommunications.org
hxxp://mail.topcinemaclub.com
hxxp://mckinseyandco.com
hxxp://mimecastverified.com
hxxp://moderntips.org
hxxp://mta-s1-151.tamsimail.com
hxxp://mta20.r1.tamsimail.com
hxxp://mta301.tamsimail.com
hxxp://mta303.tamsimail.com
hxxp://mta32a.tamsimail.com

hxxp://mta337.tamsimail.com
hxxp://mta440.tamsimail.com
hxxp://mta447.tamsimail.com
hxxp://mta624.tamsimail.com
hxxp://mta676.tamsimail.com
hxxp://mta678.tamsimail.com
hxxp://mta698.tamsimail.com
hxxp://mta770.tamsimail.com
hxxp://mta873.tamsimail.com
hxxp://mta884.tamsimail.com
hxxp://mta891.tamsimail.com
hxxp://mta900.tamsimail.com
hxxp://mta913.tamsimail.com
hxxp://mta925.tamsimail.com
hxxp://mta929.tamsimail.com
hxxp://mta932.tamsimail.com
hxxp://my-photo-service.com
hxxp://my.idnn.asia
hxxp://myaccount.click
hxxp://narrowpass.net
hxxp://networkcentrals.com
hxxp://nmail.regvirt.com
hxxp://noadsplayer.com
hxxp://ns1.checklogin.in
hxxp://ns1.treepastwillingmoment.com
hxxp://ns2.checklogin.in
hxxp://ns2.treepastwillingmoment.com
hxxp://ns2.userzone.one
hxxp://ovhsec.com
hxxp://passengerco.com
hxxp://passport.abv.bg.fbapp.info
hxxp://passport.abv.bg.userarea.click
hxxp://photosyncdrive.com
hxxp://politicweekend.com
hxxp://poolpartyrecords.com
hxxp://protonhardstorage.com
hxxp://redsample.net
hxxp://regvirt.com
hxxp://relay.soft-storage.com

hxxp://remotepx.net
hxxp://renodesmart.com
hxxp://sarmsoftware.com
hxxp://securitylogagent.com
hxxp://server31743.com
hxxp://smtp.truefashionnews.com
hxxp://sportever.org
hxxp://static.facebook.com.webapp.workbench.run
hxxp://store.soligro.com
hxxp://support-cloud.life
hxxp://syslog.acledit.com
hxxp://thissubdomainshouldonlyresolveifwildcard.liveserviceonedrive.com
hxxp://time-2t-time.com
hxxp://timezone0.com
hxxp://travelerupdate.com
hxxp://truefashionnews.com
hxxp://twitter.com.checklogin.in
hxxp://twitter.com.webapp.memcached.in
hxxp://ukr.net.fbapp.info
hxxp://utc2ltc.com
hxxp://webapp.workbench.run
hxxp://webdisk.fairfieldsch.org
hxxp://webmail.fairfieldsch.org
hxxp://wgzhk.dns15.bid
hxxp://worldimagebucket.com
hxxp://wp.soligro.com
hxxp://ww1.fbapp.info
hxxp://ww12.fbapp.info
hxxp://ww25.fbapp.info
hxxp://ww43.fbapp.info
hxxp://activityduringhistoricaloffice.com
hxxp://adobeincorp.com
hxxp://aeroservicemax.com
hxxp://akamaisoftupdate.com
hxxp://akulaku.tutooliv.club
hxxp://algemene-controle.online
hxxp://bbcweather.org
hxxp://beststreammusic.com
hxxp://checkmalware.info

hxxp://daysheduler.org
hxxp://escochartzone.com
hxxp://facebook.com.webapp.workbench.run
hxxp://fairfieldsch.org
hxxp://faststoragefiles.org
hxxp://fbapp.info
hxxp://fundseats.com
hxxp://globaltechengineers.org
hxxp://hostapp.link
hxxp://iboxmit.com
hxxp://liveserviceonedrive.com
hxxp://mdcrewonline.com
hxxp://moldtravelgroup.com
hxxp://narrowpass.net
hxxp://nethostnet.com
hxxp://networkcentrals.com
hxxp://newstyleradio.net
hxxp://ovhsec.com
hxxp://photosyncdrive.com
hxxp://politicweekend.com
hxxp://powernoderesources.com
hxxp://regvirt.com
hxxp://sarmsoftware.com
hxxp://scalingreserve.com
hxxp://truefashionnews.com
hxxp://updatesystems.net
hxxp://urlweb.dslbd.xyz
hxxp://userarea.click
hxxp://userarea.top
hxxp://userzone.one
hxxp://virm.xtrmp3.site
hxxp://virtsvc.com
hxxp://webcache.one
hxxp://workbench.run
hxxp://worldimagebucket.com
hxxp://x-tools.tech
hxxp://wwwco4testmcsoft.com
hxxp://zeroslitecarb.com
hxxp://zfmcg.dns15.bid

Sample screenshots of known C&C (Command and Control) domains:

Related personal email address accounts known to have been involved in the campaign:

p.henningsson@centrum.cz
milimil0702@mail.com
amandabuilderama@mail.com
hiepgp.bn@gmail.com
romer@mail.com
arik@hostar.org
dr.x@europe.com
JawdahKoury@tutanota.com
presmike2034@msn.com
kingston_trevino@protonmail.com
pol.michael@post.com
ben.grochot@tdfs.com
joaquin_garcia@gmx.ch
andre_roy@mail.com
bolekrejci@centrum.cz
iflatley@openmailbox.org
mikalay@icloud.com
jada.okeefe15@mail.com
manuel.herez@centrum.cz
olivier_servgr@mail.com
colemanmail@mail.com
lucasbenson@europe.com
rgrey@tutanota.com
tarob999@outlook.com
mahuudd@centrum.cz
pearliestehr@airmail.cc
ysrb@outlook.com
hr.jagdeep@gmail.com
erick_bolton@protonmail.com
yyb_enjoy@126.com
ken@m4v.me
rickey.gevers@gmail.com
tarob666@outlook.com
declan.jefferson@sapo.pt
ysrb.riady@gmail.com
contact_r.zeteny@keemail.me

pravich83@gmail.com
qq5598002@gmail.com
leila77@cock.li
klaoja@cock.li
loisoji@firemail.cc
rvanholsted@yahoo.com
ulli_neu80@mail.com
ma_picarlo@centrum.cz
mattew.barnes@aol.com
trajboj@centrum.cz
softmainnew@yandex.com
gerpsz@airmail.cc
gabrielromao@sapo.pt

Related malicious and fraudulent C&C (Command and Control) domains known to have been involved in the campaign:

hxxp://1oo7.net
hxxp://acledit.com
hxxp://adobeincorp.com
hxxp://aeroservicemax.com
hxxp://akamaisoftupdate.com
hxxp://appservice.site
hxxp://appservicegroup.com
hxxp://autoupdater.org
hxxp://beststreammusic.com
hxxp://bestweddingparty.org
hxxp://bg-abvmail.pw
hxxp://busseylawoffice.com
hxxp://cdnmsnupdate.com
hxxp://cdnverify.net
hxxp://checkmalware.info
hxxp://ciscosupports.com
hxxp://conflictzone.info
hxxp://dancemusicstream.com
hxxp://dateosx.com
hxxp://daysheduler.org
hxxp://dncvotebuilder.com
hxxp://doorbehindentirerelationship.com

hxxp://escochart.com
hxxp://escochartzone.com
hxxp://eservicesystems.net
hxxp://esetsmart.org
hxxp://eu-office365.top
hxxp://experiencewithweakkid.com
hxxp://familynearbysuitablenumber.com
hxxp://faststoragefiles.org
hxxp://fbapp.info
hxxp://fbapp.top
hxxp://fbcdn.store
hxxp://fundseats.com
hxxp://funnymems.com
hxxp://genericnetworkaddress.com
hxxp://georgia-travel.org
hxxp://globaltechengineers.org
hxxp://groupsincevisibleend.com
hxxp://hostapp.art
hxxp://hourduringstrictsense.com
hxxp://ikmtrust.com
hxxp://info-update-otlk.com
hxxp://kenlynton.com
hxxp://linuxkrnl.net
hxxp://loungecinemaclub.com
hxxp://malwarecheck.info
hxxp://mdcrewonline.com
hxxp://meteost.com
hxxp://microsofi.org
hxxp://microsoftupdated.com
hxxp://ministernetwork.org
hxxp://miropc.org
hxxp://moderntips.org
hxxp://moldtravelgroup.com
hxxp://msfontserver.com
hxxp://msrole.com
hxxp://mvband.net
hxxp://mvsband.com
hxxp://mvtband.net
hxxp://myinvestgroup.com

hxxp://mysent.org
hxxp://nanetsdeb.com
hxxp://naoasch.com
hxxp://narrowpass.net
hxxp://ndsee.org
hxxp://newfilmts.com
hxxp://ntpstatistics.com
hxxp://onedrive-jp.com
hxxp://pandorasong.com
hxxp://placeuntilknownparent.com
hxxp://politicweekend.com
hxxp://powerpolymerindustry.com
hxxp://protonhardstorage.com
hxxp://rapidfileuploader.org
hxxp://rdsnets.com
hxxp://reasonwithusefulpolicy.com
hxxp://regvirt.com
hxxp://reservecorpind.com
hxxp://rpcnetconnect.com
hxxp://sarmsoftware.com
hxxp://schooltillhungryprocess.com
hxxp://sdhjjekfp4k.com
hxxp://secnetcontrol.com
hxxp://servicetlnt.net
hxxp://softwaresupportsv.com
hxxp://soligro.com
hxxp://spdup.art
hxxp://ssl-mircosoft.com
hxxp://star4vn.net
hxxp://streetunderrelevantpeople.com
hxxp://suncommunications.org
hxxp://support-cloud.life
hxxp://systembeforeniceparent.com
hxxp://tablebeforehelpfulperson.com
hxxp://thehomeofbaseball.com
hxxp://topcinemaclub.com
hxxp://truefashionnews.com
hxxp://um10eset.net
hxxp://unigymboom.com

hxxp://updatepc.org
hxxp://updatesystems.net
hxxp://utmserver.com
hxxp://virtsvc.com
hxxp://visualrates.com
hxxp://viters.org
hxxp://webstp.com
hxxp://westmedicalgroup.net
hxxp://windowsdefltr.net
hxxp://workbench.run
hxxp://worldimagebucket.com

Related malicious and fraudulent C&C (Command and Control) domains known to have been involved in the campaign:

hxxp://sarmsoftware.com
hxxp://protonhardstorage.com
hxxp://onedrive-jp.com
hxxp://google-maps.us
hxxp://scatteredsecrets.com
hxxp://ip-phishing.com
hxxp://adobeincorp.com
hxxp://msfontserver.com
hxxp://hineted.com
hxxp://lovebluesky.com
hxxp://hineter.com
hxxp://psrrange.com
hxxp://ikmtrust.com
hxxp://citizenpolicenetwork.com
hxxp://keatontax.com
hxxp://michaelspontak.net
hxxp://softwaresupportsv.com
hxxp://reslocks.com
hxxp://mvsband.com
hxxp://vote4mike.net
hxxp://rndversion.net
hxxp://michaelspontak.com
hxxp://reslocksmith.com
hxxp://meadowhillbaptist.org

hxxp://faststoragefiles.org
hxxp://spontakfamily.com
hxxp://okolonabaptist.org
hxxp://mydateapp.net
hxxp://ckswebmanagement.com
hxxp://reservecorpind.com
hxxp://miropc.org
hxxp://citizenpoliceacademynetwork.com
hxxp://blogbymike.com
hxxp://cksbusiness.com
hxxp://generalsecuritycorp.org
hxxp://newfilmts.com
hxxp://naoasch.com
hxxp://myinvestgroup.com
hxxp://euronews24.info
hxxp://damagedchristian.net
hxxp://webstp.com
hxxp://cksweb.net
hxxp://damagedchristian.com
hxxp://healthkeeping.org
hxxp://taxprepcompany.org
hxxp://akamaisoftupdate.com
hxxp://citizen-police-academy.org
hxxp://rpcnetconnect.com
hxxp://citizen-police-academy.net
hxxp://psrrange.org
hxxp://psrrange.net
hxxp://cvssucks.net
hxxp://ckswebhosting.com
hxxp://citizen-police-academy.com
hxxp://meteost.com
hxxp://cks-security.com
hxxp://nanetsdeb.com
hxxp://psr-range.com
hxxp://church-web-ad.com
hxxp://cvssucks.biz
hxxp://psrrange.biz
hxxp://checkwinframe.com
hxxp://exitinterview-themovie.org

hxxp://soligro.com
hxxp://cksweb.org
hxxp://secnetcontrol.com
hxxp://michaelspontak.space
hxxp://testsnetcontrol.com
hxxp://true-church.net
hxxp://citizenpoliceacademynetwork.net
hxxp://true-church.com
hxxp://church-network.com
hxxp://cooperchurch.org
hxxp://ndsee.org
hxxp://ministernetwork.net
hxxp://ihatepolice.net
hxxp://spontakfamily.net
hxxp://ministernetwork.com
hxxp://spontakfamily.org
hxxp://appservicegroup.com
hxxp://ckswebhost.net
hxxp://tax-prep-company.com
hxxp://eurosatory-2014.com
hxxp://link-google.com
hxxp://ntpstatistics.com
hxxp://googlesetting.com
hxxp://ya-support.com
hxxp://evrosatory.com
hxxp://esetsmart.org
hxxp://set121.com
hxxp://us-westmail-undeliversystem.com
hxxp://us-mg7mail-transferservice.com
hxxp://virtsvc.com
hxxp://changepassword-hotmail.com
hxxp://changepassword-yahoo.com
hxxp://product-update.com
hxxp://academl.com
hxxp://dateosx.com
hxxp://software-update.org
hxxp://malwarecheck.info
hxxp://update-hub.com
hxxp://soft-storage.com

hxxp://ministernetwork.org
hxxp://bulletin-center.com
hxxp://rdsnets.com
hxxp://globaltechengineers.org
hxxp://as23-updater-symantec.org
hxxp://um10eset.net
hxxp://microsoftupdated.com
hxxp://cdnverify.net
hxxp://mamutmaill.com
hxxp://conflictzone.info
hxxp://trafficdirectsystem.biz
hxxp://mybit.pro
hxxp://mybtc.pro
hxxp://socks.pm
hxxp://rentin.asia
hxxp://autoupdater.biz
hxxp://autoupdater.org
hxxp://drones.rent
hxxp://xmpp.ooo
hxxp://isocks.pro
hxxp://microdice.in
hxxp://ipcheck.pro
hxxp://dateless.pro

Related malicious MD5s known to have phoned back to the same C&C server domains:

0062eee42577b94119f4e128ed77a89aa26db206ab77a3cdaf98dc5cec1bc2b6
01da20243c26cd677339c978274776d331b0b2387cdb085527b7f7b68fc1ac59
0860f29226069a732f988cb70ea6d51057d204d421bb709b8e759376b0c4d201
0be57d1244fefc679feb7aa9996e539481be7b8f4c9246817f81caa8c2f61a57
0d260a4ea865773a86b3fc0fe89df92c86289c0266b1dd5ab8e3174839cb94c2
102b0158bcd5a8b64de44d9f765193dd80df1504e398ce52d37b7c8c33f2552a
12e171291f0deae69509a6ef2220cd9e0b9ed0e3e8651f33824fc627612be055
1370b8491829178c260f417623192c18f18779d71149c9a8786fa4dd79c56325
17234284a1e98e8350ec6ab7f5998b53d130495473945483b967e3dc9007250c
2005bbb82a8b2b4744188be58ef5b3892ca4af920bc645e1f334b2ae62a26624
29cc2e69f65b9ce5fe04eb9b65942b2dabf48e41770f0a49eb698271b99d2787
2c81023a146d2b5003d2b0c617ebf2eb1501dc6e55fc6326e834f05f5558c0ec

2cea2a1f53dac3f4fff156eacc2ecc8e98b1a64f0f5b5ee1c42c69d9a226c55c
33c187cfd9e3b68c3089c27ac64a519ccc951ccb3c74d75179c520f54f11f647
378ef276eeaa4a29dab46d114710fc14ba0a9f964f6d949bcbc5ed3267579892
37f15647c26d475db805048d6592aa153533ac5f4373145c75e24012a51ad9f8
42ed4ab65535ae382ed00a954a564bd13ac77731311400378af90bce2a463521
45540fe0890bd5063fe2c464efd554e0e119d8501cc57cbec7e3577a9bb33a22
48264394ab80a932b9df7520e8ec57e68a652c0302f8a8a5ac2d1321b9a3c84e
48a1bd2f7ee85e9676c4eea0b353ecda2f583fbd72ced688af660fe8fdf34bbe
59070257ff9289683876d19678267f5b9449ce0884fa59e55cfdc60f9df2f41c
5a02d4e5f6d6a89ad41554295114506540f0876e7288464e4a70c9ba51d24f12
5f6b2a0d1d966fc4f1ed292b46240767f4acb06c13512b0061b434ae2a692fa1
62e33f4126d58ac36ea0e75102d36eae929ce210da80ead210342d2d91afb03b
634795a3acbae8964bb31e3ebed7f29208844978a512fc26a8b9a51901f9cab9
6bbec6b2927325891cc008d3378d30941fe9d21e5c9bd6459e8e3ba8c78833c2
6d626c7f661b8cc477569e8e89bfe578770fca332beefea1ee49c20def97226e
6dcb3f28255eaf07bb67b3515200b70391cb066111c5d67232704b367555b287
739da178a3222e716ebc81bd5f4c731fd2be8705e4d3a9a32f4b2a8ff11888b5
78adc8e5e4e86146317420fa3b2274c9805f6942c9973963467479cb1bbd4ead
7a5cb45a3efcebbf49e18c4b2397dc2bdff039d9127a8119abe4c2f85a85e1f0
7b0e7f0b87a18cc2b847674987d3d0419954e9cf62720a9f6c5f38ecbae0c4f5
7c4101caf833aa9025fec4f04a637c049c929459ad3e4023ba27ac72bde7638d
7f6f9645499f5840b59fb59525343045abf91bc57183aae459dca98dc8216965
82fc44696d1c5ddfdd5338fcafb6a9dcf7a0796235cd58184d05a2f388ed7e9e
8fe5b126a0e91ae1a523d2f4ab1c54f22d21015d5a23f798d5f257c532edd152
94a9b5cb057e5b56262195485b621117eee24fd242db7bca77e9cb4e62857a05
9f84d09b194f54f1c8b8df56ba7cb1a500b8e000746cea5ca1fe6e3ae33b25ed
a03387af06aa8c7a56a3b0f100fb1099f46676e3cb06c4ee7d1069d324c03caa
a24220fd4a7767de8921fad0a939ebb974fc16ec1b7611cc8aeb4ad97f6737a2
a37eda810ca92486bfb0e1f1b27adb7c9df57aafab686c000ae1d6ec5d6f6180
a97b1a792f7b53929a1c01bad9fc2bd606a15e8e32755daa15570e356baa0112
ab71eddda2254007cb55887b94a16cb129d2992eeb9749216cb031e9f5f0b896
b77ff307ea74a3ab41c92036aea4a049b3c2e69b12a857d26910e535544dfb05
b814fdbb7cfe6e5192fe1126835b903354d75bfb15a6c262ccc2caf13a8ce4b6
b9f23124a995e0ce8550cb916436626809c3aa5f20029fec257f114fdb82abc2
bc637c6a9dd781674c258641466ba2acb3d128ef1f1a46c190c7b7eb947d8610
c3ac697990bbb82f31d8f1d203ef7b032b3b43bcb916cecc354fa45151f7420d
c6b9efdbfbfb1d34569d7a7e8bf9a7dfe76ff9b0deaa721564da8433f6a98e91
c8087186a215553d2f95c68c03398e17e67517553f6e9a8adc906faa51bce946
c817ca1763e42bc9e79a5538152ed78c13b3a650d5a2793ef9e3bfdd6f34905a

cada4bcdbc96ae88de974b9066f84190c0512013e153e68b028b154c0bf8fdd0
ce487e055a57489c44c012e04b038998a5505da85b0e9e9406419bf91d9425ac
d06be83a408f4796616b1c446e3637009d7691c131d121eb165c55bdd5ba50b4
d1ed72922a3e987090ae3465ce27aa582e0101b0211780a0a796684a8f798da9
d403ded7c4acfffe8dc2a3ad8fb848f08388b4c3452104f6970835913d92166c
d4ea3fba15379fe36f08685d542eceec727c1755395b3ff7928a7d994bcfcf0a
d5872edfe7942e52a2db5327b5439fc23d4535788fe68be9feb4c02e56233d9d
d58f2a799552aff8358e9c63a4345ea971b27edd14b8eac825db30a8321d1a7a
d88f2a4ea0bc9eb2acf8ba534e785cdc5fb7a07cc511df6b9e698d3ab8414a3a
dc0a3ff3eb75e2d9e090a6afa5d14396c27a5bebc4e5d6ac8a50e637eb5a1422
dea3a99388e9c962de9ea1008ff35bc2dc66f67a911451e7b501183e360bb95e
dfba21b4b7e1e6ebd162010c880c82c9b04d797893311c19faab97431bf25927
e9535d0d5e8e17779b49607988cdb0547efb6abb482dab497a5f0da87cbefc96
eb413002be9e83b73e9b951758692d9d0492fab7500110ec1ce432cd6d26b6d7
ec2f14916e0b52fb727111962dff9846839137968e32269a82288aee9f227bd4
ecc5805898e037c2ef9bc52ea6c6e59b537984f84c3d680c8436c6a38bdecdf4
ee0a679844146e3d0eb623dc874b4d5ff151dddf16582774299ff65bcfff5b44
f47da6948670b2390aab2a7701d85e3d505ca1ce8cce139bfddcbf5f255dcc4b
fb9fe6352696dc954cbbca514b652ce5e5104c1b6577a50dfddc925cd46f4970
fcad263d0fe2b418db05f47d4036f0b42aaf201c9b91281dfdcb3201b298e4f4
ff808d0a12676bfac88fd26f955154f8884f2bb7c534b9936510fd6296c543e8

We'll continue monitoring the campaign and post updates as soon as new developments take place.