Operation Black Atlas

Indicators of Compromise

TrendLabs Security Intelligence Blog

Jay Yaneza and Erika Mendoza
Trend Micro Cyber Safety Solutions Team

December 2015

Contents

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.

Hashes

HASH	USE
007c82ee41939459e1bc843097e1a56287cd86bd	NewPOSThings
020f7125456744b95877f79bc0bc649593d1e7e4	NewPOSThings
02cb522137f370355de9c2e3cae7ca9a168b95ec	NewPOSThings
0868af41f7279a8cee499bdbb100084564e1aaff	NewPOSThings
0874fdc7a6212dc5f9b9dd9ca7c8dbf16abf947c	NewPOSThings
13f1f2b2eac06d0ac9a499d4a18e55e7ae931434	NewPOSThings
1a2735678d87aec490a547988ba2f8e6507bb86f	NewPOSThings
2177e275c8278a62ee1c80e7b00f7ae60d6b5a89	NewPOSThings
22001d13fb7c0c18bdc0fc60df0b41d12f774c5c	NewPOSThings
22a01b064b3c173163ace33138ef243fbf7ef6af	NewPOSThings
27e99e527914eca78b851bb9f2a4d0441d26e7e3	NewPOSThings
29051ca6c3e0c21065f2cbce8bfa2926f6d95fbd	NewPOSThings
4032e5062e8bc9ba792a9b758f12be5f51e9b908	NewPOSThings
46a0b25701f4202904964ee055a24f111dcf2427	NewPOSThings
4ee213576bf936e8df31c725ab13ab9fa5dbea72	NewPOSThings
56fe558916e51a0f81dfb207183be465199accbc	NewPOSThings
596b5792a0eaff8010ffef5bb1e109ff3b3ef27b	NewPOSThings
5bade04603e2d16487ca05558d8d0aa1b492701d	NewPOSThings
6192e520207a4ee0ae32c3a199668fc0a65dd9c2	NewPOSThings
77dc1389835f48454ef5d83d3aa3a424eac54a8e	NewPOSThings
83e9b381fd21348abbc93365d1fdf011b8a6d258	NewPOSThings
87abfc7c67a8770776ef6971b0dba3aa83039470	NewPOSThings
9105fe70cb4177b03275b49b7fe78d437a3a8759	NewPOSThings
92a8ce59ef6cdbb677c0690e2e2dda9da0d506e2	NewPOSThings
99eeb0c88105637954110727968a71321453fae0	NewPOSThings
a61672a5b8812002fde1d54169be5c4f9ff4fd76	NewPOSThings
B5b49cc3a6890a1f457ebe77a085cc2ac5c5da59	NewPOSThings

C1e70d785435186052dc226abae33d891fd00918	NewPOSThings
c2fb1d8a1a6d4480ece2325ce8c91dd05832494d	NewPOSThings
c3732c425d41b68150e0eb372d860a6ce1398973	NewPOSThings
c47c3719d74a7c0352982bf5026f60f03d184cf8	NewPOSThings
cfe25d6e4b994b8f07fdfc197c8f0b2081df4d5b	NewPOSThings
d436fc11aecf241f9d15b97f3fdd9e8453cdc316	NewPOSThings
d8cb77dd40f9b2d2363b110f79401d2ac7be5f91	NewPOSThings
f6d548f245169b965671b279dff052d5d26f4ec7	NewPOSThings
f7e088153eddbc87a44c8bac8ef713b7203c1670	NewPOSThings
f8e4435ac616d4bd45796aaee9cbb1e9d882a56e	NewPOSThings
f96bacd550e8f113134980cde33eecfa6da3ebe5	NewPOSThings
b1983db46e0cb4687e4c55b64c4d8d53551877fa	PwnPOS
670fc386dd77f954f287b3cd0d6697e732648a0b	Alina (Spark)
c2974699bfc215501614bf88379da446d84baeb2	Cardholder Data Discovery Tool
812a94e2efee245da285d4c85e2b69904ef25a9f	Alina (Joker)
f638c84b3264ff27a0891f34c85d9fa7cba32f38	Alina (Spark)
1df323c48c8ce95a80d1e3b9c368c7d7eaf395fc	BlackPOS
42af42114efc18afe726a38bfbf3fd36036a69f8	Kronos
60b679361db8413060cce8ad901006d5ecdf0d21	Kasidet
81672ade63280796b8848350fd819f3b63d3d975	Keylogger
f9b4451988f4dfbaf918a5a32c7976da89377fd2	CenterPOS
bc7618bfc3a80ea89f52362baa230ee87a24ca3f	Kasidet
a8cca3c64065961d3f8f47f1e40553a525590450	Alina (Katrina)
327181e170cac8d5076b493faa52436f9cff9d8e	NewPOSThings
a913dc86f9217a9c5163f2508d86a085013f9ef0	Gorynych / Diamond Fox
f74b17ca7a542323534a7c7766a8dfe821c6bcce	BlackPOS
80aedf2eddc9e2f39306cbaa63e59c7a08468699	BlackPOS
a913dc86f9217a9c5163f2508d86a085013f9ef0	Gorynych / Diamond Fox
29957f3b6f001debe2afa0d530e0a63afaf01f22	NewPOSThings

80fc7265d47dc623da11324ad550d45d70fea4f9	Gorynych / Diamond Fox
f6d548f245169b965671b279dff052d5d26f4ec7	NewPOSThings
22a01b064b3c173163ace33138ef243fbf7ef6af	NewPOSThings
f6d548f245169b965671b279dff052d5d26f4ec7	NewPOSThings
ca9c671bb8e40fb4864f159b1c78774f9c218779	NewPOSThings
5bf0256876cee98e20c92c8771b98f3143b07d61	PosHook
1cf29b46593f3004f1b0e0e0de6855a779aca159	Kasidet
447ef3406bc2d06492e7a217e5f0eafb4f6c4f97	Spygate
0644c56c4c0503b961f81eb85ed05e8ff9df7f1c	Spygate
80aedf2eddc9e2f39306cbaa63e59c7a08468699	BlackPOS
3cc05e28b1cd6bf5624a336f72272c89843a462a	NewPOSThings
c5612b48c7a3887c8af0bec830598046b125d2d5	NewPOSThings
0644c56c4c0503b961f81eb85ed05e8ff9df7f1c	Spygate
3f186948a30cff34861ac0c539aece70e21c848e	Spygate
808f582f8899f5f482a01c2601e6826b253f82bb	NewPOSThings
ec932d26a059a188af6320b8ca76ce6e609f4878	fgdump
37adb7c54943b338000cefce6d895c05468fa2ce	VNC Password Recovery Tool
2ac2b4742e1578c88978ba2219b0c0adf9c3389b	fgdump
0e840ae8efa952429c15c00776d63539c44fcef2	Advanced IP Scanner
a01b7f55c5edc6576d1349a0a23b781552c74244	Advanced IP Scanner

IP Addresses

IP ADDRESS	USE
89.45.67.200	Source
89.35.178.109	Source
111.90.146.61	Alina (Joker)
138.204.168.109	CenterPOS
194.63.142.101	Kronos
95.213.192.72	NewPOSThings

95.213.192.82	NewPOSThings
95.213.192.74	NewPOSThings
95.213.192.66	NewPOSThings
46.161.30.200	NewPOSThings
178.32.130.53	NewPOSThings
178.32.130.49	NewPOSThings
178.32.130.54	NewPOSThings
155.94.213.66	Alina (Spark)
86.105.227.123	Alina (Spark)
86.105.227.125	Alina (Katrina)
86.105.227.124	NewPOSThings
154.70.153.87	Kasidet
195.3.144.101	Spynet
111.118.215.201	Gorynych / Diamond Fox, PosHook
103.21.58.10	PosHook
185.56.80.133	Spygate
195.3.144.85	Spynet

Malicious Domains

MALICIOUS DOMAIN	**USE**
toorchins.cc	Alina (Joker)
jackkk.com	CenterPOS
hntrgesdgfrge.ru	Kronos
cockblockingwhorecuntsnow.ru	Kronos
blowingcockflowers.ru	Kronos
jtrho.net	NewPOSThings
chiproses.net	NewPOSThings
randomfruits.net	NewPOSThings
corner-update.net	NewPOSThings

super-cpu.net	NewPOSThings
super-updates.net	NewPOSThings
topbullka.ru	Alina (Spark)
315andro.net	Alina (Spark)
www.keycodes777.ru	Alina (Katrina)
damcodes777.cc	NewPOSThings
power-uping.com	Gorynych / Diamond Fox
jabruslan.noip.me	Spynet
m0ntecrist0.co.ve	Spynet
inf1nix.com	PosHook
m0ntecrist0.cc	Spynet

Malicious Email Addresses

MALICIOUS EMAIL ADDRESS	**USE**
bizdotbiz2@gmail.com	Used to register domains
power-uping@safe-mail.net	Used to register domains
petrov.strong@yandex.com	Used to register domains
dumps.dumps@yandex.com	Used to register domains
brian45345@safe-mail.net	Used to register domains

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