侵入の痕跡（Indicators of Compromise, IoC）

MITRE ATT&CK 技術

作戦	技術	ID	概要
Initial Access	認証されたアプリストアを介した不正アプリの拡散	T1475	ストアにマルウェアをアップロードする
Persistence	デバイスブートでアプリを自動的に起動	T1402	ブロードキャスト「BOOT_COMPLETED」をリッスンする
Impact	不正な広告収入を生成	T1472	閉じれない広告を表示して収益化する
Command and Control	標準アプリケーション層のプロトコル	T1437	遠隔からの C&C サーバとの通信を行う

侵入の痕跡（Indicators of Compromise, IoC）

SHA256 値	トレンドマイクロでの検出名
02059EFB3C8D51616910D53FEA9F8F230DA43DD8B50D4FD525DB2851271046E9	AndroidOS_HiddenAd.HRXPA
02A2D219B2A93B8595608B57587294B5709E5AABD16B3275625CC8F5BDEDCD6B	AndroidOS_HiddenAd.HRXJA
0A3513A2F0C0E6859DC330A971551519573F2C91E006CABEC32D5A4E0FB50250	AndroidOS_HiddenAd.HRXPA
0E1D3129470DCCE2DBE9053081B694E9D69F88266DCA5D317C4A8A2C6C31F228	AndroidOS_HiddenAd.HRXPA
0F2894F14EFDA5043D62B1B99A5DD748D412584D44852983B8A3CD0B078E144F	AndroidOS_HiddenAd.HRXPA
11899FB5CB6606BE16605FA5799EC4D4EE522F1BF6638A6B9817B4ADADD5C4C0	AndroidOS_HiddenAd.HRXPA
18C9A13B368A19C67F4DF739AB778E53D488835499D39F882993AADBAB7E44A8	AndroidOS_HiddenAd.HRXPA
1953B665CF16800345D995B2454A19CD6A253D792804ABC568D2391CF5165028	AndroidOS_HiddenAd.HRXJA
1A28A8C523F366B8BD73A876DF7986A70A5CF3A6973B452B114E6C5C7F876D8D	AndroidOS_HiddenAd.HRXPA
202BCB5DEECD1C9E1C007C083EC91632ACB766603CECA6363750C387CC2978EA	AndroidOS_HiddenAd.HRXPA
244EB9CD0B918F3047FD3FD75E6E52E0F5B78178686C340543E031928BC7664C	AndroidOS_HiddenAd.HRXPA

2680B08604D25E7856BB32E57D38D9D3A2C1B680A4703666A6D869F492D40FC0	AndroidOS_HiddenAd.HRXJA
2D2CC7D3C3D5933299D4C9F927301DBBE60B056871555B15AFDB7EDD05926518	AndroidOS_HiddenAd.HRXPA
316E0D285FAF96BAC43A9751E96CD57A7C317ED7D1F0A0195344D7B4AFEC4E4E	AndroidOS_HiddenAd.HRXJA
31AE394A5242BDEFFD72D6649239DA5B0AD4C8E3B34D3B3BE274625CE7C2B591	AndroidOS_HiddenAd.HRXJA
32A3C43A0DEABDE33E63955370718DB6D9551CAAC5F41DB0C1C30569ED7881C3	AndroidOS_HiddenAd.HRXPA
36A215EB76A29EBA35986127AABE33951CB8F370BFEA6013F6962DFD481301BF	AndroidOS_HiddenAd.HRXPA
3C3826477C238691ECD54D50C454C6D8EF14B473D9633D016C71E2599E28F31A	AndroidOS_HiddenAd.HRXJA
3FB4B5E79F00A40C68E0EC5795A1BFB4A782F8C3EBD83FC6AF11325ACCC9F353	AndroidOS_HiddenAd.HRXJA
4381151303C5EB1B0BB377DE9A4901B0BC9FDBEE55EA847F604BEB826903AA3E	AndroidOS_HiddenAd.HRXPA
4CD83B9F966864B7E1619F8FEAD692484BB21E57C49A6C4608E1CD13F3566C18	AndroidOS_HiddenAd.HRXPA
4D2ED05FAC041D7B410292135AEA90E60C7CF36BB0B73E4656F7697C9F31A494	AndroidOS_HiddenAd.HRXPA
51A09A0C2C199E29DEEDF262AB056516661278925 4E0130DB4DABBDD7B47AA31	AndroidOS_HiddenAd.HRXPA
5244B30EE5F44C58BDD20F8F451FC92AB88C6F117EE339187BF31AB628F912BF	AndroidOS_HiddenAd.HRXPA

553083F192D79C85F5EA89043CB455F2C8C54890553312558B9C5D7074DAADD0	AndroidOS_HiddenAd.HRXJA
57216BC3149AEDB8E294F17D18C5DB512AC460C6ADF49532834B9B4C18E077FA	AndroidOS_HiddenAd.HRXJA
580850CDCDE99153BD01E1686C510F1D33B54380692EE8FBAE854D1599F454E1	AndroidOS_HiddenAd.HRXJA
5BD9B22E47250117CDD6D8B658984A7AE942C4A166D211897A1BF8B8FC2935EF	AndroidOS_HiddenAd.HRXPA
5DB3575C1918E402430B9582232767CE88D8706F2C4EDC6FA4BCD48902CA7840	AndroidOS_HiddenAd.HRXJA
5E60A603F52375C04CB9FF4EEFDCADD85815E6C9447977995B5E5181BE0DA280	AndroidOS_HiddenAd.HRXPA
5EB22D022E3EE0381A3C9913FB33F56E1B2BA15FB96E21F7353636BC15461834	AndroidOS_HiddenAd.HRXJA
5FCB5B1C788A11866D5086EF0F93D1EB76E70A961C45AA59EF757997C2C527B4	AndroidOS_HiddenAd.HRXPA
60A978A5E8D66EB76DD5A05D5B3D0D88EDFD2D404059D34E8C2115486BDD8666	AndroidOS_HiddenAd.HRXPA
6478C8EA7B3D00709E989D8841B1F2F921F37E6A43AB50F522FE85B7F9FE1F89	AndroidOS_HiddenAd.HRXPA
64BF6FC69382849DEDB96F3B0A498623848ABD5B363F35EC2B6BBC6949956D08	AndroidOS_HiddenAd.HRXJA
6506526B69F74E3A0093A0F3BA1621532C19714AFD6244D25BE0D244D82755BC	AndroidOS_HiddenAd.HRXJA
651D8ACB52450ADBBF07520C91B8A698389F9D27AF891F6795605785FDF183E6	AndroidOS_HiddenAd.HRXJA

667A4B13765C8ECAED1275208EBA295332BFAC7FDD7E29DC8E85B78CCD54A161	AndroidOS_HiddenAd.HRXJA
6AF4225386A0CCE966182F209B345CFF7CA512F7377EC6C2A95ECA2BAA6DEFDD	AndroidOS_HiddenAd.HRXPA
6B01855CBE9CEBC6400EB37200CABA339A16957153F79F5EA77999A511153C18	AndroidOS_HiddenAd.HRXPA
6F14F976E2A09102FF7628D7EC87F2CFDB00A3D3E16DF0CCA82C1C074EF9E8B5	AndroidOS_HiddenAd.HRXPA
72A621364BC20FC1E113E6E723224C727E48819AEEB571C70611EF1B302D9FF2	AndroidOS_HiddenAd.HRXPA
777D840BD6BF19F619F17C69C6F098BAB6643E4701D8F877E366A0CD4DEFC2FD	AndroidOS_HiddenAd.HRXPA
793DEAD0F935AE1DE65C8705A2FE643CE0E1A4B1FFBE5A85DE8279D0BB5DA99F	AndroidOS_HiddenAd.HRXPA
7B3E228620B9EB7E8BB71FE69D5BC1CDD1F79C4E24D00E03AB6D4A4429ABD5B8	AndroidOS_HiddenAd.HRXPA
7FCDC9B5D7E53CAECBBF2EBF4C9EF0F5B965D7877AC3A500352EA21C432B5F6F	AndroidOS_HiddenAd.HRXPA
82245E256A02F6FF443AB29A3AB141647B94D61BEC4961F061C666D57D26B493	AndroidOS_HiddenAd.HRXPA
825451A94340FF6D94BDF95E5418CB110C465C7B79F06335C7DB6723ACCF5395	AndroidOS_HiddenAd.HRXJA
8A52129928B108CB65C8A1E8288F7B79ED2EC18DAE4C5ABDD9A802D794BFE2BC	AndroidOS_HiddenAd.HRXJA
8BF3019D3C9650F443446759D616A9C5AA7B7DF72F3C96497725E9F61F3FA9DB	AndroidOS_HiddenAd.HRXPA

8CFDC4EECEC1F0893182B63C1A60972E607BA7F5F81B1A1D7E9536AC1A6D6634	AndroidOS_HiddenAd.HRXPA
9A58369AFDC86FCCDEFA99992BBA5EE4E880C966669398A2353CA6F0D7E61F07	AndroidOS_HiddenAd.HRXPA
A170393DEBCB07CA9186FBEDDE7431E4D2AD836F2C1B6BDB1FFE9E6D476CBF23	AndroidOS_HiddenAd.HRXPA
A4D26FBA133EA892D82FE3E161D56C8CA4D184D5DE77349407F471AA5E9EAE87	AndroidOS_HiddenAd.HRXJA
A54C4C092EECF4EB911223D6C118EFE109368F24058651F6C5BF40C50CCC13E3	AndroidOS_HiddenAd.HRXPA
AAE0246899C32A882C3DC49D757091A1A8D9DF5EC32F7E9C275EED4A6478F870	AndroidOS_HiddenAd.HRXPA
AB040AFBB6EFC729F1912FAD554C03838129DEB8A5E2BAC8D42A78EE83F7A10E	AndroidOS_HiddenAd.HRXPA
AB319EF507761E43014224BA1FDF456DE94748B537BD3A6462D3B10D39283BF2	AndroidOS_HiddenAd.HRXPA
ACD61A3AFDF9612B0CEC5CF28CCE900403EDCABE1ED321AC262C614DD61C9D9E	AndroidOS_HiddenAd.HRXPA
B04F26167133A9433B4D9085BCD3C3283E55666E9B64C8DBA71EF6ED29D636BD	AndroidOS_HiddenAd.HRXPA
B281EC890820B85157777E0BD636DAC779707CC780459FA63578171CE4FAB337	AndroidOS_HiddenAd.HRXPA
B2B58254A842181FFFA734268FAB6E497256CB63303AF40AD3DF2AC674F95607	AndroidOS_HiddenAd.HRXJA
B67B90EF82915807666363 8B45ADABFCFB663A2C58505FBBF8F839F6BD62D8E2	AndroidOS_HiddenAd.HRXPA

B8FC492479C97261E04DD1F13B6C308BD848623E680609A562EFE17D92E9B384	AndroidOS_HiddenAd.HRXPA
BB0832E560137EA9B776511E2E959DE7B065E8136AFABCB39E4DFECADB6CD145	AndroidOS_HiddenAd.HRXPA
BBD407239BABC5C09966B726AAFC79DAEBD6B8AFA3C0A0C93E3DEC750A9AB7DE	AndroidOS_HiddenAd.HRXJA
BD6FF179F5845F966DDD79DFA05CC2E4F77F19EBBD7776A7EF0F854DB084E3C4	AndroidOS_HiddenAd.HRXPA
BF30E8802D34DDB6BB1872781528503F764D924EFA94DBBA2CF1BB9207E59D9B	AndroidOS_HiddenAd.HRXPA
C27A739540804D0F246EBC2592A634568A0163CF270F4915D00E5CB07F0FE2FE	AndroidOS_HiddenAd.HRXPA
C290762DECF6C2A54F2200F188EF6AD291FE3B75B3B44A6D17F3A89CE29B8F60	AndroidOS_HiddenAd.HRXJA
C2F31CCCB602DE71E423D45885D5B0F1BE3B086C8AD177AD622B9C2BE2628196	AndroidOS_HiddenAd.HRXPA
C6EFE5B30BB7F16443DE8B09D689BB91732B572F66E141460B137D50BA169209	AndroidOS_HiddenAd.HRXPA
CA79B3725B30F04DFCE0178D29F64EC9C28EABEC53EFC6B511CD540EDE3D62F1	AndroidOS_HiddenAd.HRXPA
CC5E0B72F6D01A1A017515ACD480FBE20F4C3470FBD7BA40E802DB9E4FEDE0BB	AndroidOS_HiddenAd.HRXPA
CE82F86E10F3C24FFBD3804606AE2B865B4A3E0DC795DFACA7790EDD0D7B6F5B	AndroidOS_HiddenAd.HRXJA
D2BB430FE7D289CBEFCFAA8DA5DF448E167A06D0D53E2D2CAA5EC2EC5C935162	AndroidOS_HiddenAd.HRXPA

D5FB2CB562C60D99656F9567A6E85AFE3F2A20134CA114F3B42B00BDA15C37BC	AndroidOS_HiddenAd.HRXPA
D645909AA79FADE0163211DA981C39605F8D69C67524DE8F6D63C42E28B7AB4A	AndroidOS_HiddenAd.HRXPA
DA121887DCF05DE5F758E615961ECAB4683D4D9CF81F48173FD35E59B57628AB	AndroidOS_HiddenAd.HRXPA
E50F4BB22206226B2207E9FD9EECEC4A7D1B171B5F9B5F728F98F3EE9DDD945E	AndroidOS_HiddenAd.HRXPA
E6EB8847AD6F37B3455575772B6AB3565CD25DC9E0EEB826388D946FFB02980B	AndroidOS_HiddenAd.HRXPA
E7CAE25D134BA53708C316F99D9BAF07285CD6EA5F0ADFAA9A4B14F5416B53D9	AndroidOS_HiddenAd.HRXPA
F01E2C08A77F121BE5862C2B993CD5C2E85D28BF50E93A363209B833D8CAD83A	AndroidOS_HiddenAd.HRXPA
F08060339C9EFA9257C33D3D66F84E21B5F0406B4ECAE7C70810AFA72239F26A	AndroidOS_HiddenAd.HRXJA
F2DF95EA0BAC154081924B4E1524D5DF6E12DC79BE0EF579C1A18D216ED3BD6D	AndroidOS_HiddenAd.HRXPA
F32482AD51BC7691E6F0541ACEC0F34036643028195B2E2264081114392AF12C	AndroidOS_HiddenAd.HRXPA
F51F79F723533A32E058DEE3FE058DF497952CC31BF9F1BE62F3E65F4715122C	AndroidOS_HiddenAd.HRXPA
F524337FACA11B21C442EEA51F5852E023CA84E9035481EEF14AEFDBB4131FE1	AndroidOS_HiddenAd.HRXPA
F5B3817290E1FDD911C781047670A8D31489F4BFCEB42D73B94EF98AB6B8B3F4	AndroidOS_HiddenAd.HRXJA

F61BD6BA40EF9D07F8139066F4F0AE6E40159BA4F11FFEAD1722D6F9539C663F	AndroidOS_HiddenAd.HRXPA
F6732F99770F38A6FF2F33844CB71ADA1EE22445AEDBDDA7EA76C62C8F448513	AndroidOS_HiddenAd.HRXJA
F6E679FB77B9020F6A9E6FE929BAFC13B5057F93F683043538E5131E20EF31BD	AndroidOS_HiddenAd.HRXPA
F93259CDF2083E4CC0935BC88486B38E2021AB06594876CC2FB08DAC333460C9	AndroidOS_HiddenAd.HRXPA
FC1BC44048F818D90C3151C5114FC803B23159C6C60DC00BCC08CFFB03B3F395	AndroidOS_HiddenAd.HRXPA
FC4AE3CF359D8992F0125249E39B651BFE7AFCEF45888859CE865CCE8A5168EF	AndroidOS_HiddenAd.HRXPA

TREND MICRO ™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information. Our innovative solutions provide our customers with layered security for data centers, cloud workloads, networks, and endpoints.

At the heart of our leadership, Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights with the public, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on targeted attacks, artificial intelligence, Internet of Things (IoT), cybercriminals, and more. We continually work to anticipate the next wave of threats and deliver thought-provoking research that can shape strategic industry direction.

www.trendmicro.com

©2019 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.