Android Backdoor GhostCtrl can Silently Record Your Audio, Video, and More

Appendix

TrendLabs Security Intelligence Blog
Lenart Bermejo, Jordan Pan, and Cedric Pernet
July 2017

Related Hashes Detected as ANDROIDOS_GHOSTCTRL.OPS/ ANDROIDOS_GHOSTCTRL.OPSA (SHA-256):

SHA-256
b4b70537971c1179da61907c00e1ce62ce713fd13cb913e87b4ff8671eea0ad
ef761f4819aa5ff14e14e05c49a49c9cd4f18df76bd51f1b8d33dc312213f6e1
18bde9201d7470372b6e04db866c2ce1183c3ead0eb8c05ca6e93709655fcd9b
d463c96c24839b763fb9def1dc33be1b217ea6ef77d84a7092a7cc0b4c8cea51
82a2bb72c1e3385fcc731ecbe1525fb1a5fbdf0abfa156cbae1606b0e597543e
6dc7d5ca86b2c5794ab6c899fc17f3778a54d7de222ee9d6a50b90bb04921068
b309d4f5bb3e61bba7048c19bec6773db94656c567404c960a20ce42f9d6f201
3117fb71a7bd141eb7d8975867e922635a705df5097c694ceca2e15578912516
3b4d28060c14cfcb7ab9b83339b6b38f2e35de8b270ec0d454bcb5781b5ef2c7
9000c92fffd2ee53e8d52784b9c68892c543552c157c9fcff47213ca4b9972e7
f22b834f7b0feadd17f920262b6eda6a1edfbf494a065d48206f735a2372c147
212ab6673295089c24debaec557aafd14d2bcb40b55dd342798172b7874eed88
5818470b1970fbc87d3cd48fb3ceb50a8fb66df0dd17699d8bdce62ef4851e1f
0ae2f02395e5f618c0271d21305e664cce97a259b1332b880f2cd879373d2198
2b49ef19cb51ea364fb71b2def46f145f38b01f915b55320d9dd5f763eaf8d61
56a064476acf1c675928da57d7325f42a5a1d2ed2a7890190e38a05f6689ee95
7bdf98c910eef7b72acfce258791e1a78ce50d9d71ae4f450c29272d1ca9f07c
f94008607e069f0c39f69061384af694af6418623904b4c67569b1e43a0410d6
9e413bfcb8f421a0916323028095014b13bee5dfd4bae753d0777f89bcc57145
c2877b6b49c5d8c5866bf763c45abf95095c37d241a2e098db7175415f18ae09
92d3fa65204213c046432d5e33bb4231c1035ee51d41082431d90ddcd93c51e8
b5f9ed7126d13bce244a362ce4adf77e53179dd26853e2c364d9d0db4d15183c
b688e2a7f2e299ac310c2e5f039a13c7d1049fd18595e5505821bea6c78ad88b
5808705a093158accefce5e062de766f7cdf117a83eaf8305b2e8c0a2518ee68
5e58bba9bc014472e3b2b23baa77aef5471b075236c6f6f9172e85234290bb00
be10d01b539b4aa6adaef60d39835b05618797c61ecb7d9bab26ee9bec10bef9
9d82c42fda07a6f776f79bfbe9ed5103a1a8a4aae415cf7b55c1a8cb4041534f
43c9b78e31d4368b7c50d1e276992bd7d2bee52ca7fa2d9ed7db82f53bfeca28
f52c2c0e3f4da0bc36431d0be6f760fac7553dcc531c143aa057cf388d5df044
dba32f04161897b73f9fcd4d3e4e6ec3e5506c221cfc34566cf72348d1a07688
e112000e34a82c5e3b8f1c27886be68120513cdb2d3dde257fe58814468b8e39
5d71243013f838713e45db57e39f0617afc29729b7c7829a5f7f126a55187a91
b84014224b89b9ed455bb37a0d73fdc7110228f82232a04a1127a744d304b893
241e8664db6622e0e7cdddbeac8d1e97eaf98c93d0723751568ad42a1a8ea948

SHA-256
3e27a1e5ad9b9161d4f612d31eb26ca121bfabc0309dbd117d6431f73d95a443
5bd7e738bf8a39da211360c28dcd656d6b9eebce143f6594e11d62a75e6cf311
87f5263c87b84735b6817872fb8cf0e312c9b7dc98b75dbaecf0ad163f87f07e
d54e6dd782ae46f84a3f0ee9adc9fefe56d344858babe5cec3a083b90d4b0b54
73f88353c2c8836398f2b4d3ccd8a651eb0c06fec4dfe35459044e5cb77fd0d6
b1043db6e77b6e88f353ffea26130a65fdb55b11ca7a86b1bf2724b16eb73497
42829222012ec02ef94e7f78a67979d2bcde4e9f6f94d1bc3bff17f081687b19
0a0277695e4ccbcf54b459846ddc04b162ae81798c40d4bab3f41727ea663cc6
3f4096c71a3de0ee7dfecd260d071d02ceccaf7d724a8997b6106b2e56eddfaa
4f82f043050918f184a6120143909332b39ef84b0a86a256c24128e6d80e7faf
55090b668dcf068ea652ee7505b6eebaa39c59054764e39544a27f3623279407
d57e83380c79dbfed3b8cef0427fd120722dc474c0b079a3d7b8be6a1e547591
29a02bd886c674559aa17157a631bee0629f2aa50f64392ac2684378cf7c2ff0
c75032da92eb544327bc658c4fe7fc0ee4030daf4c09f28730c12cc65ff8122a
ef67ed2919b86ae88081578652707f4b8a2121e6c5030a32ebe6d67cd629a465
4fea75702342729fac9a858b46e953605c1b6b22fd23beed0594c622ab02587a
8772ab9f293b0e8af12a6f03cef3e59bfe8c8f33a19de29d0d43d479a347859a
06ec556c379373b9a4947ecfc898b90176720bcafb7c5123ca0b1c42e4330284
cf85e1603b1717e60700fa31f765e2c0933492b5dbe5ce3c32c3bfefcb89d011
dc249b4a0c6719ae456b2c7d61867b9a5e8232e3c44e50e0469fecca2fabbe94
006e5c51e27e5b84ca4d9966e3f40156b5642ccb0cd98a58cb0052b6ffbc748d
8a0fbf8c7c8c1cdfc7e0b277951a12db3f148ff737ef55522c3b9f9a2d3a9ec1
48a0dae35c78780ac56d2601b4de2e89540995b4b960f6305d6db8ac1740ef68
23669806ba79cc48d1affc978ef2cc47a659275f6b8789ed560db4757b47505d
e5fa7262cefba7dc6611719bd2730f252c3d8e45f07d6657f538b59b5b440f88
5a95c92f5239f037894bde7633d662d32ba14f7cc4836cc81d753770a03495cc
1b41b69ff00fb86b29f750634ac4c0cebedb85245619ea5733f7566ac5484998
fb9ea01c46406d76207e6e0981580d52b60a5f49e32daeb5b4ded1dc9ec170e9
46d95b1681e6b21f3a6eff44892dc864bbfec2ffecd580634b946f2cc56ececa
0879ad90d6f9f1b955eac690addb91c01a034a087c198ba7cab3bb24576bb62f
d2cc6b7011966bd7b109af5390fbf89bdc82a55549028ea298ddc3d6e0ee86c1
e7cadfe51df4df95bbf4e576514c77c7ef7400c2bfc23192d724a5661537d4cf
4dfb2c77d881d37b2c05da7463f01bebd5bbe6ff3a8c2755670007fb05d6ac2b
610da7d04b65489227ec188f1759431468432986e2f576e64854fa17d4b807c4
85cf48adb52efbd1e5be4a4a54bd17c0c65e6cfd38239693d403b2fb4b0901be
e45db170cef67560b6444ed1296c16e59e0ba0c35272c46d6ff5c60999d36a44
fbf3f3441ed2ae726064439cd1e57f9d0771f99bd4965edf806085a4b62ca552

SHA-256
478d8ce51938a42831505354cc11f9bac22578eba23e0536b5a4a3381e41457b
20fece0ee96070a1ab1fb3052416613d9e5c3c7814ea60659da842697c6c3b8c
b29e02b0b7ec8030c4950a04d70e7e8dbf53d0f5e14139b1624c380dc50950ae
4b092395f7dd8cf69d14933b5b1b83889635563c68bbcee5aa1bf7a336e077b3
9f1e23b954a9854559c0cb0902c04bcac7af4af40bcdbe36ad81052329f1aa3e
645f7c089732ae62d87d1e776eda893f7e6f8f1cef8f1d0b3e391b8d091da1a9
77cf7ac64b5ab5614c7d7beb428e548e57905567451ec22c2cb532693ec64c10
0e2df79cc7cf1bc1f3d8f02a5d37c519dcf88bee4ac41f3259e25b65245cec42
cdf42659e9a6c24013a57ebff557bf5255824592a2d68509a2f27391123312b5
7fe44f1c122a2c7e3f1c32098f0addd1f17212c1ed96683698ff30aaa20f167d
16e292be7af2b9d5993caa7cba0c6e9e7fbaaa348379f58cd305ff955ce06cbb
1f895972793ac5bc2d362ea160b0d1d6ad96880449d9dbd01e92f89808d07583
a5b78f93e69e828e522b69cdf56b442dc45d28af1b8a6ce8e6c4e0a95234f0cf
29dad558fe387cc1706399f86b8d60fd74e9fb8e231cd693090a880240df1364
cdda4ba0249778984ef8e1fe711194cb6301bf436ca333e3dcbded551a5829f3
0dc9d4799c0c9a48081ecddb7d13ef04803deb1176fd104389f72983698592f2
a4231f932fc9ee5d5b907e2d75243f00e6ebbfd3ecaab7b332f1b02352c2973a
0a77fd2470c4bc4ed40677cd5e0202f91d4d6931188d086b352773f0040d4a10
60c54b21e40daeb513b8db8029db96598f9dfbcd2fc98d2c1f417f62d734f2d2
0f3850d41204d2eff6f2a55cd6fec56db9c24e32455e6d46f2e8cc8522f4cee2
0334af2801dd7948fca93cb712e5cd34a2d1b3ea10d56a3df81b1a3a854e7741
e3b504aacacafd4d2de28e072506ab05a0fb98099bc6e10308eeca15853e46b8
cf3a8e47c51009b143c5296bf7733e1399b92dc6a80dc218ce98a85ea6ff0d4a
388c12765d2b91f13842711ab0356f3fa79f197653f726725df758876964d33a
b1523f50de02cd2fad54d62ab4a40333a60de8a6a55f94c2883ff1ffc4b1e118
a77a77ab72f08b09d9af1cf2ef33b270b2012e1c94e6157c1ff8c1ad9d3daba5
eadb5cfccf7f30af3f8db8dcc5c008f78488c3bec0db682767631f3c28132686
f9a45f1cdabd11c1ba5431c4552aa26a3c845f167ae71696ce9e7f15f8cf9348
fa28b95b17c1eb01b7d18eaa302c9be50964a82bc92b10ef7bf13d9d11940ff5
f498b60ec551c5533d9e9691831c0123308348c5211cbaef4eb1bfb0d7433451
b87620ded1a8c3a6d2190357cfb9152cf142bd6212c95104fb4094d78a6070a2
eb22db82a7725737c492bc64850f9009beabe3bbdf1cf3755ca6fd3711b20656
d87014fe2f96b9e765cdf49eb0b1f5bfc7b6e5bd454c5d6e7048db2e9f84a177
3402fc1ba175097f73218e49648a2bdca9f95ba375eb1757fac9f3b47c96aaa1
9ca85c35c24350e980cec49a95e61d0086be642be43806782096da8e212546ce
1139b438ad6c415bacdd22ae2bea93227faf1b6af2434576c6577ee55dbe6c28
8337202bb5d0aff3914cf4ec516c835618f9760ba2c2f6c921295732ac6ff01a

SHA-256
c1033a23c8dc51dbc1916a9fa7d721462cb5fd7f81ac9b0e8683b99a43ed5bdd
73e0e9213ea2970e33dfa71f51b6e10a25a559ac606b26fc204cf4fe321dbbe7
9e7ab8c98c6a38e90e6247e95ddf08ac939ac99a30e0627a8b56aefcff9d955e
b3fe7703e4c5c97b8e88e9a3d48aae5554a1873e68528faf84a6fdc5ca0086f0
78e0d60c0e64a79e1cbee54e6173c9c625e68960ec0788d1921c3594754a63ca
2bb4a764b1ed4c85077b5969ff66605ed37167dcc5aa4d264044c353625c4bbf
197b5a735047b400a7d51f906962eb7719e4ff22b8b5d4263a712aae747dd18b
9a6ba83aa7cb4a7719601d4d9c9c3e5a4863fc5c3e18039767db925582dc01c8
0ffa95941fc9e21c276db98a69af2b985ec9c72720d991f532acd2b779fffc6b
bd2234bdbe1ba4e314a9298e37cbcfca095ae33d7ea686c2490acb455f95be94
142c0d08f7208ba1464fb4d0a1aa67ad780337ad0a1e36402285741805b90c44
baf0bb78b36206bb2685ef92ba611029b0acd2350e0ca32861418c1536baca65
9490f36eaf6cac19e0f288bd19875080f53e2452ca79974917b3b951b4c87d3f
52801eda6947d89057123eb09c69e08fd43d62d1395b840c8d90458fba9758c6
42398a332249a1b15692adde66a18a8c95c542ac7ecb25fff2374630465383c2
13a0d7648e3131e58b87d2372761425f5ee1a6ef520377e16c508b171b2a231b
a97c8cd8d6a574a0054a51ad03c463116412bc3134d48762d81774624fc9b5e2
f02470a7212b3a0351a62add30435850260be11b6b547479e68e83b475b4dab0
784e01e44b8fbcad860bfa38e15d8b2e7ec4150eca6dc7e8558663d4c0e6278f
63bf86334a5d8856b61778158adf2eac08cbc036f2cf1211d976043a8419c6e0
5eae6ff7984ab968cff0ff606f12dcffc12541f8c51f31da6f656ef670e4d9cc
b2efdd0625683cdfc97719d9bcec4d050908b3d364b7a0ee495b7c7fbe7ca22c
d0c7301ece62a10b58cd4469ec8b1e36ded089aeda9dbf50d0ec1b5c85b78f4a
68afff3ae4849a5cb3fdd3dc249a950e04bc74a195a03c4f6d40be709fe049ee
0349b01ee61460a84869a2a947802111a7b3085de590dfe123cb5a5e29b8c613
3ce6ba9af7a1e6ddc3f839b96f1d42d3aeb8738e679d7c1539756356b0e0bb04
ebe0ae2345edaf9e0439a93d332162f9ee9d3419127b4244b3c54dc7d305e89b
f57dc1d01e016d0cef749231c0ebe651efd7b0bef99e6ffdafb0227236661771
35bf708689847c08022c43ad3f210bd2f01397a4d54782596221c21adfcaade1
8bdae3f7f90788c8fa94f1ef2496680ce9609acc11c262725d9341654ffdb621
c8c381c7d3df400c0088fc90361959dfc2d6faf868f2b9ac16364f11eaf7e41a
259f9ec185398ce443a78c28d01c1a627aab3cd8666f341fb28d0f3a79481f53
3b1cf82794b1fd428d32c9b4e1f0bbf5a989329135f17120b2e141506f05f7d1
691644e245f46e7da4fd035e691ab864793ce5ae01b952ffbbbb93e7e0587134
5e08356371e35a0248dd50d59240d0a3b19e607aa8462669b60677f7e569e99c
89bc4c4447311e8569e291671cbf91ea7e63fa566a3ef255a0b472b21e41a418
b1f14c5cdc60bd0ed0cab6f274b90be5c85f79eff3213c4f452f62e718d7c62f

SHA-256
603c546a4b3710d2163afc42a2d3ca12a589e4f6a45ddcce1cda63b771eee632
0c98f843293d403dd5f821f5eab8e02ec35297f3112e96a34aba8a98dfe097e1
8fc13e96547bb7ecb655c506d48a3c32ddba275cfb8e32eb1516d02f91aa6bf6
b1dcba85194e384e87533a0629f221a5afadfea4b00ab800ec2082a79d5f1e2e
e0805eee4f09d28b5688dd9cc45972a79720c365b162bf2432649956ee688a31
0bb1bb3d377bc4f9c2fa41611b31cb4b8ee02c8ba0d782d824885ce44c572b32
2103fd2077f073ed5141198d789ef9525b676fd5208808601b8a248438fcfa87
fd8cfe70e0b64f3af0f3bac1299f7fc9d8f16f0f682d34b6b5b8a73a81918cd6
58c06e9805ed769f63c7ac01d324fa158f453956957a790e74100923d595461c
473277522c78c9a61c591f9c417d54831dd3f6483c226cc008c523110df4e8ad
f044098ab7a8773d368afab05a8ca7bdba6df729c033900bb105259c22be8607
93f0158b78ac622c1edf7999654f97188efe6fd82136412d89021657a1965c4a
1986c1def0e7b22c12a1001554d3740ecb94b6fe54f3722abc512806304d46e0
aa1d258ddace9f4cc6591bcaecdd53d54446d5bd4e52634bb9eaee4e4d85020d
b45661e02a3cc9af9664da0f51413035fe80ebcdb82fcd548106fe566d9ff3b5
320878334b90cbae5666834eb97e5365c369e3b789fa0b11faf2130975794134
0cddb0d58855dea1608116cd90dd174c8abc64fe573a4e706f7e2d7c1427bb5e
cdf3b0e42f10aeecf0c8113dae41883d9e8c04e422079b0bdd0e44087f724a9b
3a7911e198761e56ce5d5451de61971d73b8006e2ad1721075b95bc9161db2ad
a9ab7fc53d871241ecb3edc53596e33dde172d7636da5d01b1cb3c6361aee235
5ee38dd6c7ab3b2f8d7f4c666efc7b250a3170b4fe21f1de308f3f200efc42e4
6c8c01969dd5aab4792e9509b424d130da6b3c6e9cffdf522ebd2ead2d10485c
bae1c2dcc03e76d6dbfd3320d976446446e10e700f2dc69b45244038cb265060
134f7fbf5b5ffd8c1cdcd400cb07065716459c527e2f543aeaa5c1b310c16b3d
bf402dac79221047e88e4d21a8fcbbaf6f4535a91f950499933091b3b8327c8b
43842117c2762ddd463ca408271b07c3c03b1b39b999cd2f6b46044935fe2275
a8376081d42153b4947c995057eb7242290dc32fd2b515be2910e0c2d7f134b3
6db16b177b8a752647110a1ed262b611c82f5bd097e55fad074ea5c2a35dbedf
5700a94679197cbb1d19633e618884c49bdcc3d0252ae687b13a44ae76fb0e46
62f29b85500d72c071d4f5d924a4da649f83152a9172e4fe98a922ed088bb5b1
83849158cb6c55a96695bd4f5242f8adf3fe5e729c60669d446f1d8a9d685935
654e4054d6240c2f8e2a28a17eb0a97b21c6cf4a9d93983ae8356415b50d3290
6672bfc35550bc6f4c9848951808134b7719ba070227a63f057528c555e4ce83
7d1a07a742171f13cbf45b11d01ec84bf3443acf3a9177eff0e6b8c4b2664256
c3e1bf40c4192947f6be7330ffa195bfa8e18f072d4121c344fa0b20cb81e22c
5d15cfc5096fd650b718c943a77fa4509dcef81c84d118847737607d45e3bdfd
75a315c670fb0cb179f035d437de98d326d3abc040648b93e0b1f64ae57c3de9

SHA-256
e61c95a88fd66f2e4b717189095ce065f9b7eafbe799dc4fd2af6c914857b1c4
55430a9fa6fd979d9c244e85e00a2aa057cd7eb4eaa654a8ca42c8d57775d378
5f75149e414176d67b7331197b00770b2e7945c921cf3657d2d4f29833661425
534e49087a17bcdbf6d40f17814777e9d50f018dbb319d9ecb864c42d68174d3
68edfe0311705420681bbb937696fc137678c28573ef12d6cfe4419114d51e46
b0c0776b910b13da0a884112ec1904b9eaf41daca1cb51c2e04724a087ae9b08
135df84a4866c23fe77d8dbac4837979ade7a12074326817058f21d4c9551479
b6983a8b27ef8148e2ddb4ea73e37ce92cf13939fbb7982b28a4521aa422d270
32db0ede0dc2fa891c0f9e8b1857ba72fb8172dbdeb12d6a3bfdd4be82586254
561c722599bed26747e783bdb2b69d3cb0ba9563d2b81509447ed593d5abb821
b48dca023db9bacda7218f79d3d73ae300613b0d29434198466c189e692d0a70
9ecc5f50f0f275f32595dd5e5421422e85a95b7a8d0f7f2ec6b203b368e934fe
b00994acd716b91865154c4006d6fed8e90466f2e6298cb5c338798060d1e452
d3b5eb99de6c818d85a9363a9f4a08576405ee8b207d86c5e8b9627a4e53c4e9
1790e5a6be73c71db332d0b28e3a4f339e464c05002cf0c395ecc29e5a2f1dc2
3b620bc7d1807f6a23c290501f1df2e40fd45dc310932703d3ba0c08d4096b11
22c68c733c698c41128505acbccba942c94fd15c80f81067f80e457e7710d03c
d16054094b687680475d38db8d890c847116f8d2fb89e801badb11853d9f5f33
8eed4bf367904aa97aa6c87b4b1cebbc3b82a8d047efb24992d721321e3c0690
e14b5a289293e3f0089e012507bf242a968b5afc1a437d1724af73cd30d4a26e
cc4a7221a2fb7c3a0ffab24a4f808918f5d3156675a9d827c8e9c2550ba27448
b4bb31444b60f3b58076be31e4f78770d3efa631e7fa0bc0e96537b03778fcda

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.

Securing Your Journey to the Cloud

10101 N. De Anza Blvd.
Cupertino, CA 95014

U.S. toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003