Maikspy Spyware Poses as Adult Game, Targets Windows and Android Users

Appendix

TrendLabs Security Intelligence Blog
Ecular Xu and Grey Guo
Mobile Threat Response Team

May 2018

Indicators of Compromise (IoCs):

Android samples

SHA-256	Package Name	App Label
ee1fdead04a7bfc5b5bca1b30bc981861af69c7bd57a31731688d0e1581786cf	com.appolonis.VirtualGirlfriend	Virtual Girlfriend
9d1494c39bc71f8f01be24a0fc121f19c7420146eff388429ddbc68b02118ce4	com.appolonis.VirtualGirlfriend	Virtual Girlfriend
88d42c458fde0c5536bd9d3280bd86c3231bb081d12e711790138d24d345bbd4	com.appolonis.System.Android	Mia Khalifa
1cb2fc89436cad5269636883cb2654b3436198e4e77c24c444066c0dbd33340f	com.appolonis.System.Android	Mia Khalifa
36ac1332ff159d99d65c7d1765cec565d63daabb8098c291cd739a769bcf537e	com.appolonis.System.Android	Mia Khalifa
c83cc0a54946cac985327ea3b49adafaceacbb9a5a2b1384708dd8d856e52d39	com.appolonis.System.Android	Mia Khalifa
c3280cd64f441cd894653534dc5dc6fd5cf8b67a43610fa90ea52c670cf03408	com.appolonis.System.Android	Mia Khalifa
0a642d2a814f91ee3a202e281736cb613b7ed7224e987f77f391ca138ffcc0c4	com.appolonis.System.Android	Mia Khalifa
656f121aea95e2b14ab5e8f499a8d806d0de9ac003edcf4def48ec067126b8b0	com.appolonis.MiaKhalifb	Mia Khalifa
31f1eb45501a202f226f80e91d63fb239468d24a287fb03a6c4c6acdce029cb9	com.appolonis.MiaKhalifa	Mia Khalifa
fe07353993b525cbbe50d537315101a9f3d426b355c92173e1826474ce2f0ace	com.appolonis.MiaKhalifa	Mia Khalifa
0a1b1ecaaf29a216840184e691f96add728894aae62811920556e560cd1f90a6	com.appolonis.MiaKhalifa	Mia Khalifa

bf375885533a24bfb2daf6fe7880d93bb819a9af5e46cb20b767de51aed2833f	com.appolonis.MiaKhalifa	Mia Khalifa
b5c74f1e543015818b4de8b07f4ddfd60e9483f37663e709c241853963051669	com.appolonis.MiaKhalifa	Mia Khalifa
4ad5ea173aa5575f2f6eb4e0d6896df248eab05d57b7d09c56e9402369383878	com.appolonis.MiaKhalifa	Mia Khalifa
1d140d1239254e72eb7113bb14247359ff01eb348d90a0c3ca60562c32786be3	com.appolonis.MiaKhalifa	Mia Khalifa
f8666088d9d6a0d2408236dd9b81c275c63a937cf44e6c8ab3a70e2c983fefa7	com.appolonis.MiaKhalifa	Mia Khalifa
a45c3f65c01abbb4756ee563f6095a5e3e407c13a304b6df5b2858522518c070	com.appolonis.MiaKhalifa	Mia Khalifa
2f938a6c1a7f822e96b3f628a1cf6be85a6a3478ad1d7dfc51edb601d5499af8	com.appolonis.MiaKhalifa	Mia Khalifa
798f89312c9568429396bb58ae1d552bd1b74184b42b84dc58b6c96f5daf0200	com.appolonis.MiaKhalifa	Mia Khalifa
5144171b08448746bdbc31a0ecda0b088373e2246db5f8011d62f20a858c05de	com.appolonis.MiaKhalifa	Mia Khalifa
4c0d2cb518a1f224a53f82af4f4fd7a71b0e34788c19a0873bea2d576f4ec35a	com.appolonis.MiaKhalifa	Mia Khalifa
dbb1e7fb7ea95efe708ecae85bc6ceb9fe89adfd80a03202b21d052a05750283	com.appolonis.MiaKhalifa	Mia Khalifa
ffee3ad6fcef1294809dd2b3bb3336b1794c4c016634d981c325127f2a213035	com.appolonis.MiaKhalifa	Mia Khalifa
d3251de14d0ae11ee7e6f3d02ded2c2d7c64ef214937cb6bcc599a9f09e911ed	com.appolonis.MiaKhalifa	Mia Khalifa
009969bd0502a6fe3fd15970a7382899fd5ed8482acb8b7166a13d643af66495	com.appolonis.MiaKhalifa	Mia Khalifa
99f42bd03c48d074e46b3d2ac3a32b76b4b73d10a85aa05f51ebae43b51b8810	com.appolonis.System.Android	System

Windows samples

SHA-256	Detection Names
aa2454a5c4e0cbe8971ead06f80f6aa4379b190dbdfd07094ee886f0d01173ed	WORM_INFOKEY.A
72880730d5ddb1e198b95481b244d37687ad298bf69cff9aab7600cc085ffd15	WORM_INFOKEY.A
336f901b59c821166825507f662df9e4eb5520495bb7da89db88bebd3135e66f	WORM_INFOKEY.A
40d657c20d413a61c236cfc39d828d14777fe65d7eb30da663949b78fee15956	WORM_INFOKEY.A
aefa751ca27c42ebbd9609345d36930b52d37154a26c2e19d03596eedc16a630	WORM_INFOKEY.A
1d5783a8858c3bb79eee217d7c03405de52c24601b1fc4430249a98e4adca346	WORM_INFOKEY.A
bfcb447c2f1b1694a90467d66986f8bf86a0a978b263392e81c4e22ee94f84aa	WORM_INFOKEY.A
aff1ae60e09799e501fbfb6e148138a48391c00006ee155a92809da23d0d565a	HKTL_MIMIKATZ64.SMK
3eeae8dd4895201513c28109e97cae839366ef554ef212ddf86598a50fbdb2e2	BREX_INFOSTEAL.A

I.P. addresses and domains

hxxp://miakhalifagame[.]com/
hxxp://roundyearfun[.]org/
hxxp://roundyearfun[.]xyz/
hxxps://twitter[.]com/RoundYear_Fun
hxxp://fakeomegle[.]com
160[.]153[.]60[.]192
198[.]12[.]149[.]13
198[.]12[.]155[.]84
192[.]169[.]217[.]55
107[.]180[.]46[.]243

TREND MICRO™

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