PUA Operation Spreads Thousands of Explicit Apps in the Wild and on Legitimate App Stores

Appendix

TrendLabs Security Intelligence Blog

Lilang Wu
Mobile Threat Response Team

May 2017

Indicators of Compromise (IoCs):

Hashes (SHA256) for Android

SHA256	Package Name	App Label	Detection
915d3470038b65c5db3cdd006ddad2a542e13d118b2ab6467e9e71479b29a20e	cn.g.hades.dea	成人影院	ANDROIDOS_SMSREG.AXMFA
5e21caf972f65c746e947a204b1fa084e116436c4c7047a10bf1369af6a9547d	regre.trh.dwewf	AV 快播	ANDROIDOS_HIDEICON.OPSA
d5e93a816e7f73de0e73207c64673752289fd0bd7ed4924d62cae265409941ad	com.xiao.ht.kumg	幻想影院	ANDROIDOS_SMSREG.AXBDJ
fa0cd13d2780ee122211bcbef0583c6b7e81c28b25acd8f58d47e77db8a06e6f	qaz.wsx.edc.qwe	快播 2017HD 版	ANDROIDOS_SHEDUNXD.AXBRE
d2114b0e2059c53b7608566e57552be4299e5c1f1bf8c1852d6b030571274715	qaz.wsx.edc.qwe	快播 2017HD 版	ANDROIDOS_SHEDUNXD.AXBRE
cce7d114b917f112b0eeb78611d31d6cb55c0b89773e25f361765356b4b76a47	qaz.wsx.edc.qwe	快播 2017HD 版	ANDROIDOS_SHEDUNXD.AXBRE
bd6d528e713e64d5d03946eb21f4b542d87bb7dfd33696e34b6acee88306eb38	qaz.wsx.edc.qwe	快播 2017HD 版	ANDROIDOS_SHEDUNXD.AXBRE
c579250722d4010a077ffeba8ae46d4e044d1a4517d94a11537870e6bf18a69b	qaz.wsx.edc.qwe	快播 2017HD 版	ANDROIDOS_SHEDUNXD.AXBRE
9e361c65275a499b9888330ff6a463e1b67e5d986b7f160b72db5c779f3015ec	qaz.wsx.edc.qwe	快播 2017HD 版	ANDROIDOS_SHEDUNXD.AXBRE
a3eb017f09165710930230a1dd7a7966ee04bff81e2e3b37325f0082533e7bf1	qaz.wsx.edc.qwe	快播 2017HD 版	ANDROIDOS_SHEDUNXD.AXBRE

Hashes (SHA256) for iOS

SHA256	Package Name	App Label	Detection
431798afef6a1850ec6532f4242e83a90b625ead8d912d89a9e47657873e6408	com.eddie.nguyen	NightMovie_DXTX	IOS_PORNAPPS.A
cebb5a1dee4753af0ba483be8e3234e004e20acc80da02e5a5b96e1a3819eeb4	com.eddie.nguyen	NightMovie_DXTX	IOS_PORNAPPS.A
ab2f1c2674e01ffa28150a5585a488d5414fd0d09380c979e1b88a4b22148449	com.gjlixkl.hklcc	春爱影院	IOS_PORNAPPS.A
4ada39d70d05ce08c124d1ac3d5f0a10ed9f4efcb0c8b9d52854ddc921f5bca7	com.gjlixkl.hklcc	春爱影院	IOS_PORNAPPS.A
1aa7e843f08335bbe82c0b7dd5d24e1f865b5a14eeedbe86542997142d2cd121	com.wt23.charmplay6	3D 快播	IOS_PORNAPPS.A
85e61238338f944a3fb7693defc01a63c693a672573e26d1bb76deb571f85caa	com.wt23.charmplay6	3D 快播	IOS_PORNAPPS.A
cd47f65f2595a2c1d528da386255cc9dd40597385055bda8139f77e702fdebf4	com.av.jx.6	快播鸡年版	IOS_PORNAPPS.A
2b6f55dce0ecca742bd23549e05b162dcd71e278e1f1e5c587804f4f52589999	com.av.jx.8	快播鸡年版	IOS_PORNAPPS.A
69f90d24a739c96a9470882ef0c1bcdbd224a619a8818ce99906f62807038c2a	com.liuliu.yyer.010443	AV 快播	IOS_PORNAPPS.A
8314e5ddf7b08624ed38b51dd9f7bd5b122b83075efc36ece34f0424e2b510fc	com.liuliu.yyer.010443	AV 快播	IOS_PORNAPPS.A

Hashes (SHA256) for iOS (labels dependent on language on device)

SHA256	Package Name	Detection
156262a97dd097d9e94b526df9552316337dfb14ed5ab9a1444787c5df12c94f	com.yoshiya.wifi1	IOS_PORNAPPS.A
5f494e8a884223a9032523a804ac97bcd55202da4130e5aaa1b10a1c457ed01e	com.funplayer.ST360	IOS_PORNAPPS.A

SHA256	Package Name	Detection
676429e8bc19f41a2c37e01df7f3ab84949ceec4d16d6325ee1da167a67bff5a	com.funplayer.sandtrap	IOS_PORNAPPS.A
af028bd0fdbc870daa88178539d0ecd8ae883702f8c6d86f2c11f539760d5a3d	game.0002	IOS_PORNAPPS.A
737bbee4d0e4cd710bd35d91547dd8bb8a0c218a12155930c8b07f9fe3dbee67	gamekb.2	IOS_PORNAPPS.A
c3f9a877de62ca35e8345f6b3007805676ba0acab45285eb3ecec8bcd6f102a2	com.app.kuaisusp	IOS_PORNAPPS.A
14e0bc60546c474ab1fad7b117aa61cf6ff9706279258185385146d7f8d059db	com.327.10	IOS_PORNAPPS.A
e32cac8dbfbe2e7ec3f7c899387c20f9a784110b1c7f0c380b4d9a410c26f6d9	com.organge.kuaibo	IOS_PORNAPPS.A
5ba75c4ab6c7e65d8b796b2d4231290399d084c9a3888cbdefb7a81ba3c05387	com.dehua.crzm	IOS_PORNAPPS.A
d1d9d2d1b6ff7bde0648e3769b308b5a734a6d421741efbaa26868905c6cdc07	com.327.07	IOS_PORNAPPS.A
112476665102af9adfcfeeecfc618b336059933f879acf3b8234e9e9590db728	com.327.13	IOS_PORNAPPS.A
a882b93bb50793a96f41d516bbd7a37d43cb71119750b25abc19fb5c62aa2175	com.shenpeng.ctttt	IOS_PORNAPPS.A
748fbadaf1e88f04f5238ef500c55e37853606192fa4e0a729f9832214369cbc	com.shenpeng.doto	IOS_PORNAPPS.A
e559c2ed3bebcdcb06c7cd6c56db1a06b86ff0e68833d609b7f8dcc870674a45	com.fengqi.neoo	IOS_PORNAPPS.A
80930416561d0ecf764e4cfa2b89a56acd48811baf3a367bbd18e90da0eeab79	com.dehua.Stickman	IOS_PORNAPPS.A
e02a26bea3ff73ae95812cbe1cda8c0e2aafe050598fa1eb48b9b71586993a3e	com.fengqi.DTO1024	IOS_PORNAPPS.A
aeb5a746c040aed5a8b542699b99d158e604ab39ac95d36f79dad726115e56a8	com.fengqi.DT1024	IOS_PORNAPPS.A
e3a063f4f31dcedc9faba0d179f3801f67ccd7fbd62b129844e175ce781e4ab9	com.201603.01	IOS_PORNAPPS.A
002de9c5fcd5ec17d4e211bf9ebc28e0a44dd008c430fd7d45e5bf5673fd2b90	guas.bofa.gasa	IOS_PORNAPPS.A
ae3a60251f4ac4fca8f2813fa5d042271ca38dd5430fec7b467e19d57fc0162f	nhb.bfqn.basq	IOS_PORNAPPS.A
35ea15eb2821a9af1e6bfcd83f5f74531006b4087f14fde87ad54a007856ab01	com.nexmon.xfzyfree	IOS_PORNAPPS.A
368b4353118ebdb7269f9514c0fdcfa731da21e41c645e90eca98ecb0ce8c806	com.nexmon.hkmj	IOS_PORNAPPS.A
a107911158a5616047b9b5927fb36d030cf6434a849f75b7ce2f041487228da6	jie.yans.jybd	IOS_PORNAPPS.A
e4b05f064b6d58fdb5a8d00f034024f98edd3ff67	com.nexmon.vgsm	IOS_PORNAPPS.A

SHA256	Package Name	Detection
353131294afdd1f75badfa9		
fd6ac26c5ad86d6f242a505d7db0a900f37b7e8460740e2b1fb764bab9631b06	com.nexmon.learnquote	IOS_PORNAPPS.A
7a763e43fe00c0c34735befe014dadd5e56419ade86606e60fb8949ad1ce1f0f	com.nexmon.papitube	IOS_PORNAPPS.A
75b18842344fc64e14e9d6b0225162b1b3c8f358a4b00cea7f923a75f416bfa9	xle.xaza.xule	IOS_PORNAPPS.A
4ff285b0835a0e07bcaf18dd32c6484bd63e56fadbecd1e4491ca504db47df7f	zoxe.zaox.zaxi	IOS_PORNAPPS.A
e85ded2ab9c3b47da85b08579eee7e90422767164e5f8b3270d0fa31557a1179	sof.sfan.dysf	IOS_PORNAPPS.A
2ba3f1802bb9c76974ef6f2d3be69569c999b24dee3b6a70d5ab06f6dbd27e69	sen.papiyy.tori	IOS_PORNAPPS.A
8352916194365576355ff3185df646cda0425d31f7b946eebb46e1137c14d92e	vga.xumb.vgxb	IOS_PORNAPPS.A
d578ec8620d8cd44d75445d482ee43aa0e06f591cbf49c622274d3436689bd3d	com.papitb.xiaocao	IOS_PORNAPPS.A
d17edf2a8782b52ae9f8a8ac6606ffa435944f869303f2464e60ef7b13e55a20	xio.ruiqin.ttmj	IOS_PORNAPPS.A
eb31442d0b088b253355e60add3038e3429b72329b9446ac5bf432748f50968b	xio.ruiqin.yunbo	IOS_PORNAPPS.A
0fe4e431ba35ea2650840721be0cbfb133470b6dd3d42dcab377a6fec1201008	xio.ruiqin.nhba	IOS_PORNAPPS.A
218fcd29457f8a734b3747f188eacb5de29cef656b0e3c5046b940775461697f	xio.ruiqin.tort	IOS_PORNAPPS.A
6ae76655cb89facfe474e8724080e850301ba825a2abb88bf634dac58155fb6d	xio.ruiqin.tita	IOS_PORNAPPS.A
720bd8dc4dd32deb0d9df8159e5e33e64af759ef78adf837e3f2949f32606a28	xio.ruiqin.jiji	IOS_PORNAPPS.A
c7ac3866063015bd038c0b490bea25c0f35f4256b41503645b7585e76f5ebd62	xio.ruiqin.yule	IOS_PORNAPPS.A
3c7ba6b5da972130b75b74d7da658fab428e7df3864d0cf1d296f5bce4431d20	xio.ruiqin.yese	IOS_PORNAPPS.A
e1a2e69480e424170200cd9c5437bba20bc1800f959155a26f32492c2a1028d0	xio.ruiqin.xzs	IOS_PORNAPPS.A

Malicious Domains:

URL/IP Address
ygyl.bysun.cc
jinm09a.eeeeioslyee4.pw
woaikanpianyongjiumianfei.cc
238-114.ffjj-2.com
wdfw.ksmsmk.com
www. afuxz.com
mo.39lo.com
html5.senruilicai.com
e.919cp.com
afuxz.com
iosldy.hzt88.com
waszyy.com
Xmxli.cesicc.org.cn
aaaaajbrg.cn
in450.ejud7z.com
0318.weitaohu.com
csdt.isoucha.com
ghbyl. com
hymxz. com
syjlzs. com
zgqlxw. com
eduigou. com
isoucha. com
ksmsmk. com
seuxm. cn

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