TrendLabs

ZNIU: First Android Malware to Exploit Dirty COW Vulnerability

Appendix

TrendLabs Security Intelligence Blog
Jason Gu, Veo Zhang, and Seven Shen
Mobile Threat Response Team
September 2017

Malicious exploit server of ZNIU:

- hxxp://reg[.]oozclimb[.]com:5101

Hashes Detected as AndroidOS_ZNIU (SHA256):

SHA256	Package Name	App Label
02716eddfea51979a46f4f5bfc490223524b24e841590641b1b3fcf1670100c8	com.tj.tjcty04645	调教初体验
05772cbf9780777e08c704a65282ae28f3231f9e2cbbd49f8bfaf0c3a5e32bde	com.tj.tjcty03458	调教初体验
0d7da9b7d6bce9165fa065030ed0a86b40bb52cd4a355e12dea43d496ba5aad1	com.tj.tjcty04011	调教初体验
1115b3a988604c9757d444169782c2b024bd53d50c682f6aaf00699229e35e44	com.tj.tjcty01142	调教初体验
14bfdb03c638d34cfd7e69c100db36ebbec52e462cd28399ca81c0ebdd596fa9	com.tj.tjcty09635	调教初体验
151e27c69cf7db372a59eb36960d6f50896eb44cffb3f551f2d8088d6efd1d8d	com.tj.tjcty03441	调教初体验
19069ecf7e10d241c462ca9a3a437524d6f9ff6aaf7663646a458f7374495cc3	com.tj.tjcty04315	调教初体验
1c92bd16119245ff76ed03b64be81215d1781a4686fcef7600d90c6c2d3a315a	com.tj.tjcty03513	调教初体验
1d2164fdc7be110224d66910d1a84a06c8627864920f418f2890aff6a5d0d320	com.tj.tjcty01811	调教初体验
208d86e33175f6ac6c252eecc6857ace95d8824f480b32f369e7f13e4d3797c4	com.tj.tjcty10337	调教初体验
20af7c82d0c7dc8f8063d88cfa150ae3f8db89743cef07a96f8bccdd0e6885a1	com.tj.tjcty13355	调教初体验
219cda26aeb6bd398f3b7ddaecfa8f26aa0c5d792eec460fef6bc4bb447bfbab	com.tj.tjcty04237	调教初体验
2661f01f3c4a53308e312869bd734d73afb43f85d1cd49cb9cf9ba58f13b8997	com.tj.tjcty09160	调教初体验
2a2133a2064a4b3b83480abbff55a0ca73ab0f3ce9208b59b18d00193cf627e0	com.tj.tjcty09160	调教初体验
2b8039348d70fd2efffaa7e80cf6f9bc569f79a3247cbe8e4bfb79cd0ae62b64	com.tj.tjcty11143	调教初体验
2fdb1d7e66332d9398f47d7cb06bfd38a335e5311a201adb60e36c9b5f031279	com.tj.tjcty12749	调教初体验
31dab931ada06824af42033de693568b8caf5e612d79218d8d2a41bf0d34469a	com.tj.tjcty11346	调教初体验
31f8034080f5e02092fc3e88df32aa1f891e85999bbb16b468200a1571309371	com.tj.tjcty00653	调教初体验
36e74d155ad6ce0b3d546558c8f24d047088400cb923e2ae38990b3ff6c662ee	com.tj.tjcty04246	调教初体验

SHA256	Package Name	App Label
3add84fbbbd9904ce222ab29ad80bd7aa581a3e85994d3e0506191655d66b957	com.tj.tjcty03910	调教初体验
3ce1af003291e2fdd62d3651480ebba41116a29fbe2d3bdd2edace4a1e18602c	com.tj.tjcty00655	调教初体验
40b2df00bc7abbfe7a1372c89c7686a4f609dcf984214293ab775ab19eeb45e0	com.tj.tjcty02044	调教初体验
466a9238545307cffd412a0899be31144eebe3f3a28e34405d5de7b509a89a82	com.tj.tjcty09160	调教初体验
52dd0b046baad07120ad2dd756d2f2078e399023fca2990bfedf72b89dd20d85	com.tj.tjcty03915	调教初体验
544d6de789804ae7147fb5d2ae527409456ccfa93f261298d49ee94ee2ded5e1	com.tj.tjcty14558	调教初体验
60e74ee352c3ee063cbe9e3a00230b73db07b4e24bf7be0868e2357ca7d15dd9	com.tj.tjcty12349	调教初体验
60f3d4d76cf232372ef569063e01237f5081c45c2e4fecde5fde0da25f0d7484	com.tj.tjcty03415	调教初体验
621fc5c33769153b957df0709c6dc45e6837291c797dc48522127a89eac8e49c	com.tj.tjcty10137	调教初体验
6a7900241bf608aff7266816f34d60e280702227c7519277fe0965e502852678	com.tj.tjcty05539	调教初体验
6aea1e676fa099b9c902389c5eee04511b6fc60febe3ffff0b1ab13c8ef1823e	com.tj.tjcty03411	调教初体验
6db51cd4d0d90a11e3b2583d0f1311279be03ae6ca6fdfd12e0b9eeb3f7cf89f	com.tj.tjcty01715	调教初体验
723f97ff8f1f14ea4bf80ce83fcab21d03816bb8a7ac49c198e080d6e286a5b1	com.tj.tjcty01155	调教初体验
74ca2879f54ed133e6a6bdcf7e95ad45897ffafa8e43af6d293b109d08299053	com.tj.tjcty04619	调教初体验
7594f7459b1eb5d8c8d279f52990b1d974745f5167487e2251d9977de82c9612	com.tj.tjcty01850	调教初体验
78886e1992e1c077d8aa40f2157e2aaea855ac4d559a66a7a0fd49628eab0e70	com.tj.tjcty01255	调教初体验
7d81852ead34bb3f87e228f5cb69e7844f51b642d0c45929ceb11ffcbe12e6d6	com.tj.tjcty09160	调教初体验
7dbf0732f3a5111cc27d4e5d2001788aa7499859ed6efb25a1c51087faa244f7	com.tj.tjcty14858	调教初体验
81b565cf3879e6430a62a92287aa9e882cfedf0fb8d5918a3f568f47af405e7a	com.tj.tjcty04945	调教初体验
86eb4574fa0fa4b16ffaac02558110a77b99ef840e8ed32b38547cdfdf14e6ac	com.tj.tjcty04010	调教初体验
8dae0b8b52aa4be044cf6fde34a717b5d33f68dda6c7eb1d4a88e7220715ea98	com.tj.tjcty09338	调教初体验
8e595253eb227d66aa046c4d7c4c0fba4fce193822b5b456defc43fa5bd9e60e	com.tj.tjcty14458	调教初体验
94d191d7eb2dda751772d0bc4421c2fe6ccee196f345c39c00fbcbeed2f01942	com.tj.tjcty01242	调教初体验

SHA256	Package Name	App Label
99105b253ce701f03d9d486859bbc4cd0e22d195709b2a36e1fcda2b16770228	com.tj.tjcty01360	调教初体验
9a825cec9e532fec72953e754f578f683bfcac502bc88887cf990c4248a7156b	com.tj.tjcty07345	调教初体验
a2a1b423ba7a8d940bd019baca29d0d17554ec388dec5a81a9a3a87c2c104d2f	com.tj.tjcty11243	调教初体验
a4a2901846343cfda6c34846d3e0dfa01fa78147343c700103b62046b286b758	com.tj.tjcty11043	调教初体验
a799fda312167cffb3ef53c4a818eb1d0c9005935779cd9e1c839405cfb63fca	com.tj.tjcty0119	调教初体验
a8b05fc0edf36c397fc67c6f06a77887c03b2cfbac1f08b31a98cf73aeb2ff3f	com.tj.tjcty01915	调教初体验
a9d77ce84b476eaf52695ce8f343a2afa52705afe23c6f64d4d1ea25a2587019	com.tj.tjcty11446	调教初体验
ac5edd29db4a1588b1a78e9938a740bb598f34a4973f9b0d686cea5eb909842b	com.tj.tjcty07645	调教初体验
aee0ac40f0506a5545585bf07473335cc052ac713a89a14a74698f081b6a6c89	com.tj.tjcty13955	调教初体验
b13a1de26c147c202730057c45124aa9ec06a3fcc99db177fa3b957207a09208	com.tj.tjcty12849	调教初体验
b26d8a7194a58ba4c5d858be984d7542b64a6888c2c7d619be9ea3ceb80c9e8b	com.tj.tjcty07745	调教初体验
b2c7f10d758971d09bc4d6b456bac61c3b395ef20de4d56612f243ac1d1031f1	com.tj.tjcty01117	调教初体验
b4d775b539bcd7243d4f24fa2e8347bb85c5e6e86bae34ba692af1cb27a2fc2a	com.tj.tjcty09160	调教初体验
b60037848ddcd3ad55940e78e6f82ecc0f69be7bfcb5cf729767c5c24a5a29f5	com.tj.tjcty09160	调教初体验
b666edb035d4c2b1c70c8e38872d3e7e25e857aa4aba382661113def1eea9950	com.tj.tjcty05245	调教初体验
b6ae0b707798c01341c5f25b55f72bb144f962eff01cd92b78760e7a6655572a	com.tj.tjcty05745	调教初体验
b840871d9020d13a25fe93e588529e44a573d0a690e4751443ff742dbcc4fd0d	com.tj.tjcty11949	调教初体验
baa64a724dcb0119eb53f34afa098852d7faaf25f53ee7346e601a9b1a56ec2c	com.tj.tjcty0249	调教初体验
bac86e916477e812c43635f468f89b8cd7f73921369c6bdc50f6b57a04268df6	com.tj.tjcty14660	调教初体验
bb11e3fdc989036f82b2fb5ed498e3c3b890374d3c4aedde19b6735b25e43bcd	com.tj.tjcty01853	调教初体验
be2a53e3476b8e6f3b8a8eecc343b20b0a0d7114f9d7435e91d4773f31a73c07	com.tj.tjcty01860	调教初体验
bedbce1e683ed1a5b14c681b36b4e01bddf2d79ca8718eea0b6c300a03766958	com.tj.tjcty0319	调教初体验
bf441642326797c491df70b1bc66d6be7c0ef63e6c25229826538cdf60c5bf91	com.tj.tjcty04113	调教初体验

SHA256	Package Name	App Label
c02b5acb8e0ef7aecf7cb882af1fd06647b8931c86fe90259c17e50047fb497a	com.tj.tjcty04845	调教初体验
c379ea39edfa94f249ed10834bda784ede4be3e62ca66e9e012ce945e1d1f1bc	com.tj.tjcty09837	调教初体验
c4c9c2befe7c283ddc3885eef5380bf35ae59def84e58783c0aad43b9e3f321d	com.tj.tjcty01360	调教初体验
c797ebf212d3d926f7cf56d08f04b7eb00b3bf4fd654569e157e3656d7d1e0e2	com.tj.tjcty11546	调教初体验
cf4b506bb5cb14a03ffb6aacafc939365f564fb8ec3c7496ee5633300f0641b9	com.tj.tjcty10437	调教初体验
d0a75e9233d8098f87182d53cd40787bc6f9b671c0f25c3bacdd361ced24741c	com.tj.tjcty02058	调教初体验
d2dd11684e7cd53a134215f173d1bf36c0f5fbdd5a41294cbc032ec8180313f1	com.tj.tjcty12649	调教初体验
d4967b3d79442d2735c878b5c830bd13a3d7453e70470d9729920161aaea7ec3	com.tj.tjcty12049	调教初体验
d6075e087952eb78170a7f618152258bc8eda7ab1466653b843c36f533179559	com.tj.tjcty12249	调教初体验
d63ff937097330fe83ef93b3d61a5d5d1645bcefb0276c419e41427d6cfa2e14	com.tj.tjcty09553	调教初体验
d700403b46031e3dd41c6d73c555a5640c20d6755c4c1ee81f508d8150899510	com.tj.tjcty01247	调教初体验
d970b899460830472e3ee01c3cfdc14fc8bfdffa9fffd47e5cd95d12987d340e	com.tj.tjcty01360	调教初体验
d9de2f8b99643a3d46125c7517dea093ed8eaea3107127c000b6b7acfd9f65b4	com.tj.tjcty01360	调教初体验
dd76df8c0db9426e94225f1711703835b05ce81010152e498b9fab0d88773671	com.tj.tjcty10537	调教初体验
de9265a6accc363475abda87582960a63588751bd8adda3b3a682124b9b45a8e	com.tj.tjcty00654	调教初体验
e4065c645c7227a6b839d894022d2991a42825e0bc1a4230aa5bc15e07a43897	com.tj.tjcty01213	调教初体验
ea9a66ca87ba3341709f253c9d8738223900287c0c48ca2eb17805bfbf145d06	com.tj.tjcty04658	调教初体验
ec33f8dd36b3ca302d4ef382f7105effa4ab5adad81416e440d2cd6045757494	com.tj.tjcty03450	调教初体验
ec4b52cbacb008260381c9680a055a6c836b384412d484fc22041c4ff9b07f37	com.tj.tjcty12449	调教初体验
f011c168a49762c1b610eadd2797d3b4d053f6b40e65d41beece321274529990	com.tj.tjcty12955	调教初体验
f139a68b1ae7c15b569bfe7757ef44b42a5dea2095d43aaa26a1ebcb548bce96	com.tj.tjcty04215	调教初体验
fc9d87be0236e35ba59ce8a26a55a03cc009aae1175966356f4da0e9a672b825	com.tj.tjcty14258	调教初体验
fed700ebbe9e754d22703fb35fb20fc9fc896d409f6f3f08871dd3101dde10bc	com.tj.tjcty07945	调教初体验

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