

Toast Overlay Weaponized to Install Several Android Malware in a Single Attack Chain

Appendix

TrendLabs Security Intelligence Blog

Lorin Wu

Mobile Threat Response Team


November 2017

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.



Indicators of Compromise (IoCs)

Hashes detected as ANDROIDOS_TOASTAMIGO (SHA256):

Hash	Version	Label	Package Name
17DB44BC45B66B682320ABB8D5805690765B138A23519E89FDF9AD91BF5383FF	2.1.1	Smart AppLocker	com.agomi.applocker
0BB8C3FAD176971014F69E5BB06CB0E89722C448AD13FA9378D2FAF2377E89C0	2.1.1		
2366A679BFB69522F37CFE92507E1B028E10B84D4E784568B14211941B5236D5	2.0.9		
2EA1D37AA016212FB33F560721BB00772FD4CB35D01F6D7F8E7E0B6F95E1776E	2.0.9		
30C90D4EC57D80C88C1A17BB50D2B76DC2EB66FD19A0C7045A07ED682B338501	2.0.9		
35EF219DE0D4C4F0553EBA8B16DBAE90845A859488295A5BA457C81A12DD9C6B	2.0.9		
5236D23C1C97FBF88F6AEA34A2EACEAED085224D65D2322E94A8F5BC0A8002E9	2.0.9		
79B0F540DE2B82075F42725E8BA8CCFC2748FF6F7826BFF7920CE18904D14983	2.0.9		
7F7AF7A6F320108CA45D7FD16D8B6C11091A79A87F4C7BDF5C2784E102DE4CD1	2.0.9		
F226B6A933E91B6ABD89C3772223BDFF6F1D951C94064F113017782C3B1D5A18	2.1.0		
FDE63FF80C766ADEB9BFDA0CDCBF2E4067F19A58E50A497545DC3EE638699A52	2.0.9	Smart AppLocker	com.goami.applocker
4BD19667A12F8BB9DD0054473133FEF3E2B7BF40964DB8132EC5DD0CFB8A507B	4.1.0		
97272FFFE08226996D1CCFFC7BC6D6E77125117DC5244504790DE5C161BBA4EE	4.0.0		
8C58BBCD2D6C2297B80B6D25928AC6B58F7794DD9317F283C0450CB382327BBF	3.4.0		
A3FEB25D50EDEF5D5D006C07EA9F243479F8329356D25E186AE77BFB7E6AF7C	3.3.0		
6C9C1F5C075D26EE2F01A74A8DABBEDB3A11F87A820678E6F401F6504632C151	3.2.0		
54A8E0F8F7805EC33C551E2E5069DBBC2C4A9EA6A45C31CDADBF8451F277278C	3.1.0		
4F2AE1C00A9E876AF49F5B943AEB9EF58EB5E60F958BD8EA952E4BE64ACA72F8	3.0.0		
086E3092BC0D28BCA0759BF9FFE172FC4C669BED7E12A486CDD9729D67FE9339	2.9.0		
50CF7B37C43E6D9688BD50D0A8983D3BD0A9397A4898AEA2510FD91B07CDF54F	2.8.0		
DC4A9801A3FACC403CEAD1DA658354294F18AFBEADADF1B4783B6BCA674EBF6F	2.7.0		

Hash	Version	Label	Package Name
B0E92A3B4DBE477CD3F44E3D0164814D27823704C3234662751C6A0C36204D2E	2.6.0	Smart AppLocker	com.goami.aplocker
F1F6EC5765972DF3D02501AF12065D2D964D8EDCEC63A753249A994D7915E006	2.4.0		
64BFB825B0AC0C7F2EB618608DCD397F62DADB11152B022F986F4B371EC359D9	2.3.0		
6545CF7B6CBCB85E1CF1CB059A0C3CF5D3A2D9D44E80786667806885C228C1AC	2.2.0		
D95F3BFE05DCFF35ED34CA5197C14088F3D2CE921627793A8BD6005576A6E027	2.0.7		
8A6A1F3DA935DAB238407C32C294D386E01CCBBB1C60F436AA02DCD3F823B778	2.0.6		
0E5CF2F194F353FFD46611D0DC989C59C9893A7E3FCDFDBAE292D3A608FCB161	2.0.4		
FBF30FE8B03383A96BC5E7DAF82E3710CB41D1130FF815772AE4AF21EF88B87D	2.0.3		
D470DFF0ACEFD2A03E920B63F4062DFFE6656C2D962FE5F86B124ED0A6236862	2.0.1		
89ACFB97AF394358D2EE2B329800EF8F792C42A4C219779B8E8B328C8EA22BA	2.0.0		
1F8264BAB9704FE45486DFB003391E6DA20A3ED140702BBE1FD4B291AACA9028	1.9.0		
FECE4B2C214D5EC6951AAE71070E256F6628813AF066C455E84FCC1ACF7CBF8D	1.6.0		
26B1196A154B04B62C56673CA754A3A7B5489E184361CDEFEEB794818456E7DD	1.5.0		
8AF5633912298B3FF8C6D18F0C1FCD24DCC3B7ACAC232D883AD473F29361DDF1	1.4.0		
1ECDAA38B5BB203CC7684B4BB74F46A4433B778C58D0E7D581E10164F9B71298	1.3.0		
0EF60A072FA3B6E0876D042C31C25B2A49B1BC13D488E1820C7386CDD09E5F7D	1.2.0		
1DBAF263C27D923D9AC96FC451023AAAFE616DD4AEA1922EEEF23B9E177F563D	1.1.0		
12B8B4152695BC9A768172F504AFC852169154D4F475A01F8D1C6F23678E275C	1.0.8		
313DCF5A890E1A56584D7FD822818A86F8CEBE18F1CC550EC0E53376404442AC	2.0.0	MBoost	com.migo.booster
6807BF029B5A944B1E162BF0F8A0EC9B5AB8D6E0E99F1D78D4FCDB14E77254EA	2.1.0		
313DCF5A890E1A56584D7FD822818A86F8CEBE18F1CC550EC0E53376404442AC	2.0.0		
AE108D6B58D375F0B2EC9BEC4B2D16FCA79E063F230E39E4BCE35A0A743FBDAD	1.1.7		
E92E44AD4286202E2A46F0889A9D5A67663ADA117C31F59027F5148A5087F409	1.1.6		
36425123368FCE973B2969AF9760E3ED1128617FA8A5AA13BB80384FADE6330B	1.1.2		

Hash	Version	Label	Package Name
915F5C3A4649C8D15A0E3675EE79F5B57118FB21C0C8F6C156BDD77201EAB975	1.1.1	MBoost	com.migo.booster
4D742E6B4C0FD70F379BD0ADD4302FFEAED2364C44847BC615EE1207A4B43C8A	1.0.8		
60C27413BAC120F76BE3E2D05F34F42B7D3AAA72E0ED6F7A0A67E190F8FBAD7F	1.0.7		
F7345D5D04DCDB752935D7CC48E40FE39AD72AB31CBC44ADEB722D3E7E43F2BF	2.0.9	Smart AppLocker	com.googog.app
573F679388082F94039F6F0DC35F44F8017A063EFBA2D265856939462D87C8CC	2.0.9		
959DC7AF74C85281E6FD82B3CEEE8C1E804E5845F2AB77AD303E0FB4C1B81406	2.0.9		
9D5183563A924E24D587908B64AD1BFB5B864ABDD898D1CEAEE6F32600432ABC	2.0.9		
F876B2DE3332C52E80BF7569314F8E722B34199F59D8CA4A521A5F6064CE48CF	2.0.9		
AEE9916F6582A8CB4B5E210803A77DFD8812F916B50D53C6DE60EE56F8BCD61A	1.0.5	Smart AppLocker	com.gomigp.applocker
B0FF178FA7CEB8FE11F4256818521132C57279F05E41F58D04C19CCA6E559DCB	1.0.3		
D1221C96C308B3621A7DF28348C67A9758DA6912C69D52883A62BB6C48B631D8	1.0.2		
EDC59BEDF2EE2851E7F735BD3A99CD7C08049AC0BE08FA520589D366B7F594B4	1.0.6		
D9A5F96EDA98B734832CA4BCB949CA6CCB49AC88FE4882B089A3A3BDAEB9A921	1.2.8	Migo AppLocker	com.luna.applocker.gp
64D849E916251F0B1131E75ADB6D1A110C64321409F32151AAD5D9354B11CBAF	1.2.6		
05B704341BEFEF5C358C7AC99BDA808FE2DF3E7DF67F3D2A11CAA40040CAF2DD	1.2.5		
7936858458D04E4BA15C29F84B734AC7F161DF664775D91287DD9D4B392712C6	1.2.4		
6B5BAB6F034F49532A8A304530FCBD6F8C0E2A43210F1C2F7F1BACD3F90EAC2F	1.2.3		
3DB0DF7B148D6637769ACF06510C247BF12FFC05F0D8F9AB6E2DEEE8BEC2D2E3	1.2.2		
FBCB16654043928947D5D0C714C6C8FADA5844936D50817D0B06E3FC19C9CDB2	1.2.1		
5C82F014CDB552234BF19C9879962C987EA10538668DFA94BA3F4851EE4B0D98	1.2.0		
91254C551434590F3AB0707FEF0BCB900673D344FA5B910846879AC2F2C49E92	1.1.9		
F5B0B1BD5A0D1631D4A009C9986EAAC269737DF3B2447D493E916A90B5B1A634	1.1.8		
1D277DDD7B9B892892412C716D1848C8ADDF00459473C9238F399CF9DD6F7D09	1.1.7		
EEF5771D723D6FBE89E2F6F0A2DFF10240380801281FB696D86482BDCBA67E06	1.1.6		

Hash	Version	Label	Package Name
EC5C0F12884158B179A5592002C8E9C10F17035A FB27C1F66E53FCA8B983E2C0	1.1.5	Migo AppLocker	com.luna.applocker.gp
37F6F5F1664259D4D659F4543964B01A443758571 78CB1EBB30CFB4B3D737CA8	1.1.4		
7C17687F4EDCC997549B2A5AA32750C51D758666 6E4A9E0313EEC76948D9CFE3	1.1.2		
7E0080575A63400EF054CF1AFD14B367E4440F7DF 5BC3E3FF7CD3B4A4242B8F6	1.1.1		
50D9B0EE8E53DD4CDB91D71B23EDA3D8CB78054 0103F6D9C6C78AD7FA6477BFD	1.1.0		
D38FFFE5328B272DCEA91BFCEDC594C45D8138C 37438FC46AB253AD3475DE3DA	1.0.0		
A15695ED3CA3B08DC7164D5C95C3AE5CEC96FB C0F7D75F97212ACFB029D9AE16	1.0.0	Migo Locker	com.migo.screenlocker

Hashes detected as ANDROIDOS_AMIGOCLICKER (SHA256):

Hash	Package Name
489bbffd63637e2ecf3e42971511879034d9e517eb1d9401a1444374154ced06	com.vpn.free.migovpn
1663068ca94b375d0c40c54caf13e921fdc7a1c1a09880ecc8b4ba18f9f3da0a	net.ym.game.ww2.raiden



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.

©2017 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.

Created by:

TrendLabs

Global Technical Support & R&D Center of TREND MICRO