KillDisk and BlackEnergy Are Not Just Energy Sector Threats

Appendix

TrendLabs Security Intelligence Blog

Kyle Wilhoit
February 2016

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an “as is” condition.

File hash (SHA1):

SHA1	Detection
4c424d5c8cfedf8d2164b9f833f7c631f94c5a4c	BKDR_BLACKEN.B
899baab61f32c68cde98db9d980cd4fe39edd572	
fe8197008ddb257f79609f29de8c7e4404dd5dd9	BKDR_BLACKEN.DAM
11c911c7e52c127de83bfa9e7f9c050951a7553c	BKDR_FONTEN.C
058257111cd1addf0481c23ae75861a0004e90ea	
1A716BF5532C13FA0DC407D00ACDC4A457FA87CD	BKDR64_BLACKEN.C
896fcacff6310bbe5335677e99e4c3d370f73d96	RTKT_BLACKEN.C
069163E1FB606C6178E23066E0AC7B7F0E18506B	
1A86F7EF10849DA7D36CA27D0C9B1D686768E177	
1CBE4E22B034EE8EA8567E3F8EB9426B30D4AFFE	
4BC2BBD1809C8B66EECD7C28AC319B948577DE7B	
31591ef60155fff5164f9a6eaf442b998be6e577	
502BD7662A553397BBDCFA27B585D740A20C49FC	
84248BC0AC1F2F42A41CFFFA70B21B347DDC70E9	
BE319672A87D0DD1F055AD1221B6FFD8C226A6E2	
CD07036416B3A344A34F4571CE6A1DF3CBB5783F	
E1C2B28E6A35AEADB508C60A9D09AB7B1041AFB8	
345881fc59b28b9ef74367811e151434be927a09	
3a1a932ea1a95b8bc33dacaf2b2aaa764c105881	
3e49e0dd526eccfad15273acf50a8270 - (MD5)	
30abab134ffced96d9c1191da46dbc9ae4170022	RTKT_BLACKEN.D
0B4BE96ADA3B54453BD37130087618EA90168D72	RTKT64_BLACKEN.C
20901CC767055F29CA3B676550164A66F85E2A42	
2C1260FD5CEAEF3B5CB11D702EDC4CDD1610C2ED	
49af5fc6fb614131bd446f3ed9f33568ea04659f	
606573cd1dee5caf1e11d73a9d3f4068680aaf1a	
2D805BCA41AA0EB1FC7EC3BD944EFD7DBA686AE1	
B05E577E002C510E7AB11B996A1CD8FE8FDADA0C	
BD87CF5B66E36506F1D6774FD40C2C92A196E278	
C7E919622D6D8EA2491ED392A0F8457E4483EAE9	
E40F0D402FDCBA6DD7467C1366D040B02A44628C	
6e49bc82f8eb5ef5380aad1e7115c7e167c6b878	
c7081b80d0e165cb0a732851f4355f17bbd5e250	
a6dcca175949ba91ea95ffa6148bdad41f60bf0e	
166D71C63D0EB609C4F77499112965DB7D9A51BB	TROJ_BEARDOOR.C
16f44fac7e8bc94eccd7ad9692e6665ef540eec4	TROJ_KILLDISK.C
8AD6F88C5813C2B4CD7ABAB1D6C056D95D6AC569	
6D6BA221DA5B1AE1E910BBEAA07BD44AFF26A7C0	
16f44fac7e8bc94eccd7ad9692e6665ef540eec4	
8AD6F88C5813C2B4CD7ABAB1D6C056D95D6AC569	
6D6BA221DA5B1AE1E910BBEAA07BD44AFF26A7C0	

SHA1	Detection
01684e1ee4af38bb28ef6a4bea1da8d14f1c472d	
f3e41eb94c4d72a98cd743bbb02d248f510ad925	TROJ_KILLDISK.X
f3e41eb94c4d72a98cd743bbb02d248f510ad925	
72D0B326410E1D0705281FDE83CB7C33C67BC8CA	VBS_BLACKEN.C
aa67ca4fb712374f5301d1d2bab0ac66107a4df1	X2KM_FONTEN.B
8c26c70fbffe7f250aaff234be9a014a996930bc	
3298dcea06a4c7f745a932c72ffe0741e9a3a49e	File is encrypted
53bb81ab4b3029a76a483d742749ef706a521167	Archive contains files that are detected as RTKT_BLACKEN.C and TROJ_KILLDISK.C
672F5F332A6303080D807200A7F258C8155C54AF	-
A427B264C1BD2712D1178912753BAC051A7A2F6C	
A9ACA6F541555619159640D3EBC570CDCDCE0A0D	
D91E6BB091551E773B3933BE5985F91711D6AC3B	
E5A2204F085C07250DA07D71CB4E48769328D7DC	

Encryption and Decryption Attributes:

SSH backdoor key
AAAAB3NzaC1yc2EAAAABJQAAAQEAsrGnWG3XPW4tO8tRLhFXQyuM5ZcLl9tIsnlMyIUXwptcU29hGpzMWVmbAy18EEEXKtyXIlxOKqp7CWgEJWWxjsvXKB66Gp/sVcizXqbV2P0PfVMRwZ144Ui0ffrpGxWMOnp7rrByANQSPdGtJlQ/yqqFFgiM2u7ilLsREQHSGsV6L1b8krnf0BrcwQ08MD3q7tNq3H3FEt0LPithBiCpRTuA9emsowt3gtVo745Qt1GVChYLA9GilmVmBO49HAnceZA9bVFA58Keq3Jy5W1DUv3HoWJkWBHkUn2IH1LSKurVr/xjNEi9Hez7uQP9j44xk/V/kA9Kh4E3czOCDxQ== rsa-key-2013112

Digital File Signature Thumbprints
EBC5D2D1C56D0D5BA8A087106E6E2AA0847AC21F
FBD32532A03422E117200FEB7FA636BC48391BA0
E4AF247AD5DD91DF3E4CAB5E80517E91D911ADE0
F3E6FFF120629FABE005B2E1B5E2837999BDF50B
C2B724D7D2E52055D402A74C0AFE464247D6BF4A
FFD1B619595E52B27AD541ECEFB854A038B9FF9D

Related URLs:

IP addresses (command-and-control (C&C))
5[.]149[.]254[.]114

IP addresses (command-and-control (C&C))
5[.]9[.]32[.]230
31[.]210[.]111[.]154
88[.]198[.]25[.]92
146[.]0[.]74[.]7
188[.]40[.]8[.]72
148[.]251[.]82[.]21
94[.]158[.]214[.]45
2[.]61[.]168[.]116

Specific URLs used for C&C purposes
5[.]9[.]32[.]230/Microsoft/Update/KS1945777.php
31[.]210[.]111[.]154/Microsoft/Update/KS081274.php
88[.]198[.]25[.]92/fHKfvEhleQ/maincraft/derstatus.php
31[.]210[.]111[.]154/Microsoft/Update/KS081274.php
146[.]0[.]74[.]7/l7vogLG/BVZ99/rt170v/solocVI/eegL7p.php
188[.]40[.]8[.]72/l7vogLG/BVZ99/rt170v/solocVI/eegL7p.php
5[.]149[.]254[.]114/Microsoft/Update/KC074913.php
148[.]251[.]82[.]21/Microsoft/Update/KS4567890.php

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.

Securing Your Journey
to the Cloud

10101 N. De Anza Blvd.
Cupertino, CA 95014

U.S. toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003