TrendLabs

BLACKGEAR Cyberespionage Campaign Resurfaces, Abuses Social Media for C&C Communication

Appendix

TrendLabs Security Intelligence Blog

Joey Chen

Threat Solution Team

July 2018

Indicators of Compromise (IoCs)

Hashes detected as TSPY_MARADE (SHA-256):

Hash
0cd9b008646eec2deb5e856406e5699a897407f253e47ea95c56f94a254d0332
2a39e5cd12337bf2e3d94cafda1ce3baa33d765485903ed909dd41cfcd6fce6a
e987d9b8b7e3d4b67160fec327c90617f0821e99beda759b5635c45b791c1aa7
0f4346ef8668bed2eb0e35d5e091a1128aa9970f210b483e718b3130231bb0de
7f065c5d62f3221c0c795345c9e029ca78fbb3a625a1b0baf9105e5bde173970
02b430032ea1372ccf8eb5b6d129670dd7cada2e71ec4fc28532f4c368e5f1d0
2823ab88dc57f146512bf6a6a494be622d241f6deabb2776b79cd56a906554a9
6b2b30c62687419a389e36427aa417b933b20fb1420d1fa00fbde32cffcdb58d
aefb5f6fb1acd7971a31d9ce29f18aec1088074ea62ffe3fe1b1dc94b13b909b
208b7cb763c5d9b3357120b88f2c82cbff8dbb548d2208da68cb8e90b68be4c7
256abf7e6d66ba4342710ba661cbe671618d702d613d800c099829bcbc259eec
a2a321804dcaba16444a753bfa49604061c74f25e9232901f9b416cede46011e
f9c039fadf01ffe0536d2f6c4a5aa9981488ce02ec58ccd45b86c45de17b3165
ce3178f8df7d3ba666076c1aff60756d694d04f53cd8722dc9f908d940ee74a3
26abfc0a8e97b52fd906e5d12cc524057e16b86040803918b6d6b1df7c767378
0ea70c8893e80b1cde3e5c0b00ebd8a2d28db9442b8824f3cfa76ac21a4e79d5
889cce66e873acf9873a5017e231c5972a035384e724ea32b4f02f32ab3da804
2e1b4bcb8ab0a16d89ef462e6346df18f66f56c960fef746d648e2cabd567b81
ad9da26379a1d8bdad25b886fe9970382806171c0e403845f2ad2cac66cc3e86
6d9240321d657c44d63c6a57ec9e8838550a4a3eabf525936e08c0749f3a98d6
460f30dc2fc6d6aebfdeb3c6f1cc6ca65ec8ea3e35ca1a004204af5c06e04674
79967886dd8ed29459a57a895e99874f833438dcb6e3989c654ace0f8680ad97
c2ca2429ce50d9d7c371245ea64086ab1dd6b5a4db1f3f34644f6ee78c4be9aa
37aa2c6434d7ad36e22a664a1ff3057e160c622a0728f74f2b897aff7598e02d
5dc4768cd097daa4584566ae179ed27a2a18996d5c25a76c56f5aa141b298ef1
5db35e7d3912fcc5d2c01ab9ac381c4956c99c7fd4235144ad7c4eb308dc4da5
e919001215b19073f95e9843f7e61012c0f3a06243e0c571e7040f00052bc3ae
2895a8fabdc978d59550676ea33b801f5d9c436ed54a9319fca1838e2adc8318
1bb9910f41af6323c978a4a2f9cd9fab8caac5a599b7270adde2f2caf77a7a0f
ba54fa3ee7cce22876c19848cb6eb80aa8863dbd0ae76f2cf5971a0ae4c8bce5
b37ed79ce0ff00c8e25eb3f5d5c65fda85c86ace613fd9b58bc7a176abe86d07

Hash
40c36915e9427874992b56094790cd3099437e73fe30852c0f84b2dae25d0203
e77485f937d103cb4bbc0e2d8312356b495e911dbfd8b969be5a5d6a3da46257
0eedee7802771c83899a352ec7a8e5890d2b2b4d8b775764d0e159c58b803173
6ee8be313310277e49b1825336206305fb79f76f2c57b9f46ecd295d74213c61
fab35de776b3319b34ea22e1dd5c18e26cde81a3f379150dd493e50c5c00250e
8df1a0dc16e667550da6a405956117298b3e2ac428ca27891b9d68d4e040bcf6
dcff62533cbcaa5b65278967eeaf7d70e037703ff489f90221d2cb1691c29d7a
3b86a3cfa04297d484ffb935f2f1b918e959a0447446c976140b97d1beaa06d5
1fb1365076e56522c19b3014c7f6994def214f2166c891a215fecce36b8d84f2
e96cd633f617d82c3bac06082a58eee1b31f8f94d9f4a416052c8268c3b86b64
3b32070c3d676a101fb286f14bf920c9bfacb094b9ef3fb359f65bd3ffcf5b7f
4893c9f3b6dafa5ef10f95415ba6a5fc48d0cf9a3d1a52540d5ca73e31f673e9
266125abb4edc4d41ff0696e3ca3ffb48f6c8e9fd344a1c4669648b08d82602b
fe9550d25502f4b7b816c4a341e1a0856cb6e7d7c29211b08b2f6728ec81c1d7
a5861baaeb24f8961501081ee25703f6de1b0b26bd330f322de23d7d4409ebf9
18ec68e1bd9b11f22e481d48c415f8d80edb76e9032ba4e1d31d87e16eed9959
c7ca18fb93439d5efeaa92dbf81f2aca07ed0f9f74d78c71d2590655c6bf2551
d915d7646f4cc3cd33bccf62fd5b92334620f4dc00b0e03e82e876635ea00938
40fbdf080b1cf16856e835bb4aa50cdcfecb61f34aec9ac8364614d380e75ef0

Hashes detected as BKDR_PROTUX (SHA-256):

Hash
7d74ed8248047fd22419d0dbe8989107e80b7d09a6cd163ba5b00ed86c14dad5
e4bfc544242d42affb9c21aa007a69ac254aa864f4634941050d900b3df5899d
855a2f4c64936a4a026aad4337a23d7736cc8549e05528cc0b2e692a508926a4
d75c8571a41342a3d95a58da0975a109702593b383b9233e2dafac3da66cf98d
65fb1c0b7b72977936b84d18a0463ca773a417e570f05bf33ebd71730abd0e6a
df9e9efac15143e34b0890218bf51d903b355f78947fe424bc6ae41251ebe2ed
183586f77027da934f94f56c6f55a21e7ceb3c6286815fa9d8404350dd775111
975acc22aeff6f175562346028512c6ac58e9f01cff7e9df7f075b204afeadf7
d923636b2d58ea33a25bc3ffe0d5a25e7423ee31118f76d80b31a7a390ed44ab
12a520b0cabaa0962664d2cb48538f4a4e4c98ab70b48e33a782857a6c5f2341
ddb6263b6fe0462147fac4a7121da4cc16730b765320fe45cf6654c5b83d7770
5a682db0d2fb1f0ef852087875f8ce0be7461e22037a704dc0eae8ead09919a2

Hash
1502013ebb106f66563891bb26c33a230c5dc4390d247e00df0fe407ce3bb259
5703727953980797ea14b4ee75e4d6269a8eb7fa1d28ac52c7efabbb81bcb3c5
3277ed56fa81e25f1c11617bb1325003d4680c746cf77d79faac0486204a8b32
7dbeeb2f2c7e69b61ed761a928eaa3211717b7ef9708f282e718fde8f3ff1963
13fb7f0c4e00b176486737d39b4a7b528465fcc3f13a6e348c253cdc31b8fde5
c96402784f6e18c3646f1609f405ca086864999ac047f7092dcc28b8122c85c5
e30426df099067fdaacb8210f8dc29d0db8d766b3780263f371e055986b34d21
2dc3d02204397cd528ac6e9ced3341038e9fb4c6f15b908eee4b4ddb4b741b85
0ce1fa65d6f4da1668b8206c4d8d03316fb62d64e77a3d38bd346dc63a1c16b2
b04c2fe318089a4734ae2b90b705485a550607c0e9d6cfcd504db40002ef5620
0dd80b8b79a2ad25de086ef2d76b92fff9d921a93a43e2fd3a987c7ea246d482
742455e7689648b5736b6a4805dd628476c2d2668cdd6a5bcf1b6483af8af107
4470701357bdc537f9d7192891def19e72073486e746d5fe51ed49422e58a1ad
ad9b459b21e53f6062b90b97ce8050800d886da11ad0d6878d51f4745dcc45d5
5ecde607e96d441315df7a5dabec267639e045472415ae3f831fe47f2e360791
093a792a5cb5ee9e11581f6c5d3deac752450e905304256b5ba708dad7e16d32
44bea3ac4b4d640d9e9a29fab7a0853023caf013ab08827083e3b856466768d7
c6ded732066a59be240a01bb35ed0761137963a95ec38d8344bf59971ce1e2f9
5b2f54fede70c0855a1922f11dba224b59f2815599b825e161d169897406a3dc
d17f368287e52270a477808f782bf9191da83f626e0c89b255a5788434d9db2b
2ecaeb93d89c5452e1d8d7f70d440e56dd55caecd8579ec460574de48d2a20f1
c07fe008ce1ed20bd9e7470bcc12ec31d8f53886bd5bf71e7d10a7b981b177ab
52246272befbfbeb6e6e0b290f8303cccab843ddcd585d0744afbe66449f5174
4b6b88188c983fb726af0056ce01dac37420d5b9f14e3bd62923549acb860ac4
888a99ac63ea526025afd94791085ccdb4772c82de22dcdac8050e0f4b1489f0
396a680bd40ee6f67ee4e85d7928256b04dbcf56507a5a0237268c910ea34378
e037059ccb1927e9dea40a4f59cd3b6fcd5067af1168ef92445758ae9390c174
bed088b76bc2d12febf498dc39cce0f2e4caf5c003946f75354768f9b604e9c5
5de0e6caa9670a711bb45e02e886e7a61342c58e6cb11e2ac5d602e62b0ef727
4a0ef5b393e7e4b20f24f1bf16f583fa13cb71fe9b46613b923316f261cd90e0
00040fc24aea1ad8392083339c3e618bf2ad1577c0730a44568ad2e06bc2ab3a
57114b68a7d32a4266dc9c87870ff75e09bcd797a388c3bbe4e35a3700153109
0077b0fa5c00518e23d15fd69ebfffffbffe6f0dcdefc354e9e14f4b27bbd635
933d4d54f8bd1838f16369a5f6cc0fc5f01b1b2df738943a752f858ea0f30228
014a0d94837705d7a084bce93e6b6d6a9bbb08b16dcba6aa120105a5f104341a
038bbd439f331bbf360c7352bab27efdc25b1db056cad357977a62cdb0ab1e85

Hash
4c3532f03c8bb09af06b7253264d041b35b142d124103c3821e366e8b9c2c69b
04751c2f2d0eab53c0a4d4ec69879dd59e9529c5b4500e1292a39bd5c3120bab
047ba17a92cf7918bc3399f550cb8a3c70ee34eec2c55edbbff94f41bded047c
072b4447f665c646069407aaa7313ff554541ba4a3c7b7494ee0a669a92cc34c
0760e18479b5e5f91143bd067d8d9051a4cba4178c8a4dfde7dc57678bda57d6
08f47c1972f83809fd82522166006fcf658194e587cb92ba2fb5836725bcf43b
08f8f3439344713e356597c0fce59a4610b9fc8c610bf187eed05140022e0fdc
0a2a9446afc2af570e0e74084011d427293130e0e8d58a3046e850abf78905f1
cbde7402744f341e88867386f0e4c0a58563378da0da70e51f610ed616860dd9
0a5592f13613d5cebb6a47e378754b98f97bb8fec1b895595f1281a270c70c68
0ab8e36e3caf3ed4c90fc65a39c0c36a00d7eeb5412ef51ef8d532f883b73ea1
0dc4bbada63c5b97c95e4eee988c155c918302a51673d94eccaf8f2bc660e83d
0fe20476dcf7db9b336b0ae95c406eb9d99b01d3cfdb55cd64d16ab2db378e00
52cebe05655d0bd973c0976c1ea7f7a96a3d94e4370de08aa1fe8f65a22b5420
9f3810fe44205d09e7fc0258fb5c00c6977979406c7f77a97c2f91aee1af72a3
7a016c8d361566c07a9bb0a79f793a9d679838cc7c3de26a43581f634eb889cb
14177e0ba3c09d3a2985c925b56f0f945d93969006a5eb72c6818838dbfcdb20
102b108a29ec52974f290c0fcd96af257a31832ebff62f13b3faf4f0865b706e
109058dc73e148a4ba40b5af35a4835b8115a663faf76f3ea96c6cb766bde381
127de6a44c2dd602e0dd11ab2c0612da827a376057b89aa7bd6497d34805ca1d
5785801c13a763c64c38c0c1bd725fff0f1f29d929baa5a4ef879fe5db3a94b1
14cfcedf295eccd2e0408684aad1e11428edf8a51138a4045df6911e18dd32be
16013143b53b3d2f6792cb9e08359a278e95e5e42179cb2cd8aed994ccd9fdb4
796bdecf5dfc0802415b8c3f8d733ebdab54c498071a9d0033c13f213c78321e
1961eec6a2ad8f6e4a88b313c90e4fee19eaa31e5d53adcfddd40fa3083911d7
18eea861b47c43e8c42e3942e78dde4cd26eb0a8a064db2e61c142b67fce8f81
1adf4897fbf018409088ac23e38c552b24cf3a42f675549fcf90e78d7317792b
49a9f0ffb769cd4fc754bd590b466e8b33813e6e428c78bcb2bdc8a773931cf8
1b1de95878cad09f1798049e54c0a44bbdcd55ab60784a5ce9137811ef217add
1d636c2de605174cc6bc66a1e9858dfc5fd61e683ce33f1cc82c17455ff781af
fcf2948de490fe8e82f311a0edf15f8b87316188ceabcdb64ab5a86b1188653c
1e2a33974a24e75712da6a90d95c49644ed939e39df13e91bfad8c01036e5f29
d27a79082e31ecb4b4d7a5c190bab9c1ead970c99120081caf249a24d64a5e42
22e86c74353e79469d433bf0bdce3d2fe24247a5c8e2bce751cbbaa9005216e1
3e34648007d75be691fd491b5a0b49c8d639870a2a31ea7cab63b73ebd44eb93
240c1cbdbd8c091bb1d1dc4f6b0fffac536f18465813441b21364c8ae55c315f

Hash
51bc81234e64ca9b9804be0346102373a1f6cf339d6c92199e1275aefff1dc88
c67258883a1ef5b7611812a5ed20ad838c3230fe2920e921277ac4402bf4f306
243352333cb5460e79b59700eca2240f8acb06edd9d28a30857525c5b91f838e
2bbb8aa2b4ec3f2619bbec4219299e623647282c52000e4e95be54bd16a4045c
2e39b2272dcd936c3e0b55747311a44b6419196a2b53c7f7a7deafcfd0599822
2e5536ec5f1717c6ef4ed0a1cd88091f37b198cabc8cc29a33892a69a6249bf5
2ef4309340dfe69913773373d1d5a770847b6858390bd1b2ef0d6cbf99f05562
2fab18a0690734520e670026b5b4e87b352764e34f214263b27080c79dd260a2
342245b72be4439d889fa163abf1b21834ffc9243e448f897eac1475dc647a05
35235afd638c9f7e3a96165e1a979a85b8e61ec7ebd395638ed9c78b835a2d8b
359fd9f6138eb2e2b5540ca449383d765947348b29615067a6de9f2dcf9f4e9a
3755d05682223f11e401f72d61048c9fff3196491e1f927aa446f4995f15d35b
37f62cb8390bfb42bc222a9d98ba08f3b9973d8338eda6ef3542d7224a3e6a27
3aa0874ab7fed2c95471087afcc8bf8c7e3fd218c18952e3e07f5fc8de42696f
3aff9129a11783bc50d59b7b6c45e26604876b8d770e47db9638a5ce74c212e7
3c24a0c92e4fd38f895c5d30e262409502998571fa16656fbd2b1f04105b9dc5
3cd3242e4f9e498995810b3557930b4af1cd5257ae93ff91ebb86bfa3993aabc
3df784e32e4dc62872ba93aafa0a66ac86d97cf4a5a03e9c7174884971bba7c1
3e6b33cc7ef8b60c4cad49ba3c9641ebc4f0cd056ef7129b9ac06815a7778a29
4125d03e60dbf0ebe33351f523595ca791a3105117b46f4734516ca836f302f4
4f69ff1b92db49f162f921bb4b6dcad7dc35cbcebdc8b6f491ffd3d51439fada
4217fe4185163859c092b64753ee54a15d2bd9d72523042a4347a7a9aeeea88d
449380d711d7e89be5e2dd313ae936d7c89f010f1dd4e69c40709f310b1ade70
49b55843740874f6c0c51d2c9b13975cadc6c26b3a2951c3ed7e334d223f5d26
4a78d19ff50e3d3c3edb183a12688e5e28b576cf5475da569e77be8fbcb510b3
508faa08bef10f1c95b44061e276b30b61834c31a000ad0a9be5f4ed792068d1
50bc6fc67fefa8c45a4a49c452c5050a4ee63801f667c6e35a1d8692f0be7878
b4b8c2a98ba20488c16b8cd4f9fed116c23f113cadc6523767058f9b793d8896
5190e1bb857d935826d8edf030c44c39bc767c5e37ad4df4572919b64e06bba7
585873053a547e1def99ada94037ec5efde12fdb971bd724af20216d80d15ea8
589226556f11d83a5917f424fa4ef4351f004bdb43b8ef93bbe13d86d915809a
c581349e626a456c12bf5577666dc456e02239cdd540d7e04a98b3b751413a2a
599d4b808c7e4cdbf75f14da3098c39a9648019ffdad13502f024e84aa5c645b
5c02202a7ed0aca6c11210443990a52f860ed6f687f78982d68516c48a1a6c74
614baae3538e53f02fbae891bd2dd77accf2c4c470fdde8336b2a85cfa5c126d
61f535eea49fb23e790263376dea5fdaf73be1e4ebff47bd7a67be8bc560f068

Hash
6267161a4e883b0bbbee26328a27a0cfa6568ba18c754ebe7b715772f137db67
638bce7fd6804628b38cffebd38a15855be4c3e6df1fe7788584fa8b4db23566
6557e6922914f36a67eac852870042abd4d6ac71ed453242092a531c6b3ffa11
65a479c3653c42784bd3f6f83faa382f15ee6aab90d7f798bb4c8e1355a96c2c
65fead0aa99e46b7c960ea185354cd7220b628fd01ddc100323a58cec07a77e3
66711574f62eb70a41f9822787472efe54c51f609769bc0cc6de9233b30f2bc7
66765342be54e4944cb719d9daf4ae053dac2c08eb277808d11c4337ff688739
8ebaa948ecaa97b732f0d22a3b5f5db4d8c3489d5ae9147d081c1f585f326007
674f78f85457d43adc8e59d498cb372ea5b156cfe0c92898c245a071c1c527d8
67894993ca2bfaba64de03454b788e64216153493e3bbcbd43963fe2865881b9
6c834ec48e51acb5f8f92d0a449cbaa336f379f541aa5a52e38eea5c8ae72194
b246b8027aedecb5540f9249285c744193ef50ee3dee1549b192bd3a0b27a61c
6fd68fd43fb347157b8da33379c690cf476d5653cb4810e2584413649e71f6f2
e62f5e2a24d4404ed4f53be57fc1e989c21c3d49be7fc4e65ac579c8db53c185
702cdf7f5e71fa5d2e9408b3d447c3e936fca30760b52c4f5723a998bfd98e34
1f5fb201eb55876e7cf40ed9e3db1eb11f54757f2216f8d169c9489612814ff7
70bf1ca198d0c53e232440f4a8d0af6c37b32618f21b64f9aeef4c53d6b46b81
7109458989fadc71a1f61218bda31e2f04b8838fded548e0bb91e80ee9f01e24
72061e51bfebf7640f70a2bb693434c08122808a2c89dc5dbadad6d43ff8aa94
74230834a5b1f727c44988fad24c4998dffea9e88c8e35d64636f9aca672523e
766bea863a85bce1d81c82bd9423ee51af21cc23ca4713ed4b4ba2f00819f0e3
704dbee62f8f91fab316196564c4b661f454d99c74356a9d9b77b18ff8648902
777c80b2690f6194c8ba1711552935032906e88e0674899f80305ea9120777f7
77fb1de8698022650e5efba43a7c96446ba45167e242a0c45f8f34c5dd4ee14f
58a8817397554a2e80e7b1dbf75e31c50d3c2cc061a6880927b28bb5f1541f25
ffbca5087897892fc90a5baabb66eb77e006112b7921457d873973de685b3409
796159c479eded52cecd44610caa90b17a9d5d679a6d57f7e99a61eed3ce0093
79a3f28227d442bcd86a054c1c68c5bd534570a74e3a3b901ac5a130f0ce8d8f
9344c690ae2fc84fb8dd1a91a47ce515fd00d605a7c8572f40305637e8ae90b2
b6b2aa96e1a8b76c29234ad21c68a5a96d19aeb445ed3c344b2a6b0ea68046ee
7b391d12b762471d146b51204b719ee2c1f807615589177a8aed9bb8ba1cdf17
7c0b8eb146458ab1a5b216e65145368414f9b2a717c177daf701916ec4761ba4
3e5a794e84dc42703512775295491e018dc42a2378c4d94df5548980516a6aec
7cf94cc7d2f89c400f99ccf769adf1899ec79143635ba6abcf85e7a9b9fc3e3a
7d5152c192455039065c88d797b69d78430b4efff3e529433acdd79e1e08d0bb
7e6155dd253c99deb37a56b55c67a00863ee8104897edac0237d04457e5a4d68

Hash
16b6fe7083ecebf90ab4bb4e7ad83ae0c96db7a3e39baf5c4f284d013002280c
7eba20a5fd5b50fab4924ef4b98b56023cb2b584f3b20a9d4b0fc10a04de0358
7f6373c161c51474b9c14aac897a845ae9a891e28a0e2a16494f5a1c7e0a05d3
809f12927a8e2e06aace61eaaf2d9fc41dfef5e3c56f90766b36b6f2163acc60
839a877ee55092978dcc6561ed3c6ea331c4d42f67e7ab03a344221d0b84b635
b133f68c4dd80adc83be284635b47120b24e467519a323f53500c872e791cff7
8545ac2a44427da65735370d024927f074113d59b3839d953be24620795d2db9
85f577a3d9e7f67bc5cc0a8fe3cf088bc3e2807a67d761c4c1f1cf58e3d89986
88d9b3114d71bb5756f92e4b7b674338e6781f138e433631b8ef93abff2a5e0a
8b6bd1cb7b8d74bc921f06a4f8a473847d595c1e7695357d406d13fd6bc51318
05361796c131e1ea9a15b689b5d93aabc328a4ac48e7e22e26e21b71354a9f97
c6fcbaac99c2b4b1ce85d6a7fce27a581f1f5328d89677c7525e77fe4e988ce6
8ddf4c7005864cdab79244460f8963170f66267dce5cfc78a3ceb87d71afc990
ba90c4020a7de2bfa7190503d64cee518210199f34996f399cfad002aa82f3c8
8e970654cfddccd8dca572c8009cabc9730da8f5f518545073ac69f9b82e7c36
90bc44e28105cce982ba2724cea651086a9f29edf5618ac906153898e8809ca4
9104963eb5f14ad05fce1c551c9e89e52bff050c8257f22e506382380e1592b2
79a3b37aa3f826748c9c184321f9d36f42b86ac9daac734c3a836b1bad3f9a75
625226124b50fb998d36cb38298209dae10ff2a483bb7df1c424f77a53b0128a
918130aea27566c8382f1297979f41637237748df2510a4e870c7e6fafb4ce61
921c5590120917a9eb932ff8012d17a26399f1b54ae333a660929515f370e8d5
93c2130db3d7b1acd9708f65276a575d4b47ea0a8a537474a0bd9261c22ad6dc
c52ac1494f3787e4dace478c554bc9334d475625f404c3dd4475eef1957f6cd4
964b2b0abaed0604223bcdf7b5dddfe545185231d8847fb686040ae9add65eb4
99f830af21c9ce7787157563dfa8ec694bf5916e60b12e2f96b38755abb51de9
9aaf34fcba74208e51bbac6576a68f404fb7907c97be27ff5e5972206d080e19
9c6c6dea9658b2a97f5db8da8ed88614566a72b2bd9b0742bb42bcdab20d06e6
9ecbbe4c82b96da8464a45f3f875df9be103cecf53763a5c4db57801db71a824
9fb35927df7fc957f4ac01ba42ceaae1dcec98db393662f99661b1097a1b917a
a0be4bdea14557832761ed5dbd2f6ab043bb2ec66859a187c6b13832b6bfc1fd
a135ece2ca766fcb0753b892c3421a2e2bdfcc6d29f8b195b4ee086bdb485f2e
a141590e4daaa68f6a8b1dfa5661a5c9e4c6783dcc108febdad443ff08522db3
a25c6e913fd5b2a96da502fe5d14c4279580951c15d780943d8a6ec05e2e5409
a3ce80a782610645803ae37a5e93e55da1f0667b2c18f24d49cc4c06e29f2518
2ac07292806ce759d2b1b580bb1ef4d46a7921414cc7a30b2849bf36482bd361
a41c2298f012eac995018b6256ef2a1fdec34c0587fce832df283ec5750119bf

Hash
a4a157e1e66a4a55e95278446a0c680eca5c2134b20e4a4229de98211509e7eb
a5876f9e7c3839de44830a2da4994ece9935d1e4ff379efe73b2df3b2353df20
e26971dd41c32afc6ba13323168dc8aa3392cd3ca383ef4a322c914fae3f6d1d
a6925ccf46342ac629280fbc24cc5f5f87318bddb59a412528e1974fa80a2647
a696daa9855dd4abec60c907ed0b87e0b3252af4a6e81459ff9af31aa9cbbaaa
a848517c32b5ba2dc6015304ae9a6e287f0020726c92b96fbb6ca59e4768905b
ead1d69df44d6a86d240be11025448eecf506295f820621698a9ed6bcee72544
a87b9e5b8527d5b286c5d64892b0b870ab9ba788ad0a691bc310dd36676550bd
9918b8bd2a90e13496b340e932cd0c0f2288409fcce0de66740c1f489adb6b33
f312191cae8109ab840343981e2b290c9d345cc158ebd608d8ba1df57a6ecb27
aff2941f12ba1eb4a4c039a32105dd60ecc44f2a5dd7b0adaeaf71cfa20815c2
44d3c89e9cdbd26a04e795934f97305a9bcd000ec4111205fe2baa0845413f86
b042471c799a25792d79b2325547d30391ed136ff09b5155ef6b298081f66ace
b14802e72717fd5fc222b2f98132faabc0766e10453561505d295ed3d8c045bc
b18fa37c35e840fc3a95559c4c607551e589c96959e62ea7710349cfa977c669
434c9df65d8cf9cf469b890396cdd4b52a56137439646a7dd1460ef549811150
b416b43160aa33038bd000a277cee801db198f83a27490e4da197cb46cb640af
b4f7346ee9c36f5ea58ae3ae549645bb7ad73463fc27d50443817309ec450b1f
b9530837d9747433999c8d6de6c436d40697fee271d2d38ac8cd24df2889fbe1
9d740ef5dfc0cd07a7d6847bd7efe60d1f85246550e31b940f20bee41c2ca9e4
bba997d3e2046b96039d12a2457e0f999d4577f4418e7877ce4f5a85b0d9919b
3bcc1aea47c456aba1753197d60e2f6160a9ea198ca9dab1b1b002dc3d70c8d9
419af7e0a76fee5784d5bc667adb5b5963bad08969d7ba73ff60400deb4e6fd6
bc742e6db440f8e0f17a8930cb4fdf8615f1c2f5d455a1a9f0ece7b34f943524
bd43bc5d037bdd2c9bc3db8e9ee3e6ce272e39bcb150014ca2912fccb12360fd
c0879137834b57ed4d7c59a1972737e74528032a39ff7ca8aa2560b9babb8d3b
c0920f4fcca8b769c182fcd6c5c26ff613956e4d5f061e7de03ec37fcf0399ec
c0f8569ba45413e1bf01359f0b06e187a7fe0394b15ed6d4bad01c42900a62d5
c11881c8974b8b0858a9e950f36d9784603d25617d6800a8d1288973fe8b8082
c1d5bc73162289534b75dfaa42f3e2877b9fbcf330db6e301a0bbcbae263b120
750e9ed69489e342cb9c0ae5f38cc6c58fbfb2a58f76a5334805713867c16dfc
39e8914940113238696728f7af1a845d299d861c214efd4321607fd226a5b288
c2a84a7a61d105e24d0156eadef054d859f538974e6aea42c5101fe39f4f2b0a
c3ac97e3e88ed60e4061b1681c5d444a864d59d573db0e6ee31076489ae6f314
c5344560b0add73121b5d082f972781408e029a24924ca8d4afbb02e7a5e4119
465480c574bfa716da8bff9d74fc4897cb73fa5ffe0035c9dbc33a2600651501

Hash
c685cc1f7c61703d74dc2991a650f953da35f83af1d75232003d82c142bcfa43
c7c8a31adaed86b0b794c79f9a7211a63bcd88cbe2888e972f7b009a1615c052
c937589a2184e614f626093ef8c7c0f4ae949a880e94d6067d5b1eb7ac485fb9
75712267b820d5f2b345e5a2326c4b1cc49acf2d99b1110dbbb8789e5ea98cdd
328afb6f88f31882840b81503cc24f4ba23e8556bf837aeab78553d2127353bb
c9d803c5f4b551dfd867814aa64818472ef67d5411ccb6e42ce79d080ff6cb3f
31c167ce079e868b5ef7b2eade838bc9a8a65e3ef0040e4a978297ba2441ceac
ce10f25e72d0b684e3a245deae8bb37348e5ab06bf4bc416ebff3ee2f0e18ff2
d07b1f8f8c2dec9126d087fa3f2f95801888848eb8051b005238f4e6516f1fd2
d0f4a1c606c969472bf2a8f87a73a7171df43d339bb4fa894086b328844abda2
d1f573fe429060f5fb53c3ab23bddef2350e732798089a18e18a7241ab5b6ac2
d251bdeaafb392980c1eff33ecddf0b02bf5f58d744c9a85846596cb60f73487
d4b292e243ff23f3e1ec1bfd4cb2a652a00aaae94ebf545540c91ee0e85a4967
d50966045ee38fb2caa33fa3b38009b7898d39553e59bbb02fa9dc72fb3c0659
734b549c0d4d739f068f6f8077d0f4a1b654cbcc0f5c988c8df9abaa868590c6
d5419a691346850d8ee6ee4ca1ced9859ed9a05bf4879c4ccef63790102e4082
816b3cbbbafae91200abc4f945020c5b4873163b3209f88a29a5f577ed71176d
9529e35b501fdc5654387621e379af22c269c39443f8f1fffdeb29e8a91ce5a6
dcaf291e1dc16bb7dbaaca34e1dedf4957fe64cb4daa8fe6935ff8d697297e3f
d569c4e8c5deed0adc2096894b5f14018d655ab6d227581434290b4e2c9dcc52
50538f68bac60f7fcd67870293fe5ad22b327a218daa46d2645e621cef192273
dadff322a6de09d9c283ff71b3bf9c01e59e365805fb90a8b19e7cf705a15a6d
db8adcabcc6cb5fdbfa9b798e5bf26572f252f2a533ea9f0c4ae275718cb4386
db9089ad383a6841eb24cb54f6fe4b81a2bc4a2077ee3d1d5b4c73d08b0b018c
de076c4a92e8fd52896c7eaf1cfc858d818f9211c03a16e0164f89bc1a348efc
e19e7e8bb5b79e63551bfc705e089c6e1860db0f2391d732690b7c8c43410f2c
3b1f573956277a792ff91e58e22fc553b9bdd1ea38ff20923b0d5bf61d8992b4
e24f67ffbd330248f3c1a08ca18a1067514b6164120d92e181791ae471ae2151
e2dfa4460015efde739e3eeee9cbcfe8be6a4ab5f69ccbf3571f44c8b266dc35
e4c561a1bb26cfbf280da608621cc1be631f929a497a5ad44e552794b7f81919
e5fa951e7617e6148136ac1d569a184f39d6f6e20cc6639678272fff5c0ca1a7
e766d53429ae9a4898f2f74edcce2b7c9e34bbf4aed7091f591c246eaf0af844
e9121b8d9ae10feec24b87b573aa02c00ba8e9a57575b937a188f49cc5d839f5
ea047af966f163e9edd9aa967fbacdf44ea63a65c83240e8f40ab8104156727a
eaedb03e725c99190946ed5a13f813c6d42dfba18e5f8d0164b47e0443916d01
ee6ce3c491f18bf1224af068b5d5ca77bfddc02a077e28e34efb1daa36400384

Hash
b4831bf30c12e050b84b1e89276edb186d12a896d445edda737a08ad44883c29
3b4d80069beed743c9050d6b49ec0dddbcc2e080f8454a6129bf7952a9127fec
f5f23591cfe058cb901df10dd8ea13364145a55cb51d02bf743465ea2202499b
fa58f1936f11c1eae0ca8f7df26fbfbfd0a8042dccecbbcc70c4d4d823d638a1
fad6e322b7f651b93ce3d4364bd800ae5b0396a7293bee4a78fc0dc5ea7ae354
fafcdee8011d6f76ad7a9df5cef9668ef49d1b20dc80aea680540af2a1e74c62
fbb7ff709ca65f1b522c1124cac92c2f7c89d26e6bd525979f7de2981941fd23
fd7670eb02d28ded25c4602b17bfe191a0e1bcee3b6d0fe77d240060f6b579b3
c16d3e8692911c91f206c2c89ac19b9ce055c5cf85955230cc04cf07e780df1d
5a81a46a3bdd19dafc6c87d277267a5d44f3a1b5302f2cc1111d84b7bad5610d
56bc63bab6eb39620a2354786be1fc83ca2d671a65b2fb721dff8ebb37e14477
233b722d86c7ae5117dba82f66c4466025a5aaf5d79e328fb7ca914f52163b09
0d78333872a69335ffaf88b656203f80c1feacddd34222fa55a9265d789ba3c9
8e150cbe800f53e9d793ae81f04f38477b05545ca6ce88ca3b01545e93afd475
17480ec6f3870b95bd3f04d246bbcdf986f6f4ec766add4183531f64a11d0f58
de534035ac566b463497bc793f6e7d98ada1b2138b1c71aea8afdefc4d45d56c
3a790a81a516654c7e0cde57860302c50a347b8892d5df228dbec715206f5bb8
c087a219e19dfadcfc362b8d6dc34f1b099a9d28b8ac52de14ee69234e7a31fc
a185fc824db672a0f232ff17fdd54a822a75a55a73e7bfa0b037533389724811
5c0946b1de0fae8f43ee64bbbd7fc8e09c9b0bd41e0eceddc6ce4a69ca228ae5
e0c8acd299c3facfe1b1f42a1352dbfe11f8680f33746598e0ea081b5ba7521f
0c32291f06e8b941b793eecf03e40bba49ff6ef5ecc8d91d3910ab0f3c04d4c1
0cbb1438b05108ce185f814ddd8460d4209fdcfb37c92e7efae145514ddc8141
f7dfa7153d314d28f6ff6116611cca5ee9bcc562cdd8e1a649aa29a3069b777e
7005af1e6b164d36212a9da584648128752ceeb038f02d7ed2bf77a133a41c75
5b48c6893f33d43d0121d477f5acc7eca3bcd69244e4c83436fb453d568d9499
01dce18bf08729e030a935d28c6cd751b8cbfbf0ad65006c8b0a172b1299b6c5
92616ffe01b32d3c3608f8939bb55e6bad17fbf6cc247f30a07bcd7de37d9141
44f040ce334bdbe0158fad0446961ea5f1cd1099bd121992e73c344f7b13cf80
8593d519377d4ee61a8f3f72b4e936aca1a4e0c9a91cf880922e1cbda7dfb347
ac87f201ff84fbdfc9f8b52b3ea62c59fc89d2a636138c8f749965e6ec540098

Related command-and-control (C&C) domains/IP addresses:

IP Address/Domain
123[.]51[.]208[.]81
45[[.]]76[.]194[.]59
59[.]188[.]239[.]218
111[.]200[.]189[.]88
113[.]196[.]70[.]151
123[.]125[.]114[.]169
150[.]95[.]154[.]165
184[.]169[.]144[.]229
58[.]158[.]177[.]102
11[.]36[.]214[.]134
11[.]22[.]33[.]44
11[.]36[.]214[.]181
219[.]76[.]208[.]163
183[.]60[.]188[.]241
185[.]53[.]179[.]7
192[.]241[.]211[.]213
211[.]43[.]204[.]125
220[.]246[.]16[.]209
47[.]88[.]18[.]79
54[.]248[.]229[.]24
58[.]158[.]177[.]102
59[.]125[.]88[.]98
61[.]147[.]125[.]184
61[.]170[.]201[.]107
96[.]44[.]155[.]21
abcpees[.]webhop[.]net
ancelon[.]webhop[.]net
anitacxb[.]servebbs[.]com
bi-apple[.]net
bitdefender[.]minidns[.]net
ccc[.]th-fish[.]com
ccuugo[.]8866[.]org
checkerror[.]obama20009[.]com
cheng[.]pc-officer[.]com

IP Address/Domain
cometocome[.]8866[.]org
computerupdate[.]servegame[.]com
cooperlzh[.]liondrive[.]com
d1c2f3[.]3322[.]org
data[.]lovequintet[.]com
divineart[.]dyndns[.]org
domain[.]uyghuri[.]com
enterdia[.]zyns[.]com
erbilin[.]blogdns[.]com
feng[.]pc-officer[.]com
fifaoopp[.]webhop[.]net
gmail[.]servebbs[.]com
goodhope[.]no-ip[.]org
googleads[.]serveftp[.]com
handinhand[.]blogdns[.]org
harris[.]3322[.]org
hinetrouter[.]serveftp[.]org
hongzong[.]xicp[.]net
hzcj[.]8866[.]org
hzong[.]welikejack[.]com
ie-update[.]sytes[.]net
ifsbsa[.]bounceme[.]net
ihe1979[.]3322[.]org
intershare[.]zapto[.]net
intershare[.]zapto[.]org
introy[.]toh[.]info
ius[.]uyghuri[.]com
japanisok[.]selfip[.]org
jmjm[.]bounceme[.]net
killabcd[.]9966[.]org
kingcoast[.]3322[.]org
kingcoast[.]6688[.]org
kingcoast[.]homedns[.]org
kmtzh[.]zyns[.]com
ksforever[.]no-ip[.]org
liumingzhen[.]myftp[.]org

IP Address/Domain
liumingzhen[.]zapto[.]org
liveupdate[.]dyndns[.]biz
lovemoney[.]2288[.]org
lyle[.]3322[.]org
lyle[.]homedns[.]org
mcrcancer[.]podzone[.]org
mcrcount[.]bounceme[.]net
mcrcount[.]podzone[.]org
meet[.]servebbs[.]org
menberservice[.]3322[.]org
microsoft[.]dumb1[.]com
mkmk[.]bounceme[.]net
mmm[.]freesite[.]us
msdndown1[.]3322[.]org
myblog[.]bounceme[.]net
mylife33[.]zapto[.]org
mywebpage[.]3322[.]org
newton1666[.]3322[.]org
nothingtolose[.]3322[.]org
nothingtolose[.]changeip[.]org
olyone[.]com
oohshit[.]dnsdojo[.]com
own[.]webhop[.]net
oyd[.]3322[.]org
pklei45[.]3322[.]org
pklei56[.]3322[.]org
plscoverko[.]meibu[.]com
pop[.]miyazakihousou[.]com
popo[.]bi-apple[.]net
popularcat[.]hopto[.]org
pvp[.]scylla4421[.]com
rainflow[.]dontexist[.]com
readdook[.]selfip[.]com
red[.]istme[.]com
sbd[.]7766[.]org
services[.]dyndns[.]biz

IP Address/Domain
smtp[.]hitachis[.]net
sportsnews[.]chilichi[.]com
stemba[.]bounceme[.]net
sweetbug[.]selfip[.]net
sweetcard[.]3322[.]org
sweetseed[.]3322[.]org
tempfy[.]9966[.]org
tempsys[.]8866[.]prg
tencent[.]ikwb[.]COM
todayzh[.]sytes[.]net
tv[.]kingdomcer[.]com
update[.]ddns[.]ms
update[.]ns01[.]biz
update[.]support-microsoft[.]net
update[.]toh[.]info
vnn[.]dinhk[.]net
web[.]achteins[.]com
webcache[.]zapto[.]org
webhost[.]j2ee[.]us
webmail[.]hinet2010[.]com
webstation[.]webhop[.]net
webupdate[.]selfip[.]com
winautoupdate[.]acmetoy[.]com
windowsupdate8[.]3322[.]org
www[.]bi-apple[.]net
www[.]fisu[.]rr[.]nu
www[.]lycosgame[.]com
www[.]s27[.]dondon555[.]com
www[.]sctw06[.]com
xinxin[.]6600[.]org
yahoo[.]jungleheart[.]com
yahoo[.]qpoe[.]com
yaxiko[.]bounceme[.]net
yitiao[.]dyndns-blog[.]com
yunmin[.]3322[.]org
zhngzng[.]mcchrystalvs[.]com

IP Address/Domain
zwy2007[.]pc-officer[.]com
abcdns[.]bounceme[.]net
popftp[.]bounceme[.]net

Securing Your Journey to the Cloud

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.

Created by:

TrendLabs

Global Technical Support & R&D Center of TREND MICRO