TrendLabs

OnionDog is not a Targeted Attack– It's a Cyber Drill

Appendix

TrendLabs Security Intelligence Blog
Feike Hacquebord, Stephen Hilt and Fernando Mercês
Forward-Looking Threat Research Team
August 2017

Hashes related to OnionDog

SHA256
d68b02d652c7c82ef978462be1e9e25fa0a91a20ea1fe229dbeda7613d8c421c
caf4b03118e5c5580c67b094d58389ade565d5ae82c392bb61fc0166063e845a
b35b7a1b437d5998b77e10fdbf166862381358250cf2d1b34b61cf682157ff19
04e87e473d34974874dd0a5289433c95ef27a3405ba9ad933800b1b855e6e21a
e20d0a8e1dec96ed20bd476323409f8f5c09531777207cfeda6b7f3573426104
8b91cfd40529b5667bbdab970d8dba05fca0952fffba8ccbb1ad9549d204ba85
0ea456fd1274a784924d27beddc1a5caa4aa2f8c5abdf86eb40637fe42b43a7f
7461e8b7416bf8878d20a696a27ccf378c93afc6c8f120840c3738b9508839d2
65d226469d6bdb1e7056864fe6d3866c8c72613b6b61a59547ef9c36eda177dd
8ed20bc6e8ad762a629abe544e110f6560f21a0dec1d0ce5e0c6ebac5e3c9845
02775a347a3ff8bd9e2ad572c87cc0894925c24d12df7dc27012135e8da27987
fe141ccafe7fe4d935e6100266a9732ef05fbdf9f480482d94511d12ccc65114
32cc632a78e1920207d91500e6f9eb53789e4a772062630f8a97ad252ffc7d9e
cfda551e1dafc0277c465c58ed7cb2a4080c833637a867844bf98358cab079ba
021d0a574c091669e89b79e17c7e10be9c16e30966183fce52355442fd561874
6dcd5b87e36871acc4aaf3681cbbdafc53bbfff948057aeebe8b3b31ff12f74b
efdde1199471b31e005d4b5f625ef6007de8263474ff9d1d1bc33d4b18038d6e
d7880fb06511169bd6a9b0ac4e85f229eede2d74fea9b852cd9bc079b714e87af
cd45576293f9e4944204e06c39162d5868da037e8ceca50ae78230978471b34a
6022dca8696fdeb2b96e346432beba78343b368178910084d932eeccbc77f74a
657c1f898a24ae132797541fc7f8b3795e5311558bfa2144a3a8307c1fc2b074
676d2f37714d97a0661c430f909578d5baee86eb772c2d8c908f67d6a9205d60
bbffa75fae80d9948f70aa4082c6afd511ab1a66bec8c875c5d0173a899615361
51d0eedcd6fd1c17a9f45128c05c31d1799b7373b49120b2f9322fe49c54e03b
b71f6bdaa5c125cdec06e24c20894c41aa0b3ff46bb0192d486ac2c67bed44ef
09a163c85e811ba849235c6ea2b0b68de26b14474e0bf73534ad2da82221 6564
341cf0a437efa95edce1af1e5a501dedbce82587d362597680b13bf57f305fe5
2785586432c166cf240b511279b503f1b9172e1abcf77a34f4eefb4cc3d8edd8
59c30861327a4b2f724fabdb1e5510a8edde30ddaad8bbd041990e72db79b218
78d0eea998efcfaf7f663cf636aaf3601a610a353400 81768255a71eebfbb325

SHA256
27f5e36b7955eabaf8359ac44ec288b89f8ea6caf9a715f8c3171f2780223fb5
8576999f345f1affe583a3deb7ed9568f82c1268693 1e0e3e054b65eed87bec8
0b6a4ebbe9cb81c79366a4021779cc4942d3741d9ba1ce47a73fd6d1b74d0cde
19f5e7facf4fdedc5f57fc4250340a8492efa1924dd498c700b980279475d401
8c32f95528b540848786e3e319fe2bf7b2c94edf2a793b2e7a69b0ad12672cd5
3671dae45e85908eac947719e3b1ca747dc7d6e01c9cdbc93b7145429ee3541c
5b02a41d9e7a85a8342947bbb024b52254cb612fcb0fef628009ac0e3208ca78
7ce2b81c5b998cb02d18d4e680a512d80d8cc810a193809e30d4bda1030fd536
59a91f8558b873de35c4009377fde42512d597edf23f36a115817b2d5f22aed8
a2e66cb026bcf208a75b44d7742d9d8bf48d8760d081a76ddaf0aff97f448afc
a796d114e4ef606a9bb6509678b8282c3049d7537ec2b7b52cf0752cf1fe4a67
44a47f85ea9b331b84899ecd0d72c891ea6bcce2ec89e957d03ff3d1dd7313e4
7c0eca715a01e2c3af83769d41c8f52ee3f9eacfa44000eb7b5f1bec09313a40
6930b5d5d8df2a4e1351995c9b5c1f988242ee5a7486d9e7481c7b7b54d93cc0
ec0435761f7dc69d7cf4837704c71ec37bbe1e717f97310328c7415cb7c9632c
7411b8569a2a2dd0e9daaf2dee4978897f284a985aeb1c9160a5f981a71eab19
bc9310c2903d7467c2f8079f10ce32a35bd756c9e2482e9f2a3448cb59ccd75d
48496ffaf326b1b750cae04852d6fe27691 4358e08770ff8b4c27bcb739c05a8
adc225ba659207a4296ebe6d410da2d8a9f137f5f2e3b496c829840054c2dbf0
c8091a68a7feb59c84ab94bfa5e8b7c03d6235b26bd5dfc9607cd1afd211df79
25f58d026b9edad6ec70b85259492765a35fdcc25cfc03ff16bb17e4c28c6bee
6679f5b314344bc73fe05f42e1f7a570c5aa32918269f5f10418d94cb7baa19b
9ce8ab6c638333 17df723543a76a55428d57aa908fe140ac286a469646d8b6bb
eccfb3d553eb4ad90c88a708012177f68032d1cb74d6237b94308ab0a5d22e7c
47df91e4955da2171242c38a1eabc5bacaaa2ffa10e83a9f1aeafad5d83 11262
8a715139876a59e25adcb6c9c9d249e08d426a47f14ce683fb10e4195aac973c
fb1b61510fba0fcb6d46617a37ee1d31b8db508e89bbc38d7e568b6ffecfc2a8
0c7f1e12c205782fe9aedee6dccd40dcf75318e73d98e4799bbb24441dabada5
d725fc704da1336d800c7ec99089ab4f28495217f561b5a8a64acbd9735983bc
94b3c877c4eaab587cf76afae47a293e5520a2545f65324db4f02ddc736d1306
0889943fb8a7146088f5c64563da6fa7f7741da70a46b8444c438fbd46df44b3
1366700b85f58bc520e2a1299f2e6b6a94a937ee4e4bdd6cb6ed7c18b04b82d7
50e12b0fa6e04e860cacb66665a32d8df2667f21ba5eeecb875fcea54d8d7c2d
8f955bd4cfe0ddf8d9bea4bc2eb9bb952b492df9ae5e634a627f610df52c9ef3

SHA256
9dfc6f9806d6c23c167e0c57630a737231b1dc05cc53dc93a3d186e2536 17942
0a1cc104e2da8613f98d6145afb4c045bdfb3e30e6fc1ec1b61f195ebc8a62d7
25bd8cb3e3a85044c6e6c5bfc1cbae3c5f7002193018a28b4c29085872c0de79
4333ed8da7a62577458a218f94e485cca61a958fefa0f38216e5c157dd4bf4c6
6e776637b2dc4f59a97fc80b6d94dd5c37f30191e317b9c3eff12d3f715c136a
2c6fb1f2857b3559c114567e18d0df2d6ec44ea0945694c2214696d2b113791d
a50961545d70c51504d9e9141f94ce4ae54d52f195867f3e6d48e0139e267c8d
37731c0a16b1cce6c5ef2ea545404789c7abc544677ec9ca4dcb061ac66aebae
b22fe683a6f6186f85d2cd8bdb8283bd155a6b081a709f71bce57e07d7a35357
c406eac2bc6482b2032345664566791220417a362895b5472486e5f19b0d3670
f9e7c489a6425647d816da862ed57067029c01b8a93f957dc24b859cf85da109
21069305dc8c2752633afaa5587b138050e83aadfe5452dddc01dbb6894cc0df
e85ea2ca047da9ccc1d9aa2a45d0b5146973c9a8be7f2b5110855424a761ed84
a5372808797869c13e468ae05b40edfcaf731c540980f780f54d87b46d1074d2
aded85302beb377a7f9e80c3b08ab4aeea3c657c971d7d7f80b756c72d0321b4
7eeed7d7ca3799f3c22fcd77e1867a1368e61ecf2a3dd51742749d612f84f9bb
2e8566427f2928a2741a693b8dedb0590b98e30a9dcb9dea1e88851b751a0417
309a1b59a42660a73ec337805215cd6571d6475699e9a22545a176cc3b507a19
0e2b2aee7e6f17711a2de624151fa470ec2488f729872 1c8d17db1b3fbce0127
859e9bc37727ebd3edcfb58b85048780c40a24a3a757cf99205ed78ba8aa0b98
993eddb61df6f55b128a7ada786863b51a11039b2456204d3099a925bbe7094e
64974936868eafd4fd53a7b68bf1d9590d831ad92e8f141c5bec46ae7a5c4caa
0d6224d93e8addcfa5484ff6e2de2df14b3844a56eb47b9fc86e7e004e5440d8
66c40aacb45ec111e6c846b7448ef7bd910222145cff6cb1726010fa7e55dbdc
a3008faf7a5eb47e9640c96589f88821a3c658ebafe47a1a32c3a6279e8ca522
cfa04049066c370c1d45a5fd0932d25f73104b6bc7258c4ed94774970 1ac6434
7f80ff85eb742b1690cb7c6746e0f76689def2b681c98c50133e02ace2b60863
af45b09a94ccba4c5430d9be17eafeeb165a3866833a691d369ff6832457e2e2
9bc88e1a3ccbce34e79402abecb240c469fab1357ab78f546fa2ebc9edf74fc9
11487fc787cb338ce95743ed311d4a2760d597a3706d3d845c578f86c46c96ef
bdfc0a14d4d77af159f5d20f62239b7e8069ae7ebbe4dfbd21ee1c9bef2331cd
b09a3a5081f61c5f79b1c30e753a7b6a8885a18e7d198aa03dfa22727f286202
d8329cb2b2501e9962afd893484a7158f0c716539b3358db91fb2a30b9711fcf
f4c890b06a9028160b1784829c07c2a527da261919597f58417c9acea2b1e79a

SHA256
ddd5665924c9ae76ad74e5c016960041c7b1590b9ba0605818da97b004616efd
142b0fac8d8012dc99b266210dd91d0cc06ee1a02e1fcc51229dcc7f7ed2356f
9d3f238a7cfda5c9bb877bc08a5dd0ff497577d6b920e1a3007a3b4911abbaa98
ee628238b687d5da9e527d51b03fe1d5d6967649a9a2bd6a0825d08d51cc392c
c87092a656b55e9c85bbac40cfcb5290a1fbb9f28b08dfef65a837dcd5472ad4
e7216aee90e253ad0f73412378e1931e7d51480f6ef151a545c708f7f14157e3
cdd54a1062a2435c2be8e68412 9f58c07afa0ce9d97a7400b7f7b97c22414627
a00ca360c6031fc554306dfac1614eb6a4d92b60162b35fdbc8de0cd1a046653
73feb65831292b0ea5cf3b00d209168d254bc1d5251b5789fdcae227cdb3aeee
2712eb170d0828e4a72c972bdc472f478a19cfda313c18bd80fc5d38862b9ab5
5f74c79979c7a294d045f2e8da2c88330d0f2def2b16990033772bceddf2cc66
fba8f9b2805df39275fcec6dd8560a85764c13cc9550eaa05040697 1966d42f8
c0bac62f0ac543e54b9f9bf33f34939c02175585883dbc924d5d9514bacf4f4d
abb98e8cfe3a07945e2e66ae9434f6c5347b6fed58d2cf77d88f6e3468eadb52
7ac8469c772b876e87ce5cbffdbc0c6162e685ddcb22e275f6aca2d38a901d1e
4796ea421ef859b25d8f01a15f0e1825c7eb8f9358395223b2c6441a4ad5d14c
ca5ecd31f043c9111545aa6d1ddec8b44832b09b2308fd9dc0c7b21ea15871bec
f6dfe0b761627af690261a0b3047a18a00bdb00b1a5e085b787528e90fe3bc6b
b84f16e0ce94d92856bdf15ddbae47b0a7997d6e49838c99e37e900aabbc1f4b
6dd79b5b9778dc0b0abefa261933211444236a1525d03227f150e6e968999fea5
a1a55db417eedb05cf0637bdb971b51dfab80777da43c03632dd7aa849ce7e3d
771a93a229730fb998ebdeece02941d04ade375a700b8b6f7d6e90ba6f57ab97
4eb259145d4e16d84becea2f7c4ac6117a3a00e267203a3da13a70bdddf93c6a
19ced8ed70cb4bf1a4569bc1b0c978a5def366f7fc17cc3b34e00dd51f0c101f
19e3aa92bc16915d9f3ff17731caf43519169fddda4910ad5becb71ef87a29d5
e3027a49dff553b39f80974c36f20ca2f474abcdf79f7ec9af7b82210b8a45ee
7e12a43918ec9e2b729b936dbbfa9c6737acbf0110b1f357af4a83 10dc421b04
5b891f01bc4f413973fa87b34328c59ba48693f3d286804cb5d5ee42a6ba2581
f5180c7d96ed9a1b84f7105f20bb954b9d000a81f7a7a1a92f4c15632974a582
e95f11fe9a7c5e0ae62f8a09256cf8fb6c7e4bee04647b273d357ae734686057
a5f236e223c2ad096aa53a079c35d70819125df7f78a35a815e73d64627a01fb
14753937ad812ce022af066926a4cf23ab52c581d1b2c6ccb9d0bf6e6fd0e321
002a74001a94097ffe7db360977e0c032d5a3ca0f8fa3a97230b702e7cc0f96a
2cca60a4203317b34c6ddf0b493641e8234cce81ce47e8d5748baecb0a54b3c7

SHA256
d70e6c5b58443f6a5219bcb9acbd2886ab5599340349aa8341a70f14e8e5f008
c73c52ba6ba637c3caf1abb54225484e521d04ded56c16b7e57d63059047a5dc
7214f2c9fdf0986c8595c837e368b92890f3e7995dca3d8a333c0c5bd999c048
24408c0ccab096b89214b83e053a47941e447fe271ebaf6dd8096972 1f19d15d
2113b988d5d157d27d96571166e4fe7e049f110f36fd4cf581b2131474730e7b
1f5215d8629244419cce265d3e99f971b9d6080d6f6c61233b0081033a00524e
0b90f63c0e166a0c90309fc301520ae53c1417598f53325bba462e690d60bc31
01ca27842b51417e82cc17e1414fb45f8d9751bafc65befefa46efc8a39a3d38
14c0dc3dd99d19d807c64bc0a271ea96a2f02034a53108715944e4486d3cf1da
f3ddfea30ad747986fa3c544cffd676bed7d98d4efefc78a44a7766ef56b9555
d76392c7c98ef4b511a1baed176919f4f4166149804 1809c5198e90eadb10155
d5b8db004ed6757ac882c48064b9dae6f14fd5f608fdb9a8e5d8dedcecd8d958
a1221b16005c113d68876818193e22b3bad7fea75eb986f3c4a840a9e411dcc0
999c1d4c070e6817c3d447cf9b9869b63e82c21c6e01c6ea740fbed38b730e6e
8d171e6c75baafca5a81afb6dd0db1ecdb4812c01fd15691e24ef752463ed7a1
8234964c3376a64e599c26f9271b56d0a08b0bfd744b21cbdca2ddb27908f609
801790e4dd3b4dea097c596172757a64a3dd88af959d801b70ed397282d30f87
51dcb12b628a76ba4622e0eafc45ff46fcd0dc68ab8cd709b7dbe7ca02262967
938eac8dfcd29a5af94435adf5fabb6a3606e9ea8e54dcf43e61790cc657ec93
3bcf2c27125cd1972e494715ab9474768f786481755c4f8262838018828be17d
371d41290a194b55eca6b31b42c52bfdb8536c94703b60b63b255347d3caa381
2c6f1ed0e6aee0670dc663c56b576d34ad4a166ba6e805b7f6e066f8506ed387
f2eeaa46293fd2eead9204850dad4cd6c7968cb75c8326a9a723d8407586808b
a57d6ca446cf42a7fb0c0f57e397551ee8b80143202fd83f4af1f58fc1005492
0b01ab3290bcdee9de30857773583222abd3451c8958194a3109fbb0ccea0934
8ad3808d334c3f121d75d2fb0bdb3de0930794b1a91796de6b307305055e1eee
5c2a5278bdcab5eeeaf8ae99f940fe53720f718f23b38b647ea8db79741601b5
fd03f3f65979ec7b8b6055f92f023b08f57c3095557d1f00d88f01f4d4cb46b7
82a3dc0116e0a9b10bce21960974d7807cb1486cb35cf34f667c9a7ed48f428c
430d84e1a4a5f173a70691eaf26be0e4835a707f91e7fb6f29328e70aed9790c
cd5b03d25f8fc55468f7495ff8c3a41c4b1e248e4a4a58e23274837258417e1c
ad038dc980db8e6ec238be3c75e41be1b55f1a40edc935350fc1e926a99ed30f
72e36170fc562ffd588947fd601b445abba4a4ee18d1d20a5d1fbf0e0b79c88e
10ad851a902988f07617a62f286a09e8bf7c19ee44fbf0e212f8cced48fcd04f

SHA256
726d6624da0ca41747c3f3ab3217d903263b83c58210ef2c77f71d5aa2b89b5f
c4dff924b7caf630862feedd2a170fbf748cfbdf57b121a5b102b143a5a813ab
81fe451ce8f6104f967f8d2ca396852254c8ddd1fb59cf796fd5afe5d53491a7
953261cdd69de339e6b93ff92916eb8f02ecbba30b0efd8d73c6d8593efc362f
fd39455190b473eda8b6d9eaf344c35bfd546714caab618ed50e895331c64c47
17e588895e43eb13dd35e82ca9cff24a83f27066364c84c77ad3ada95328ec20
e467a5ae45b0d513e595cac20e101a0dcc24af606a8502850f63d41a34eb17c9
3455b918d86868d2d7cb891bf8b94b6f711333dd67700366ac9d014cdcd7fcf2
a63cb4765526de361c83da3f82bd1fcd5131e597b6184ed463e65f0828e9dcb6
0f358abccad1b7ee9265286cdc9655ad4af45c225206cf882b149b3899cf4b0e
ee2d947ae52249310f82fbb321dee3ff162b14d25eeea99dbc51142067cd9c69
ac026007d7274596b407cadb69c5205d0e4bca4b26beb31c94938fa011913bf6
28c26876af2ae471e2ba773a3f806fdb5ad2442976c21f4dbd6d74fd1fbe452e
17810e5db058f948601f5752e16308f7767ee870976b322d6f24a71fdab7244e
0fb492bea2228553abe5da289f45d068559cae7414b8c0a2010cd3ca93c19cdc
478a9b24009e911a7445f3de42aebf08e45d59e8294073a71aa21342c2667be0
d603fb7fa016d5875c422295c20f1258884707115 9f18aaa7f91e04abfa36668
cfbd199b12d8e311ab30a386a3ac6af03b7cf2ea2c3226642ee000633f6b30d9
99205db61b91d00d2840de04876a17f3d4ef02076e9e68323f2a162cb502ae27
4ef916c67a5845571937bec3ab8a701765d14a8241065aeb939280d1f6319a6a
f832c27d29ecffd1274be868ff3c4a0c660701358d1639896624962de3b2b09a
4e036545c634605ecde6333e7b540877b0b5bdb21a034098e938f257d26c59b6
ed788e7930460f9b598e93ffd9923257b98e9f43b52d37b28d5b10efcc15c192
06fd2dc2baf33e36a2b29e4c8925e7cbdeaa39eee03f91f19e100d3bb8e4612a
59f07aa0600a4b1d9bfce24c2edf52fe1e9450af3e0ec2b1dcfdea38f9fc005e
01db1f2b5939aedc280ef464455ad96e9f7f6a9542b56fc676d027c85087e5ac
74d91296df284021bfb0639d5811fe0782de0e5b625b475a4d6276c7466fb33a
1a6769911bf8b5105e6bfd49e8e08b5805753137488ff961409b41c37e538163
b56ddd87378960fa974aa4ff8fc3d2f6b1eaa7c89a9bdace72441c21e7f62b04
d624a8414f665f50e9374a1c2af5617564b5aecd42e82ea2307a835ed48918fb
46fb5bcea417d7ff38edff7e39982aa9f89f890a97d8a0218b6c0f96a5e9bad2
1ffa34f88855991bdc9a153e01c9e18074ba52a773f4da390c4b798df6e6dc4e
f8c71f34a6cfdc9e3c4a0061d5e395ffe11d9d9e77abe1a5d4b6f335d08da130
7564990506f59660c1a434ce1526b2aea35a51f97b8a490353eece18ec10b910

SHA256
fa5799c25b5ea2ecb24ee982a202e68aad77db7e6b18f37151fa744010f69979
1e926d83c25320bcc1f9497898deac05dff096b22789f1ac1f63c46d2c1c16a7
a6842143d8ebc002829c3b532b2b34883dc25e4cbb2efedc5c01879d3e34244a
945bf304020c527124458dcf49788cffbce64de6581552e01c442e8a61b849d7
dbb0878701b8512daa057c93d9653f954dde24a25306dcee014adf7ffff0bdb4

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