‘Godless’ Mobile Malware Uses Multiple Exploits to Root Devices

Appendix

TrendLabs Security Intelligence Blog

June 2016

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.

Related URLs:

hxxp://market.moboplay[.]com/softs.ashx

App hashes (SHA-1):

Local Exploit

Commercial Name	Sha1 for infected APKs	Package name
Geometry Dash	01b3e575791642278b7decf70f5783ecd638564d	com.robtopx.geometryjump.admobplugin
Mobo WiFi	7ebdd80761813da708bad3325b098dac9fa6e4f5	com.foresight.wifiseeker
WiFi Anywhere	34b7b38ce1ccdd899ae14b15dd83241584cee32b	com.foresight.wifianywhere
Mobo WiFi	84c444a742b616bc95c58a85c5c483412e327c50	com.foresight.wififast
Mobo WiFi	50450ea11268c09350aab57d3de43a4d5004b3a1	com.foresight.wififast
Mobo WiFi	aed8828dc00e79a468e7e28dca923ce69f0dfb84	com.foresight.wififast
Mobo WiFi	44e81be6f7242be77582671d6a11de7e33d19aca	com.foresight.wififast
Mobo WiFi	d57d17eb738b23023af8a6ddafd5cd3de42fc705	com.foresight.wififast
Geometry Dash	17e5be80a4ed583923937e41ea7c1f4963748d1f	com.robtopx.geometryjump.two
Mobo WiFi	9f586480fbc745ee6b28bfce3f1abe4ff00d01b1	com.foresight.wififast
Minecraft - Pocket Edition	888f10677b65bf0a86cf4447a1ebc418df8a37e8	com.mojang.minecraftpe.admobplugin
AndroidDaemon Frame	74a55e9ea67d5baf90c1ad231e02f6183195e564	com.android.google.plugin.dameon
Minecraft - Pocket Edition	5900fabbe36e71933b3c739ec62ba89ac15f5453	com.mojang.minecraftpe.admobplugin

Remote Exploit

Live Launcher	e70b1084e02d4697f962be4cc5a54fdb19ce780a	homescreen.boost.launcher.free.small.theme
Lock Screen	a3e84c4b770ef7626e71c9388a4741804dc32c15	com.iodkols.onekeylockscreen
多多每日壁纸	671fa9291bf465580ec1ea1e55ce8a5ce2d848c7	com.dotools.dtbingwallpaper

多多每日壁纸	e10efdecab3998cba5236645b5966af6ff4162f1	com.dotools.dtbingwallpaper
iDO Calculators	57795c32f75a02a68b9a8acb5820eb039c083a16	com.ibox.calculators
Live Launcher	c74eb5fa1234620297330874bd23605158a890d2	homescreen.boost.launcher.free.small.theme
FlashLight	5d2a08d7c1f665ea3affa7f9607601ffae387e8b	com.foresight.free.flashlight
Easy Softkey	416b1fe39eaaa4d83c7785d97e390d129dbea248	com.oeiskd.easysoftkey
iDO Alarm Clock	7809e1b6f85ee0fa7f0c2a3f1bfdc7fa668742bb	com.dotools.clock

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.

©2015 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