TrendLabs

REDBALDKNIGHT/BRONZE BUTLER's Daserf Backdoor Now Using Steganography

Appendix

TrendLabs Security Intelligence Blog
Joey Chen and MingYen Hsieh
Threat Solution Team
November 2017

Indicators of Compromise (IoCs)

Hashes related to REDBALDKNIGHT/ BRONZE BUTLER's decoy documents (SHA256):

Hash	Trend Micro Detection
5fcd3ecc594fbd2a45dac8e3c547cc191e77e4f2d27368603010d74320507a5d	TROJ_TARODROP
b649fba2dd727cf326850e4f435f515b2485c9311f7fb0cdfab5dea403e4ae7f	
22efd7bef2fae9ae8b8393d4910880cb50202631472ade48fb25a3e802e6150f	

Hash related to XXMM's steganography builder:

Hash	Trend Micro Detection
27f3a4c757f6e81a0546e47b97cbaab5e5e2b82a6ec2694641cd41ec47b90766	TROJ_STEGOBUILDER.ZKEK

Hashes related to REDBALDKNIGHT/ BRONZE BUTLER's Daserf backdoor (SHA256):

SHA256	Version Number	Trend Micro Detection
8a22a6b52620d0d1beadba866b32ea3ae7d3ac2619717957ed7b867cb47fe005	Mini Edition Version:1.3G	BKDR_DASERF.ZKEI
1d5f1b6f9618cde91d7443599a2220d477a7190a6be6c48259d2224e52268815	Version:1.40C	
8e8742d6a802c7e56f2f223cf3cff0ac18e77cc6aa96d0b306e5d23220736bd5	Version:1.26A	
fe8f9d5eb5fbce0cdefdc9adb32c59fa8a7c630344a5340cffef09e5ceefc273	Version:1.50I Mini	
f8458a0711653071bf59a3153293771a6fb5d1de9af7ea814de58f473cba9d06	v1.40 Mini	
5c3ca904c979a2adaa201e1de76e857237357edd9842e82af2f40555df633ee0	Version:1.40B	
2a6bcb1a5262fc7d93ef533ee98979a75e958468be3c5e395b09e02fc150f08c	Version:1.3J	
9b3f263b3ad2b262ed43c4b16454ea3890658b76a8b0e25a2808a2f6610a07ad	JustInject Edition Version:1.3J	
446e71e2b12758b4ceda27ba2233e464932cf9dc96daa758c4b221c8a433570f	Version:1.40D	

SHA256	Version Number	Trend Micro Detection
dfbd7754d0895b6340a7beb6ad2e5eec3bc8043e23debe63537f179b1f14dcd2	Version:1.3G	BKDR_DASERF.ZKE
b1690facbce9bcc66ebf18f138dbbc10c3662a2034c211e0c414e47c7e208b4a	Version:1.50A	
b1fdc6dc330e78a66757b77cc67a0e9931b777cd7af9f839911eecb74c04420a	v1.51 Mini	
4681e3556c6b4fbcf1bdd7ed18af3ab7fd4b27bb94a92cef735a8263c831265a	Version:1.50C	
7afb8082822bf3e55c6639ed2e272846c6be0e5c1fd40402b8b0f69e37402461	v1.91 Mini	
01d681c51ad0c7c3d4b320973c61c28a353624ac665fd390553b364d17911f46	Version:1.40C	
fa9a3341649e798bbc340ce9b2fe69791fe733aa9e46da666ce13b8cf7ca8f4d	Version:1.14.02.180Z Mini	
0d4860468a5eb86f7b30f012f176c9a67388f7e0fe0a88fffa3f5702af3d1118	Version:1.40D	
63cf1aba54cdff8c48ce4b2aafae745890d91b4c8582abebc1d2ed7cd18f47dc	Version:1.50A Mini	
04080fbab754dbf0c7529f8bbe661afef9c2cba74e3797428538ed5c243d705a	v1.40	
7dfaf8090b94cf737617dd4d5ceb2849447f54db6a6da4880cd18dd9bbf8b320	Version:1.50H Mini	
b0966e89eae36a309d89a0c15c8a07677f58130fdc76bc98c16968376ec80626	v1.90 Mini	
22e1965154bdb91dd281f0e86c8be96bf1f9a1e5fe93c60a1d30b79c0c0f0d43	v1.43	
33a2a7d229d0917224c5972358597bf2fc354d97a1976081a9312c77387c2a15	Version:1.50Z	
4b8ca82e6f407792cfb51de881f06b86bd4b59f85746b29c3287aee0015b1683	Version:1.50J Mini	
d904b65e23217b5b875b3488a5e0f86970931cd29f57ec993d3c34a907c00395	Version:1.40A Mini	
ccc0f0df164336f5fc394274e54fc08c3cb92e1e849b3dd3bce72f23a277ad3e	Version:1.3K	
c7fc0b109663e9334f0547930a10840d68952889a043095d1e48f3d8a2e0b5e4	Version:1.50D	
7b01a4197228c51e245781e6ad74a269bade4026fe7f6f6e430af8dc31dda841	Version:1.28B	
b705eb3afac0782f1d808b9c4e5029fc3744e07c831114da91f9cca4f1dbe0ad	JustInject Edition Version:1.3F	
5abd15f9ba639468c0bd1799af9b36ea8b9a42cd9faea02dc02dc4125308f97c	Version:1.26A	
9213a16e55d283d9d3f8a0377fa01f0b49abc81b4eecd7f41a30f2aeefea82f1	Version:1.27C	
15abe7b1355cd35375de6dde57608f6d3481755fdc9e71d2bfc7c7288db4cd92	Version:1.50A Mini	
a51e4d5810182b75374e467c844141672ffb5a54a3fea781cc5aa58086cf7f07	Version:1.26A	

SHA256	Version Number	Trend Micro Detection
34251fe49998c20e18964056578c4e171e5337dbfceb40471bbf42cf78053bed	Version:1.3A	BKDR_DASERF.ZKE
2dc24622c1e91642a21a64c0dd31cbe953e8f77bd3d6abcf2c4676c3b11bb162	Version:1.50G Mini	
e2fd17445d81df89f7a9c1ff1c69c9b382215f597db5e4730f5c76557a6fd1f9	Version:1.50K Mini	
0a031665d05e82038d620facf9d4a86a89e78544f2f770f579c980dae2e252bf	Version:1.50K Mini	
337834f13f6b6a290f997102cce604f395fdc3be510b0db590f6298005cd3144	Version:1.40B	
5ede6f93f26ccd6de2f93c9bd0f834279df5f5cfe3457915fae24a3aec46961b	v1.76 Mini	
f06b440052bd2c2eb127c33c35a80c4eca34a06360d3ee1bb37348d6029dc955	Version:1.14.02.180Z Mini	
03a981039c48fc04a36aceae2d568ad3998aede562e276556cb279e7a56dfadf	Version:1.50G Mini	
52f07f619e24d38681fb0d8dddc39027ea73a35f28feb2a10d0c5e1830dc45e1	Version:1.26Z	
b1bd03cd12638f44d9ace271f65645e7f9b707f86e9bcf790e0e5a96b755556b	v1.415 8M	
a727a9f5ec1b9e2083ab0d14b5dc139fae4e9ca455b74c3594ba0e25659a5d61	Mini Edition Version:1.3K	
56750cd75e9bc6c278faefd0bd8e0b83027212f509693c5ed7952257c9079474	Version:1.50G Mini	
a4afd9df1b4cc014c3a89d7b4a560fa3e368b02286c42841762714b23e68cc05	Version:1.50G Mini	
837ab755bbf8eaaaa8aea077b1228978eb888c3b9b1ab420666c5477385e884c	Version:1.3G	
89a80ca92600af64eb9c32cab4e936c7d675cf815424d72438973e2d6788ef64	v1.413	
e2f174f8368b46054e6ec2feec00b878b63e331ba3628374d584b238a95fd770	v1.91 Mini	
0ae1996e75ac11fadcc30f42a6ba0bf8c4afae7f75dd5ab4e0d03d6ecf095615	Mini Edition Version:1.3J	
f2d4f3ef28f5c8aea46a9a07a2e08e1a1d2d4dd6d5416d264c2a78ce1972ea88	Version:1.26C	
9c7a34390e92d4551c26a3feb5b181757b3309995acd1f92e0f63f888aa89423	v1.41	
0ad4e43b784a50a51d682b7049715057e691bddfc2e38ace4270fec1e1784273	Version:1.3H	
2a39372dea901665ab9429d2f15b3f4fb10706423e177226539047ee1ac3e4a3	Version:1.15.11.26TB Mini	
e8edde4519763bb6669ba99e33b4803a7655805b8c3475b49af0a49913577e51	v1.40 Mini	
a43004b96a9f221b33c85d910af1c288e772423b08268bf539aebe52044a9244	Version:1.3F	
4b64b2a784644f63d3be14d7c45ecfbf0e135fb080bdcf52f0b6c86e8f16bf48	v1.72 Mini	

SHA256	Version Number	Trend Micro Detection
db8b494de8d897976288c8ccee707ff7b7967fb48caef99d75687584191c2411	Version:1.50K Mini	BKDR_DASERF.ZKE
4e7352c64ee4de99bb6a6a4259a2f0d1ffc717a223b81c945ff992ff4d26a986	Version:1.26A	
f8f31f73157bf049b318429c1d60ad7ff2851e62535d95cf8d121216b95c8602	Version:1.50A	
236848e301d71cab6e17a0503fb268f25412838eccb5fb17e78580d2d0a3a31d	v1.76 Mini	
85544d2bcaf8e6ca32bbc0a9e9583c9db1dce837043f555a7ff66363d5858439	Version:1.50A Mini	
24a15f36c82433ce505aa839db46e9cc833de4c7777dd986bc421d4524b71173	Version:1.40B	
5984d4e01a025aff902b2e9df9405b7772fb8a4bf1e717ef111af5017e0bc285	Version:1.40A Mini	
94a9a9e14acaac99f7a980d36e57a451fcbce3bb4bf24e41f53d751c062e60e5	v1.91 Mini	
c4e02d0a3f0ca0caf9ec011e37f084d7b33c679512a6fd7a2ba9b077c85ae2db	Version:1.40C	
f4e7b20291d80e01d0d349d31a921c3243a3dfd412e56e7ab819cda4a2a374b0	Version:1.50J Mini	
21111136d523970e27833dd2db15d7c50803d8f6f4f377d4d9602ba9fbd355cd	v1.40 Mini	
e4c7832101280b6900f91a9468b79b828708e0b87f13a655aa0ec1b03cea7c83	Version:1.3	
216f64207d04d1aa8ac7ed36ff8ab9e79cf50376e91a3a03200fd4bceed67267	Version:1.3E	
b03c6c4b349b1dd56636ab314bf3ffd11de0b3c459c63266136840534 98cf619	Version:1.28B	
2bdb88fa24cffba240b60416835189c76a9920b6c3f6e09c3c4b171c2f57031c	Version:1.50A Mini	
421ff96f145ccbd0b45404453a1591cb8ddced9d745fa69eef8ce20ea4ee5dfa	Version:1.3K	
b6f7bd0bf5c21a2579bc36f483906f7cc02984249ad47a6461ebc6ac9bc8890b	Version:1.26B	
db6a6a4f675cba87405c9c7b016713d3e65b052ffc6c8963764a3d3788f432fa	Version:1.50H Mini	
cd90180f256416b7bd4fac9d882ff66b248a1bca7a283777a9175eb225481f21	Version:1.50J Mini	
c6000c00fde81d58e63829374664151ac4c568252003fbe7d3fc742c6bd48d21	Version:1.40D Mini	
41679622e34ab635eb63d48bae021dc25d861c0fd58adb6066ac5f7d5fab52df	v1.41	
6682a7a898b41cf0b24cab1eedd76b0e062d9677c8e408ee9f60736815ee4e3f	Version:1.15.1, 1.26TB Mini	
68b59f65665677f77ad2a3c8f0cb565c38ee098aacc1a71618442dbe0835d8a3	Version:1.50F	
2c449b562dfce53cf98acaddf37286cfb2d1e9da1536511a08bbd24ed93624a6	v1.75 Mini	

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