TrendLabs

The New Face of Necurs: Noteworthy Changes to Necurs' Behaviors

Appendix

TrendLabs Security Intelligence Blog
Anita Hsieh, Rubio Wu, Kawabata Kohei
Threat Researchers
June 2018

Indicators of Compromise:

SHA256	Detection Name
04012161d2c0450ba52aa2bd2a032bb79d0171f1c86bb7fcc68089f1dee41050	COINMINER_MMBTC.B-WIN32
f43061a81d4fa7333b2285fb1dc014260fd59466ea3b464071b2b238bd9d3e3b	TSPY_BANKER.CBBCBF
5d1ab25d7280432698e17be4bf11b87b4068269dbcc055d7a0fa4f72e8140c4f	TROJ_MAILBOT.IKB
13eae06352ea8bf2cce1d1741109828164fd9cd4ffd96f4f1164c0e105a772b0	TSPY_BANKER.CBBCBF
e7ef8078720f8d7937a2bf2764be6f4e1f81f9a1020413b5ec0e698635ba7873	TROJ_PROXY.TORZU
644ab8d77313f99c5103940b53768ac25e515d67478f05b517f12f50e087805b	TROJ_MAILBOT.IKB
28d9f32ed13fc1e31c5ea6cf19727051363608591 5bc6c88cb415f534ee5551a	TSPY_BANKER.CBBCBF
461d96cfdd8364eb5b65a926786370ef1a565029108cfefe13f74f09c6b6bb4b	COINMINER_MALXMR.SM-WIN32
2cd56836467dc221a4b94b0cc43ec9b699a7f45f0e3b3b1c49f4f113033701b8	TROJ_MAILBOT.IKB
fc9c33fdd9da98815c43e1ebd9b525a7f87b106f1f2730ed86cba3b62c7768a5	TROJ_DLOADR.AUSULT
6fd1f4173c363fc4cc768bb57bfe976c18524124ade749354ae696a1e2b6a5ea	TSPY_BANKER.CBBCBF
2e1a263eed517d775532512d4fd82d95701a045c2073ffce916f3d10d8862a3e	TSPY_BANKER.CBBCBF
f0b973142ab1b1cdae868a70168afdad6d55111d9ce30120f2b9d027a5888d33	TSPY_BANKER.CBBCBF
6c8b947ee752def677f02a2b3f583eb5ecb4e0ee03cbb76ecbb6e1d190d00219	TSPY_BANKER.CBBCBF
10171afc2ba8f44e0fe2ed49f271616bbc8212e6a786f4e7db1e92c6d60c60f8	TSPY_BANKER.CBBCBF
834f7ac9892677cf37203372aac93c06ed5d4098048859102d3e6c73e537e74e	TSPY_BANKER.CBBCBF
39eda265410d45f5556c5873895151bcd7e632f66f94cf2369a2fff4c759ab45	TSPY_BANKER.CBBCBF
2defa48022e672c01ec93c36f2e3e7f787a6bb020cc086466549792fbd5519	TSPY_BANKER.CBBCBF

93	
6566777b6c561b19e6210c678231c8e17fc90cc44d21096c0eed1f0849952887	TSPY_BANKER.CBBCBF
477ebc6654f0a1b27b149e58527ffea33bf8cf4be64d64738bb2c509fc7d0478	TSPY_BANKER.CBBCBF
90466c1fd57c7f815e298b1b3d4a88296361147ed6285423cceafda826263ecd	TSPY_BANKER.CBBCBF
4c14551a87b483e8b8acc4f6bf9b9ab2216f7fbf283f84c809327f3175092bc5	TSPY_BANKER.CBBCBF
0ea3cde4746ae508093cca570f9544d10e217dbb7fa00fd25828cf2b811876d9	TSPY_BANKER.CBBCBF
468679f39bb326ace1a1850378e9e8ea6008d90c07396db373342bff95c804d5	TSPY_BANKER.CBBCBF
ea82f2e8d056ca87aaba2cb9228101fc256d63a2478289541ea29825654f4dbe	TSPY_BANKER.CBBCBF
9afd0818375bef1d653f299b2868d9ba580b9ec2a3bc2de00f9e4a75afcac470	TSPY_BANKER.CBBCBF
e69c141ed2bf6bc14ad8ed862db21cd99b151c85d47d3cdd7935cd498d041dc7	TSPY_BANKER.CBBCBF
2fc7b7b0011788b5b9ff6727cf792b3400dc2a8bde50a578f42c17186d0f9ffd	TSPY_BANKER.CBBCBF
65478532ffd4762f215cd591153fc193eb24664026b6892164af0b4951b0fd61	TSPY_BANKER.CBBCBF
c0ac1d87eb58434f8f43f49fe9cbc2ac4b6ff94b9a3e206f6085e77604fff6d4	TSPY_BANKER.CBBCBF
d637ea6da6960beac972917d3836944f289fa9f615bbd95964dd958e75bf6117	TSPY_BANKER.CBBCBF
d6d1bf53420b1ee8b35b93663fce5fdf3234b11d06b965c171afd030f26fda0d	TSPY_BANKER.CBBCBF
2c7bb71703da93572993c2255715df0b33df6d02dc14194ebfa9642f2a46b02e	TSPY_BANKER.CBBCBF
5231e33c1b5b23a7de9445de86dab914014276d0a01903ee1c263fabbd5264e0	TSPY_BANKER.CBBCBF
b6e9f0c325a3b07b53a5de026d9ac62c0c1b79007791a0b5ad0e8b5a6a99fbf1	TSPY_BANKER.CBBCBF
cbbb7cb5782fc511b0813f7bd7417dfbd4b05d6e597791bcb142bbf00d262f8d	TSPY_BANKER.CBBCBF
9a7951f8d721011a9e74830524b525daf576e2ee0ac5ca245e5899773896af91	TSPY_BANKER.CBBCBF
54c80e1f51355fda11647917af27e4c1a0b163b24d5ccbd8d11100846ce790e8	TSPY_BANKER.CBBCBF

a5d7c59d5b83002b3fecf7833632c4d0275ce5ee1c4775d97fafbd150a975c77	TSPY_BANKER.CBBCBF
47851fa3d532925adcef38f320f6cbedcb404c26f9ae12657013b37b08cc403c	TSPY_BANKER.CBBCBF
23e2d1485b4544ef9d9337fe07b1cef6f8560322fcd6185d10b0ae38c1b74ee2	TSPY_BANKER.CBBCBF
45d2f70928b5606ef3bd1d2cd2c52df94d02a88f9fbad297cece040223f06ec9	TSPY_BANKER.CBBCBF
0dc3a061132064392588c392cd9f657a20a74254c29bf48e5a76a328f0c97cdb	TSPY_BANKER.CBBCBF
d453cdd226d18150fe1e042ec52aacef3ee34e453aecad6765f9dd3c3c32a09b	TSPY_BANKER.CBBCBF
fd2752f1f2f6e6d59d899047e1c5fb6eb5e18de065a324f48949ec2528bf82cf	TSPY_BANKER.CBBCBF
bcbd36b414c148453fd210a186ac2161d7fd5b26533477b3351c9e6095566199	TSPY_BANKER.CBBCBF
f75e47c6af263e7e8e7990fcd0445f388cd0d1b74031c6da9b93a4d38a3da98a	TSPY_BANKER.CBBCBF
4e851a281b486a4b98fc699790c2c2e0003062fc4ae4b2ba4797d23a34d57c62	TSPY_BANKER.CBBCBF
1c3d0d8a8ddd4dfd9f1ef96d51dd7aae8bca40203d6e9385ead87f8a6aba8399	TSPY_BANKER.CBBCBF
c953c7323d850915a488a2ec1801dfb13b40133961e4507f1012259ec6d811f3	TSPY_BANKER.CBBCBF
41adaacc0e0e9c30bfebcdf13fec6aa996955437ffbf86cbc96318fdfa9f697e	TSPY_BANKER.CBBCBF
f02cc25fa39dc31480e0a96f4e4f0f1c6346e247882045414e00dcef572a03c5	TSPY_BANKER.CBBCBF
3056427ac6f288c5e156907786cf7ad4ac90ae17c990af57c41c33bd0e126af7	TSPY_BANKER.CBBCBF
fd14e746c280255fffceb36ca38b8137c3551dd20cf1e0cd8603ed415c734fd7	TSPY_BANKER.CBBCBF
f9b02a0b8782bba28205a01b1965e12734989a48b293680bc13a76ed070e87fc	TSPY_BANKER.CBBCBF
dd0fb8de39c7c4b6cbc8c72dc91d3fd9d6db6b6f75ff5c12b7509420fa38f9aa	TSPY_BANKER.CBBCBF
99f2640cc55f63a47e9a1c2bb708e95711de1f2f5760aa8bb009bbba87a7a419	TSPY_BANKER.CBBCBF
1fe62be117ccf14405bce36615b282ab6756c07aff6d9027fb64b20de6dbd502	TSPY_BANKER.CBBCBF
559b6c5299329890d33eba8bfdc2b0271643f8001532a7dae1cd62dcc0b46	TSPY_BANKER.CBBCBF

369	
93023161b8d1057700cfcad8afff6ae83b429c91207873777bdc96e7ea7dd942	TSPY_BANKER.CBBCBF
71383d3156a9cddc960d6d6577de81caaa3d02387968a294fb0afb3a1da60346	TSPY_BANKER.CBBCBF
56e5b0c5f6e0aaa6dc6fb9d16b197b90e494cdcef02f109249485b8dceeadc94	TSPY_BANKER.CBBCBF
d050cfce66fb3a5174e4f43c0c40e44c23a05e067e9a3fd17121abf0be25e88a	TSPY_BANKER.CBBCBF
e041bc4e190abc46082217fe690edef13cbfb6a44a2a2b2546cd09c7dbef06d4	TSPY_BANKER.CBBCBF
dd68d6b2d4546d4e14fa94000f05f3b935dee5887754ee51d55fe5cd25772bd1	TSPY_BANKER.CBBCBF
1277b3a864fc2a595549f779edc7fdf41a874c64d9464021a893f196b6c52106	TSPY_BANKER.CBBCBF
7491dcbd39b31d2eedb0f17af9bd2bf7a2b6c96bfe3c63ccfba715de731907c6	TSPY_BANKER.CBBCBF
7b7e244049f38eee2d123590ffdf957aeb2b06e15e8ec9700815a129c2228e4f	TSPY_BANKER.CBBCBF
bd3f10f6d8ecf1e093970756b5a9f707e845c1a503e9a38c0cb90c0a51e02c58	TSPY_BANKER.CBBCBF
152e575c7a36840ae281d667130902d5d27cbe2fbe09517a6cd2c7cb5be486b9	TSPY_BANKER.CBBCBF
616f871b70ece95ad67e5616f873337a49e5fee632d5857c28c76c82bf58e638	TSPY_BANKER.CBBCBF
5ba4da8eb2f03e6a3929e92269fbda3c18e3ee2e22d08c3a592c1117eb67ffac	TSPY_BANKER.CBBCBF
063db0a90a49f3339430c3ae49cac957d011412fe968ac1bee9792a76aa97650	TSPY_BANKER.CBBCBF
0a8b1fe5d78667719d7b04e9f6afa5d4af529d87f11874d8406652d0c7f25d0e	TSPY_BANKER.CBBCBF
74f5dd483133af96ebebe9a9615aaeaacb2ed2aa50724ad978a74d70e506e8be	TSPY_BANKER.CBBCBF
ecb6c14e323f0cd242d3f0142bb27782e998dfff6aafb68560c45a65b6397ed5	TROJ_SMALL.FOGAI
2d1243a423eb9bc45fb1d0f76a18f2239917c969700189175320fffa7b04b4e2	TROJ_SMALL.FOGAI
374b17af044d87e69b87768b18336e0cb5588c5c9c66e30e39e98159c9dc8a13	TROJ_SMALL.FOGAI
f7b5b4e1bf177604c3a1f97c0dddcdcdcec927c6837a9d83e986973a91bc71	TROJ_SMALL.FOGAI

21	
696062147711a0f806dd99ee48bbb1e05c339bd1d63ed14679f88e2f3ac9172d	TROJ_DLOADR.AUSULT
565abf916f22d7f364705d426cfe16d94f4c1d79a2ab35825942237701b5f7e0	TSPY_BANKER.CBBCBF
8fad7737ba680d96dea1192450b6d94691702f0be2496b38489aa196f5ab6959	TSPY_BANKER.CBBCBF
a04a5bc4cc0c9cca4ae10d7777b7e0bfb98d1613472884562e7c2f2090b0c458	TSPY_BANKER.CBBCBF
98df84690cec0bbfa9e9b7258eb5c570cc4fb9ebf055858a3be4a2586d635d14	TSPY_BANKER.SMNECS
bc035e7e86f434bc5641f8475ffad389c04e1dc292a5e80ebe628ef823506670f	TSPY_BANKER.SMNECS
5305b87be20d4c8f00cdbb9930849c95feae383e5e465181ca32d88abe941815	TSPY_BANKER.SMNECS
59ac8cd9a3d18ed358503f2a0d5d44f5a50c5b08fc891e04fc6e0e70d765ea46	TSPY_BANKER.SMNECS
76aff8db226a2a8f77099b624ecce6635c4e75ecf2226c45200aa10d49de7f42	TROJ_AZORULT.B
8aeadf51fc481e5fb0e207a7d12e237483a26a4e55c0851f085ba1a83b2b61d7	MAL_DALEXIS
72f02e516e8bf219d05d2ba290d9a697c1ed20cd5be05a7bee780dad00d770f5	TROJ_AZORULT.B
ff695521b17bbd7823130c017da97d4a1633a2c09bf61c0d5f9d11b6b2a0bdbc	MAL_XED-24
903c5f5e956cf8c0ca0bc14e46ccee5c3da5b46c46514240b9f8e936607d5437	MAL_XED-24
55a61f6b657f2cc41a00ac6c08f39bb0ab6e34b5dbb38f37c1c8fff67a1ef00b	TSPY_PASSTEAL.AUSIPD
c71e8dfd7d1bbb3d25d22efba73a0c6201c3ab4248ddfba11d04637c1756d02b	TSPY_BANKER.CBBCBF
84bf187449b43a2f5f935398cbcb53c70c317e086456d2801d0f5efb103028f8	TSPY_BANKER.CBBCBF
59a96af1015793c949df1e01a33e3e1f4eeee8a93bb958ea2e917c4c23a96c32	TSPY_BANKER.CBBCBF
6c9145bddeca679d9cd3d12f922c54796f47cc45d1146940950e3e52fc95d403	TSPY_BANKER.CBBCBF
e852a5407212989b16bfa7056ab5ccdac093ffbfc561706a829e8f88a0aae35f	TSPY_BANKER.CBBCBF
c31b1a5561aee4baccd52899e42d4fbb4dc64f207a91c5c933737e5fbe81b48b	TSPY_BANKER.CBBCBF

14f060feb699d04fb14c60b95fbab4125dbb6f234ccf1d8b15a037115056a174	TSPY_BANKER.CBBCBF
85f3b4aa2b63341d9478f87d403ea031699848284ce753c3ee70ad6f25143027	TSPY_BANKER.CBBCBF

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

[Type a quote from the document or the summary of an interesting point. You can position the text box anywhere in the document. Use the Drawing Tools tab to change the formatting of the pull quote text box.] [Type a quote from the document or the summary of an interesting point. You can position the text box anywhere in the document. Use the Drawing Tools tab to change the formatting of the pull quote text box.]