Kernel Waiter Exploit from the Hacking Team Leak Still Being Used

Appendix

TrendLabs Security Intelligence Blog

Veo Zhang
May 2016

App Hashes with Detection

App Label	Android Package Name	SHA1	Detection
com.android.core.network	com.android.core.network	5ae5f5a452ab5a95ad384deaf54db66581c57227	ANDROIDOS_ROOTNIK.AXBQ
		6b6fbbf805c39b6df388c68f5a4cc1aae4804a7d	
		dd18770852293330ccd3a9f289c224e5b7c394d4	
CoolLock	com.fun.touch	87111b27284d5f2083bd7236667a4edb5a1938e2	ANDROIDOS_ANDBG.A
DeviceTest	com.you.goolauncher	16eee42c951c018a3c25c586c5f3d22ebf9cea84	
	com.qugoo.launcher	466c7a3f6605fa34ff76e271c4dd07329885262f	
	com.mopub.launcher	66e804c15f1b001fbcfc1a7eae97bc1f50bb9e9c	
FarmJewels2	com.game.kenriv.westasia.vegetable	c929047d2df48af86f1f4eb9f2a96c7e0b46eca8	ANDROIDOS_ANDBG.HRX
FreeMusicDownloader	com.mmp.music.x1	859a88b8aaebb3ce81681a5767846dee6344d923	ANDROIDOS_LEECHG.HRX
iLauncher	com.go.apus.mi	373fbb26ed81dcf0c5385f0d522f0892eabce6e5	ANDROIDOS_TOWELROOT.HRX
		58681c5ed03a939872d9231d03c04b96fff574de	
		d31293b127a555ff86e9b2b9ec5ddb2f739f9002	
		de4491a8d9828a4f3c720bb	ANDROIDOS_TO

App Label	Android Package Name	SHA1	Detection
		cfa54046bab9fe5a1	WELROOT.HRXA
iOSNotificationCenter	com.kukool.notiman	0e8832e2ac7b6e5b01d0ee94f5b7aa9b30d642cd	ANDROIDOS_TOWELROOT.HRX
		218799b92371230380b323d4fa3442b52a32509c	
		23bf056f2d523ce3b5567954b06613147c6a31e0	
		253bd35632bd4a472d616e1b020baacbddcf73b0	
		2714eab94d3c631bf45af162fbca2faadf428e35	
		413a20eb2b37783663d38910ab4666579b734dcb	
		4f7925caef9f7f8cb1f226c8548ffcd1a2b349bb	
		5463ca33d7b9cf4cdad68d02daaaf0131430c469	
		5ffacf768d86e1c4c8dac6e97de03abfefc82b81	
		6822ade60764af705f7484ed51cd923de9923cf4	
		71de8859cc09551aea9bc9b812f859260bbb8489	
		7314127e9b63b58746c17f0ec2a43b8965f49990	
		77fc0fcb7f66cd1b822e47cda44e6103520e06f7	

App Label	Android Package Name	SHA1	Detection
		7e10b9377aa54197c79a8cda22c37f0fe5971789	
		7f5ee5b3087b03e4dada7bd8fdaa893f9f20f623	
		86bc2848dd63142a14c6ea5be7765f7266c2a957	
		914de3fcbf2998c76b2845e30057271476d92452	
		ac60f736ec41c6248f4ba662dcfa6ce539b8bfb3	
		b8f3e24ded787a1893b7908915cf5f798007aadc	
		bc955f5ad0ae6272e8e66f5315d9225b6776cac4	
		be127f7115654d7a4c9c576629ea61de86887124	
		bfff5658ea456da4ca393c747886688cb803d08c	
		c052d095ab041f2604cd25c7caf44db8cc846056	
		c46d91800f9a3875003c64a7ebc644361622678e	
		c9fc3d26b41bc1c31e7a7ec843c3bb031a93f137	
		cbc659c44fd80afe20428ee29e90b8d9b7554f84	
		ce936eb601694568b5b9bc4f42be6077bb07f517	

App Label	Android Package Name	SHA1	Detection
		dd5013833b083b5a7b91eb b4db26c45f5156cac4	
		e037731797bd6d16e897f96 2d7c78d78eb3fa1a3	
		e08ae0ed6eec500ba1eee8f 849892229cee564eb	
		e16ed3bfc2ea50c45f90ff20 d61cad77dd4d790b	
		e31654d34db5f7229bb24f5 2b4f3c4e02e7aad7d	
		e6330b39c63f2a630fbb625 60bf9f0d04d3d4651	
		ec2cf3d280e87608d649764 9cdc277f122d4c92b	
		ffcec50d044bb5b153b624b c6eba662e187cf9dd	
LauncherIPStyle6s	com.kukool.notima n	6d98ad6544e65a9c36c601 a1d8f4b702d1e4b076	ANDROIDOS_TO WELROOT.HRX
	com.ilauncher.ios.t heme	77388cc8d24d44098e5b93 604b4ac9f700b5d325	ANDROIDOS_ORI GINXZ.HRX
Maria'scoffieshop	com.cafe.game	059f9c2c025c302a0a86051 c50bf95dfe6ca4805	ANDROIDOS_AN DBG.HRX
		0f182cbd6e11a7fe8871e93 468ce0cea58583f45	
		160b572c060e400602c7ac e54ba69f616c29d3d7	
		1eb49b4a20299ae46bd0a3	

App Label	Android Package Name	SHA1	Detection
		d3998de1af0a5137a4	
		28af0b3ee4aa26fc448ebc975515dbd1951ea27d	
		36bd9808223ae69235e9aafd0b524024bd3e8f1e	
		50bac5cf8e1ee18184a32f4306cdd319675bd78f	
		51e1e75ae672d5a928fb75fa1564ad300927eb03	
		5b79eccc99447d35d67c43f4817f6efeacc61bac	
		61ed377e85d386a8dfee6b864bd85b0bfaa5af81	
		6a87eb750b4c99d9fce03b5b1827821862f9963b	
		6aeed49cdce4682cb7919038170ea123b57a8b50	
		73b514583518edb5ee99ff3592f4c160d25fe521	
		7885c5777a37fe3f3e521051e55b8f0397aa4281	
		859212282e29608e5d64240da16657ec178aba91	
		887814a719c0920336e49e980fda1f91d4a060a5	
		8ffe2376796b8e2cae4e565528f2ae9976d99b1b	

App Label	Android Package Name	SHA1	Detection
		915537bfb49d559b1accd5e424eaefa53b93c7ec	
		a5bb3739a4ca1a240677928156c6f063011d4f60	
		b9dc66009668c4a1984cf388732072d023113d1c	
		d8dad4300719e3ab4ec8bafb7bafbec2ecf4532a	
		dd4cc8f00555c160b421d4b5dcde460db14a25fc	
		e292a22862e8bf68fe15e02726f82adfd33e18e9	
		becdd6ca251672109e61461e596fa8f9de01e1a	
MotionLauncher	com.xui.launcher.how	31b2348e0fc4d6b14c98e1b5ceb52ecd4a5ace6a	ANDROIDOS_ANDBG.HRX
	com.kukool.iosapp1.kulauncher	56bb78096d3c18a0e991b368ecd830c5a0d151e9	ANDROIDOS_TOWELROOT.HRX
		ec138cd5fc431d7a00244980e52ec86de8f753ba	
		feca9825ab00c2b21d88e8984f92a403294e7eef	
SmartWatch	com.mic.allintouch	a62fe3797b12acd0e476008815f5cb71a60caf83	ANDROIDOS_ADUPDT.HRX
WhatsappManager	com.ifb.manager.togoogleplay	a342056e93566a21463756e90a3b6e76a9f557a3	ANDROIDOS_ROOTNIKL.HRX
酷酷斗地主	com.kukool.game.ddz	243e38e1cfbcafd03a58be832b614b2897d6fe32	ANDROIDOS_TOWELROOT.HRX

App Label	Android Package Name	SHA1	Detection
		2cb41a231497eb0952257728204579ed80dec078	
		5ffd80248935fb88f141ad9d7425cc520b3c9b6c	
		683a55b66392c16e4ad9024ef796d6a0a81adcc3	
		ac40d8f043e07194a62dbe67642db87ee0474d4a	
		c7edbe54f92b77cbe221a7d5c53c15060230ca63	
		e8e0243f10c8f7c460030c1ce53442d2a35aa8e1	
		ef7aaa86ebda5951b274cf1fb0c58475bbde82ea	

Related URLs:

- hxxp://198[.]58[.]103[.]210/apks/Launcher-free-77-2_9_1027_20150203-ch1.apk
- hxxp://apka[.]mumayi[.]com/2014/11/14/87/872076/iOSNotificationCentertongzhizhongxin_V1.12.20141114.1_mumayi_a391f.apk
- hxxp://bcs[.]duapp[.]com/kkddzpub/ddz_111_2.4.20150214_kkyouxi.apk
- hxxp://bcs[.]duapp[.]com/kkddzpub/ddz_115_2.4.20150328_kkyouxi.apk
- hxxp://bcs[.]duapp[.]com/kkddzpub/ddz_116_2.4.20150408_kkyouxi.apk
- hxxp://dl[.]elevensky[.]net/apkf/apk4/M00/20/43/wKhklVcDgCSAXKAfAB6Mii6hPR4075.apk
- hxxp://down[.]mumayi[.]com/481177
- hxxp://global[.]ymtracking[.]com/trace?offer_id=37770&aff_id=100032
- hxxp://hasoffers[.]ymtracking[.]com/aff_c?offer_id=37770&aff_id=12400&aff_sub=${SUB ID}
- hxxp://risechen[.]b0[.]upaiyun[.]com/up_img/189_1449304750.apk
- hxxp://risechen[.]b0[.]upaiyun[.]com/up_img/245_1450852420.apk

- hxxp://risechen[.]b0[.]upaiyun[.]com/up_img/278_1453282667.apk
- hxxp://shouji[.]360tpcdn[.]com/141103/a6109cf978a908c77bb13e9b16ae1b55/com.kukool.notiman_10.apk
- hxxp://www[.]anzhi[.]com/dl_app.php?s=1869695&n=5
- hxxp://www[.]anzhi[.]com/dl_app.php?s=1873847&n=5
- hxxp://www[.]anzhi[.]com/dl_app.php?s=1930012&n=5
- hxxp://www[.]anzhi[.]com/dl_app.php?s=1942641&n=5
- hxxp://www[.]anzhi[.]com/soft_1869695.html
- hxxp://www[.]anzhi[.]com/soft_1873847.html
- hxxp://www[.]anzhi[.]com/soft_1930012.html
- hxxp://www[.]anzhi[.]com/soft_1942641.html
- hxxp://www[.]mumayi[.]com/android-481177.html
- hxxp://zhushou[.]360[.]cn/detail/index/soft_id/941948
- hxxps://app[.]adjust[.]io/ezottk?campaign=aff_100032&install_callback=ymob_cb/conv?transaction_id=c33cbaab-c12e-4624-956d-f73cb940bffa&adv_sub={android_id}&adv_sub2={mac_md5}&redirect=http://198.58.103.210/apks/Launcher-free-77-2_9_1027_20150203-ch1.apk

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