TREND MICRO | research

The Rise of Earth Aughisky: Tracking the Campaigns Taidoor Started

Appendix

Indicators of Compromise (IoCs)

Domains

Domains
1122334[.]zyns[.]com
aimimi[.]xxuz[.]com
airbus[.]zyns[.]com
airlinesflightleaving[.]thesizeofearth[.]ourhobby[.]com
aolmail[.]ddns[.]info
article[.]phdfa[.]com
Artor[.]terelation[.]com
asia[.]publiccosplay[.]org
av[.]phdfa[.]com
backupcoa[.]serveftp[.]com
big[.]qpoe[.]com
bigbang[.]ddns[.]ms
bigbang[.]myddns[.]com
bigbank[.]cnkk[.]org
bigbigbig[.]servehttp[.]com
bigkszb[.]twgogo[.]org
bing[.]ikwb[.]com
bitcom[.]polaczyk[.]com
blizzard[.]apchnetinfo[.]com
bnhxalex[.]organiccrap[.]com
bulk[.]indonet[.]org
cart[.]skyseaweb[.]org
cca[.]us[.]to
cier[.]edu[.]tw[.]us[.]to
common[.]taiwan[.]twilightparadox[.]com
common[.]taiwaninfoma[.]uk[.]to
customs[.]bot[.]nu
dayan[.]onedumb[.]com
dirco[.]jetos[.]com
dns[.]dymantic[.]service[.]fbs[.]ocry[.]com
download[.]longmusic[.]com
duth[.]ahfree[.]net
emailfromsm[.]mpsdtupdsda[.]ezua[.]com
exchanger-online-thalesgroup[.]zyns[.]com
expiration[.]toythieves[.]com

ey[.]acaro[.]org
ey[.]uk[.]to
Facebook[.]ddns[.]ms
family[.]mobwork[.]net
faqtos[.]ignorelist[.]com
fareastone[.]my03[.]com
find[.]usdc[.]ignorelist[.]com
fsc-kd[.]ns01[.]info
ftp[.]boonty[.]Got-Game[.]org
ftp[.]hinet[.]dns-dns[.]com
ftp[.]kingdom[.]myddns[.]com
ftp[.]lily[.]onmypc[.]net
ftp[.]newmc[.]dns-dns[.]com
ftp[.]ourfriends[.]sexxxy[.]biz
ftp[.]twnic[.]almostmy[.]com
ftp[.]wlksbb[.]MrsLove[.]com
ftp[.]yahoo-inc[.]DSMTP[.]COM
global[.]smart-house[.]ga
gmailgroup[.]mooo[.]com
google[.]apchnetinfo[.]com
google[.]ddns[.]name
google_service[.]ns01[.]us
googlemailinforma[.]orge[.]pl
gpu[.]wikaba[.]com
H0TMAIL[.]ddns[.]info
healths[.]jumpingcrab[.]com
hinet[.]dns-stuff[.]com
info[.]chemoimmunity[.]top
infor[.]nttcom[.]tk
intweb[.]mobwork[.]net
iPhone[.]linkWebSock[.]ZoneID[.]uk[.]to
iphone[.]site[.]web[.]fbs[.]ezua[.]com
iphone-ex[.]info[.]tm
itunes[.]toythieves[.]com
jgx[.]explorermaker[.]com
k1fsc[.]ax[.]lt
kaspersky[.]apchnetinfo[.]com
kcg2[.]gov[.]tw[.]allowed[.]org
kdmm[.]t28[.]net
kelsdc[.]compress[.]to

kilomier[.]2waky[.]com
kingdom[.]myddns[.]com
kingpsng[.]twgogo[.]org
kuangd[.]new[.]hack-inter[.]net
kuangd[.]new[.]privatedns[.]org
kuangdao[.]serveftp[.]com
list[.]googlebook[.]mrbonus[.]com
Liveupdate[.]jkub[.]com
liveupdate[.]Jkub[.]com
mails[.]grousp[.]allowed[.]org
mains[.]tainoetnde[.]bgphome[.]com
manated[.]dynamic-dns[.]net
members[.]viaopen[.]net
micro[.]security[.]services[.]rebatesrule[.]net
mimimi[.]VizVaz[.]com
mobiles[.]chickenkiller[.]com
moea[.]jumpingcrab[.]com
moea[.]strangled[.]net
moeaidb[.]ro[.]lt
mofa[.]ignorelist[.]com
mofir[.]twgg[.]org
money[.]terelation[.]com
mosec[.]twgogo[.]org
most[.]gov[.]allowed[.]org
msnlive[.]25u[.]com
music[.]apchnetinfo[.]com
mysweetpig[.]news[.]minecraftnoob[.]com
name[.]itsaol[.]com
news[.]mynews[.]photo-frame[.]com
news[.]onmypc[.]org
news[.]rockspace[.]wang
newsda[.]opsdatus[.]greatfinder[.]org
obicsystem[.]ntt-nexia[.]tk
ofa[.]fartit[.]com
oop[.]crabdance[.]com
oop[.]gov[.]minecraftr[.]us
oop[.]govtw[.]servernux[.]com
oop[.]uk[.]to
pe[.]publiccosplay[.]org
photostw[.]twgogo[.]org

pic-yahoo[.]ddns[.]us
pqsl[.]servernux[.]com
prefers[.]kboyda[.]net
privilegecom[.]theesponsibility[.]crabdance[.]com
RdAccount[.]dns1[.]us
relationship[.]epac[.]to
renders[.]maninta[.]anichgroup[.]com
rfvg[.]karlosb[.]com
rt[.]skymeto[.]com
sacstartapples[.]mohwfreshman1[.]otzo[.]com
saitama[.]map-shinai[.]com
sceyf[.]ibmmt[.]net
sci[.]dns1[.]us
security[.]MyNetAV[.]ORG
skype[.]mrbonus[.]com
smtpgov[.]eSMTP[.]biz
soft[.]update[.]cloudns[.]info
sorry[.]iownyour[.]biz
sososb[.]twbbs[.]org
stonekiki[.]freeddns[.]com
symantec[.]apchnetinfo[.]com
taiwanmail[.]org[.]ignorelist[.]com
tdns[.]verydvcd[.]com
TheoreticalModel[.]onmypc[.]us
toolbar[.]DSMTP[.]COM
toolbar[.]qpoe[.]com
trace[.]leecantu[.]com
trends[.]crabdance[.]com
tw[.]americanunfinished[.]com
twmis[.]twgogo[.]org
update[.]madacity[.]top
update[.]madicity[.]org
update[.]msapp[.]cloudns[.]info
video[.]itsaol[.]com
voicetube[.]citytalk[.]crabdance[.]com
web[.]stonekiki[.]freeddns[.]com
wephone[.]us[.]to
whlu[.]congci[.]info
widcards[.]abousts[.]fabioabreu[.]net
wlks[.]ServeUsers[.]com

wmdshr[.]3322[.]org
www[.]accountinfo[.]ssl443[.]org
www[.]american[.]ddns[.]us
www[.]bbwlkszb[.]organiccrap[.]com
www[.]bestcom[.]dns2[.]us
www[.]bidsd[.]justdied[.]com
www[.]bing[.]ikwb[.]com
www[.]biz[.]pcanywhere[.]NET
www[.]bnhxalex[.]organiccrap[.]com
www[.]centers[.]allowed[.]org
www[.]economy[.]ServeUser[.]com
www[.]enjoyit[.]longmusic[.]com
www[.]facebooking[.]otzo[.]com
www[.]faqtos[.]ignorelist[.]com
www[.]getadobe[.]dns-dns[.]com
www[.]google[.]dynssl[.]com
www[.]googledrivercould[.]serveuser[.]com
www[.]gov[.]organiccrap[.]com
www[.]gov[.]toh[.]info
www[.]happy[.]MyNetAV[.]ORG
www[.]idb[.]dns-dns[.]com
www[.]info[.]IsASecret[.]com
www[.]jjj[.]ns02[.]us
www[.]Kaccount[.]moneyhome[.]biz
www[.]kdbb[.]ourhobby[.]com
www[.]kelsdc[.]compress[.]to
www[.]kgoogfsd[.]freetcp[.]com
www[.]kilomier[.]2waky[.]com
www[.]kingdom[.]myddns[.]com
www[.]Kmember[.]wikaba[.]com
www[.]ktwods[.]lflink[.]com
www[.]ktwords[.]lflink[.]com
www[.]lily[.]onmypc[.]net
www[.]lookup[.]ns02[.]us
www[.]madicity[.]org
www[.]mbank[.]moneyhome[.]biz
www[.]mitac_com[.]dns05[.]com
www[.]moea[.]dsmtp[.]com
www[.]moea[.]toythieves[.]com
www[.]moeaidb[.]dns-dns[.]tw

www[.]moeaidb[.]qhigh[.]com
www[.]moeaidb[.]tk
www[.]mofamail[.]acmetoy[.]com
www[.]mpsdtupdsda[.]ezua[.]com
www[.]mptudp[.]pw
www[.]mybb[.]dns-dns[.]com
www[.]nditd[.]top
www[.]newtw[.]otzo[.]com
www[.]nscnet[.]tk
www[.]oop[.]ddns[.]us
www[.]oop[.]itsaol[.]com
www[.]ourfriends[.]sexxxy[.]biz
www[.]post[.]ourhobby[.]com
www[.]qtwlkszb[.]dynamicdns[.]org[.]uk
www[.]rocky3288[.]changeip[.]org
www[.]skyfd[.]com
www[.]software[.]acmetoy[.]com
www[.]specas[.]OurHobby[.]com
www[.]symantecAnti[.]ItemDB[.]com
www[.]taitra[.]fartit[.]com
www[.]thesizeofearth[.]ourhobby[.]com
www[.]tipo[.]dns-dns[.]com
www[.]tpp[.]otzo[.]com
www[.]trademoea[.]onmypc[.]net
www[.]twitter[.]otzo[.]com
www[.]update[.]mefound[.]com
www[.]wlksbb[.]MrsLove[.]com
www[.]workstation[.]mypop3[.]org
www[.]yahoo[.]serveuser[.]com
www[.]yahoonews[.]twgg[.]org
www[.]zoneprenuin[.]crabdance[.]com
www3[.]loginlived[.]com
yahoo[.]ddns[.]name
yahoo[.]mailweb[.]sxn[.]us
yahoofacebook[.]345[.]pl
youtobebig[.]cnkk[.]org
youtobeother[.]twbbs[.]org
zbAction[.]dynssl[.]COM
zcrd[.]twgogo[.]org
zoneprenuin[.]crabdance[.]com

Figure 1. Attributed Earth Aughisky domains

URLs

URLs
hxxp://beautygirl[.]1apps[.]com/judy[.]asp
hxxp://bingo[.]ikwb[.]com/asp
hxxp://blogs[.]vizvaz[.]com/mysite/images
hxxp://booknews[.]adaone[.]com/apps
hxxp://cisco001100[.]port25[.]biz/mysite/config
hxxp://cloak[.]zyns[.]com/e_bank/img/design
hxxp://cmail[.]zyns[.]com/mysite/images
hxxp://dska[.]ns1[.]name/media
hxxp://eadc[.]ns01[.]us/private
hxxp://eadc[.]ns01[.]us/web
hxxp://engine[.]justdied[.]com/web
hxxp://featuresapplegx[.]1apps[.]com/defaultgx1[.]asp
hxxp://flow[.]parujas[.]com/images
hxxp://fourk-asptree[.]qc[.]to/index[.]asp
hxxp://google[.]serveusers[.]com/wam
hxxp://inc[.]my03[.]com/images
hxxp://iphoneapp[.]1apps[.]com/index[.]asp
hxxp://joboss[.]1apps[.]com/data/index[.]asp
hxxp://kmtccc[.]1apps[.]com/index[.]asp
hxxp://mobile001[.]ns02[.]info/mysite/images
hxxp://mylinux[.]ddns[.]ms/mysite/images
hxxp://nationalobm[.]itemdb[.]com/mysite/config
hxxp://nationalobm[.]itemdb[.]com/mysite/images
hxxp://news[.]durbh[.]com/images
hxxp://onl[.]myrsoftware[.]com/images
hxxp://sdr[.]mrbonus[.]com/release
hxxp://ship[.]acmetoy[.]com/web
hxxp://skdghvka[.]1apps[.]com/index[.]asp
hxxp://tcpsung2011[.]1apps[.]com/home[.]asp
hxxp://tonyr[.]ns02[.]us/private
hxxp://volume[.]dhcp[.]biz/images
hxxp://wikipediatwaccou[.]1apps[.]com/indexpf[.]asp
hxxp://www[.]video[.]onmypc[.]org/web
hxxp://yunso[.]MrFace[.]com/images

Figure 2. Attributed Earth Aughisky URLs

Loaders

Loaders	Detection Name
a1066cfd823b3fad55fa7572e5be16a2e7cb2ebfd14fd8f3b6af4f2d6392421a	BKDR_TAILDR.ZTEK-A
bfef45c0797e01a5294411a8ca488093032d0974a8b0bcd92cbb2da4567230e7	BKDR_TALERET.ZTBH-A
66bfdfb5dd6d44960944e7f5d6132058f4faf1b72b22151aeba2469037fb04e6	BKDR_TALERET.ZTCG-A
97373d59533f52c5b7469e9e19ec06b9dcf4b3a7f32b2fdd6561116e8eb78fdb	
353ba074ad58985bc1383e557dfbec8785c80d81900094af9f70e3afb7ca8a9c	BKDR_TALERET.ZTCJ-A
6860ac794097c39284af178bf81b8ee99b78bf095c15ed645b057127bef7a301	TROJ_DALGAN.JE
871cb0b02214a5f9c394220af40b5da302f176fb5f1cc5ff1fdd9fa3582b3ee2	
6240d314a9da040c5fceb371668d57d799438bca6156e27bf71346e707a9be74	TROJ_DALGAN.JG
e604ff4e21f89c586814577ecc6eec33d4c4f6b5c414900f2cc6d3282abf8acb	TROJ_DALGAN.ZTDF-A
cf060da38eb21370983ea61029fc5669dd263e404a213f4571c7af1d2574fe07	TROJ_TAILDR.ZTEH-AA
57df5a83dfcbe8ed656e6fe146508625edbe9c5f476c24ca8b4a669be270179d	
54739934c82f7822f0af9cfdf851678b83f4f8b43dc786df3ffe1e4aeb179111	
503e8b90b470219dd7748011fe2a8b096212b2ffb5dca3e984952f9cc49f1563	
5c0d88e57c0cd5e720441913c961be71c95f59e7e17a128a3dfdc78bd2b06c6a	
085b83cba2a086929f3b838635d95abc31f5595ae0921af3100ca3d0563a7ce7	
bc1a331ce58808bf7f2583c72e614d0e623d0399a06d83f9a21290daf76a50fe	TROJ_TAILDR.ZTEI-A
1476e338640068220297ebda79be3a692a49916880b29bb65f8c448bed4e554d	TROJ_TAILDR.ZTEJ-A
f3dd7b30daca1ea58060124cba263b3aea62c320f12b1354338bf9fb8405575a	TROJ_TALERET.GC
2fd6ce8eec9b1b189d67c4c41dac13e15a290b71267320003c3f69d7d096c458	TROJ_TALERET.VQK

Figure 3. Attributed Earth Aughisky loaders

Hashes

Roudan

SHA256	Detection Name
933608c4bdc6a307a60f7d0feb18ec2852cc8313fb3be6067634cd2e1e6cbc66	Backdoor.Win32.SIMBOT.AA
b7d357eb94bca74b9416616176260908383 6ca0133de25cfb604b23eaca22c22	BKDR_DLLHOOK.A
d06b514318143e81fcdfee35b19a50943019b508ebfb5edf27ce5ea19ae65e78	BKDR_HUPIGON.ION
03b31a44df6a62fd4b44d3144406ef903bbb402e43a7d8547cf5594977251493	BKDR_MOCELPA.A
01636faaae739655bf88b39d21834b7dac923386d2b52efb4142cb278061f97f	BKDR_MOCELPA.ZTCD-A
9856553261f62829d019ac684b7621d0f2043b62799f9b42d4c4c8e410dfa78d	BKDR_OSTI.A
06df72f045d5518f519a5cd29b5bb5afd6c7f8098a51213f3897bf670f517855	BKDR_SIMBOT.SMC
08909439d1f7c15c17d231154a8983525f9ce6dbf9ad2ae5c93b3e2cbed69aea	BKDR_SIMBOT.SMC
099b01bb075995dd8e4de6c5fbf1e90a1c9c19ac09d82a3c9718d7876c043790	BKDR_SIMBOT.SMC
0ffb60c77a2da662cace3821af56cea0bf922fe9834fe34b5075ac4799463668	BKDR_SIMBOT.SMC
139237ed7c40eb2fd46eadf3878f29b080ea81c671196b45f53268558fa0f131	BKDR_SIMBOT.SMC
158ba90c3fe5844005919f72cbfd92014e826c75cfedcd05a8fdbfab9dbae049	BKDR_SIMBOT.SMC
172898de3033ffee8d49cd98881800e4d98c56e049a59ef6106385862c4de0f8	BKDR_SIMBOT.SMC
19570ad17429ba8995f2afa2ed635eafe06a4da290a663487ef053d097759b4d	BKDR_SIMBOT.SMC
1abd9bf9eec41508438b721771002e551c165d4bca2d52eb6b1273d2ce81dd5f	BKDR_SIMBOT.SMC
1bb842431ebbf4d0dfe453f146c6cffce7b232e9ada0f728967c0107e245039d	BKDR_SIMBOT.SMC
1e0166518f5d1905b60be80793dc1d55937d2a8d08eebb82b8cff572eed29eb5	BKDR_SIMBOT.SMC
22f793d016fcd7aae6f7982194010cdfb64c17b27bd6e7fc48fbccc588fa3db0	BKDR_SIMBOT.SMC
255ea379b3e83b5d8ef957e041dfd590f00fa02d1ed3a2850450c16d658f860f	BKDR_SIMBOT.SMC

26f11877ad790ce00e77a4164a82d98a93ec02e0b85d1f93ae370e43cc47a5f3	BKDR_SIMBOT.SMC
273e1b31020f0171e8acea4348fbef98fb8fc2c1dcd98afce729694b20de877c	BKDR_SIMBOT.SMC
27746788f37fdf94e1738b009a6be47469dff78f4752f01dc70b307625012eb9	BKDR_SIMBOT.SMC
288251486c965480db495597cf6b96983972b212da0dedb9a61dc344378c59a6	BKDR_SIMBOT.SMC
28e438a9388ce3bc748490ca6be1330caa843a0d8ba66fe44f4cef86a5fad0e4	BKDR_SIMBOT.SMC
2cebbc1dfecbcd64ed1cebfe44600288e607583631265fd8f5661b70f5cefe1f	BKDR_SIMBOT.SMC
2f10d6d2b346bfe4e5c9cf0c043c5000a469e3293ac515e2b8a78527b566d59b	BKDR_SIMBOT.SMC
341c615f25657daf40087808060b2e1bcaf879c8cdd4e659636a231cc32348dd	BKDR_SIMBOT.SMC
34b8876ba982aa5bcec023dc7591441f3a9ae805263bbd9f4a8c92d1e19d994a	BKDR_SIMBOT.SMC
35228ac8ba165be86d5a42dae59db92b6d94060cd99f78f12eee8eb02c1388d6	BKDR_SIMBOT.SMC
35d4e2987448f1f059e1c9c0d9da0752efe1ab54d13b593d4492f71dc490f5a6	BKDR_SIMBOT.SMC
39317fdf48b868f7788ce72b24779bbf2637eb0966b02b81181377fb135607df	BKDR_SIMBOT.SMC
3b86042f37200bc27f6d445d648621a326228cd072e6c79b91861174f96ba304	BKDR_SIMBOT.SMC
40e5490c885a8d1023e79b06df992d3c911a843774d63bff83084fe244e4a628	BKDR_SIMBOT.SMC
413e0335e411d5ede4c43340412442655ba07a27bd4588940c5e9ad0f3feb13f	BKDR_SIMBOT.SMC
41ca1f666c4ce546e836f0d593e2fd2660854f31e89357de2e1b93e85b75d341	BKDR_SIMBOT.SMC
43ac233d2483377cdd61cb44a5c19f23d934af4ed54b57e626526218708f3f4b	BKDR_SIMBOT.SMC
44f2d0b8bcb3c5d9d0644a1c1dc8a7dbdddd8e173c4cd4e13db03471a7ed91ec	BKDR_SIMBOT.SMC
463f40bf47a7f64a1ada9b2b89c4b28ee738701bbeb5d0efc2f052de86578dcd	BKDR_SIMBOT.SMC
47198366a20a8eb4cb1ff5c3769fa8dee1bcab9d1e6258b3a19ffa28b644eb38	BKDR_SIMBOT.SMC
47b314f6de708bc7f21944295d57c7026356da5209380e6b17b1a372de2b3167	BKDR_SIMBOT.SMC

4dd701d2c40ca7b1172f5a2e8bd0dffbfe62452d03664788be32aad46ae8d7c9	BKDR_SIMBOT.SMC
4e72389e72ff30cfc1ffbbd3a444bd56180c96a0ea5643925ad8255a46f95317	BKDR_SIMBOT.SMC
50b9c5b1013b086320b296e7b18e0a0bd305dbc815058dd3b495f4507af5b77b	BKDR_SIMBOT.SMC
512c11137fceb5cde732daf66a94bfc205fd0396af0a5b2801d3e258d7ac70f6	BKDR_SIMBOT.SMC
560b5db7eab3510ed4f8d5a7c3bdbc9787d8c63fa1154f093a55f9b1ff0215bf	BKDR_SIMBOT.SMC
56615496be414183dbed9348b6ed278ceb4287cc4c8be0a4d8bd115477daa806	BKDR_SIMBOT.SMC
59c72698c3bb47c2f1935d0b67c96d904c61920d08022e3fa65816f9c8901b07	BKDR_SIMBOT.SMC
59f5651aa18f8b5c71f95d7a32b8d2fa1c26e081dbac824a9e80e349a40fd3c0	BKDR_SIMBOT.SMC
5ae56c93b442191313486b52132de7532ba729fa1eb786ce926769e6ca90b01b	BKDR_SIMBOT.SMC
5b83f6966ac0d8b733a0038faa5fe52b56518bb33a85a25e7bf35add8e2b62a	BKDR_SIMBOT.SMC
5be76ded1c6a15911fd384d2b3f52dca1253380dfd35af106da62464cb2feebb	BKDR_SIMBOT.SMC
5cef55d975c5aa687c55d9ce308d10ab444b0a3e744b01235d0353ab2166c2f9	BKDR_SIMBOT.SMC
5f80c0354abb5bcde65073b41fc21262dc331dbf8d6240861e1efcb9d054397e	BKDR_SIMBOT.SMC
5fa3162254f8e4ab9d3eaa144ada231b4e8a9ce93f2f457cb4e7505279222ca0	BKDR_SIMBOT.SMC
62b07e79cbd06000fd9cc9ecf0cb29561fc1065c84148870658aa6475e157039	BKDR_SIMBOT.SMC
646d4021d5d06f72c931e67af064580927c7e9c9efbe7d91299edd562c235d19	BKDR_SIMBOT.SMC
65af7439797f5cdbe0863acdac946cb52e362ddbda9bba83fd8cb05b24befa73	BKDR_SIMBOT.SMC
69802ebba3dec1d7302235a3745b4621afa0bd98b5e6e5587b7faf4a1853843e	BKDR_SIMBOT.SMC
6a7f94fcec7b8e9d0427ac6a16ae34fbc674a2eee20490df71dd0dad5d59908a	BKDR_SIMBOT.SMC
710fbe29ced3eefc787c9374523064a908f09d42feaf9de4a5d0c502339650e4	BKDR_SIMBOT.SMC
7290f53c9dce1a820415a6ef765f5c9a28940b2e1ad5bae84212e60134878d89	BKDR_SIMBOT.SMC

73c8c96c37140caa6b0967e42abe609515cebc28fc0cabfde2245d48b5ec9ef7	BKDR_SIMBOT.SMC
79a901667518f91deb39f867f13d4ec9b72959adf282109dc6a73eee620a97d6	BKDR_SIMBOT.SMC
7a899cc4bedad4243f738a1cb398c2c926e8cf818596c4a0cfdfade94094b20a	BKDR_SIMBOT.SMC
7b02c9eefffbd9d444a2d190e72633aab4916f448291a3046839db3c164d6ec0	BKDR_SIMBOT.SMC
7ccf43c5c4d6340fc570919e69305accebe8e7d33ce4ff2079406e8f7915557e	BKDR_SIMBOT.SMC
7e7c553313d3c551a329368a99954d6c71e423da0e8532f387d7e62622649323	BKDR_SIMBOT.SMC
8a9af4a3316027123e0dbd1173c7c7d2a23a9310a3ffb8c430dc7fab6c91bfdd	BKDR_SIMBOT.SMC
8e091ec9b5d6cd6f016f19c1a0c0db353ec84383541c0dff66f492bff42f1295	BKDR_SIMBOT.SMC
8f89644a48a700eb823129d6031aec00ade5eb3e15c37f98dde5ddcc20053698	BKDR_SIMBOT.SMC
90a81d21ecffb854e4461062dad485d88e855aea01b429fc946a122ed093bdfe	BKDR_SIMBOT.SMC
943ffd9f42c2ea1bbdd31b375c6d06e740303dd88df6b1d296c198d6d2dfd737	BKDR_SIMBOT.SMC
96693077bab7b230c1d5a8bdf85f7d4f42c2f0866b49d09f3e7f0d0d62a37d06	BKDR_SIMBOT.SMC
9b9cb6988f5e610b4c2c3fd9bbc4f1e6167355e1afdd1192fc5408239bfde688	BKDR_SIMBOT.SMC
9ca56280e5b22bc4c0a43fda4ae9b5695fa5e246c6c32bb4ca9dd6ba9af93eec	BKDR_SIMBOT.SMC
9dc429d6bdd6a71eb55624fcd71ca71164b651f4a22ae807a6984cb7ae9f3be9	BKDR_SIMBOT.SMC
9e1e5689182d520655798f243ba6a36ce5e4a073a3bf7b48ff7d5fe1c2af9b12	BKDR_SIMBOT.SMC
9fe8d71b38340707ea856c0f72001b3593ad0dfb317847367ffbdb552610ed38	BKDR_SIMBOT.SMC
a056cf0833d19273a1fec72a2741800f2132f69fa9f8ff7405bc3d1b1fedb2d9	BKDR_SIMBOT.SMC
a0700618a376a887e18ca1711aec28b61bf27a1cceb942ded51c04160f8817fe	BKDR_SIMBOT.SMC
a19cd249f245da5af90e942c05fd038b159d49bcb7465b4342ea94e8fc79e79a	BKDR_SIMBOT.SMC
a611e14e3f7e1581976104568be0e401ecdd27c97b6ac2c63e4b7eb99d847081	BKDR_SIMBOT.SMC

a8c6b6f544c68478c238498883e174bbf06522522e7f4edd641c393990e4eff8	BKDR_SIMBOT.SMC
b14604d542fb8cb6540fddbf70c50ddd609ffe931286aab4ca7a9b29fcf1bce6	BKDR_SIMBOT.SMC
b1bf95f5d9655131a61a6fe9240f609246f5e07358b4f4e0ff5bc45e483a5dbb	BKDR_SIMBOT.SMC
b40309679096718e79e66e0d15f935a6147919074e18e32a8d8c2d627612db51	BKDR_SIMBOT.SMC
b6e4ed4dc008b345f7212d42a36ac8d0114145f4b80b53b67aefad5ee4720375	BKDR_SIMBOT.SMC
c0b99a82464f2cd66dd00977a6d29c23d643d4e9658c15c98c3233756f37cf82	BKDR_SIMBOT.SMC
c0f25400e8b0aa963cc1ea6850c89b808dee4a1bc1bca4171e87fed34f198320	BKDR_SIMBOT.SMC
c3b01e6dfdd6b46e1eb57953125613ee03f61e1f99526ccb268fdffa3a3b9390	BKDR_SIMBOT.SMC
c462bc933b92df8c7af6d4f5237410eb6e329897709629ea7b4e6060a1fba143	BKDR_SIMBOT.SMC
c4718546e8f5880a8196ee9e8f52d2b713e77bc61785b7c6a128b1ec94922f57	BKDR_SIMBOT.SMC
cac11b33c7b204b9fec27e4dce9713caa08a26beca0ace93af737421f3b0202b	BKDR_SIMBOT.SMC
ce8ef8c85cc5ec214bd3cc2cf96d7ece76ba97bb67d4c60aab9ff95f37d66508	BKDR_SIMBOT.SMC
cf234b987e831b8c5e7022b1113dc0f058a4e52d1e84c69d3f195d5f33dec21c	BKDR_SIMBOT.SMC
d284967e02c30e13b5a12b5b4692c43d86899b4542602ede20817feca19e69a5	BKDR_SIMBOT.SMC
d2e00a345534792422c5d1805b11eeb526478521993ce91e61528f5afb995473	BKDR_SIMBOT.SMC
d558071a11ab6ef532be6b554b50e0bda6f7de98e9f721349dc6c9ff23c49c0b	BKDR_SIMBOT.SMC
db4a81b234d90bab880e73272fa901bfaf155aaa417b74ca261504d6892d85e9	BKDR_SIMBOT.SMC
dbc65e23bf55f0c2eb42d0c356f0b21d49b5ad10860f0e0ed944298ca8d0e07f	BKDR_SIMBOT.SMC
dc701f277309f7747455d6eee3662d25fd8c81e84d7f07a4180295f71f610c80	BKDR_SIMBOT.SMC
de6f078d7dfa87f843e480c7ceb76228026506997f9c810b5b274b76b98cfd51	BKDR_SIMBOT.SMC
deb2d0d2bc35f319f1a2f8baca6517990474d86022c00e184780b0ec03b6b9fe	BKDR_SIMBOT.SMC

e15e8e7164dba2f94e50b0fc3b3716993584d7347e5ba881a900b7e1e78c7825	BKDR_SIMBOT.SMC
e1f19fa71f02fb4929ded69c0ff961018d81790219dc3dbcc6f1c1bbd50fa51b	BKDR_SIMBOT.SMC
e5379c8e1a2f0565f9205dc8748969423eae54f89d798082c3d6d2350e6221b2	BKDR_SIMBOT.SMC
ea5e96544ef954f485b843eac5aa2aa09e4d46b4c7baf1c44dfda644a0e9e0df	BKDR_SIMBOT.SMC
ea6b421a38c59e83420580ecd62f35fd7a3fb60d805b942b9cea5b42a6dfaef9	BKDR_SIMBOT.SMC
f060ad8f6ea8bb9f74fffdd73537a36233f4af463b67a476f4384af5c6cc6857	BKDR_SIMBOT.SMC
f0e34678fb0b3600590bbe475098ad6ab64f89610a4153706f99f17d91adc9dc	BKDR_SIMBOT.SMC
f10bdad7d9dba7c855a21813a69eb52c8928a8701d6edd0409fca8f14477b4f6	BKDR_SIMBOT.SMC
f52df15f9f53fbc6902ab41912bb97d87202c4f136289e26c75bbc7ea8ad12b9	BKDR_SIMBOT.SMC
f5877af9d1e0c3776764b23e5de93d26f8772b73c0030499f850f918a693a0f0	BKDR_SIMBOT.SMC
f6af1ab0ec9b013779a8dc7aa3056d2a5c85a9cf1e16a060e3c187b44a5ba271	BKDR_SIMBOT.SMC
fca971b3c2c152cfe33853c2c8a95e48599ff5e5dd1be709ed5706de7acf37b7	BKDR_SIMBOT.SMC
fcef47342b46b3e1e72ac83a14dd665885f730296d1459bfe3c344972ae5724c	BKDR_SIMBOT.SMC
730fbfeff815dfbb1f98d118a0ddb21ed917d9da83c43de59ea23fa48fb6dd3f	BKDR_SIMBOT.ZTBE-AA
3b1872f03141d10694cba05b23c38575813128fdd459dad70036e14164b4ac12	BKDR_SIMBOT.ZTBF-XT
9f534ee24b64fc083f5c911e05202dbd84f9c797e646a22c4defe25ee34ae850	BKDR_SIMBOT.ZTCL-A
fe4692365557df36c86bb316561b346ba3fe5f64fdece9fcea975caa8d040fe2	BKDR_SIMBOT.ZTFH-A
7276cb1049f4c9db89b1d830881859809a152eb38915cd4ff85e9037d227227f	BKDR_SIMBOT.ZTFJ-A
0338b661c89bdd77cac82ca474fdedf106059cec6e3feb0f83bd5fa5aa564709	BKDR_SIMBOT.ZTFL-A
507a0ad7798518240f50ec5dedcdf6db8ad169d262e0c2a504f2a4f069fd5c6b	BKDR_SIMBOT.ZYFJ-A
994a7e805076953f19e1a7b417956407d311643fe4cb71492541595508fa6a64	BKDR_SIMBOT.ZYFJ-A

c111cdadb08c53f7c5aacf21ab4829c736018c635ae3cdcfaa99ed14e2bd2f15	BKDR_SIMBOT.ZYFK-B
12b8d52392f9d66ce72ae72d749ae6d10aa253d8e0548207ac7d15280fe7fa97	BKDR_SIMBOT.ZZXX
f8b5175fa8a236c233ff354e5a4fc77933654ee3d4182e2ac0cd4bfb33b4d2e6	BKDR_SIMBOT.ZZXX
920d6fc64f7ca42c0b15038d9befa459c750d28e67ad8eaad2441fd0532b2fdc	TROJ_AGENT.BIFG
2a87fde7baf66a4fbfa9003128cbb287ac6cd0c1fa4de516383a966fda7b8cd8	TROJ_AGENT.MARA
8d9dd4b1053daeef665b46f7e01d5452e25145737d75fd992556d2751111cdd4	TROJ_AGENT.MARA
fcaba4d2bd3780f61939830160f4c8e07a0ad77397cd98675e601186335c89a3	TROJ_AGENT.TYUAL
5bd19b11c9269f34524190f27a2c3cd90a0f4cc326c521821bfc47b97c15d825	TROJ_BUZUS.ARH
fe718e425c32c0064558901c5cd70938d7e78679ad01f3c36766f9066b96cb65	TROJ_BUZUS.ARH
1d6ff45dbc1b7b31feccce0ce19a4f94da3a03714468fd9fa2bdf7accef483c2	TROJ_DLOAD.EOY
2e1c5b7f6318cfb5bd4d9b50c98097da6abcdc347fa51861555323db2274b415	TROJ_ELDORADO.AC
d7524a39361dece117446308649f6c0e4c42b7a7dc6f61334a0cdf25fc25d178	TROJ_HOOK.GO
0a7e8fc69499516f4525d6a42e132335ea38da1b1fc15dbe445a93e148310d5e	TROJ_RUBINURD.AC
1c30bc701552dbe832108c2a44baa3668d26685049a9a56bc442608963884a28	TROJ_RUBINURD.AC
4ea21dbfa314b0056ba29d4277b4a4bc4c6fddd0a44e721d9777a12a435ac54c	TROJ_SALENI.ZTFJ-A
e37d990bf8f6eea879e44e0761062e2fc43ca36b7cf398f496e77aabe8eccabf	TROJ_SIMBOTDRP.B
fb67c121dd84156ad840feb3136ddce57487d3b895b2127f5e0fab20e493aeef	TROJ_SMALL.WRPT

Figure 4. Roudan hashes

Taleret

SHA256	Detection Name
7ba17e1598d4105f13ff946e24fcb85a534542fffd9b8490269ad67fcbc697e1	Backdoor.Win32.DALGANX.SMZTEH-A
c8e7545add6b2c92d411d031cc8581a8c7647ae1b7748a43e45dbc61f5791a06	Backdoor.Win32.DALGANX.SMZTEH-A

97ae60afef214a481e06fbe6eff903128c0c43703595fc8425ac68510e814bad	BKDR_DALGAN.AA
60e3c7799d139a0ca99dfdf875bfd86942ec24de7106ef4548fef65b67e9cbab	BKDR_DALGAN.AC
ec69324abf114870a06eb3b386963a321ddd5ce95a4676f2f455858593644949	BKDR_DALGAN.AD
6ce22f1cee0f00f43fd9f860cf16b35b7e0e0954d7cb116601426df651e20e59	BKDR_DALGAN.AE
a405063a86e1dde029d5f271657a48cdabd5eba57082f38a6ce674dd1bb084f5	BKDR_DALGAN.BAM
0c4effcfea39f9fc1649bdaba92485209cd80c4b1e164a5a1d8d8a193bfdb025	BKDR_DALGAN.JE
769e4d9489071cc2bd7be784ee133b9e1092683c8949d60ea5c8f0299a2ac05b	BKDR_DALGAN.SAG
94f84853ed7d84db241489a305e78cb0950ac6a04deeba53883c183703b35f76	BKDR_DALGAN.SAI
ab440245f05ed74e5e6e164b6e955b1fb78ab67403a316ef722ff2898280c0bd	BKDR_DALGAN.SAJ
09b4a4ad613f88d9419df7cd1a590fde5e1c417b192bfb3734798d2a494102b6	BKDR_DALGAN.SAO
e6be801913c5843ebb0ff9a9d674f0defe2afb19467946fdf413d537f6cda09b	BKDR_DALGAN.SAQ
009904358f39cead7ffff292adc9c56a60c8c502fe831044b6afccb0ee84e208	BKDR_DALGAN.SMZTDA
03ffb0d6ae5dccf1941b98417d234aaad52ffb9558989a1a977c09ac7aa6491e	BKDR_DALGAN.SMZTDA
1642bf9539da2b8e48871242f1163afd539eb46aa5c52a02f955633f199163d0	BKDR_DALGAN.SMZTDA
1bc118712e1eabd22ffd7b1cd318bec195f754dae9e55196a7d1238fc65f0f9c	BKDR_DALGAN.SMZTDA
1cdf65b99d9f0752bd2765299bf8a5db8716a23e6012e77db2f2294298502d97	BKDR_DALGAN.SMZTDA
2215c3f6b42f4beda0752264db78178531e4ee4f72a86fc8edfca0d0e656d7d8	BKDR_DALGAN.SMZTDA
25feccc6067558357612aa20e73a11efca4c8437686ed5d88facd66ec488a171	BKDR_DALGAN.SMZTDA
2baf5557cf1aefd32dafea2e97595fa7f682e7288029bc627e5b653e721030cd	BKDR_DALGAN.SMZTDA
30964541572f322a20b541e2e5eedaa5f20f118995d4b9d4c5d5dda98f09f3d2	BKDR_DALGAN.SMZTDA
368bad8e955b426695f2ef051d7754b219c8c38b82d0ac850fb0413aeee641cf	BKDR_DALGAN.SMZTDA

37ad186caa2e8e88deb024d3166ed30be4e899170ca63f413750a987edc4d3f3	BKDR_DALGAN.SMZTDA
37b657d867bbd4c538f0b41b1c4a086119e7abcdf4037d62b5a5aa17e2711303	BKDR_DALGAN.SMZTDA
3dce21de09775984d6944742aa485c4dd2518daf1314523ee5b22bbe014b5033	BKDR_DALGAN.SMZTDA
463c628655ce128656c77488c19cc0cb01ad4522aa16b6df0f4d71e6c066868a	BKDR_DALGAN.SMZTDA
49f652be494a104a903d98c46f0fe9face6c70165177bbc4fb7eb88ad36cc06f	BKDR_DALGAN.SMZTDA
4d0f04b76bdc5386857086ccb222038a1f23d9362881959d13f7abc08a53e5cb	BKDR_DALGAN.SMZTDA
4f2499ceda4c9c37d372250c78db8e028f04cd4422418104137942a1f9933cf5	BKDR_DALGAN.SMZTDA
4f3816408715aabc9391b9cd5859b4811cbbbdb0412d91d48d111c55dcfa7b23	BKDR_DALGAN.SMZTDA
5377ddf1937326604bbf436fe3064ce281f02e427d71a758085f925f4e80af43	BKDR_DALGAN.SMZTDA
539402f112ea2eec1651823d7f61aa0bb379dfa528af400d8abb9ec3ef6e8a94	BKDR_DALGAN.SMZTDA
54e480314f5f74182418706a8c4e8be58545080a9fbebed4a9a4d3059f04e61e	BKDR_DALGAN.SMZTDA
5af5daaa201316a3273a7cd90b64b7a73a5272a46657ec50e8b48737de7c8e09	BKDR_DALGAN.SMZTDA
60831743228c2187f6c0ab966d4cc052b5bf618a05cf8582c07a2bf9973838e7	BKDR_DALGAN.SMZTDA
676c3e018227a127e291f8cb92b8d56d82aed4976640cf7f23121ed102bf7685	BKDR_DALGAN.SMZTDA
6c1fa67afa58d3ba859629fdd832d020af50e34bc35ca978d24fa63e3b117bd6	BKDR_DALGAN.SMZTDA
6ff6109749baf7c0b09e10bbefdc68bae2446e784ea986a90b891deb4e2bd31f	BKDR_DALGAN.SMZTDA
726c175e724f306a8a564d44869717eabd603ec18db96349e3da1ce8e0a355dd	BKDR_DALGAN.SMZTDA
7a8e464340f01dc109f5f053d333cc3a44e847c30d80051eb2ffff79aa7e2f3a	BKDR_DALGAN.SMZTDA
86dfb07a1de0169561f803cc163210159c76f926d58f6efc653365058907b866	BKDR_DALGAN.SMZTDA
89362644cf0e54fa53d07d13619c7cf2364088512fe792cd5f9c67aa5e6e2da5	BKDR_DALGAN.SMZTDA
8964c7f7989f6240de3d0cf1625ada2418325ca68b01ca444b1a391cd17f7039	BKDR_DALGAN.SMZTDA

8c5549d23127f4461a843b22f438aaf14fb127feba6c37fdefd3521d48499ed5	BKDR_DALGAN.SMZTDA
914f1b7831c01e517aabd262ae1d0284699d43b6786512cb9f7b192e4d672435	BKDR_DALGAN.SMZTDA
91d641349ebed6e2a83c5974097cc51d28d2bd9538af975c8674099f2ee67a36	BKDR_DALGAN.SMZTDA
95f487f0542dcfaedbce371cdd39615c7ec07d33dc28fae656aca3c94f0f09d5	BKDR_DALGAN.SMZTDA
99d05767b329c4e649e131d8b5598dde00c21520c6dd5baaa8632b530de9c5ae	BKDR_DALGAN.SMZTDA
9ae7d4d2702703fa00b9c476c84c0d1c07e27c61a78c9f3baa05b26ce624a2eb	BKDR_DALGAN.SMZTDA
9f5f2835cefec3130f764f27ecc9368d327f949d6a7ba24526f85f5357845d6d	BKDR_DALGAN.SMZTDA
a117568d5cd1775a68b8a2607c1f69bc99ab7cd5caab94cf5cfa1d89909804ea	BKDR_DALGAN.SMZTDA
a3dfde00d288fa9deb506b14e2f54dd12f480b991ac23f8b5679b60661046e2f	BKDR_DALGAN.SMZTDA
a7fe8613d80f9fd8aa5ed83cec6955ded3f47d67327efd2e9124fea8d7682eca	BKDR_DALGAN.SMZTDA
ac0d24fb32af27950b6a608a2ab28ff6080b1a36e2d067131ecef888e4b0e2be	BKDR_DALGAN.SMZTDA
acc0262fb07599972c5198a33ece75d1cd5189858c205238bda05a886c4bf392	BKDR_DALGAN.SMZTDA
b3bc1aba4e7b766fb50b3401629ebf80f6120a5d0853d5d7091e6a6d379b959f	BKDR_DALGAN.SMZTDA
b53b0d6d83af0002f9c63cd2ffe51d9494b587a73470ffc9c9b3da93f826522c	BKDR_DALGAN.SMZTDA
bc2d7c6d57a7a71dca9d48261f48363bbc6c629defe7373407b794a6dcb87deb	BKDR_DALGAN.SMZTDA
c4577a1005744208b83dc8fea98f661a6333e46db14946bc01bf51a2039a6249	BKDR_DALGAN.SMZTDA
c4e070cf74f8de6d2651d7901141a837bdce08edc82b0d2f69e6be1795cf0c27	BKDR_DALGAN.SMZTDA
d13e0284e5ac5c7067884545f43deeff5caa86403b3c0e5acd5cf3458d2d9633	BKDR_DALGAN.SMZTDA
d458fe4c822b81ca83db6841488b38e2cadfc6135414317b0edb3e1dc842b731	BKDR_DALGAN.SMZTDA
d7e9a35fbed3f3bd6b40e84a0aafbe181fed57f701719224a935479e9cf4e18c	BKDR_DALGAN.SMZTDA
e1c72d403f385f256f8ff5893e62b4475df776d40d80997dbf6d9ea4fe9c8099	BKDR_DALGAN.SMZTDA

e56aa1f7d8b31c6b8acbdd82a31e948672e9b3d7970ac330e52aaf3d5e5c9c28	BKDR_DALGAN.SMZTDA
e6f9cad3ba751add05cc876d1336def308d866d823d5c5da070e0ff369f9eb01	BKDR_DALGAN.SMZTDA
f1ff86e3321c39ae876e32bc75d16b9b678368b5f7910e199c2d707c07275b6a	BKDR_DALGAN.SMZTDA
f45f2e643a96a62ad9249aad8df4939f1b370f7ecf3693584b0e2d46a2579d84	BKDR_DALGAN.SMZTDA
f5089c03b6ff9285de06003c30bddfab4bf22656e70c5a195eee9e5a7b2fedd7	BKDR_DALGAN.SMZTDA
f5f6389b73e2bc994c96678ef827b44f2ad6d6e939f76305dac6033528ecc502	BKDR_DALGAN.SMZTDA
f942a91f201405333e9b6df428c001d2e9f05ca8bbbe3eb8a4b559d4807a53bb	BKDR_DALGAN.SMZTDA
fbdf672eaadba929d374b424387ac9a0da62f7ea46a98c4980aa14b45a62d3c1	BKDR_DALGAN.SMZTDA
0dba8ea32f49bd9a50dd0b0f3ea8c2d3e0927b8e2db7690de1cf6c52055ba181	BKDR_DALGAN.ZTDF-B
11d83e880a61d3b5ece6dfc2931e7e0b30fd617dceb666a2f57a25d4b8a84d64	BKDR_DALGAN.ZTDF-B
2da23cb9de736c04445a2468c3f052941ab2cc4d21a4c27b6df5f78e8be1025a	BKDR_DALGAN.ZTDF-B
30357345896a2403b07c24b71f6b4d318718cff73a04bcecc8072b4edfc045c6	BKDR_DALGAN.ZTDF-B
7f6b40a3f3ca68fca859fa44d135f110cc6525baf01ce1674b3c02e0bd5c66e2	BKDR_DALGAN.ZTDF-B
c21c5160d6f1f24b69e4f5fa1521ba53376dc9988ed843bfbe973cbe2c64804d	BKDR_DALGAN.ZTDF-B
ecf45b1540e99d8a5390240e7a23d3a401e8a5f67de4ed71de0be58e50762357	BKDR_DALGAN.ZTDF-B
baf66aacfa61c3987bc7edd9141f0157ee10a7af98addfd51a0668e50e6f4a96	BKDR_DALGAN.ZTDK-A
e903952298e694e2becc1fb68e13fa4f6143981bd628cca9315ab92401a0b4ab	BKDR_DALGAN.ZTEH-A
a3baab16dd814f5f467e54cfda051cf6e823c40f15c7df0fa4e0717e2fbca6d9	BKDR_DALGAN.ZTEH-B
21e8191cdeeeb4cfee6dca2ad2e91a23d9d00e7f218a81ff8a8d17b4c4066dc7	BKDR_DALGAN.ZTEI.A
3a831b29e873fa77f1a1e1ff172aad2435a20cc1373efffc5e8ed59e8764651a	BKDR_DALGAN.ZTEI.A
596014faca8b4d8585d4028dbe05a877a6a9e2697c19508b6f30b4ee7cd1558e	BKDR_DALGAN.ZTEI.A

d0c76f91480dcf7986288bdac964980c13829dbd7f0048c08661faf8b53de980	BKDR_DALGAN.ZTEI.A
d6950cb80481c06bd8ea1b70fd17e7fa54377d8b755194421c99a89bc84294f1	BKDR_DALGAN.ZTEI.A
e31669f52c15b506a77fcf263613db295b2c5bf2db125467bb71720afceb13b1	BKDR_DALGAN.ZTEI-AA
e780dac86151fb47c50e4919a3909a412374f9ce345ca22fb388303d317d688b	BKDR_FARFLI.XXVT
414d093276aa5fab179ba07ddd2ca3d31612e117913c4f0e4ce88311ed561f5	BKDR_GOSME.ANI
837cc1294292f47d061034b81100d9d7581c609a4a555e10be5c6bcc96d5921b	BKDR_HOOYA.ZZXX
c46cbf38062e7b886e349b2b93f7f223ff50985a92444c697437a6353b63ba41	BKDR_LOLBOT.BA
b52a6fea4cb6ccce8ceaad9652f571efd4e65b1d964d5eb52126b7a46e6ade97	BKDR64_DALGAN.A
0967e7318fea7050cf6392c183a923933776dbc03713c438e6bf8ad3ef966ead	BKDR64_DALGAN.SMZTDA
430f9b1f3c4fa9991454b005c26be718e8c94b14540419014e6f43dca62fcf54	BKDR64_DALGAN.SMZTDA
46ed25c5010c2f66e4411bddc65a6c68ffe8f0382e5b9b56ac2da4acc77c3622	BKDR64_DALGAN.SMZTDA
d684af514ae00dec038002861b7ef63181162514b774d5ed333a569141ebd627	BKDR64_DALGAN.SMZTDA
e0683d0ee25a1a2c15aa60ee5056a8860c3b381f01949d9b442d943f7764f224	BKDR64_DALGAN.SMZTDA
e7d8bca6ae09f02ff95313dfb99c797fef06d7ed64649119a566e5a1eec89f12	BKDR64_DALGAN.SMZTDA
e7805e68d624322768c0e25daae47d0dcb292b98a8e2bab6c1657e08acacdee7	HKTL_PROXYTOOL
c642567d290130caff5d94f6f5009cdce1d80315e566a77b87648e736da8f6b3	TROJ_AGENT.HJP
8905ccb6eea80db8ba32db06bdd6b92cb0d729fb38655eaed30f7dcad03053e7	TROJ_AGENT.ISZ
ab3b8df66ad6aa96356819be02be06c36b2aa62ff45154fb0886a6a89996a195	TROJ_AGENT.JBD
b422674ca7c4be0cf325d2f0fa9bd7b503cde11fee455ec94c40a5fe42dace06	TROJ_AGENT.MM
fa35c4511e2123fbee77ccd6bdf2c745cc552335f6ce0a217698abf35ab64256	TROJ_AGENT.NMP
8356fa7082449182fcfb64e383fb0a2f4648e73eb1305c5140820a35a8a1a28c	TROJ_AGENT.PP

5f916f95b66ecd1f1b7cd03b7b7774c5ef8945a5df79655a137d6aea48e66f01	TROJ_AGENT.TYUBO
1a93cd42915b283e74f33b270604c304ba463de2cf38df17b9ddcc1ed335cae5	TROJ_AGENT.WCB
706b24c581f11b4a9235096ff9e3275e50df8d5aad0f0a67c8f9f8b96dc0c246	TROJ_AGENT.ZNES
86bb1f3a56a391198d31f93780cf561c69b3132dcc30e770e29f547081ed433f	TROJ_AGENT.ZNES
8c4cc6b80b3e6b9ed7e8b048c5e8a199882ff6aa8cbdc2b1434b8ebebee8df53	TROJ_DALGAN.END
7d804e554e3ce562cb5a6c6aa728fa36dc87b4bd1ed8e116b52d3f3c743a6f0c	TROJ_DLOAD.MD
795054f6c7db7d4c37a89d01b2ec5bbf72f99f145773110e1197ddb1f5dc494b	TROJ_DLOAD.NF
1e5a0cac80824907b46640a1b0a1b27fd941644c303538fc7c9bdf70d1ae532d	TROJ_DLOAD.SMY
3259b73facef39694a18ff6e6e03b6db5a5ef37324617b06c8d99ab8ef48bda8	TROJ_DLOAD.SMY
4ede2889154e9aeb2d2c918ad2e6f23966660f08c13fc07667f1a8d3bb56ddb3	TROJ_DLOAD.SMY
72af3cc0a1d287849c9681daf9a8a21cbb4368b4b7fcdd7fb0023a790d42263d	TROJ_DLOAD.SMY
81096a811f77af18675bd15865eac5972ceef62f2c8153ef767fcb4794d0b0df	TROJ_DLOAD.SMY
c1715bc798f9e2bfe9ce850cad6e1a4aea19b691f19d121a56269815e8b0756e	TROJ_DLOAD.SMY
177e600abd642af5e95fd52b4b8ce7e2afecf23d09acb6de39c7d87273698ac7	TROJ_DLOAD.WSM
8fd467e28f5ab78e7c1ef0e45addde1d73131a4d02515c9b7454449590d5378e	TROJ_DLOAD.WSM
b3cde3e0677653678e674988d0acddae04004b603d5a49277756588324db9546	TROJ_DLOAD.WSM
7f77de9eba924ee9633725507b82b1d94d84a8f4c415767265c016060643d998	TROJ_DLOADER.ADDR
482eef0297e850aaa10a2429936cf772df640762db9d147fddc3b5bd453213fd	TROJ_DLOADER.EW
65d04fc2588ed8905679c5b839cfd555881d55ee1e1995c856106ba2f64ef01f	TROJ_DLOADER.EW
7beec609fdec98ca7582fa1320cd77a546eb74542ab93fc760970baf5912ad77	TROJ_DLOADER.EWS
e672121f27eb8791bb1f6c11257ec6b8751b7b98be40a7acaad8dc42c6f11348	TROJ_DLOADER.VTG

6d544e42ac1ec120b73d10c90ad9af9621ac024dbd608088969c3c49043ff3bf	TROJ_DLOADR.AVN
839cecafb3501bef33b30c0f90df1631c24b291f9088a4c283b5881b3a62eedb	TROJ_DLOADR.AVN
003faba86e864355000efab5c96ed06bfaa38603acb3bd669646dabacf0dff55	TROJ_DLOADR.BLK
9f1479ccd34591906ec2b8696606e7a7b2ff3f88bd5d9a7f95fdb196c36fff68	TROJ_DLOADR.DMA
7a6b871b785c13e4f4876ba333d9d19fae8314ba5efb9512a34aea9e9848ec03	TROJ_DLOADR.JK
3406ab8e86cc524598a536e7f5603370d193a48f7fec628bf2e70bf9c44c55dd	TROJ_DLOADR.LMX
70736e5cd45c204a187ec73016aaae0d76bd12651cb1baa1673f7a48095c5a92	TROJ_DROPPER.EW
cfb0cc7010c583cf652657af4d1bad802d6f3b6d5d0e3e2884abc44c540cbaca	TROJ_GENOME.BDY
55f42637efc98a945abbcc6041f4589037077fe3a9e1ee356abe205d2637dbbb	TROJ_INJECT.ATH
a057a634c3ff30ab30362db8257163cb7e424769f82fed0c1d75cecd66686254	TROJ_INJECT.ATH
632a93bb9aec0be340c0605049dad4f6f6aa73977886ca1d49d0dc6389d65aca	TROJ_INJECT.OA
cc7e51499a32e991568ba07f5e7041741c7f0cf0919f31ffb30b37a91cde5e83	TROJ_INJECT.OA
c4ffbe21a3a7bd08734bf6918ab26d427e88265d42e575e1a8f10be48d1a42df	TROJ_JEJEFYL.A
538a00e9ceb92c0832219edc92a030d55ecf87ab404726a55c910906999e78cf	TROJ_SERVSTART.ZZXX
e1501fed8f404d4c4fe703e9106183f44ebaa8f394a8bca4c0378529a8d7f364	TROJ_SMALL.KZV
50961457a4105a4de1262a8aca010320f80b0ede52431d6e229b3280582670ab	TROJ_SMALL.WFH
82fcdffa3ad1ce142bf7d396ded876173b81ec98b393873b165455e8650b4282	TROJ_TALERET.A
9089c9197dfecb21fa934e8301ec80815fc86c50da30ead70374557c3fcf2b31	TROJ_TALERET.AP
d8b0e46b8cb9a160805bdfc6c30e59ee0e2d029a47bf1dbbe5cea171fc011654	TROJ_TALERET.AP
e6f5898cfe4f869902c91c1fc60c7f0b8cec768d3efa4f7930598d74f7406d89	TROJ_TALERET.AQ
5dc6bcdcb5174003357209f81b2b8002b47cb4ded4468de82ed96b0811dc9d9d	TROJ_TALERET.AS

d60c7dd03a0b4f4e82d910ba19966f8783ba10178a1ce2466b2382cd025d8754	TROJ_TALERET.AS
f58bd224cfdc5cf8fafdb4f244f7cfd0f9c6ba40c4fc3948ab0fd7aaded7ed1a	TROJ_TALERET.AS
135480c9551c04995aff76a1a346a5e6a9bcc00981eef43b67e42dc26c114051	TROJ_TALERET.BK
81367baaa42db2645e321d7b3e20f1de6e31e063c23be3cfaa6d63019b9a81bb	TROJ_TALERET.D
e12600471cdde2a8101687d8b36bd35d0916324f332d01bcdb22a4f844485513	TROJ_TALERET.HU
c66dcc63f3d48c07bf012489b109a11ff98d0739d137e2ed64d07880f4bbbe54	TROJ_TALERET.MJM
193330fb29b5d77b47311df7e5672c60c10b3dad60f5241c85ddf7f305220a61	TROJ_TALERET.USCY
bd49ff634c6e03742d9f35e2571e6a2fbf3a957350a0fc9e469f13ed83b2f5cb	TROJ_TALERET.VPT
0bab6a3ea6de936ecda37b4363c73c04bb578ac87fc2434781b3012c3fba463d	TROJ_VUNDO.UJ
f73db24a6c257d6b0a00abbc013658fd7fb88d3f07edea8d5c1523631e5c7fd2	TROJ_VUNDO.UJ
8a09725f28227ce177f66708990405b130e469233b3c0ac903fdc4acb7e0b21a	TROJ_VUNDO.UJJ
815398ae450035ac7485aec281a7f3bf2524b9c7ad99173322de459411c08c6c	TSPY_ALOT.LA
0caa0446ce05b491bdcb651a1c68ba864c1ebe65117f90e5146ed9a9f00677d1	TSPY_MAGANIA.BM
15d340bd241923cb58a768f6941bf079f39f85bb4f256bc2b37babbd3f110192	TSPY_MAGANIA.BM
59410a5b110f6a538591fa0ee7b674a77936d128db10063ebb72eeebfb9f44bf	TSPY_MAGANIA.BM
5e613386076ec188bc0a646c8bdf3443b28db13ef577e25da9cd5c00e1f88f2b	TSPY_MAGANIA.BM
66e2a5a432141675f6a00e1ad66986d697280c0023337f3053c5818d7987fb8a	TSPY_MAGANIA.BM
82ba25ac7f8123d681d968196fd5d189a0212ca8c17148c52aff50a03c3c4bee	TSPY_MAGANIA.BM
f2e2be15a72bae626425627bba35b279a8b9fae83b72f85a5d7df92ae43178bc	TSPY_MAGANIA.BM
fbd150cc00e24929bffaa3dcade63b8ef9da8ffabe658cd23a6a5260c525bc8c	TSPY_MAGANIA.BM
744ae842efdd80f89f620b72d51bd25b7a7b37122759bc554f3b0cfe9a71111c	TSPY_MAGANIA.JKG

4fc320557610e6bf3dda2fc29f4a52e8bc967653e99eb26c3667c8daa57d4878	TSPY_MAGANIA.PF
5e81288cf1985d37bdd275f49efd927c605e3d7771c22aac6dc80b8718fe3ad8	TSPY_MAGANIA.WB
d91567341a26556448a991b0b8e3f395c9f60f672e52ea6cdca0983c2444af9f	TSPY_MAGANIA.ZZXX
07db7603d2d27a08553d2864cf2bef3c9515635e0f8692514f42c1a0debe8eb4	TSPY_ONLINEG.ETG
233ca6a3eda97e3f9cc7856af0d86d340696ff7503418ad2948cf8879389c0c9	TSPY_ONLINEG.ETG
37adb950b9798cdc5e13a47f48d3a9045f90e7cbd579a36b204d8347e2213efa	TSPY_ONLINEG.ETG
41305c540e04db6ccb9f2375c93b409250a1c626e59827f5aa23b56c96b21f32	TSPY_ONLINEG.ETG
4d5171921213212593af3bd8a46d634642c00b53a6703b2a8f86214f960cf3ec	TSPY_ONLINEG.ETG
54fafdf56f44d2bed0d97524e13d1238b3e35a919652f795ef9de0e63d9acf8d	TSPY_ONLINEG.ETG
9c273b0e1ec222a7f384e509088f5b0bbab6c958f3852181c6fef19379c66458	TSPY_ONLINEG.ETG
c4c0927cebd695393a5417f4b7ca1804ced604a8da2640378dbed2694066bb80	TSPY_ONLINEG.ETG
dc5d02bdc825af40e0d41006c37fdab829fafaa9897656a603172737a51782e6	TSPY_ONLINEG.ETG
fc0d31376fcce0822da0aa6823654ca49766584e9ad3a1d255013d39af23da43	TSPY_ONLINEG.ETG
fea3ee89538b846bac59b42e020fec9f7b4468f21af583f54b8e5aa3bdc4a330	TSPY_ONLINEG.ETG

Figure 5. Taleret hashes

TWTRAT

SHA256	Detection Name
f3d388a07bae0113624ea9a902766089ecdbcb0b07d8d59cbe2a31e858359ad1	TSPY_ONLINEG.MC

Figure 6. TWTRAT hash

Specas

SHA256	Detection Name
df774e92737e40afab2f3049f55ab510362303a6e7a0314e0e5269c3ba630b7c	ADW_CLICKSPRING
00ea65f5124ce361ad9ab628f99681fb0428b9058bafc2ca38cc082eb93965c9	ADW_PURITYSCAN

18ad6621aafcd9a781a622c8eb4aa71cabcad5d527fd98cee4e82c72e8e36b26	Backdoor.Win32.SPECAS.A
24f359b93a7bba75352cce73041f7afb55f50678fb1c8ea7bd6a9e74a6eda998	Backdoor.Win32.SPECAS.A
eb2d91af4e3020eb4eaef23d55bc882905e06f85e07fd21bffc93a7d56c783dc	Backdoor.Win32.SPECAS.A
ed8e06bb9e8771fd06090f44cc15e3ab5a78a6ee7482779db8d36728ceaaa0ab	BKDR_AGENT.APLL
30d06ef11fa3605154cdfeb43d38d96213974cb33600fca7ed18f0a6fe673823	BKDR_AGENT.SMB
3bd69eda223299022bd9ad511cb03ef1cb9d486015b5c1fe356b2df8572867fe	BKDR_AGENT.SMB
778dafa4573eea3787980df2c85e9b7840ac039e2b2bdbafa7188d0d2bcad04d	BKDR_AGENT.SMB
b5c74a12a29533797fa3b641566a5a855c24905282847dc3381a7dd405405fbc	BKDR_AGENT.SMB
ba87072731e0831b816f0fb55ff7e9862563e27be4e32648cf1d64492909d8a1	BKDR_AGENT.SMB
22f83791448e7e8985fcff249fa5574dde17e4f70bf8bf0f66e0d9d854033920	BKDR_POISON.WAA
07514f5341a081b70c120e30965ab2b121126644f43f77429a8d80ebb2d4827d	BKDR_TALERET.SMZTDBA
0b538c35183ae629a2ee1f02f3b85e37fe5a9721fec083bf746bae6f1a0fe31d	BKDR_TALERET.SMZTDBA
0bafb65c02e302192ccbd47078b2c6a68c743315f7ae5b8cdc2ce09da4608938	BKDR_TALERET.SMZTDBA
0f3a00e1492a6604caf08a40ba7c4f179581d68a32ef526a4414a1d95bda322d	BKDR_TALERET.SMZTDBA
0f3e87f41ef699e4b20d3531fbfb2c0c2d67a5e5f473b5a82530ddf09034d0cb	BKDR_TALERET.SMZTDBA
0f402349b8b67031915e11829c7afa9c8d35184863453a5addac441fa72ea833	BKDR_TALERET.SMZTDBA
127ac818747bbec2f8b4f820199565ebd9933cb01202524a7c1609a07854c72b	BKDR_TALERET.SMZTDBA
1292cfeeaabe5515255fb456dd991500c3fe4618f7a2ac97b7831006c07cba97	BKDR_TALERET.SMZTDBA
285ee3ed6df17bde2b661cefaa7b84e7e6ba65f517922876453a34e1cfb161d3	BKDR_TALERET.SMZTDBA
29e3375fd22da536004f76686c76a1aa7cd19c19a1b71d73d7cf0841c2d76832	BKDR_TALERET.SMZTDBA
2b783d8e34cb630e5e04372d8450493c068453b524bb55f0fc3cb733d7ad5cbd	BKDR_TALERET.SMZTDBA

2bee2273779454fcfbd89ad051c95454e003a39557d6739052b21ae267c6afd9	BKDR_TALERET.SMZTDBA
3aeb27ae9a260b7d8306629957cf023645d20f4054133924dc33271fec1f23ae	BKDR_TALERET.SMZTDBA
3c352f4e3b9f5bfcaa2195e4c422f350015e8bf1c2ca41ac673557adbff14317	BKDR_TALERET.SMZTDBA
3ca83694ec3584090037de695fc7dcbc482f673a59c1b14f390f508eabea9552	BKDR_TALERET.SMZTDBA
44ec7327ffbb2d88e5fe1c289f394b830b7a43e004a7e4ecf7ac5f6cd6825c74	BKDR_TALERET.SMZTDBA
4780379eecf48f8df026f753152c536edc2ddb722f041dab3592c41789ce5b42	BKDR_TALERET.SMZTDBA
53ee5b09954ec8eaf19fe02c71d750b838b761c49f7dcf992cdafb8c6b5ac997	BKDR_TALERET.SMZTDBA
599d4a6160efd1827c13958e724a2e22e03131ed4069f912afb559a572f33a74	BKDR_TALERET.SMZTDBA
5c0813a748b21373224d08b76f2203cabc4a6c8d1d3610ab9b7f05964ff032c8	BKDR_TALERET.SMZTDBA
5c64438acb8b9edcd547c12297ffb85d3fdf12de521d1492e189b98e5b1e13a2	BKDR_TALERET.SMZTDBA
6002d2288211846d1d370f36542d8c3cbe9e748746a6443efba17fcdb2bb9f72	BKDR_TALERET.SMZTDBA
695bcce1aaeabfca5c2a7bfdb4d8cdc84d4c29d4f8c1d969d08a66bdc8babf8a	BKDR_TALERET.SMZTDBA
6bfe6d101e5a915270ec2071632190fce6f35cf54b96b1b16a4fdf932b38b46a	BKDR_TALERET.SMZTDBA
6d032f10165cb18fa5c3495958d07946dd79ad2810d8d8074c5beaa366470d36	BKDR_TALERET.SMZTDBA
6e36109fa58eac24dec72deb7bd2a3bce457cba6e60bb905839b1163dd1cd823	BKDR_TALERET.SMZTDBA
75891bc0e6e00d4b5808cf1ef5ca3ff6d6af2910101cb3554177ed677f90399e	BKDR_TALERET.SMZTDBA
78b16ef73cc39c068c6562b8cd4c849ff513b5b7441a396a9e1a8ada9298be7f	BKDR_TALERET.SMZTDBA
78f06504484b6144ced9c72ea70044fab6ee93d690fd17bc8f849c01ac109eec	BKDR_TALERET.SMZTDBA
7ddf09bc7889a37aa078abdfea68b1f5b476fc78814349272abc41dd5ddd03c1	BKDR_TALERET.SMZTDBA
860753a46489de8471e08e645864ac8c56204afdad9146fc03e17fe0641541f5	BKDR_TALERET.SMZTDBA
8d0c58b712f8d8d4a2a27dcfea927ee1755ee424d249c8f3806fe42461f4e518	BKDR_TALERET.SMZTDBA

8d40e6326a4f8a46b84dac3ed7b5c9b777c6176aa031d03ae6ff28df55e7e768	BKDR_TALERET.SMZTDBA
8e19f1ca3ffd4a11603618910efa414436fcf93897ccd435237d1bb9a0cfdaf0	BKDR_TALERET.SMZTDBA
949fa2daf4fc77005928771de21682a2a614939bade99c369a3d90fc01fa4cdb	BKDR_TALERET.SMZTDBA
956752fcaae5468725ad7c8005d070e5f07cdcbe7f43c29e783a7325acabd199	BKDR_TALERET.SMZTDBA
962f857a0ee759a208cb070352132d15feeae8a9626759d10bc6e66003f49a35	BKDR_TALERET.SMZTDBA
a2f97121fcabf4ab7817dfb333326971b59b68648c6e887817b3c94ab35574c7	BKDR_TALERET.SMZTDBA
a5259f43913a925282e1438d779e045dc4d9d41d44a2f942b063f713a1dfbe36	BKDR_TALERET.SMZTDBA
aa2f82b92bad6cb859d3fbc4a9143329ac82b264b04346c0e90127ac146539cc	BKDR_TALERET.SMZTDBA
ab473bc425bfe909c4d50ec9af72e499eede0add1cbfbe97c3443dc93d647b83	BKDR_TALERET.SMZTDBA
bb2a104c20c837109e3d5f2a345c58c6f3af24784a3ac9287c5487d9d3ade3a0	BKDR_TALERET.SMZTDBA
c13fc95fa75bce698d061ea2e36272a575298cfeb0418c9208313b1736e1dfcc	BKDR_TALERET.SMZTDBA
c3cd31c3344d6eef95e7bffc80d8484db3c496e6752d2598a3c962f1c35e987f	BKDR_TALERET.SMZTDBA
c75ea8d16392c78689fd4b4e0aefc0101fde5399e8f437e1b1466ea3149de5f0	BKDR_TALERET.SMZTDBA
d417177bc46d2d5a7670687ca5699ff531e68d8bd0182a47b76d95d182209e77	BKDR_TALERET.SMZTDBA
e190c784cb2d7c01259bd03ccdd5f09e1f3a3b75c594974959bdad3c8315e3c9	BKDR_TALERET.SMZTDBA
e2a2cbdbc76c0144d9fbefefa3cc5d997b08e6eb51918172b04a5d3888103252	BKDR_TALERET.SMZTDBA
ecdcf9b5658980a2c0ac60b6f249702aff76c61f57210c3481d85c2c95bbc7dc	BKDR_TALERET.SMZTDBA
f059b1ff8ebe652dac9d9eccf40f5d327fde796349adad43c06f1fbd8c16266a	BKDR_TALERET.SMZTDBA
fb52d9caa3d916e36612ecf74f681c5c8f7e4fafc9cc22d1c726aa763e670d3c	BKDR_TALERET.SMZTDBA
fc024a74fa73a9a1f461d4130a29b2f952339cb7944d171e12514657f5660a03	BKDR_TALERET.SMZTDBA
0242790889318fbe982789115d4b7b7f92aff192acb3c54e55d1579639e9b510	BKDR_TALERET.SMZTDBB

059443bd373bb5bd62ae7f84337d2e241f21012f410e8cfe427c70f1d7020d27	BKDR_TALERET.SMZTDBB
0b2c57adc91ce52d25e0293c0dc5ad9c2c7c16ab29c9f5a837c2bb3f657e56fa	BKDR_TALERET.SMZTDBB
181d04085e15e65467c85dd2bd0a8e88db7bc15ba39a9f6ac3e915237a9e778b	BKDR_TALERET.SMZTDBB
19aa16d1d797dd541904ebdcbfdbdf7a864e1f8b1685f1b7379cbe97945014cf	BKDR_TALERET.SMZTDBB
1a4e0c95a03902e28f280f1f38ae29117a5de916832e9ddbfdf3f39421eed82d	BKDR_TALERET.SMZTDBB
20301b57effb30056ee6125415400527df59aabf25f955ea27410e3ceb0711f8	BKDR_TALERET.SMZTDBB
2329b7d1f5d9ba3306d5171c80040b42d04479842a4b6266ab1d612a190a18ab	BKDR_TALERET.SMZTDBB
30861ca664b32a7641017cecc037d0e9319301466bd1ed12cd6a4efeb04cb6ed	BKDR_TALERET.SMZTDBB
3345c174d03563fea17d4dbbf5aacadae4a67e47e33101febb0d8993b3e81000	BKDR_TALERET.SMZTDBB
356d28991c2d5c7f0226230d800500f3ad2ce36c38efa07504250b9d5423d8f8	BKDR_TALERET.SMZTDBB
3bd6ea8a7840aada36eace64564779aeb259ca56b4cdd7e5e35c5281d273a84b	BKDR_TALERET.SMZTDBB
3cfab73ec24c4170e945021ffaef46d36117b9f9f47c5032348f20a0a3101f5a	BKDR_TALERET.SMZTDBB
47a0743d488850ce6619fa629e0437e305c21b4b1cb6c85549904b0bb9625ea1	BKDR_TALERET.SMZTDBB
49bcf172498570fc9f9c044e7e2eba56fcdf9532ce00dc881710c4d35c6bcd74	BKDR_TALERET.SMZTDBB
4bbaa2efb8b9bc582cec70ebd795b95893cdc43ad31c2161ad532b59a513e91a	BKDR_TALERET.SMZTDBB
4f928b31517540aea534c154b60d1cdc19e3f2d6440647f500497e7349813d1a	BKDR_TALERET.SMZTDBB
4ff0e9ab0c54b4e6da25580fb3dae809835479834645c7fd1288e189b04aad6f	BKDR_TALERET.SMZTDBB
4ff3b664dd615dec4ce58250905d67421f641c0b7705ec062d66f98ba6248c0d	BKDR_TALERET.SMZTDBB
533c5ecca0003a11371995246ec590a06000a774ec17ca2b91e2f38a68dd0f8e	BKDR_TALERET.SMZTDBB
661d4ad933a24d761ed5b7a750055831598941bd5f3ca6d448a3b610b1774aeb	BKDR_TALERET.SMZTDBB
775b4e0f9599d10b3cf811026ab6557c7311aa106ad1fc0959a13492a1eb755d	BKDR_TALERET.SMZTDBB

82c548c5c9ece18817abfc2fa4386a593e5f82315259c7a18f8a6123cdf0e301	BKDR_TALERET.SMZTDBB
8644deb557e0a304b1e895ff1c3ad0400d06bca11f42c9493cfc70119e11c075	BKDR_TALERET.SMZTDBB
8b54aa71f8a6b4ba70922128ea19cdcab941a4f495b56da2222c35d32c4ff897	BKDR_TALERET.SMZTDBB
8ea30a3001edffae388cb62f15645d980cd6116f69ff68ae3caad231594367a9	BKDR_TALERET.SMZTDBB
910b9c343cb051d816393e8292a010833a924240a75c3648b3964365e436f5db	BKDR_TALERET.SMZTDBB
940397834d269a87c2f31985e5933b21d38fb004744187cc1d9fecb3377e8238	BKDR_TALERET.SMZTDBB
9b686f1ec6549e5acca6ea19be7ddba0ec86bcb9b1a9dc5ecc5a8dc537e11db9	BKDR_TALERET.SMZTDBB
9e1f9d60325147f0ce9b2b217108eb3ce53def7e5feacd27a1da3667f19462df	BKDR_TALERET.SMZTDBB
9e8058fe4f65ca7f62fc76ebf31b9b4af2437d5c8145cd88a920beeb18233286	BKDR_TALERET.SMZTDBB
9ee29153f4bed6291a424fa08c029c6e55ed1bc1fffe22978812d9418c724e3c	BKDR_TALERET.SMZTDBB
9ff6639285ecd792bff3959e6b8390827f65f613fed501975005765290cffe0d	BKDR_TALERET.SMZTDBB
ac53a0d148745ad9a2d02c0decf74d8dadd9f50de8473426fb23b0b35beb71ff	BKDR_TALERET.SMZTDBB
b65ea1705425d60a0ae4543bb48e65ffbf31168bcda50de2ed9bdf32354c1c89	BKDR_TALERET.SMZTDBB
c5791fe94685e12551f0ba4bfa776b846f764fcb7b2a5c51fbc870072b1bea83	BKDR_TALERET.SMZTDBB
c5e88bde66e0c1bcda45e46c302a43d9bb802d60552784f8b9110a8b0910d9d2	BKDR_TALERET.SMZTDBB
cd9bc61e851d543acd04545dde898252b5a973086c9e6d2b4abba3d334916cc7	BKDR_TALERET.SMZTDBB
cdcd3061323a7df57bb86a2a75b36228fc59eb44f048c3516c2f94fe80b029c1	BKDR_TALERET.SMZTDBB
e0734636e1edf0863beb684845be9afabfa6e624de10856148878263fa51cbd3	BKDR_TALERET.SMZTDBB
e4c07fcb820e95ad11ead2ec3683609da5d278145cdec975affafffacbdce6c0	BKDR_TALERET.SMZTDBB
ec21f7cb32909719582bd8fda16cc75f2243fa3e1c0cd5c043f4d0305b77db6e	BKDR_TALERET.SMZTDBB
fa26e7c75b21e5187160400a410d9fac418456f5a025206046d52d584b4acd93	BKDR_TALERET.SMZTDBB

ffdc1369d6fa4a8cbb286fb731892fc4389f9cc5627106515f220dae95d5a4ee	BKDR_TALERET.SMZTDBB
1d0244ece1b340f09bb75592ee392ede7c756ab45d7a3d7f33965a322e22aa02	BKDR_TALERET.ZTCG-A
12f2f05207f1b936584f105f8e719a78385b6e93e1766ec8b02fb454b16e94c7	BKDR_TALERET.ZTDH-A
0b03a9661b0b48d6243d128684e952d7e5f510a3e4797b8e9b1f173e0b349178	BKDR_TALERET.ZTGG
06c5d4aa21e6b816147430d3b7d883a04190e39860a93ee44f1ecae31de40ee4	TROJ_AGENT.AVEM
0eefbe7df23550ecf801cd4759af6bf4bdd95601034f7d4447237f8fa7dd4aa5	TROJ_AGENT.AVEM
4c283e13cb489a0d35a734a948a0e24b060ebfe9a9b940a7f41d6f433c6a5375	TROJ_AGENT.AVEM
633c736758406471d28e87ffc1cb1deb197478c50b134eca29b28f51f87f91ef	TROJ_AGENT.AVEM
1a847d0047a1339a048dfcc5e7a24bbbe17f8adfcdbd66d3691d740d4e33327a	TROJ_DELUDRU.J
e53a6ac0a5318339e477a8828b8dc702bca7a16aa9e3506ac8a662b9ea92d38e	TROJ_DLOAD.VTG
a19b4de507a8b25e2ab733a1d02a16bc1eeb34a5b5fd2b21d7da2cc4bcb55bba	TROJ_DLOADER.AJ
97b9477c5ea132dbca49e46044aa862a9148ff0f466c535ef1ddd3b1a86b8570	TROJ_DLOADER.VI
43175a9a59cfdba46e2fbfc443b529c66ba1bde370b8f254260013fa104eaf40	TROJ_DLOADR.MM
1c0c1fb1d823c1343480ecd38bdcaa0dc83fbaaa9700e293c5b56506de69fa70	TROJ_DLOADR.MMM
26fb841b5c4a06d7227ad42612559c6361a641623acc7139c5a3179701776395	TROJ_DLOADR.OX
b879273d48abb57be9e708f64ea9e48b30d33783af008f67506f4de7a0f77cb7	TROJ_DLOADR.TPL
38e588150244c0adfd7ec5293547e4c09bb706399a89caf429d288c78edf6cea	TROJ_DLOADR.ZZXX
2e9fb686202a53f2db3136ee6ec094b584772abe110d1c97a39e02ae7bbe26b2	TROJ_GENOME.SMBW
d3bd276ec8bbe5d6d3fa7736223a4d82d45a6ddcb4974697b7437827c55df3ba	TROJ_GENOME.SMBW
84b495d14989f86ae512c0b316c1c12cb69ea0a9f7c2650ce06114b6c6d0710f	TROJ_INJECT.CFV
1c18d3344e9666b3185ff4d709dde9416a8bb0a52bc3522a4deae73e68181103	TROJ_TALERET.AB

6360e70bdc1c52838c946d47d64b938f2aeb8ce06242265e3822301fe97089ee	TROJ_TALERET.AB
3505f46a3222d2ae7bb727d241a1b5a925b31d80876a31881b5c9ce41fb2e759	TROJ_TALERET.AC
2f3c5f2e9452456dcb9d7c19573d4c93e52979ca49878a5c640506c96e6da539	TROJ_TALERET.AD
5b936b967cd232e0005e6217c1d8bf0628f59a2921b2ce8c7ddf8c35fab2bd11	TROJ_TALERET.AD
e0118399ec11063f086a6573a00fc2c34bbf87a8d81388468defd5b01962b3e9	TROJ_TALERET.AD
6f23a8c917ef1400ad868a024444909d53ca3a0c86deaf98fb807f4edde5a474	TROJ_TALERET.AE
92db9c18adad2198103f953cefff43e7b77475f1ecadc762a2d5b877d221b091	TROJ_TALERET.AE
03267093c6037b4171ba0681f092386b29a1c1c7986f520bb6a3641df259164e	TROJ_TALERET.AF
e0be71252e0b03bab5a92ab9c162775ec9f7967fef295e84ba48c7ced4a6271d	TROJ_TALERET.AH
2e31890f1ba1c003542308c16ead3cde7cf529835e537fd02da92e07bfe8cc31	TROJ_TALERET.AI
45708e13dcb673c4dd24e339da0bb0f8a22d0805c89f7d2d301a71ce288b6ee4	TROJ_TALERET.AI
62eba79a07cc7a5b1c8d082510c22ddc1610e127c891fd1977eac50a053e8cf4	TROJ_TALERET.AI
be5bd174a0fd9e0936f62196177b71f3c571ed56f1c01ab3afc17b3080ee3c82	TROJ_TALERET.AI
c3c25a4fae27a99fc0ea801f704e5a452ac7f0f9c70f540bd52030646c61ec1d	TROJ_TALERET.AI
7fdec12503d95caf47a1d4dcb4f864d6735454a89334005fef71d1505b9ca906	TROJ_TALERET.AJ
a2f8a462809ac39ea879c2ddcae14e7a445f9ac79bea2f770f5ed4ecd1daec8c	TROJ_TALERET.AL
6299fd9c8233e5a894f0de226840c9a89ec5c811c48843bb6e29d2d10d8e698d	TROJ_TALERET.AN
cb28e7456cdc88c54a600bb287d737fbf46fb3f44f0390074a037f2441566e0c	TROJ_TALERET.AR
0673826b3b3a0d1a7cfdf93dcbef1d2530a0105f8b8665bf3f22b7605f929d3b	TROJ_TALERET.B
3e1dcac323dda24ef06c98dd0bd9e0d2165ec398fec52a7a8600693fe3fd5c95	TROJ_TALERET.B
8fee68979f91ef958d1d0163dc723929f8b5538da4347fbb5ade78d8e063d80f	TROJ_TALERET.B

96c530f1c4a62d8e3dcc182e556613191f973e1de7dd92bfa1a65284a340728b	TROJ_TALERET.BH
e69c9a5376383292e6ef60f369a3952ca4466433dc694084a51c6d96a8261565	TROJ_TALERET.C
0cd36de5d3b463a758d9ffd8fe7efb3b9d4fe9ddd6f36be447ee921f9d386dbf	TROJ_TALERET.D
4964f625a5feefddd9bebd1e07a0c5ba4266bdbd755cf619def242d80c673381	TROJ_TALERET.D
72a668fe9b37c3fe048e8aae4e96c47eb485272c8686974f562a2f02ca1becb6	TROJ_TALERET.D
9d53fff8dd18d2cb3f20d334a6d97613d7893d905d258748389acfa1bd37c2df	TROJ_TALERET.D
a96f7322f0fbc5c6c1d05eb6bc0d5e7cde9ee870c0557bda025bba8f8957f06b	TROJ_TALERET.D
ca378f7d64ccd2c66fc9484569bdb74148c1be41d0dc07765840b4093df992ec	TROJ_TALERET.DLR
0b00f22628edfa5063b53f8253831bedafc421d8fa42230325de363d5206dfea	TROJ_TALERET.E
5ebd79f40893efac8d3a3c166071b1db913c7bc91a75c3073f20b69a4c859455	TROJ_TALERET.F
64c783b6e4c31a7262d0d4c30566a017bdd6e8a5b1b9e3fbc7484323479b1784	TROJ_TALERET.G
4d38c462449b16a2e2bfeb01f27c82bd524842d4208d456bbd05c58e5cef873f	TROJ_TALERET.GL
62487b300235c502ea02a4c1e56a26f4173e15839e490e976153d7e82f4ea28d	TROJ_TALERET.IK
eef70077638ffbf3ab6d0807713055e7373665e23e7ecd7a8f64f1fa525bd527	TROJ_TALERET.J
6e49218ed534f7f7a1fabca5ff2eb183eaab1016573fa93c8009d124767d9ef0	TROJ_TALERET.JDR
1452ad40f42f54ac559f21d44fd5ac001f870f013333295a2729e06388f76b88	TROJ_TALERET.MJM
f2aee055c0434f9dc04c981b0bbd5f45a41b618fb282b186832a04ac83397776	TROJ_TALERET.MJM
fd968accf691098c4967eed3f27c23232327671f661cff746b8a55de36c12a84	TROJ_TALERET.TY
7090ca773cf9331acf30ccc15e82ce454303825a0df9366dc824be3a379503aa	TROJ_TALERET.USCW
68265fd59e5b54a67065af4f19d347ff2a427713b4bb0aa94d50088d6025f1a7	TROJ_TALERET.USCZ
d3bc2c2d78f66be48f9fb06d5aa3020f2ef38d6e5fd630193febae063bf9b70a	TROJ_TALERET.VI

c3afcfabe2f45a9aa44930107bcd5c09edb1cdeb447c8f742b299ff0c75af5b1	TROJ_TALERET.VQF
17616504e6d57464e1676e61295900f162d594e2b6d21f15add18665a98454d4	TROJ_TALERET.VQN
2da703c62bb752753c4344039b6db060214b6ef45412dc27c095e935cc97c42d	TROJ_TALERET.XB
b9e76a4278c5833422fe4b29d75bcd5856863b2fdea180f65250fa260b200bb7	TROJ_TALERET.XB
68c82c8152bc8f0040fad29dd666c5dc9e26811b9995de2614d8d1e10c07fe11	TROJ_TALERET.ZZXX
6bdd3aa1818801bfe08668cbdad4c89bf1c01ec5a53047fccb017d4cd0c1f055	TROJ_TALERET.ZZXX

Figure 7. Specas hashes

Taikite

SHA256	Detection Name
08a443c92507643d9362551ce2ad8cab855555e1a7cb811939877800a16c9202	Backdoor.Win32.TAIKITE.A
27032f1dd34ac61c7c01fee7ed966dddab2be93a2ea405277f4a3c36775a4fb8	Backdoor.Win32.TAIKITE.A
ace7840417641cd3ce2b2f2aadcc9ad59ef1b04b4339fc45879928d04b1f7078	Backdoor.Win32.TAIKITE.A
e3266a236f380cbe39088914828aac18098f767382f9f083ed4ff6b5fb191230	Backdoor.Win32.TAIKITE.A
e4c672007f9f6910ff7416a4cc4a25925bd641cb0f60bccb03762f9bcf67591d	Backdoor.Win32.TAIKITE.A
8e1de10aa317fb80bb1f287ac6b713d410b1548862b99cb67941acd7f3e0cdf2	BKDR_KITE.ZTDE-A
16f190fb22f3d252b090defb22c05e4a560a1cec72136c8a90578bfb8c742910	BKDR_TAIKITE.SMZTDE-A
42a1e657187685d390446983d4d4a2d944e7fe13379ede9a76829280892ab18e	BKDR_TAIKITE.ZAEH-A
50cd57403c3ad659d9bb7047b2aedd45373be1ddd0eebddca2f59c603bf315fd	BKDR_TAIKITE.ZAEH-A
579ddddedfa124004e6fdff309be7fab3148b78bc6671179429a6778241107d0	BKDR_TAIKITE.ZAEH-A
6cb999668866418c90cdf49be90fb9c79fabd8be4d3bde3aad00dd2470c0fba1	BKDR_TAIKITE.ZAEH-A
77e5b2aa26afd28bc440245b7b0b8b34e35dff25a5c3c523aca9187a3af37218	BKDR_TAIKITE.ZAEH-A
94a846ae4be29be5388211a4a9bf2c7d85c8390da786d7f6139b01272be1bb7c	BKDR_TAIKITE.ZAEH-A

b6e6c939b85c912239a9358f8931b87369aae23a4b72cf6434e8774317233d17	BKDR_TAIKITE.ZAEH-A
d668c1a5f9aad83e3ad213416e4940139de22125701731240e883aae3cc61a97	BKDR_TAIKITE.ZAEH-A
dc801663c60961f302ac9635e899d2c0f31af0a157b38ccef9c3a94574f398e9	BKDR_TAIKITE.ZAEH-A
32b09386f8b2483f500e55d771cce49a14534d2919c3e3ebc799cfb8cef52ebe	BKDR_TAIKITE.ZTEI-A
5512c51e1e93108a91f04295bdb1a1344b266e620731a0835575f87b93df3c3e	BKDR_TAIKITE.ZTEI-A
793f5410bb5ba8eb8ac7d7fbdb49296d4f48bbf657a5c5ba51c06a9ed69ca1d4	BKDR_TAIKITE.ZTEI-A
bd7f5e97f350e79fad6d283d4debe2066a8b9120c7549142288ab5f67056c9bd	BKDR_TAIKITE.ZTEI-A
922aed79664efb62bd2b95d93ccdcf19f85ab49d18bab747037217deb950f0f0	TROJ_AGENT.YMNIG
17b6db528f465106d5d48bb793a56eca4fe4eb26159cce56dc8de8d6c770fd54	TROJ_DLOADR.YYSVX
0791f9c111e1b7991c2c5388d3f67b0bb135db6d819f67f127daaa6a782d2730	TROJ_FORMERS.AK
cc3bd39e04a4a2728f7b1f20e805263240da32729cbd064df63e24be6869763c	TROJ_YUFKUCO.A
3ae94775697e0720e650c252f915b8be22e5e02823b5a88763519d513d8f27c6	TSPY_ZBOT.SMYH

Figure 8. Taikite hashes

SiyBot

SHA256	Detection Name
206f91560d5c78501d60275cf39a91e0b1789046bbe1e3ca3bf23681a7dbe1c9	Backdoor.Win32.TAIDOOR.A
efa7d4dca967a1be582a0ce90f68face7bd35117ab8c4ed8edfb327ced8f7983	TROJ_GNPOST.ZTGA.A

Figure 9. SiyBot hashes

Kuangdao

SHA256	Detection Name
0bd714b5a16690a5d7d6780bf1a444202f8d5aa263b5b16cdb89d737d9609575	Backdoor.Win32.KUANDAO.A
b4bc61c9887a446812fab5d48cc42de2c72f6dc9eb8fce1c9c45141151675cb6	Backdoor.Win32.KUANDAO.A
b62a3bcb6e8b9b5d736a9543e338770b93c68c24f19c375811e688975fa2364b	Backdoor.Win32.KUANDAO.A

de1b2afab58ba07ab0c65ce6627b5edd29e48e6d753f5739ae696625f81d65b1	Backdoor.Win32.KUANDAO.A
fdfa9d3d20cc8934f6bafcd407dee1e2e33d48f93b1b5d5d41b8436e04a81764	Backdoor.Win32.KUANDAO.A
1ccb3261accecd9dbb52467825cb63b5a7801380b8546813efe01a251394ab86	Backdoor.Win32.SALENI.SMZTFH-AA
23f1f2abf39c225d846795aa08889d8a6192cea7c345bcf9a36b15738ebc28e0	Backdoor.Win32.SALENI.SMZTFH-AA
565770e1e324dc0ee9597c8ab86ae7f5e6553fc5ef1b8de05242a17d1cf1e8e5	Backdoor.Win32.SALENI.SMZTFH-AA
5d0231e3f0378a6e1a791e5029305ae6e67bb513246751e4b5edc2f5ae780175	Backdoor.Win32.SALENI.SMZTFH-AA
8367248aa5f5d7e369d02386a794aa6fdfbf3ffae75b89b16edcf4afb3e44cd3	Backdoor.Win32.SALENI.SMZTFH-AA
acc047f91487fd8caf228c117c405a131469575ccffc54c204b43b0dd9524bae	Backdoor.Win32.SALENI.SMZTFH-AA
c804e554c676e46297e9c525ad1004934a4b90335c9807b7128b529cbf05694d	Backdoor.Win32.SALENI.SMZTFH-AA
ef4abba8b6580e37f105d055d831e2a17715d5edaa6d37516bd76d83e34794a5	Backdoor.Win32.SALENI.SMZTFH-AA
3ca978fcba2b847241432622f3301976c41a06026c983a2a4070bf8546421569	BKDR_AGENT.BGWW
302797470d400e5e15fa031d0b6cfa1455ca8f967f4e17a9a158d5df450f52f7	BKDR_AGENT.SMBG
7c6c5cab7aae2e445241237489130d80f66215f00d454c1d77d8c02fc293dadb	BKDR_AGENT.SMBG
c9582cc2f38f38cee24120038a7606ae667b8b8239d3a89cdee70b46e340cb2a	BKDR_AGENT.SMBG
af2c38b90c5eeb883c035cd4ab1e8cc1de2ba81dca31a561137442d61d1af4ea	BKDR_ANILES.A
5fff707b7cd9a6ecfe5d120480af23b1ef0f0d64db3b0c434b5c74b39841e44b	BKDR_GOSME.CA
a0967392651eadeb78a4fc654f79a8bbfc299e0708717c152dc686b50aff3973	BKDR_GOSME.CA
23501a7f2eab90ea4c32da1b0bea11120e4288899ecc55e0c43aee08ce95ee97	BKDR_INJECT.GJD
2b384e077d2888b5db7992818e4caa92471449d67dc54335607c15c7c8b092ed	BKDR_INJECT.TPA
dae5bca490251c0090603de70125e84f124abb2f3b5c451c41e1c7f44bc2b426	BKDR_MECIV.PDG
1c5c86fa4abc4721d2b3d57e94cb08b79105f09e5e9827cbe55850c4374cce43	BKDR_NALISE.A

e874a20ec3a67148ed1bcc9235e281833eb04f18e9425686b1356246629b7296	BKDR_NALISE.ZTBD-A
d3602f6a299b35bc7a9fe43a69922b9583bd35ec46241054757a250190030aab	BKDR_PROXY.SN
0820b8cec0b958ad91d0109f21086933ba73f2eeaccf59dd6a2a5bf87e9a38f5	BKDR_SALENI.SMZTDA
0a4a26f1eebf820e4672b5b6fa8ae9c7ad69ea2aebff5141056f937ddbfc2c07	BKDR_SALENI.SMZTDA
0bb58adc1a486cdc7b0c43b22f4878b31abe7987bc15dc9a90e437d40df96d8d	BKDR_SALENI.SMZTDA
111758ed8b2adc6aee49a3d121013aec3262f004251f06684270d8b5239b8830	BKDR_SALENI.SMZTDA
167101b88a7df8947dfaabc0bccf263b513cc4774a10a4419ad076c0f2ab3f02	BKDR_SALENI.SMZTDA
19c2058cbd8cbe78ad9c3a9e9e0cb478bf0639e6931e8c2906b5fd38b6ec2d80	BKDR_SALENI.SMZTDA
1c7cbaa397401a13995686f15e8b6990a0a1a4fe2d4e448b8e7f8bd1c19bdeeb	BKDR_SALENI.SMZTDA
20f6561b5136c4104157e87f1cc2e31199c6be154e489e04a82c28dd499c3f17	BKDR_SALENI.SMZTDA
25c0aa418125b3879c43d169b3ce1c042fff5234756afffd5c2baf153e8ed39d	BKDR_SALENI.SMZTDA
27749eda59cf1c8aa723c04c99d7131147fb1a14a3d6a02d1ce25fe8429e9f81	BKDR_SALENI.SMZTDA
348e35d94290ca25a2b7684e6aa1af0e8b46b0118b8a7c50e1d720bde925daa1	BKDR_SALENI.SMZTDA
36049d1b7176f3c8a16fc83d30900846a95764a44a9e90722f5315dffe610737	BKDR_SALENI.SMZTDA
38716d3548608824f1300392112800cc3a68ce5ef81df9348bbb049ee49941ad	BKDR_SALENI.SMZTDA
39b12a314ac792594e31a470a337793bf208159591ea3382f9253dd07399bacd	BKDR_SALENI.SMZTDA
3b50e9e8cfdeb778d956dd3c861d4ca7011021028b8394ecd91ef8ab68d0888f	BKDR_SALENI.SMZTDA
3baaa93029d2ab3fb73885f900e92679eb9783776ce8441dc5b98759a102b305	BKDR_SALENI.SMZTDA
4254a22000a8d03a5a0752b6eb1572a489468c789c9067b71391207548dd6baa	BKDR_SALENI.SMZTDA
48a410c40c0f990492d053691a20a3b0b52cbdfb36923e7667fd7dfd34da5d68	BKDR_SALENI.SMZTDA
4a588fc0033da02ce30b9de4c07592159e35e861b78c0fe05e0d370261b29204	BKDR_SALENI.SMZTDA

4aa1ed329869aefda57bfb51ed9efb2878366134065cbce61de80b82a7751863	BKDR_SALENI.SMZTDA
51a5285651ebb98a7561522f349a78afd4c69ade1d2c83fd8d2a727477b0b4d0	BKDR_SALENI.SMZTDA
550b4a36aaae8b44e563901e93c68c309fa66d8499be27f0b879a206163122f0	BKDR_SALENI.SMZTDA
5a6a4c3c43fde5d51c2f1f67f8ae878f6cee3b9dbd733043be66b7390a21e607	BKDR_SALENI.SMZTDA
5c601aa8b5e3c91212e6e91ec149ae40850f2e2f38dba5360bdc40c0a1f6aa73	BKDR_SALENI.SMZTDA
5dc27449fb69c78bcc3dfeb3e906df73cf5c9500f3149174580f8cb6ccd9c6e3	BKDR_SALENI.SMZTDA
5e498131cb7e55c68dfa13a0d3a1430f4d24b4353f4644b6d2af0bd3db7b70c2	BKDR_SALENI.SMZTDA
5f3aa4e64f12a83824cc4ae1ebaf81072714f92d840e64ff411fcca40fb42fd0	BKDR_SALENI.SMZTDA
6066d0075baa95ec442e6518f7040447cda3c6dd18e97df211e34803be6a3b63	BKDR_SALENI.SMZTDA
7f435b76040a290eea422509c9de13bb297b285da1b37018db1db85ccfd24b68	BKDR_SALENI.SMZTDA
7fa0a543a1b87d2a4fb12937a8d1858397d5b98aa4514a3ec2908200f80d3b21	BKDR_SALENI.SMZTDA
8a546b734adb0ce1dfa82cddfbbaa2005be98aef06d5eb2a1985550e15655d2e	BKDR_SALENI.SMZTDA
98a0902343359d5e6e19f37c317d227a748ba023840dc1db28ae89d743db184d	BKDR_SALENI.SMZTDA
99bc274074a69bbf239fceea24ff7ad41f4bab579bb0797be2be71a0c18c436a	BKDR_SALENI.SMZTDA
9e257dc0dea632b3baa93f7862f0f3a6d2dc2d0d0fa6ec23e386cf2b285bf6ac	BKDR_SALENI.SMZTDA
b2068aa91893a499c2753ae983d590f69a20f4f11d0e80aab146c0a593ccdf32	BKDR_SALENI.SMZTDA
b36e0214f193b6ebd217238b151ca5fbe55b6c129386eb60a66e90667019ddbf	BKDR_SALENI.SMZTDA
b8e9bd97489d1a802a1b04a5047429d5deb116aade0e4872c1859f7b2262c322	BKDR_SALENI.SMZTDA
bbe5e7f46b912084c908b48ef05e6f8d9ff316d79612b5cb19f3d0bd7da7675e	BKDR_SALENI.SMZTDA
be567370ba227a5e683d2538e5544c38be8aa9949070f58f2afc900189fe124d	BKDR_SALENI.SMZTDA
d0409dadec9016f257dbd8e5c98bdaf9650ebeb4016a5aea77d5284255967482	BKDR_SALENI.SMZTDA

d0accf74e93d4c0244d3bdc3abcf424050737e978a08c6252c3be8203acd23e4	BKDR_SALENI.SMZTDA
d96d577a5d507ab7d68670a5656fedb5e4ae268ada6d3953164dcb01df791e10	BKDR_SALENI.SMZTDA
dcfa13366b07caddf6a3aa387ad04b188c80cf033fd3443613fba9efc7aa9468	BKDR_SALENI.SMZTDA
df6dbf1483dacbd9f8de96a2ef4e29d9b81216421feb266e25d01eca224023c8	BKDR_SALENI.SMZTDA
ed4c5ef643296e4bd1e26145f3ec432fda8272600a9636d4d23976a568ffd79e	BKDR_SALENI.SMZTDA
f836c323c61c93eaa2dbe03b4a4c79ab6ec649fcb5cf26a5d0f3d43538c91865	BKDR_SALENI.SMZTDA
f8d0bc05e97e33a122e30d8f403f7b7aa3af1832b4bcb082bf53f63d06d73f4f	BKDR_SALENI.SMZTDA
01d93df48e53d39fb3f19bdb33f92683448d9b2241c06e410427d64af2d2d440	BKDR_SALENI.SMZTDC
038ec18444fe3b59ce245726a93c32e3deeddf69eb6ddf6189da91324af90492	BKDR_SALENI.SMZTDC
040837cca8a9a0efc723324fa8c45b6fd5e2433949b883ee7ae0b02add23b1db	BKDR_SALENI.SMZTDC
06d21f19b9d30740723105c0e0c91efa1db842bb62ec44d6bbad07ca5849e79b	BKDR_SALENI.SMZTDC
12dfcf92775ad2b393cbef734187c302930eb01053ba3d4f93029885370af60f	BKDR_SALENI.SMZTDC
268e2a6af5be69b550fbe4d4044a23b7cb97a9840d9b85cb14a0c144d15549f0	BKDR_SALENI.SMZTDC
2e368dbdd73754ae33cd5926639a51ebb54d376b62e67cdc41fac64aefa1719f	BKDR_SALENI.SMZTDC
39cd52a897cc2800ff9d8a2eb56ed0b72327ae49141198616a71424e54850454	BKDR_SALENI.SMZTDC
40ad817959c34f6d56243d189a60006ea2a42580b6087f19db6375f85e3f6ac0	BKDR_SALENI.SMZTDC
429df7d366404b13677eb8a993be49a6fba4e091ee6a4e4f8f538f6499115c13	BKDR_SALENI.SMZTDC
454b1b946c7a428785b21386876944f45951836a7b4b249762f6d77766b7f5e9	BKDR_SALENI.SMZTDC
46d6b1ef24225944b2204acbe5507cef21ae3e6b1a61c42430d00fb14f25af47	BKDR_SALENI.SMZTDC
482b3d5e9beb664d3ff71e2489039d653903cacf19f6ad6da4445cb5a0d47ad7	BKDR_SALENI.SMZTDC
5461c5461a2947d1fc3d1e6f3ee35eb783c0b51d46eccbd82c2f361c926351cb	BKDR_SALENI.SMZTDC

554a37383a7e64de3f226a65cd22c6b53f2f48f612146f32d89796e1d2de223a	BKDR_SALENI.SMZTDC
5fd2f74e4695adbe98df424acfcf1ab42dadd0af70b172596233339650cd3359	BKDR_SALENI.SMZTDC
6b96c12d10d415c5370d9881d037490fc2153cc7a646f40996e4e03c8812afd6	BKDR_SALENI.SMZTDC
6c1e7e549489ad3e2b782f25b5e94e501525c0ddd0e92c079adedeea1a53a9c0	BKDR_SALENI.SMZTDC
7163aa32aaee89daa7f0401ba6c0aebff513d094dace320781ad4c46dd3e874b	BKDR_SALENI.SMZTDC
8bb251ed04c7b35131458abd31e07862808f8d797e32b5518f7fca04cfff5328	BKDR_SALENI.SMZTDC
906cf2ecbf29b4b66210a8b64eec57cf3b1e65147096d5c2856f43178fcd345c	BKDR_SALENI.SMZTDC
93f42acd198aab3898b21f5f6ceaff2b00d204abf63447d3d816a342ef4b803d	BKDR_SALENI.SMZTDC
96e6ae4a8090933cce47738c171409d2db1d97489fbc32c3bccfae2fcfcd3007	BKDR_SALENI.SMZTDC
98797ce470be994abda0b04d4e9d29e8514f39ae4653de7f47475910ac6e4812	BKDR_SALENI.SMZTDC
99d030a5f63ccba6c2f6f1f0ddd50586b13da7f5f350649d018035b53d4a8d54	BKDR_SALENI.SMZTDC
9ca926c7fd06aa31ddfad5bdb9462b6697676bb5380073adb1970692dedfcf5d	BKDR_SALENI.SMZTDC
c33f4c4aba6e23d205f1ffbf8d6f2a2b20387a7ba99e2076e7606e8f5e95d9e8	BKDR_SALENI.SMZTDC
c3e596848fbc92f90c247ae0fc9289a20d37aadd0361a12797adee0d89059251	BKDR_SALENI.SMZTDC
c74db54acfc0c8f322fe5d895ed605f2e2ef6e2b403899200d14b4052cbf0e8e	BKDR_SALENI.SMZTDC
c9228df83785b6a51509a46a87433a4d53fbff0ac814b19e244082024d0e9591	BKDR_SALENI.SMZTDC
cc02727131f48f94263a50c0397e4020429537cf900074e7cc1f55fad8a4b756	BKDR_SALENI.SMZTDC
de468e58b31beab4cf5276f4040204daad44b3dc7520486c1b18b45d49adcd52	BKDR_SALENI.SMZTDC
e0972d926065013f8c53e342b7ef476bdf33f984f8dc7fa8336bced9811d2209	BKDR_SALENI.SMZTDC
e21151f6cbecd7bbee7fab9b59970205e4d679f21926812ae2648f3b61cb1f5e	BKDR_SALENI.SMZTDC
e50923dbe3462b7083e01d48fa2a6ae0026a8796b967b7992563d1a457fdfddf	BKDR_SALENI.SMZTDC

e5f3c3053da3707274b8e958a4b498f70f8a92e1beae74da5ea49174e255f898	BKDR_SALENI.SMZTDC
ec48a3962da18efca24c986d95e9d53092b4ba77b66122b442303b0b99396fae	BKDR_SALENI.SMZTDC
d68404e25c5829231a1f43301eaf267ca23ea7237300b3b108a02e62bee76c4a	BKDR_SALENI.SMZTED-AB
178fbaf86781c8cd81f03a945cbf686b95a2c8569dbf2f00960149fbb5ef04fa	BKDR_SALENI.SMZTED-AO
964c3e6a16dcda9d9b6c21c623884a23ee70c969e7f80f0726391e5bb8939717	BKDR_SALENI.SMZTED-AO
aab2168ff32b22c1cd0ada050e60b0544f52e2e592b77473499f93ec22658ca5	BKDR_SALENI.SMZTED-AO
bfdfe8c32d9987b8a2ccf35bdbdf6dc6e1386957228580b8457025635579f267	BKDR_SALENI.ZTDK-A
02dc47939e6e5f402a2a9f58b04c95175324271bc2aa58fda9f3a1cdbed86d9a	BKDR_SALENI.ZTED-B
0852b6431061b6d8f55626c06694ab3e3fe0e978b54ca8e017c6cca82bc7d7b1	BKDR_SALENI.ZTED-B
1a4e17fa21bb019deb808e286b024cfbe836d4944ad6b9421a9fcb6daa0fc412	BKDR_SALENI.ZTED-B
32c23dbea178ac63245f85ca30f1f8183501b683903324b2a05d37f5c14849ab	BKDR_SALENI.ZTED-B
74941b96c5a2e84e8e63d53efa97083e760a54b70e6bd9280287aa0157f39bc4	BKDR_SALENI.ZTED-B
7c5841f19740350d36a0644205dcb558003a58739d420d344e2a78221663fac4	BKDR_SALENI.ZTED-B
946b9e31986712501b7de9aecdb78b7437cb09b857fd14f2522b7b7eaa7fac25	BKDR_SALENI.ZTED-B
abaeb7eb649a87df84cd1524a98ae06d95886b123a2825171f4ea2cb34e13172	BKDR_SALENI.ZTED-B
b347d4c13ac47ad764204cf7b3e22e75de8c40ef3fd342a7115a3f3bb2278359	BKDR_SALENI.ZTED-B
b5241208e51de3aa0f84d353913bfa091ea0e7f4d54e07f8715a3efee41ad833	BKDR_SALENI.ZTED-B
d3f722b758d94b21ba53c161f1b50d69e106bd68f0ae632647e080a1132ec2b0	BKDR_SALENI.ZTED-B
d63a5ca223e0a39f6619ce947214af8894b0139cf2c31bc7f746f9dcd9aa8c36	BKDR_SALENI.ZTED-B
e758ed4c5eb0f74eff1a15805281aa91c73ecc190143aad771db671078541318	BKDR_SALENI.ZTED-B
ea1a147f010b34be6eeb076c6725c9e62577baa378673525f9698f82c187b1a2	BKDR_SALENI.ZTED-B

f01ed6ea159e9ab99d03ad86161bf574094e0d112909a7833ad1ddf72f4bec36	BKDR_SALENI.ZTED-B
54446ea074bfce42f13a46b62732358ae8e130ad3b6cf8e2051d704851f0553f	BKDR_TALERET.ZTBH
b77b3fdac66a5f711c7467f1b29bb37f67f9f068e6cebcd0359b09f901c6cdf5	TROJ_AGENT.AA
a1ce228afefee00f7e305ddb8c33bbb44f69acccead736891fa97e49702264b5	TROJ_CRYECT.AL
0912326d325f4f3d7026e6bd322bc872f3a82d5efdd9b82ec9651e0e2c21c44c	TROJ_CRYECT.BB
977dee964f775554738fb87418e331af2ce7ef931939b3c5f79b6136e0fdf01f	TROJ_DLDR.ZTBC-A
5e57aec7b56134a2cc2489e15fd2561bb96db2cf23e69cc09b35f1e39e193f6e	TROJ_DLOADER.DND
4f91ea42b0d9ee3e665af6f9f04561b1ede3a20406f66d20402dee8942548e6c	TROJ_DLOADR.CPB
34c1e61b72332360c45001cbfa47d1e0a08530421e93209d3b9d8cff2edfed1f	TROJ_DLOADR.GCE
0894ff6bb79cb469bc481e71ba822110118b6ea547b0b337380e6cc24480bbf4	TROJ_DLOADR.KM
c4d475cb21531dfa7171fa3d1dddc8681a07efffa7aa8846a6b8ce4f5240e5aa	TROJ_DLOADR.YMNIZ
1d26864bb5ae0b5664df39faf8293f49a72e7c329ed9a68ff03d9391de1e639d	TROJ_FORMER.AA
9a3b580fa97dcb8b16ed9f18c3213dc4fcd92e9ee47d2e548befccf03efbb2ea	TROJ_FORMER.FM
b6d5c90129c98e2738774d38d57120160befa4b76860dbcd0ae9fdf56ada8ef1	TROJ_KRYPTIK.YPS
c2f6855634e399c7de9182fc560a8d176ee70df14dcbb2f1c8d86cef018fa4f7	TROJ_PROXIFY.B
038b8634e6871b668d119349eb2a1aba9e6138f78b3d10cee43149ac5ed6e23b	TROJ_SLINA.A
a6a701ab7eb621c1236f82775b12a9d17f14a1ad83792ed26bf4c38543107609	TROJ_SLINA.BB
09f560225803aa5ffee478744838d6923e111077cce57ca764f625aac622d479	TROJ_SYMMI.AH
14c3a76fc4a55a4beb928eb0f34fedc6bb9d565149f57b0df14feabe751a3454	TROJ_SYMMI.AH
37927715ffd15e16faf4cac2056b298b3ef76c8969b732afdf01fa4a48fe6728	TROJ_SYMMI.AH
574ba01bce1d431a281129c27b2fd089bcadb8981ed10ca568d9cb46850591e4	TROJ_SYMMI.AH

85ec4e638591c4e10237a78f2a581fd7facefd1e6ce9caee5338c41c3a35540b	TROJ_SYMMI.AH
947149fcaa95b16ac9349012e75b20c4fc61c82d2278348c9130e1e2012cbf8f	TROJ_SYMMI.AH
9502a4b23e87b99e45196fbf418ac82d34cba6f99a8e37482ec9a35f80eaee69	TROJ_SYMMI.AH
a484d264916bfdd57631f15e987d8ddaae98daac5daf62a70081d12ab4fec533	TROJ_SYMMI.AH
a6c0623a5f293acc196eba2b47ca08870704c5538e4ff13c5d53875044129f65	TROJ_SYMMI.AH
b44a5b0a1884359164dbbfddcbd80d65d6109054f87bd848d8e57c5a733f6ca1	TROJ_SYMMI.AH
bcd1e0060875a94bddd8e162bf51175fd728651f8283705df767d3c28043347e	TROJ_SYMMI.AH
d83db7567063128d69cb2749450bd7d8e03904306f44c0d5ca031ef3af8edf7e	TROJ_SYMMI.AH
f0947559 5dd54d52cf161bf191b3a13cc180f8ef9e7e00380594338d79fde731	TROJ_SYMMI.AH
ae90dd0b3d80730a45d9b32d31664fcab384e5a345dbf224593fc888dcaac34c	TROJ_THEWIN.A
20590c554f441218e4731a89e88d048a1c144cadb6b464499e1097d7f88ff796	TROJ_ZAP.ZZXX
739da6117c75cc61c62bc87e149c9aa91e2b4d1d842d7c3ab7fb30a7a498a6ee	TROJ_ZAPCHAST.QE
818874b6d89560df7fd8449432cbbd0b5de6f6f49ee09b3d4cdc7432ef792584	TROJ_ZAPCHAST.RP
1403b3c9e9540c0f16f0c34d7c598ea44d57132b4d98226f5854530daa9b3a6a	Trojan.Win64.SRVSTRT.AB
b5a774b09b7fbfaee9b9e08efcec4d917b26c31a6a2ffab67fa8b4e5228cb7bb	TSPY_AGENT.XXTTN

Figure 10. Kuangdao hashes

GrubbyRAT

SHA256	Detection Name
0537f7e2c7673c74f78063696bf780fc2ee25724ab57737014a4d292af2f1a35	Backdoor.Win64.GRUBBYRAT.SMZTEH-A
48db856e8bf8b02cb8de18ce7e26b10a46fa5da5ec0353bf9aba9337826381d5	Backdoor.Win64.GRUBBYRAT.SMZTEH-A
4ae57448d2c3d8959833979cc697eb886d9683e6dd467d8296c04a46eeefc475	Backdoor.Win64.GRUBBYRAT.SMZTEH-A
54833b4ee70b9173ab1e166fa1d076de67586330b52ff21341352c05e79c1ed9	Backdoor.Win64.GRUBBYRAT.SMZTEH-A

d465340f83ba851873a08b3a02cc7a8ac0207d227ae954ea0518d0cb51819a0a	Backdoor.Win64.GRUBBYRAT.SMZTEH-A

Figure 11. GrubbyRAT hashes

LuckDLL

SHA256	Detection Name
3f5533b11899eeefaacd684a9d2d0682c888b7e0e8cb996045878c19fc1040a6	Trojan.Win32.LUCKDLL.A
35609aac28b6a4f153d1cb6a72af2c9287e16b853203b581e8533d4fae18dc78	Trojan.Win32.LUCKDLL.A
51f15ca72ff1afa8b8615d426dc634d6e853de82a3b127c95f3473efdb3094a9	Trojan.Win32.LUCKDLL.A

Figure 12. LuckDLL hashes

K4RAT

SHA256	Detection Name
d3e8c1a67cbb9a70ab5a2ef7701e786db9e3cf1a251db93a47c975433eb9ecef	BKDR_TALERET.AL
0efd9d90f4b917e157a76d90484f85ff2b5d5d518ad42398bfe6c0e1531a3d69	BKDR_TALERET.SMZTDI-A
318aac3ced39c629e2044210d3501a849cf1d07d62a9444834a49fb11687e42e	BKDR_TALERET.SMZTDI-A
661840ac8fa45afbceddf142b5500c4aada2df0af8f8c816854e7e28d1c1568f	BKDR_TALERET.SMZTDI-A
8f0b1aa9dfdb9e8c94839d4f9678a5048d807735b2725abf2e4d34265b8cc0d3	BKDR_TALERET.SMZTDI-A
8f3f3a74e43330bbb87dbc520976e5cf67e68ae86d77f50fce6f232cc8888a40	BKDR_TALERET.SMZTDI-A
9ad19d9f3fdbe9a8b2e1ea5d9c288d848a65ae58a7e528bcb8f184ed9f401efb	BKDR_TALERET.SMZTDI-A
e4907f0a83ea2dbf0f8033eb98aee1b588c9c65036cf0230ef351a53867d0127	BKDR_TALERET.SMZTDI-A
602befba2ff4aae4cd6f78cc6925d8ae6ecd3fe9bade4e2315d40fbc9fc067e1	TROJ_TALERET.USCV
a9b8c6dcc7840eb829d2b871c586015a603934645723635e81638f96c77af076	TROJ_TALERET.ZTBJ-A
05e5e1b1b54444c37c6a073a5bae407bd5b5566fed20c01b4fb6ea23aae2d1cd	TROJ_VUNDO.XPBG
2a5c95aa32ffdb31db1be222c13fae51513d5290e22a7927cb63ce5950244cc3	TROJ_VUNDO.XPBG
7b06ffc277e270a18fe07fca669ab10a4cc1dcb29c1b9009dca7e2edf882d4dc	TROJ_VUNDO.XPBH

d83d2cd4a9ac1d4cb0c149020cc1d8604fe36287ec382e89f122748eeedbcfcb	TSPY_GENTA.AX

Figure 13. K4RAT hashes

GOORAT

SHA256	Detection Name
0f4645fa0ad08df3d0fe65f15650b11f68f2af0727d2e29f3696ddf652fe173a	Backdoor.Win32.GOORAT.A
554c7de344a9675f83856190f69c02b90ff0d1d2f08f0b3ef5ea66b73ef62c34	Backdoor.Win32.GOORAT.A
7a06814cd0a33aed11ef477419ad91065042c9de656d758543e51888dd5e1d5d	TROJ_DLOADR.SMDM
87fb725f8344081e81275c59cc7d7ded3d81d94e9efbc2e0edd4b0f7f93fb854	TROJ_DLOADR.SMDM
3e1b3f1201915cd70e8ca03a86bbdea4b415cdde0bad309e97dd236ab18543a8	TROJ_GRUWT.C

Figure 14. GOORAT hashes

Serkdes

SHA256	Detection Name
2bc7cb139ad0581a6e7e24bd8add840d929192900523a831502baf829e28c3fb	Backdoor.Win32.SERKDES.A
66dfa8425a6df33f8278c6b3ae0fd83b49ec493a781f7e0c02570771e534edae	Backdoor.Win32.SERKDES.A
6922189cc78f1c591b709e51ce02529309ec9edcf29d24a3c189c10070137dd0	Backdoor.Win32.SERKDES.A
890e10dce2eaa0bf89d2b6fc73133db2a042281f4613a7c0f2ae9fff293251c5	Backdoor.Win32.SERKDES.A
1757b1aafc119cfbabc6f25fb24cc9222728abd9c158c6c5fdab68e54f587664	Backdoor.Win32.SERKDES.B
20294a1ac0d51f2e29366bec9961283b85904210bff46084713274e119d35a20	Backdoor.Win32.SERKDES.B
26e0f7a46112314b0cbfa03cf548650d418cdf377bba5c0b57efb54a6bdb5356	Backdoor.Win32.SERKDES.B
3abe390c63340f0ae0907000a9c430348f4e35cb77d2e398625680ba51672a7e	Backdoor.Win32.SERKDES.B
4cf04dcc02f2f2cab2065e220401cfe55b451913fafaaa18593e18849a17a0ca	Backdoor.Win32.SERKDES.B
5888b026ab7df42ed32d53038e9b8541cf272f0010385694e2ba28e0454f14c2	Backdoor.Win32.SERKDES.B
ea48a7d33f2598eda29e587da28c523914b12fc6dde5fa04eea8c8acbf3fa083	Backdoor.Win32.SERKDES.B

e24e0ee355d56a9e55f3993a9694ab25cc265a0ad9c8653bb3f7d23b1edba854	Backdoor.Win64.EXFRAM.SMZKFA-C
68ccc6cd1fba8ffe963e1a87a137ed4378a5c5b42cbd679851227d4b8088a02a	BKDR_EXFRAM.SMZKFA-A
22e05ebb06947af2236f57432f06bd94c1eb4e76472ccaf3ee40335383a30815	BKDR_EXFRAM.ZKFI-A
b2a0a6add0f70c8470f4598544d1368533fbbba29af62b84434a59b867930754	BKDR_EXFRAM.ZKFI-A
f091d67b5ed6549582e83990ae4ea27f83b1f2a71307eb47ccb784ffc0ecfddd	BKDR_EXFRAM.ZKFI-A
6bdf56146d57a961fd43280412baeb7843ca5b69a931e83bcd94c24f27e8457c	BKDR_EXFRAM.ZTGD-A
379204894c709f24df999e664a7491b13e843c09c661ada886c53743c34a05d8	BKDR_FARESCO.A
e693241b3b29ea1b5af3618898f640e7aff6a4571de2ecaf9396a849b56a2599	BKDR_FARESCO.B
3c0bba029f0d9a95833570464367d53e62c26a0fda7ac4e686f56818c9b23662	BKDR_FARESCO.C
bfdf2175de7d49a470a275801b090e537b8435c5aebdb04e0fb9fca4acdc7f7b	BKDR_FARESCO.E
c5c69cbc20f10e3f2b5dc87e6574204199ecfb8426b6a8b5e1dbadd79640bc1e	BKDR_FARESCO.I
e69ff363f19a5a914bc5eb399b7118a7ebba23f4f1127b40ca816d73619195b0	BKDR_VLSOB.ZCFF-A
4ecc4291bfe7d84305c2f5ca4f4b0875f45460b2f1ff1cf31545a1040acd2bf3	TROJ_ARTSKY.A
0ddd8c3c93676f4e822a12eeb768c65a866d21c5441eae5922342631d36eb08c	TROJ_DDOS.DESTW
c377923108a2bdae1c06819eea9db49ea7883537a31d92a904405f6d813ab4b6	TROJ_DDOS.DESTX
70ae56f2a798773d11ce986b6cacecd2e95301a13d535118818d5aecfcea2f97	TSPY_NIWCONF.A

Figure 15. Serkdes hashes

ASRWEC Downloader

SHA256	Detection Name
ba5a57592ce69590fa062b8dd29e97781d355de90ba519302d861ff52f9bea11	BKDR_HUPIGON.ION
5b13048e95d96772a498dc2863008c06edb12bd69860106cab0ec85326021144	TROJ_AGENT.BDXC
690f08ea33d65ddcbff961dae25b40fe74cee2157dd11f826d4f44daa24a8342	TROJ_AGENT.BDXC

6888d4c21e45e9d007a2fa1722f2eeda47879a480bffe820eb5896b641f5671a	TROJ_DANGINEX.WD
49cc58433c7f752e49de7c670d96efb729eecd7d2abb8f099c0edae79354f06a	TROJ_DLOADR.AEL
29fe1c0599e44d632fd6eccd62550ebdeebd3c4616f4849f2cdf4f64f6ab3884	TROJ_SIMBOT.B
899fd14c1cb67ef65e314d475c5fba16afef4cb7d96a4c2bbd96b77b3cde48ac	TROJ_SIMBOT.B
05f0b1b4be7edfaa8fcc0df6bedd5239fb88de1eb30d83fad067fdabdd168681	Trojan.Win32.ASRWEC.A
2f1dd3fe337c49da1499389920b1e4649da4dabfce7fea30acb1f9e813e06209	Trojan.Win32.ASRWEC.A
3886f7af43d8cc5e94315ded6d06344f86bb8464c9d857219caa97394427ae92	Trojan.Win32.ASRWEC.A
5c22eb19858f28d0f28e6b77d821b026a52857ecd9dff15020e027e50d293e0b	Trojan.Win32.ASRWEC.A
7cd20f4b94dbe2d1d29bc25dc8b827a74db0d916d11451b058253de427acf66c	Trojan.Win32.ASRWEC.A
88bd7ea4b2b044c35917a9172e0f9163aaa1b64d366068e1a60ce2efee9875cc	Trojan.Win32.ASRWEC.A
8a156543e1c7d06af71eced066acde20bc7ea836e6a288aaac2277d37c3440a9	Trojan.Win32.ASRWEC.A
980923e43efdc0e6fab638306ac5285ebfc2af848f4659bfd0d0cbc054fb007a	Trojan.Win32.ASRWEC.A
9a5623a11426cab6eb3f0c956032e54c1ff05031338a68808eeaa0b5de250a51	Trojan.Win32.ASRWEC.A
a1c91ec192633d86219e6a78b640649485d816b5a054ce3889929e0fde1aad7b	Trojan.Win32.ASRWEC.A
b0ba08f9d77692928719982dab6a0a33545ef63a5dedc6ca4d5b2a79657722d3	Trojan.Win32.ASRWEC.A
c7bff5dde08339e4eb06bd9afb934a730811f43e700e5a7e10a5f536b33bcc49	Trojan.Win32.ASRWEC.A
cfa4b0b977d2a4aeae55a3bf1b369b462f5722bcd05e998a2f6fa7f125d48055	Trojan.Win32.ASRWEC.A
d45fcf2d0dfa3a1785f164bce102598cd3e0c1d975e64af902f42c1db1f7fe0e	Trojan.Win32.ASRWEC.A
d49e0890c0c623bfcb9a479f4a981de756eb02eac55907f03ea8b87b63ad727d	Trojan.Win32.ASRWEC.A
e4cf98be65db03a7231d2e3807241901a2541023e38fee69facdc25ce11cb58f	Trojan.Win32.ASRWEC.A
f8aadd4c2d9e16ac5e85a9361eb1d0dbddbb4edf772218459035c5f5aa645b0f	Trojan.Win32.ASRWEC.A

Figure 16. ASRWEC downloader hashes

Buxzop

SHA256	Detection Name
960b792eda29f72dde96e8f4939f66209404b8c4be188810158c93516373e4c4	Backdoor.Win32.BUXZOP.SMZTGE-A
d27d40c84484d949e67d2e964f3b3cf0d47140ea004f85f65d75190d20ea5e82	Backdoor.Win32.BUXZOP.SMZTGE-A
f61818fe8b74d3af78bfc287db30596d8ea6ae122b7a8b6f1cb0e08db24fa679	Backdoor.Win32.BUXZOP.SMZTGE-A
1024758ff0ff70a00de18d04d83c13113b8252df79084c803930d4ebfae2b1c2	Backdoor.Win64.BUXZOP.AA
09858e869838dc89cf34f722d19068c2a020555d9403576d4e7697ee843093db	Backdoor.Win64.BUXZOP64.SMZTGK-A
d429ce3b1382ef864bc329c5985c1d29b6e65baa02587ebb4bfc4e1cfb887743	Backdoor.Win64.BUXZOP64.SMZTGK-A
f2d69cfdf0fa3991121a732930ec026d6f462c939a9b822a4a9e1cf812124f00	BKDR64_BUXZOP.ZCHD-A

Figure 17. Buxzop hashes

Comeon Downloader

SHA256	Detection Name
69301c671e3720a72c5d6a2ac82ec59f0cdefd2c907b3a4475987612f15d6226	TROJ_DLOADER.ZXX
0a136f45a8e603c42408570c10894998807e61e74362c7c1fcf4b68f4f75c662	Trojan.Win32.COMEON.A
47ec0281f8c390f463ff1955fc85613963fc27f4ba4d7141903ec004f8b9f3ce	Trojan.Win32.COMEON.A
e66818dfb9c2a5762b5c9e633026e2431018c16eb47884f6f089508e80e8e9ba	Trojan.Win32.COMEON.A
f3065a78822ae2090b181e6d680db736e89b4e5b00c6684171b162b785539756	Trojan.Win32.COMEON.A

Figure 18. Comeon downloader hashes

Illitat Downloader

SHA256	Detection Name
f4fa9529d2726398447896db2a25c0bebe41160e86f6a3f441492e2a1b6ee7c9	BKDR_SIMBOT.AZ
9fc10c1095e2a8c4348f52adf026f20ad0e18be054447b88dce00aebb8491315	BKDR_SIMBOT.BI
e905234a74fab57debe3f4dba4e007c4c568c4897530eb53d10961c5b46f72dd	BKDR_SIMBOT.JRM
ba890b660293fbc2f6da6636b1de791c1db91bd175b22a318095a14c2f423fb5	BKDR_SIMBOT.KAV

1a27c59e03ce43f064fb8dfdd4b226458f9c31f0f831688c5ed5f308985f4d1c	BKDR_SIMBOT.UKKZ
b6a13f858e28955458323893429c6bee0c12a5f93fd8464538bd0fcd63672988	BKDR_SIMBOT.UKLB
3121520e79743893250458819b911df68bed47db6b11cf930409d90fa0e621b4	BKDR_SIMBOT.ZZXX
83b65da234aec033f30938ae66e6f72019a85bfea9fe6b96b46707360b8a7161	BKDR_SIMBOT.ZZXX
08b5c05ed470bfdf304d2b9d92487ba018470da3139a42b753b5681670ed253f	BKDR_SIMBOTDLDR.ZZXX
0a3a736ee4e1fd6dad1a595ef4d8eaed36ebebac7faa65f4c606545297de6c99	BKDR_SIMDLDR.SM
597fa233e4a1fece0eb954aad1e9cc25efdd8401c44fb4248fe5a78054450b9c	BKDR_SIMDLDR.SM
5ec070ce70a4fbf00c2b311160343f7d6f52a6dfe7fc442a88fc41816e12c3fb	BKDR_SIMDLDR.SM
668c9fa2b5775809771f5e8740b00b88cfb2782d9dc2fa71c096ca9064308ce5	BKDR_SIMDLDR.SM
69402ea5f3ab723c9cb21c965ce5d1b9c2b9545dbf5ab1f39bbf04355b93d308	BKDR_SIMDLDR.SM
a5106388091a33d0ff044ab51f6ad676c2925ed960f15f8b8abbc27504aeaf5d	BKDR_SIMDLDR.SM
bb2c1ff336a9d4a7177f2a7ea95ecd0a725b820a17d4102820b575804156f025	BKDR_SIMDLDR.SM
ea06000ee8b43f2f2c8bdb3ee69502e0e790e216bbe74f04cc04981de9cf4f2e	BKDR_SIMDLDR.SM
d68751f0c1240e48d8ed3b49472c2c8a411f6c27dbc7126bd056c6c39c637625	BKDR_SMALL.USCU
0a784ed8e2be97798d3391de8ddeeb0ecef7dcefe0c5b227e42a3629b7146762	BKDR_SMALL.USCV
f90a289fd49b7e5f586cd032cd9a94fbe415d6810ccbc4264e262cf6406d4eeb	TROJ_DLOADR.FUQQ
b3cd3d18a76476488f1131b95d2dd3ad822f2afe41cbf961a9501a0c78acf8cc	TROJ_NTUSC.ZZXX
e990dc5a05ed823fbf408dc5de8a2b488423fd750d4edc87e6f4e799083a38d0	TROJ_SIMBOT.BG
a08ff669e79c9b298716247cd2f0dbd790ed49a8add8d85f24480e70a8897b37	TROJ_SPNR.30HR13
f97d20eebc9047219ac13f2c016d3fdd010ab2885ab91ec766b40db87ad5e968	TROJ_TNOI.A
04428d0a63e3fafb052237b3bfa4f0a15377f54232d0754f7a076e2e19c3d444	Trojan.Win32.ILLITAT.A

09f01a899d17b402cff5438186a7a9b7b70e745c271302c4b5fbe33eb8c27da4	Trojan.Win32.ILLITAT.A
0d25465cea2442804cf27aba64621fea1255ce4b376150e5138aef301f713789	Trojan.Win32.ILLITAT.A
15a15ca80d72667e2d140a59dd155afcb9e88be3621715c5d89f9c69ed20e3f5	Trojan.Win32.ILLITAT.A
2b063e02272d21a17056276fadfc196d6d9b8c1c37f157a93b316311e6ca8f55	Trojan.Win32.ILLITAT.A
49d426c39451448f4e283d9610043270c4beec6266e0084abd15fe39f86ecb1e	Trojan.Win32.ILLITAT.A
4a9da3efc99c9d566a50c59911de563e2955b64672e8d684a6c69878478230e0	Trojan.Win32.ILLITAT.A
5b5a67dfeb5ea3c0e18f2cb3734c3f7924aab5331880381d43293ac04af99f02	Trojan.Win32.ILLITAT.A
5f6f1f6c6808f72ae003677f54ced08f7d01ff188b3fdf272fc45f919135be23	Trojan.Win32.ILLITAT.A
607c78e43461752d1b1eaf07a22079f2f07b814d2d270e1b2a6bad710199a216	Trojan.Win32.ILLITAT.A
6cdd6ca04be1edde2e7507c87d3661c75af18ef149038a0355179216672d5ecf	Trojan.Win32.ILLITAT.A
723314d0b8ba1807f50da159e8892b637d25a921cc291c7025d941935de8e18c	Trojan.Win32.ILLITAT.A
7d33b22498e67a1f408b226fd0bc72bc903995d8a368ada18515a0712626c6f1	Trojan.Win32.ILLITAT.A
80229037b8d30a52c98498ab313d69cb381eb6403e6d6b53ead5ed1aaecac53c	Trojan.Win32.ILLITAT.A
817f3419387d081c4d4e3bd3faab73c35d4e447371218dc7534e34d8cda513a6	Trojan.Win32.ILLITAT.A
822541fd66624b81a3e105405fc37d038debeab2880cdaf5699251c29002aeec	Trojan.Win32.ILLITAT.A
85315b09cf65a1e8681f6db05a49c484115866eca4c2d9d0adca4f4950fcc521	Trojan.Win32.ILLITAT.A
888f21bc0a36b26601ae231806f5f2442cc93894425c9949bf03c1e517d2d18c	Trojan.Win32.ILLITAT.A
9aaf8cec05477b1f05821e9a3828b57c1961d89887738e2b94d8c86bf2a8cb47	Trojan.Win32.ILLITAT.A
9d891f3a8ea48d2bbb18d251a5d3df7c6be159e4fee3628917c0bf04766e7e34	Trojan.Win32.ILLITAT.A
aa9aad620fd909b202f2b78cadbc912d767a7faaef30cbe469d0c2d39e0033b2	Trojan.Win32.ILLITAT.A
abc8e000822b968702bbeeb178ddc9ffc4ddb3f853061a22dd178bd2b00afc4b	Trojan.Win32.ILLITAT.A

ac5816214601354c0b8dc6da2dad6be6cebc20893227becf1ce2dbe28207c1fb	Trojan.Win32.ILLITAT.A
b0223da6002cc9e208c998865b5dcd5529844fc27973e35c191ce6bba9d8c1e3	Trojan.Win32.ILLITAT.A
b7da17a7c5032bcf9bfce9af473df55878aa95c3af7c915beacc4ec10c0c9756	Trojan.Win32.ILLITAT.A
baeafd81de83116cd218ed8eb03764df75f1ca71d117a3ba166a3ec8b46f0016	Trojan.Win32.ILLITAT.A
c2c0bfdea4c2eaf5c03b80a27d7a23decf9429c0142a62f62b179e87fbf5b542	Trojan.Win32.ILLITAT.A
c667d80b068e2133783b1253029d852cb4409cc6339017a4017828baa6a0b6b4	Trojan.Win32.ILLITAT.A
cc268c4dfd3fc7611f7cce993ca20d9b10f0e971a655a229a8d599ac9de60dc9	Trojan.Win32.ILLITAT.A
d34eb556119bf9a9fcbfa03628e06f4da38610dd618e4df304754a93380afbfd	Trojan.Win32.ILLITAT.A
d7ee0ebddb3944c2f3e9790e79392ce0d320e50087e9ac1cf3073b9f8ca9f6fe	Trojan.Win32.ILLITAT.A
dc8b57fceaed3e408b60e3603f34d9899e0f8b458e790db7a8239778d2d6d808	Trojan.Win32.ILLITAT.A
de7e36de69262ac5c55a6c444b1888579bc0b64f92316b6b07a70144aaba565f	Trojan.Win32.ILLITAT.A

Figure 18. Illitat downloader hashes

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