TrendLabs

Necurs Evolves to Evade Spam Detection Via Internet Shortcut File

Appendix

TrendLabs Security Intelligence Blog

Miguel Carlo Ang

Threat Researcher

April 2018

Indicators of Compromise (IoC):

Hashes

SHA 256	DETECTION NAME
1fbad258fa1b21723770281ee12c7fad25a1f7ee6012be842c8660f9efff7950	VBS_SCARAB.SMJS02
748e202a2c932dd43bf98f0ad611f79e1c8c1653ba03dae4416981c57a30d343	VBS_SCARAB.SMJS02
502497f5d165b64a2e287d77a06b34abcdedff227089217a874f49f58b536e92	VBS_SCARAB.SMJS02
6599a9e29bb7c607d1a13dc43d8df76c17c93449b654d4e00fb96e02eea2df32	VBS_SCARAB.SMJS02
4f9b95867b6118af70625b49760b75987e152425ab9420f83160e9cee8e79eb1	VBS_SCARAB.SMJS02
2c5d0ae2ed1596394ee8aaa2affe57f7fc62e7338d70f761c906091e00ccdfa0	VBS_SCARAB.SMJS02
e4c5422288d38cd259929177e8d2a2aedf7d6e2c16b19c437be3a36e43601b69	VBS_SCARAB.SMJS02
e8f8fec213d7fef4fe23dc28740e97e40ba5a180b6fc046f334e2971f428ca9b	VBS_SCARAB.SMJS02
2cd60385887a69f42a945006cbf418834356a5ba6e764fa2c1bea4b4336698f0	VBS_SCARAB.SMJS02
04f944284dbbe0f28902a31d1c28b11bf10b22bbff170e18b7d6a9aa213f1142	VBS_SCARAB.SMJS02
f21e070fc12eb506400bef4d5cefc52666ae53323f9dae93300fbbd3f0d25d40	VBS_SCARAB.SMJS02

de209c862d415b25c1a2b38985829c1f04513a262b11ef139930ebc7c4a82d98	VBS_SCARAB.SMJS02
c59f7216ba319749d14e097fa2a090262bf1321061e0b7794f98eebf287ad273	MAL_CERBER-JS03d
e22c5a72111b9037e3f98d7f7e7e3135ddb4fcdaf85e90ca0f9b3e0492232235	VBS_SCARAB.SMJS02
2535c52dad357d25e5ad05f89977c8fff622d99ca145328debf9c5559ec9f4d1	VBS_SCARAB.SMJS02
0bae076148e9c8a4c0d5f9c2080fdfe155e760daa74e14e132e5ea0b349b7280	VBS_SCARAB.SMJS02
b196bde744b8a3d28acd2bc76bca2e415f98d5544c11dc82f7d90ca25dd7c13d	VBS_SCARAB.SMJS02
e0d150a5764e1251d6dc01137419d2ac5092edb2350b6f880a2d30f59f21648b	VBS_SCARAB.SMJS02
ead15d62585d13a7f5eae9f5280db7b54f769039037a375630240a65507acf54	VBS_SCARAB.SMJS02
1b3194d6c06478e877eca6da44bda2f18715d7b9f811568e5ef5cddf86da9130	MAL_CERBER-JS03d
7241f86c2952fa2e1ef78c1515b919a0e0c4b934180d6a81f81bbfc075a3d2b8	VBS_SCARAB.SMJS02
77f164474edea3adf67422771b851c3b1ac6526a84d85671f72bd6e2f513df38	VBS_SCARAB.SMJS02
23a89dd8429748cec6b2250d2980dc3798bdca07367ddda0e1d8c73b0d3b4b47	VBS_SCARAB.SMJS02
b1dbb1ad6e5608a809e0ee3111aa70ca0e4f4fb8842466b55cc7c23be3aaa948	VBS_SCARAB.SMJS02

fa5f5beaac5ec303c3e9b7b3d9def7bdd676d58d38f9849a51ab304786e0de94	VBS_SCARAB.SMJS02
6fee5f477baa3b76805da4906fbc081d74c5e40a0b70e701c7ee0f174f26e354	VBS_SCARAB.SMJS02
fb14086aef4e0c707ed8ee79aed13565b738b9d2f799db94acc77ad615df4356	VBS_SCARAB.SMJS02
35009fdc37faeb343e850e21a4d3990f8e3d34fcd7b8fdf7f7246c1a9d6b35fc	VBS_SCARAB.SMJS02
6f5bf47325dfe356f86adb871d638a05b6fa1b6bb65c8f55a2749a3ba3c2a491	VBS_SCARAB.SMJS02
2e3e168c9e0d1fd9f0e7b561e370c4f2edfb49e6fd5d5c487aa8eec4035c56e1	VBS_SCARAB.SMJS02
8c9851f4dc636a7ce622b726618a603488655a3115894ba02e0d684516239380	VBS_SCARAB.SMJS02
5005de2a04c1105f8ba5c5aa1ba30fd669fdb5a39b60f41964116f7b5d6b2b37	VBS_SCARAB.SMJS02
bdd39542eecf972cf785f0a3783769596ad16f6eae61e73824ad7d6719b258f6	VBS_SCARAB.SMJS02
86a6227cf0c81a7f9221206fe5a0bef4c94df38f4b95fdb976fad0b23579fcc5	MAL_CERBER-JS03d
82d7cc6af7713293c0990c33035379201452ad58a0180163c4c3e40e27d9e6f3	VBS_SCARAB.SMJS02
48b0bbffebc217c584c2fe7eb3c69e82d10fb16db29accfebd220bb50380698c	VBS_SCARAB.SMJS02
14928d3f23804ed5ba0d9f7e02ee06c0d2ef2155a870c77c2b2e6cf771b00e20	VBS_SCARAB.SMJS02

b64bda5f26cb2d5566dc91860c19d39d83a9a15bc575cb84747197863f941f46	VBS_SCARAB.SMJS02
845e1fa87bcab2359bf5d03f6cf0f93717c70e25a55633b04279ffb8a08f876d	VBS_SCARAB.SMJS02
40c01bf77af3a377fa18ba34a2d07f7a8de04b6379b61511d76e17cba120a771	VBS_SCARAB.SMJS02
f93b85be0cc6ac3aaf4a8ab910af8bc9c9f148664e5ad2b6d011f50cfb1b3909	VBS_SCARAB.SMJS02
f1e8f6ba5eca8a7b8a330dd7cc25a963e98d7eb705ed1cb8daa3417f0eeff255	VBS_SCARAB.SMJS02
d7e21f661997f0b051ab47b4a85af3a549f2c877d165c597ba0899849c6dfb08	VBS_SCARAB.SMJS02
f3ec0f14efacaf71273b01976fc9c7f3c9b5be2e4e79d64b4ae6ee73a38a3e6d	JS_DLOADR.AUSUIR
135dde22e025005226470bb00df15a5882664ba7be2890e4fdf773a22d2286ff	VBS_SCARAB.SMJS02
c28dec4a1c668f2b0808b7261594f7acf158896f6b159c299a257191bec46d7f	VBS_SCARAB.SMJS02
2a4aa54359e2c472022c4adbfb44d7668fe4f09c25d5b9c8bc2485c0b29a749a	VBS_SCARAB.SMJS02
6335c60a0f66b9a0b209c8ac345423ceec98a9508b95246f4e7e2e62786b65dc	MAL_CERBER-JS03d
8b4b4e93c927bf9d107965b904ecfe22e4c66a12a739f16fba95f8853502d394	VBS_SCARAB.SMJS02
94a661acf172a288ecb0ddd5b97490fa13c7b9e4ee9a73321d24c5d7dbf155ba	MAL_CERBER-JS03d

8e8e0b905054a3320c5aa49657df54975b92da3b4fc083f2c155b109c45c25a6	VBS_SCARAB.SMJS02
9c8fc92674b4ea500f3460a8dfe01b086f0fff40c547fbde8760c96f5c046a55	VBS_SCARAB.SMJS02
2aa831dc0f27a2d747435c16990a3294f776799f0c1955c308c9b2e397a85538	VBS_SCARAB.SMJS02
956b63f7e9bf7c5b21f591d12bc12ec59ab180a7a694f5bd38b6865300b723f1	VBS_SCARAB.SMJS02
92e2ef830a1c1e282a2e3620c1a25c821ed515009779acf6b850217f557f7915	MAL_CERBER-JS03d
c30e8ca3173401b001de02f545870a3f25d42d892f9596d8641cc3324afe8840	VBS_SCARAB.SMJS02
2ae04579eec0f1af475d06388c8b8a13e63ccbe92474f66115fe17d3f7b902d3	VBS_SCARAB.SMJS02
298f84bdecbe3e0e23f80a76254f802f253e054c04cc3a16ed4fba08704087b7	VBS_SCARAB.SMJS02
15a0bd5dab10341655ac110644e332e8972a1a531adee278657d528d5a4acc0a	VBS_SCARAB.SMJS02
8ac824b167d9f23f02f048d9ea1657d2f070a38add1406a968255f24cd2adaf8	VBS_SCARAB.SMJS02
cd1eb34f3a45b257bed15fdafa4b6a9788b158f1dfe9b9255578595221f92973	MAL_CERBER-JS03d
345c3862678d7b979f8f51422aac4382532d3624bbd75bb2205d4ac32e752c17	MAL_CERBER-JS03d
1cefa19e1bf8cda11168921acf7e2a61750f78cbc15d375fceb26bde73f66feb	VBS_SCARAB.SMJS02

f0a137ab92846fd99fb8828d36cd98ad46f7f1dca7651d4b0b7fed3dea78b6fc	VBS_SCARAB.SMJS02
778c2dbb1da203e30394b0a923e55e35697f4432efc1f0f0c3c41d81a7a90860	VBS_SCARAB.SMJS02
a8730e6eb1ce1c0ec91fd2371d53d11feb51afcb6e25f1dcbca7efc665f50934	VBS_SCARAB.SMJS02
f1881b847abea278660466bd8eed5cfb6415909769475fb849685acc2d110f5a	VBS_SCARAB.SMJS02
8d4b317a21a7685e4066ef040d003782511be50790eb708ad26006f17cb6acee	VBS_SCARAB.SMJS02
47ffa8fea4986abfefb0de951bd3f829480209c45817b21e3a3e6cd9e27ebc0a	VBS_SCARAB.SMJS02
3a4cd03789ca51d53718508a57a2c59500ddac132c89f50fb5d95270e95a73e6	MAL_CERBER-JS03d
4cc82919276e65f58fe841f0da69d063fe5e196a13a19458f47b640f1689c813	MAL_CERBER-JS03d
d05f4d98e44d14ac64ebc1170142232912cde36eb77c0ccd2869788036761257	MAL_CERBER-JS03d
f1646224bfbc4d1c657bf47d7c496ac1282817484ca5a613d5a181b2ac112002	MAL_CERBER-JS03d
76ca7c477b0af7da335cccdd951300c26a9f13cbe7e623d94817d92e1723f53a	MAL_CERBER-JS03d
023baa1f2500bcf1828eae79bd49f5fae0d3e39bdb19267f01b20c84984cda5a	MAL_CERBER-JS03d
fcc257db11a49e1fb12658a992c04f75cd0cfa4010ae07ee10c4a8647df71791	MAL_CERBER-JS03d

a25f0a95a1a953013288d503bcee88f1250425678ad06161b8f7d5e85cad18e0	MAL_CERBER-JS03d
90ae1b460196df46aa5eceb7733348ec06907ea5e12639a97bee9a8660eeeade	MAL_CERBER-JS03d
0428be098c0d03f630d4eb7cda6b8694596c9eeebea17f2ce7e4136b9340d218	MAL_CERBER-JS03d
03e4d28308eb99a8c39ed499e4f23c8ff7580c32a399675d4895761c3791151d	MAL_CERBER-JS03d
e212fafdf27f579678e5ef217e79d9072562bdfaa2f571b9785218bc833e0b44	MAL_CERBER-JS03d
a9c4c53e851a58971d62297723de1d8cb73889c912f05341797603568ee838a6	MAL_CERBER-JS03d
d1d66e8a8bfd7a5abd738437dea48c2aa7e438f32e8ca953d4ea40f915cb8a9e	MAL_CERBER-JS03d
76c7020ff73beee56291b2b05000ae7e3663d92f3e4ec44a309a51515cc4aa7f	MAL_CERBER-JS03d
43cc723616d7b6c893b240db71620443ab9217cc19ae59df729fa2048a1650af	MAL_CERBER-JS03d
d1ee8a04e22fdff87e027f50bfb48e1f9cb20c4bce330c0e8ebef8802d5756f9	MAL_CERBER-JS03d
aec8ce3910920d09cd73edff6fe30b2154e3605ff5cd073b9be77dc53b5691ea	MAL_CERBER-JS03d
f79dd28832c3fdac339a701f73ffb2113c5e1add5dcc59643092d404c309e4e9	MAL_CERBER-JS03d
af12f11f6c8ad3a2d07275f4a0e9505f623c0b00554f6fa7ff25e2828ecc756e	MAL_CERBER-JS03d

c4f3fa4a9c84db632516d0b959095fc7b1fdf644c2f5efc32d44d48a9685c031	TROJ_FRS.VSN03D18
0f2f0756f59a70d886de0f97aac11f2f63d61502e8946f407b770fa6ce847f31	MAL_CERBER-JS03d
cdd343e4d903241d24997809c3b72a784cf2de36e13c8c5bbcfcad012c9ccf05	MAL_CERBER-JS03d
d2e701ed3cf082b1e3bf2347ebdcf71353f4dafae82a83ab23c226a8e3e7da27	MAL_CERBER-JS03d
c9978d21dd870699596e3ec15e2750624ea4d356fe9a94bc277f16641a41c0d8	MAL_CERBER-JS03d
82c4347908551bdcedced44c7608f6ce21efb254ed0203aa66223bc81da49ba4	MAL_CERBER-JS03d
0c1fe5ec678d9b9917212bd9d4879d6454aec7ff2d20c2057540e7af8f7c714b	MAL_CERBER-JS03d
2ec2c650a57e601273d5f9dacf69d7fac8c1b454991770b65f3ba4a854a70c41	MAL_CERBER-JS03d
bda0a0a3c8f5443c17e518910de18339240a86783464133c5bd631a776a34cdf	MAL_CERBER-JS03d
c29aff59dddadf5f0260f4343f123fde1be089997c16ce3c440a61506e2dfee5	MAL_CERBER-JS03d
a51ad34ccb701af345b6d37cb8f6a726e105d725d377cbc796b2f880d979c5be	MAL_CERBER-JS03d
b1d5e926016491d8bded5aaa29d8bb5a96614468e53283a6b43f008dadea6d6d	MAL_CERBER-JS03d
04e96c7a6bd4ce5ea57028bedf7c3abf8d961d65c65337f5297684228134e93d	MAL_CERBER-JS03d

928ffc036b623b0411a3d50571c1297397a0e4c72273ad1d89f815ac5ba16677	MAL_CERBER-JS03d
918be9a58770b65cdff21a8bc95d4be296259e545162b2c9f826bcdb7dd0b975	MAL_CERBER-JS03d
1d89cccec8c1c66db35e6d21866102c7cd6d0fb186b539871c76fb5e9998440f	MAL_CERBER-JS03d
d708c607a9de7c3f8188eaa94f0fa700eb53a6733ce7c176bc4fd99bc443f38e	MAL_CERBER-JS03d
7ce3785aec3d5fe4515082aed0f4fb08ef4fc65c8fc5fce5ec038fe010f7dbd3	MAL_CERBER-JS03d
6822d3b61544a44104e1ecba40e09bf175abe5ae1f8f391b91a45da2ef2c1812	MAL_CERBER-JS03d
e02ee08cad5e7835371315774c526e62afe1b754dd90d339e3c355fded3ecb5f	MAL_CERBER-JS03d
aeaeb874b1a73e2dd83b1be2ace8ce65cfc62c951d28dd5a46e3c8b72d99b3f6	MAL_CERBER-JS03d
eda46d89028298b4410fa513726149073c8fddb20c64e4e9f5b656e9cb35822b	MAL_CERBER-JS03d
f8b9bd23dab34e9001d2b734cca71c9915d52b6cf4e86f966ce8ed60172464be	MAL_CERBER-JS03d
4c6ce4083dc4d92e91b332f03605c767c246d3d2b90f4c839d60bf9bbee44301	MAL_CERBER-JS03d
c74ab94de5b1fa5367b15defea0952339972205ede8f940cbe19541928bf53ce	MAL_CERBER-JS03d
59d2111f29384fe105fffe5a58e5f367eba383297be70d82ec3dffaa89068171	MAL_CERBER-JS03d

4476da27b0f03d24efdaba507fee7c5eee28fd0ea7a220963bdf080f2c0542eb	MAL_CERBER-JS03d
99403a72a6f1913a7906e962a0d843b2298b401bbb1c46e4413d1b0abf09f81b	MAL_CERBER-JS03d
2f4be5d3c670ac9b1a78d389f869daf93bbda6f01125180624cae30c1b58e774	MAL_CERBER-JS03d
f2d2ee358841aeeefa92a01a4dcd5b1f29f19b9354b752260045aedc9ea1de58	MAL_CERBER-JS03d
3c24f8815e6edfe0b23fbe9ca53b98e9f2440c6547a1d520bc9282ef8355062a	MAL_CERBER-JS03d
360bc096f7b5f7defba0884051e246d11cee0ffd4bb630b40456fda2ef28bd4e	MAL_CERBER-JS03d
66434e84bf67f488de484d282aa2185277157549668a89fee73bdacfcc4ce406	MAL_CERBER-JS03d
409b1989f4ba7411e3c357d04522f9daebfb7a3ab3ec3064366cb14b5352506e	MAL_CERBER-JS03d
86218766de6d8c7035e52b94f1a2a2f8c26e8c174f6e587797f15d0b14c2a253	MAL_CERBER-JS03d
cafc30eee0afc6ea3010bb95fb6c24f35b6e4297f664e33be0653342524d7021	MAL_CERBER-JS03d
092cd0f01f5aa85b7e1b7858c515b93d6486f61da7e8ba11f4488feef9c7fd30	MAL_CERBER-JS03d
36b6406fe05691bd435f21a4749acc3ee42aac2aefd6c0350d689fe10a39116e	JS_DLOADR.AUSUIS
76b3437a2548d62a436f95a1fbed7b05c6c403fd2b17c72e0aaed60db5f1fd1a	MAL_CERBER-JS03d

bd385e70889d83897ed1099d0cc50211433a53fbb02f5685af201910f251b711	MAL_CERBER-JS03d
d477620d5ae3f032c819ef2ba5e67ae81d23a34e1fa9cf8a08ebd562d2adcacb	MAL_CERBER-JS03d
17b80212028f5ce1058664c3bd6d2dfcd7bf5374db691ca6ec3dd626af368cc6	MAL_CERBER-JS03d
18ad1472564629dc2e5159a9a192fdf718eca4fa7c2baff13834639f0b389256	MAL_CERBER-JS03d
76a97d72dfa5eda99778849e62caafb90af0bab94ba09b3aeba2e8a8930dcefe	MAL_CERBER-JS03d
2876e2c15453228deece2b44169c95488be1cbf8ab5a17a07d4be94483ef2c32	MAL_CERBER-JS03d
2a2639ded7ff98ce2412542e2da76fa336971da5b40d3f90f4739a5777ff7b0a	MAL_CERBER-JS03d
20ea9f2ca4d2e5e8b79af3ea438152394b1cf492ff594edb7ce3df38b45dca60	MAL_CERBER-JS03d
c81ed79bf3ccd44c12c23295069a12527146c788124986614cf08dc00b87a83d	MAL_CERBER-JS03d
bff61ca109f8a20eb19e1eb9a922c8285d079111b5b3f3f993ef1f7624963d8d	MAL_CERBER-JS03d
66f497c3a524c27d14fdbaae5d60b837e18fe07d4fb9c02b546e92b7f85bf0cb	MAL_CERBER-JS03d
2059e50a0346a707ec0a4b9fcb1bccefe444e8ae0221dd33989c5e819f83d6f5	MAL_CERBER-JS03d
e588a3467de8f63dfa12cf8e938ebd19b649852249f50f0e8a71fe93fc62bce0	MAL_CERBER-JS03d

44112222cab7a861b428a76af7067ee562a9fc8ad213d43ab83aa8f7aac4343a	MAL_CERBER-JS03d
f2fc2c82e4e9653f2577bec7f504f0b1d361b67cf0016e9ab18baa79621f2f79	MAL_CERBER-JS03d
8b1d2648e356782fd3d6c6e3b3c3dcd3b8f72e35cab6c9299f06333083e1944c	MAL_CERBER-JS03d
bc17ce4893e24c5faba59efeff05b0e05d7f5ad04a8f2c76844a6fe91b1a778f	MAL_CERBER-JS03d
143fa063ee02b9a9539455263015e9296285f97758abb5384604ed33eff744b9	MAL_CERBER-JS03d
7c19f6a070c1206ab7388fbfc17b805812ba17bcd753f8a3e6a357345aa99871	MAL_CERBER-JS03d
3fb1175af894d2b157737628169e5cd43bd489952c55ff9f255e0054223329c3	MAL_CERBER-JS03d
bdb33dd59e6ffc03a9ad0e58f3f280436d876dfa704c1d0e59601ebc957e38cc	MAL_CERBER-JS03d

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