RATANKBA: Delving into Large-scale Watering Holes against Enterprises

Appendix

TrendLabs Security Intelligence Blog

February 2017

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.

Indicators of Compromise (IoCs):

Hashes (SHA256)

SHA256	Detection
99017270f0af0e499cfeb19409020bfa0c2de741e5b32b9f6a01c34fe13fda7d	TROJ_RATANKBA.A
825624d8a93c88a811262bd32cc51e19538c5d65f6f9137e30e72c5de4f044cc	
200c0f4600e54007cb4707c9727b1171f56c17c80c16c53966535c57ab684e22	
95c8ffe03547bcb0afd4d025fb14908f5230c6dc6fdd16686609681c7f40aca2	
7c77ec259162872bf9ab18f6754e0e844157b31b32b4a746484f444b9f9a3836	
db9de8ff7ed80cf7563502c25d6aad2e2fee258da407c52a6c4a2192f9170d14	
4fe3c853ab237005f7d62324535dd641e1e095d1615a416a9b39e042f136cf6b	BKDR_DESTOVER.ADU
a606716355035d4a1ea0b15f3bee30aad41a2c32df28c2d468eafd18361d60d6	
CD10FFB7A88F0D2EC69326E7A13F00B9ED211A3A719F89A755A29494FF1142E6	TROJ64_KLIPODLDR.ZHEB-A
752b8e93a8f6803b265dd3a7cd39df86997cf99900426635b1b97dd665bd7f9f	BKDR64_KLIPODENC.ZHEB-A
8CAD61422D032119219F465331308C5A61E21C9A3A431B88E1F8B25129B7E2A1	
efa57ca7aa5f42578ab83c9d510393fcf4e981a3eb422197973c65b7415863e7	HKTL_NBTSCAN.GA
1e0564ef867fccea953efad7fcf1f5b76d9ac51cfe3eff37a0eec38583cb0553	HKTL_NBTSCAN.GB
e5bc4c5794483273dd610ae69913d473440d5533d4f8b2abb77cd64f5af47374	TSPY_BANKER.NTE
6c1d8c4afbc7f85f05fb2e4d17e5553255b0195a0b56ba5309e362e2156debfc	TSPY64_BANKER.YWNQD
2a6f218c6907859a62673116625500b11cd855f28e32968e84e4d1e0558b47fb	TROJ_CVE20130074.B
00501384ff0a9b6c20f12961008ebe5d26858f65e89b59b14d26cb2d115e1833	
c1b29afcfddb79cfd57545b8600922150843ae2b170fff9aeacdeaa17adbf792	SWF_EXPLOYT.YYRQ

C&C Communication:

URLs/IP Address
120[.]113[.]173[.]207:8080
sap[.]misapor[.]ch
www[.]eye-watch[.]in
update.toythieves.com:8080
update.toythieves.com:443
185[.]7[.]61[.]165:8080/view[.]jsp?action=BaseInfo&u=35794290965706

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.

©2017 by Trend Micro, Incorporated. All rights reserved. Trend Micro and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

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