TrendLabs

FakeSpy Android Information-Stealing Malware Targets Japanese and Korean-Speaking Users

Appendix

TrendLabs Security Intelligence Blog

Ecular Xu

Mobile Threat Response Team

June 2018

Indicators of Compromise (IoCs)

Hashes detected as ANDROIDOS_FAKESPY.HRX (SHA-256):

Hash	Package Name
f24306d821019a0824a05b60b53c9ce5077b0914c26beb607608bc10d88bc43f	com.post20180123.deliv.off
e1288cb54727e673ffbd90ef4fcda2079d9f8a3d7b22b54b4e4726864462987c	com.post20180119.deliv.off
3192b5beba912e2cc46eb5468516276bb4f6dfaef8105e70a5ac8f2039484575	com.post2018.deliv.off
ab12a6b49ee1a3c5f0ebf39bfec7cf3c3145b6414aec088bc972c3acb33b9ee7	com.y2018.lott.online
54f74a43b81252160f4e9d5afc81b6aa14034e870ced1d333ce6fc58967bed2d	com.post20180123.deliv.off
5da20bc5a488138534dbf5bfe83f6210c769394f91a41059b977b270af899e82	com.post2018.delivery.off
7682e02105fe576b37d38d3732fdd021b88978a08b466cc82aab357a1fc69f50	com.post20180126.deliv.off
8a3daf55ca380ea041a6f9248117f75cce8e3314ce0b6a755751841ead204aaa	com.post20180123.deliv.off
15d9496dd4189ed0f708c3b5ce0e9b2850d3815b260a0d24028cf82b71d08350	com.postman.delivery.online
a7607e0bd258d8bf3a9f00ae300688761781929296b8999bea13cf457711e442	com.postman.delivery.online
e32977610a6ffbbaae1cca18e2998f063c0a9fc6aa03b6e0961511ef0ea2935d	com.ama.emea.off
848fe0a0449b43290144beb5b5f21dcf60aed00425db67a56c9756d42b4f3985	com.postman.delivery.online
9db13c90c7d0d68a5bc8b642a8d7162f643e8bea676f8d120be86ae443bb8ad8	com.postman.delivery.off
ce5f784af398ffa48343af75fe4e455e3416d96edf5aa7edbab3bbfd307ab016	com.postman.lott.online
87b2ced092f7d40bc67f97ab64d33072ee596fc88bd4998daec16edcef892149	com.postman.delivery.online
8c1b7ec4c97b9703a9a63431a75b2df559479c39f8d0fda69d0148c64e9881e3	com.capital.nhn.cap
93d6a9ee510fd282e43e251ddf04cf6b9ebf569509499d762e0cad84042aa359	com.capital.kbb.cap
0e8942a15cac3165c779f09e108c06671a78a047f12d4125b601ffce8e18fe44	com.capital.nhn.cap

Hash	Package Name
67e29543afad8a63ea9ed923b554d981e9029b39a8a153f7c5eeb139f89ce2ed	com.capital.nhn.cap
498db597de24ff15130d8b7fab11de8188a5044d7a8fe78cf5f5e0c570e681ab	com.postman.search.online
c5ffcc2da3c9a1e43321c4692ef1fe0f7fcee71fa9750684619606efaec9444e	com.capital.kbb.cap
2eeb3ff6ee6eae1de9455caf052a5f8c412ce34474b2b0cf827b0f55480ecb33	com.capital.nhn.cap
d1c97135f76357ea53f2a5f567361e6bf69040a0b429974993017a7281d11435	com.postman.lott.online
26190f5e46cba833c0fe513fca0b8eb6d9ac778a1f89c9b1a55e441421b82862	com.postman.search.online
7d68c60835e4db574413045803fca660656695059e01a5cbdae9a8435447f211	yy.xo
7dd33005256d88e96c727214781fb69fb74343bc2ba953f158477965a5f4ff2b	com.post20180403.deliv.off
03e9750d532ca62adb850d7473f755c44c0926cdd72c90b4d12de62e0b55b51c	ss.go
3a41f07537b31171e380ec7b7ec3e5a9d5a03bc82ce718ebb44c7504d348c57a	cxc.pello
46e5aa3a41419b2efa1a80149c21e4ed2171c942ed09b45ca768dc94e80f2165	ss.gao
202698a4b8ed690f4691cac36e5160b22a34f673a76427254a68dc528181452f	com.postman.delivery.online
4aa80aa852299e4e59e580da8fbd19b7e11cb1bde6214873b5c94fdb403d16b2	ss.go
9294078aeb314d5ef6e1d793e7e9d686f7bcde322ba75f6c0d3e03295ed5f85b	kl.po
4bcb771b6c6868dc2f29ac6e866fd106d2b5fe175f1879ac7973597c11b4c792	fuo.pello
94ff87c81a50d25e9acf7c46ec463f0aff88483eb4f63339cd833595d8b76cef	kl.po
99b1c2e8383b13366ad601743b36222bef18e2c16311bd500d327fb2321ede63	xx.xo
4c5af61c8f39a024c74eda6a4711d6fcecb9100d5fe65a40f044d7b9ce97ca9e	com.post20180326.deliv.off
a28210ba197c88e2d80de2efcaa4ab6668b8901ffaa121e947b1771d851b4b85	ss.go
a43430ee3b6990515ec1ecfc14e3a75ad8eb108b90eeb49a06f9f77b1e30f032	com.ama.emea.off
02e25d32a39917bd7c32aabe98bf5f9880fdc8aea4670e85169bf6dc6d6256f4	ss.gao

Hash	Package Name
aa93b9139a48ed7b3bc799cc8b936767cd2a66226b8f661ae1eb0550d5b58659	xx.go
26ee6ec62b94b3dfa37d7ba85eb5f8a5756e69dfee5919588e5e6ef9b89a8411	cc.lllo
63149d40f85bdad3d153a0b66ae4dffaa8c9d0bcf04fa93a4878f4d26fadafbe	cc.ello
c7f813fe0182fd0640bd3bac8ab25c38c9d0cf97d337bda750dc008d52773db0	yy.xo
1a0fcb4fc1ede7db7c1d640e97353df74bb7b49af3f431f29a8e5117fe3a13e1	cc.po
6ba1e52337a6a01c6b6ed0f2c8606fba8e525d2aafeb70ce8d8ec1c5dd1a0e33	duo.pello
d4127510117d7672669539b033519cb32395b4a82525630d30b8510dac77ddb8	com.post20180403.deliv.off
70d3cdabb350d8faea25d6972752eca06ef329b16676121ce44b295adc3ba388	com.post20180326.deliv.off
1e312fa3a04d06f559ba018babab26ee95f5a9b0bc5de12e0106501fb5d061c8	qq.pello
e755a29c3b3d96c937cbc909a76ec360cd172d16acc66da06a151216975e8f0b	com.post20180326.deliv.off
e8bd53e52cb89aaeb892138183bf786f787a6d7660de0ec176eb3dd8652047c6	com.post20180419.deliv.off
ed4308825a0ef3b5c5cc380daab1d8f632482897b70d2f7c2599eccbb2ae851b	me.chunyu.spike.wcl_permission_demo
ed7a482681469d46e54f23c70d2ed85b70be707e9b8efe70c4c1c22444d83cc3	cxc.ello
847a4c80af76b8134a950a23acdf0a5a7ec6f6bb1adc0179d2362d71f4710297	com.post2018.delivery.off
b83b536df5886be80159f47d08123e82044c91001b07b0c3569bfe1f622985bf	me.chunyu.spike.wcl_permission_demo
00a0d2e255e0c806947dba0c4a8ca947ed7c34d6afbb6af69386d55ddaf309c2	gg.pkkllo
ca112c63ec11491bea459353299f155fd580e18a1beae99d89f9e4c1ad1eec55	fu.cu
0b2eb2d885308355ee4fc5946891dace1c48b1aa96e76575a367d2b7a7e797fd	cc.llvv
2b9617759705f27ee4523748d7d50667489b65108972905350b3dcaf27c046a6	bie.si
f18093895495fb5ed1ab7d5613147ee61a9a27dcf85b6d34ee0de7e9adc34ddf	aa.pkkllo

Hashes detected as ANDROIDOS_LOADGFISH.HRX (SHA-256):

Hash	Package Name
b6431e28c65529f0cf0d388ff65da8801b5b5443de9b1539362d3aac8437678c	zifen.com.app
fc4cdc78adf49d9176b145633fbbe0cab1d2cee17d22f0f5fbb9f8f4d97f0d66	zhuxin.com.app
7d580f5fb49fd97d08f9b4adf2704bee8d87beef772a8717b58f1b15f1c2d712	yamaxunss.com.app
c70bc2bca9a497fe9be7621a6a9cfd95671f67bbd5db99f0225982f87fafb47a	xinsheng.com.app
5777c1f925c738ccc2b7be47fce968f20120f3eaf2c65fbbfba74229abf28c5f	tongzhangs.com.app
7cdec76a6c5c36d12e9e9bdc912611b5a1a4d4d839b96d1dfa3e198cda661d2e	soni.com.app
b318326bd5c77016aca9d65318eac8f1c14ebe48db8467103546d1d7dd895d43	softbank.com.app
20acc4b2af3b7b549c494c2fc26d8791276933f9612dc7d9a8e884d851cebd5e	sanling.com.app
2764be8805bacf86e3a60bf5094c35a62960f913d172b2586978df7b3081dcee	sanjings.com.app
c9be63cfb3a1915ae06243ee08307fb40c8ffbdf72772cef9344d315966bd9ca	nihong.com.app
8fe32b829a984e2a714ce78602746a07b46d64945d5d379b5407f898dcbc47b0	mizihu.com.app
b001fff3993240040398b12884df11b1372cd05c74e1ae9c2045ed02724de202	lt.com.app
3b99251906d9d10bd2237f5e02cd57c6efbf349c15e8f52e3d58f8f86f203b7a	lisuona.com.app
8d7d4cbcd41b610fc9a0f39afab3435b188227183ad3df21499854be0bb90836	letianss.com.app
01b4118f090664fffa192063297ed37c4076899681c2215db3acf55698c4dcbd	bits.com.app
168aaa4b53f45daeae34838d5721a268a855cb66cb6c1483d20c7124ebb08a36	au.com.app

Related Phishing URLs:

- au[-]security[.]com
- au[-]securitys[.]com
- au[[-]]service[.]com
- docomo[-]security[.]com
- exp[-]sagawa[.]com
- ico[-]bitflyer[.]com
- ico[-]bithumb[.]com
- ico[-]coin[-]z[.]com
- ico[-]quoinex[.]com
- id[-]my[-]softbank[.]com
- id[-]softbank[.]com
- myapple[-]securitys[.]com
- myid[-]softbank[.]com
- my[-]nttdocomo[.]com
- my[-]soft[-]bank[.]com
- my[-]softbank.site
- my[-]softbank.top
- my[-]softbank[-]security[.]com
- mysoftbank[-]securitys[.]com
- my[-]softbank[-]securitys[.]com
- my[-]softbank[-]support[.]com
- mysoftbank[-]supports[.]com
- nttdocomo[-]security[.]com
- nttdocomo[-]securitys[.]com
- nttdocomo[-]support[.]com
- nttdocomo[-]supports[.]com

- rakuten[-]card.gnway.cc
- rakuten[-]card[-]security[.]com
- rakutencard[-]securitys[.]com
- rakutencard[-]support[.]com
- sagawa.oicp[.]io
- sagawa.top
- sagawa.vicp[.io
- sagawa.vip
- sagawa.xicp[.]io
- sagawexp.gnway[.]cc
- sagawae[-]xp.gnway[.]cc
- sagawa[-]co[-]jp[.]com
- sagawajp[.]com
- sagawajp.gnway[.]cc
- sagawa[-]exp.gnway[.]cc
- sagawaexp.gnway[.]cc
- nttocn.gnway[.]cc
- secuitys[-]rakuten[.]com
- security[-]s0ftbank[.]com
- securltys[-]mysoftbank[.]com
- securltys[-][-]mysoftbank[.]com
- softban[-]k[.]com
- softbankjp[.]com
- softbank[-]securitys[.]com
- softbanksupport[.]com
- softbank[-]supports[.]com
- softtbank[.]com
- support[-]docomo[.]com

- support[-]mysoftbank[.]com
- supports[-]softbank[.]com
- softbankjp[.]com
- rakuten[.]gnway[.]cc

Related command-and-control (C&C) domains/IP addresses:

- 10[.]123[.]12[.]143
- 103[.]26[.]76[.]73
- 111[.]250[.]157[.]50
- 118[.]160[.]114[.]244
- 118[.]160[.]115[.]202
- 118[.]160[.]118[.]88
- 118[.]168[.]60[.]40
- 118[.]169[.]187[.]192
- 118[.]169[.]187[.]22
- 118[.]169[.]187[.]223
- 142[.]252[.]249[.]46
- 142[.]252[.]249[.]58
- 142[.]252[.]251[.]38
- 36[.]225[.]14[.]226
- 36[.]225[.]187[.]95
- 36[.]225[.]189[.]69
- 36[.]227[.]130[.]2
- 61[.]230[.]103[.]80
- 67[.]229[.]35[.]227

- 118[.]168[.]59[.]199
- 118[.]169[.]184[.]117
- japanpost[.]oicp[.]io
- houtaijp[.]gnway[.]cc
- jppost[.]picp[.]io
- mydocomo[.]gnway[.]cc
- sagawaadmin[.]vicp[.]hk
- sagawajp[.]gnway[.]cc
- sagawar[.]gnway[.]cc
- sagawaweb[.]gnway[.]cc
- sagawa[-]web[.]gnway[.]cc
- tijiao[.]gnway[.]cc
- tijiao3[.]gnway[.]cc
- tjserver3[.]gnway[.]cc

Related Twitter accounts:

- https://twitter.com/luckseven4
- https://twitter.com/tuwoeiwa1
- https://twitter.com/siumakuaw
- https://twitter.com/sekadeta
- https://twitter.com/SevenSeven5257

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