RATANKBA: Delving into Large-scale Watering Holes against Enterprises

Appendix

TrendLabs Security Intelligence Blog

February 2017

Indicators of Compromise (IoCs):

Hashes (SHA256)

SHA256	Detection
99017270f0af0e499cfeb19409020bfa0c2de741e5b32b9f6a01c34fe13fda7d	TROJ_RATANKBA.A
825624d8a93c88a811262bd32cc51e19538c5d65f6f9137e30e72c5de4f044cc	
200c0f4600e54007cb4707c9727b1171f56c17c80c16c53966535c57ab684e22	
95c8ffe03547bcb0afd4d025fb14908f5230c6dc6fdd16686609681c7f40aca2	
7c77ec259162872bf9ab18f6754e0e844157b31b32b4a746484f444b9f9a3836	
f488c9e6ec54a2475d557be08b8866ce44dd47d4ed4403b360bab1abd468ce39	
c720910f2a7f1a4b4874faee82bf5cc2579e75d7ed23418130f3fa6e26be2b84	
b8ec4a8b3588f3f1164bc38327530ddce1c93f43194e2d247cc6f935ec71fcee	
4fe3c853ab237005f7d62324535dd641e1e095d1615a416a9b39e042f136cf6b	BKDR_DESTOVER.ADU
a606716355035d4a1ea0b15f3bee30aad41a2c32df28c2d468eafd18361d60d6	
752b8e93a8f6803b265dd3a7cd39df86997cf99900426635b1b97dd665bd7f9f	BKDR64_KLIPODENC.ZHEB-A
cd10ffb7a88f0d2ec69326e7a13f00b9ed211a3a719f89a755a29494ff1142e6	
4c2efe2f1253b94f16a1cab032f36c7883e4f6c8d9fc17d0ee553b5afb16330c	BKDR_DESTOVER.A
efa57ca7aa5f42578ab83c9d510393fcf4e981a3eb422197973c65b7415863e7	HKTL_NBTSCAN.GA
1e0564ef867fccea953efad7fcf1f5b76d9ac51cfe3eff37a0eec38583cb0553	HKTL_NBTSCAN.GB
e5bc4c5794483273dd610ae69913d473440d5533d4f8b2abb77cd64f5af47374	TSPY_BANKER.NTE
2a6f218c6907859a62673116625500b11cd855f28e32968e84e4d1e0558b47fb	TROJ_CVE20130074.B
00501384ff0a9b6c20f12961008ebe5d26858f65e89b59b14d26cb2d115e1833	
e535cf04335e92587f640432d4ec3838b4605cd7e3864cfba2db94baae060415	
c1b29afcfddb79cfd57545b8600922150843ae2b170fff9aeacdeaa17adbf792	SWF_EXPLOYT.YYRQ
6c1d8c4afbc7f85f05fb2e4d17e5553255b0195a0b56ba5309e362e2156debfc	TSPY64_BANKER.YWNQD

URLs/IPs where **TROJ_RATANKBA.A** is downloaded:

URLs
vip[.]9fx[.]us/phocadownload/vip[.]exe
217[.]126[.]199[.]182/phocadownload/vip[.]exe
217[.]126[.]199[.]182:8080/vip_app/vip[.]exe

C&C Communication:

URLs/IP Address
120[.]113[.]173[.]207:8080
sap[.]misapor[.]ch
eye-watch[.]in

URLs/IP Addresses used as command and control (C&C) server, and where configuration files of malware are hosted:

URLs/IP Address	Category
tradeboard[.]mefound[.]com:443	Virus Accomplice
movis-es[.]ignorelist[.]com:443	Virus Accomplice
1[.]215[.]228[.]230	C&C
107[.]190[.]190[.]21	
116[.]168[.]107[.]32	
120[.]107[.]163[.]79	
125[.]214[.]195[.]17	
129[.]221[.]254[.]13	
131[.]11[.]224[.]116	
140[.]112[.]14[.]16	
169[.]45[.]142[.]150	
17[.]61[.]46[.]70	
18[.]200[.]16[.]237	
182[.]45[.]75[.]93	
196[.]29[.]166[.]218	
203[.]66[.]57[.]237	

URLs/IP Address	Category
203[.]67[.]31[.]17	C&C
204[.]136[.]221[.]47	
206[.]94[.]195[.]86	
21[.]190[.]190[.]107	
218[.]224[.]125[.]66	
32[.]107[.]168[.]116	
36[.]61[.]131[.]78	
47[.]221[.]136[.]204	
59[.]120[.]19[.]101	
59[.]173[.]0[.]74	
59[.]43[.]86[.]123	
70[.]46[.]61[.]17	
82[.]144[.]131[.]5	
86[.]195[.]94[.]206	
93[.]75[.]45[.]182	
203[.]67[.]31[.]17	

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