TrendLabs

GhostTeam Adware can Steal Facebook Credentials

Appendix

TrendLabs Security Intelligence Blog

Kevin Sun

Mobile Threat Response Team

January 2018

Indicators of Compromise (IoCs):

Hashes detected as ANDROIDOS_GHOSTTEAM (SHA256):

Hash	Package Name	App Label
358F9C6C04B27ED54F21833F3DB8D5C56D530C2FA751DC4D04DE5FB7DEC20B8A	vn.media.facebooksaver	Videos Downloader from Facebook
F6FEABAC83250AF4FE4EEAEA508BF35DA329C97D5F0C1A4B87C483F80EA40D50	com.dtcom.instasaver	Videos Downloader for Instagram
A0C3C5F5B4853F133F0494C100CEFE23DD0CD2FE336B41C7701DDA53751E3571	com.vn.playerdownload	Download Videos From Facebook
490C59836DE17622CF9C804B57E80E2241EC4A0183E0A325ABB658F3FE3A684A	com.ddt.mediadownloader	Download Video From Facebook
5942BB3BC9511D8D084B3174106EB71B5982F5E3577192E1906B914063E92412	com.downloader.ddt.videosaver	Download video from Facebook
670D1D4476F1623DE9865C50D1F8E9414F1894DC26235C7AB18F05214B7D6E28	com.ddtapp.downloadvideo	Download video for Insta
786657C19C57B61AC2D4CF3F106B64EAD3C282BE34FA6CCA8384DD5411FAC0C5	com.ddtapp.downloadvideo	Download video for Insta
17D788D6A77E4BB2A59562EBAC24568337B095CA9E63E6A1559AC3ADFEC26FE3	com.cosy.app.tool.compass	CompassPro
307AB2E817CECBCB308595061D90EC496A6523DFF15BF85A07C27FDE11500EAE	com.tool.app.CompassDigital	Compass Easy
26F5F1368081D614BAA3C9115BF84E2FF036CB5C0400FA3F77D19CDEE74A8E47	com.duongdl.facebookvideo	Video Saver From Facebook
4E8548F34F5E19C6E96B42C8008F11C7AC909DC388147325FFBC43F7420ACA00	com.bitfree.facedownload	Video Download For Facebook
4CA7E3284020BA1020A90C6F63AD9756BAD6C8AB29BDCEE128E23D9B0C8FD163	com.videosaver.tienit.facedownloader	Video Dowloader from Facebook
D3F0B5F7D62F26128BEE4B13F56F82A172A4FBF3ED632149681A8BA06C1CCBD5	com.ddtapp.tubevideospopular	Tube Videos
50CAD37A8FC9E317FD521F32A2ADAA0B2B5013832864DEEDD10B078A7F661CF4	com.softedu.sieumaytinh	Sieu may tinh
826B54C697A6D9F76433C6DA1539CA28346C5D0444738A5B132BAE43AC5F5498	com.appmaster.ramboosterpro	RAM Booster Pro 2017
069FB0344A1E73326C0162E8704A4C07695A9597073FBA81F7B1D9064EEF6389	com.dlapp.ramboosterprovn	RAM Booster Pro
7069FE4B9DA3810CC0E1F6C3C193C92128D462BBDF6E5775138AB8E5310AB255	com.appx.tool.scanner.qrcode.qrbarcode	QR-Code
A5F527D03E478EC60B8146D50CE76F535A43D71911D7BE2D881D9AC8EB6C900A	com.dungdl.app.free.qrcode	QR-Code
9EEE1DE1AD3891E370EF942C6695E6CC4C869EA46668DA349CE4DEB74F16E81F	com.cosy.app.tool.scanner.qrbarcode	QR Barcode Scanner
CC9FC4F212BAA98E503ECC473433CC8644C1710DE9ECEB5255B0AF3B37BF1967	com.tool.app.scanner.QrBarcode	QR Barcode Scanner
02E74E72FD3FA73A804ECA491127D8E372147C30EF4373DF77B9F1C075CC0C72	com.bitfree.app.qrbarcode	QR Bar Code

Hash	Package Name	App Label
17B177BF20AF8F61A62008663B1A110A071B44539B021A538BE884273B5EA926	com.ddt.photocollage.collage	Photo Collage - Youcam Makeup
68FB726F2468A8DE03C92330DE97072477C70D4CACBA4E53ED717D194D6D6626	com.ghostteam.blockhexa	Match Block
7D04F9C0698D6B15A68FB88F8517672A7EE8FD4A03B466287A752FF945A19C4D	com.vimotech.lichvannien	Lịch Vạn Sự
2A714C1BB6EF061D6BCF0AFBFA4B7609CCD40D0EB4C13F15143652C034B02402	com.lichcom.tuvi.lich.mautuat	Lịch Vạn Niên
468FD3C715A59D90AEE2C40E861704E7B63530F966C045C8D4335AFCA61AF906	com.lichtet2018.lichvannien	Lịch Vạn Niên
CF0366A75CD16F9EBBADF69694628BD052B5CC45BB3F565F77764D674C5406AF	com.softfreenow.lichvannien	Lịch Vạn Niên
9487C07C014F0E8AA130FC2A1EF3ED0CBA7A60353C1529BF400A0FD1CC61BD45	com.appx.tool.tuvi.lichvannien.amlich	Lịch Âm
1138497B05913D4EA710AC064C7143C6E2577B306880AEDB5B71D87DFF643B39	vn.media.instasavervideo	Insta Saver
4C787F011297C28751B13B6AC99ECB3465E3ED023F87FC189DCF1DC1D7C42352	net.smartants.matchblock	Hexa Match
67E333ABDA6865F3E1B34529DD388BF579CE950AE29DA717FA2BE84CEAB6C065	com.azmobie.blockhexa	Hexa Block
EFCA498B6A6715337CDEDF627690217CEF2D80D1C8F715B5C37652F556134F7E	com.azmobie.blockhexa	Hexa Block
1000A8DF37005CD0D76E08709D496480A9FA6ADC6B76817FD3571D6945DD6B04	com.apptofree.compass	GoldenCompass
EA9C392D1779E3630053BF5B469E2AE10FDABC90D27030F1812791D32E0E3B54	com.cosy.app.tool.Brightest.led.Flashlight	Flashlight
7290470ECD151F40F82664EAA3ACD248C7B29E72F830DA195BDCAE9A4ECB11D8	com.tool.app.led.FlashlightDigital	Flash Disco Pro
A04C47FA54155D3A2DA45921B61ECBBC953A0FFCB8E0FAEA4BBC325FDBD0002C	com.tool.app.led.FlashlightDigital	Flash Disco Pro
3D04094251D48AC7F42D52FA460AB46384AF656581EC39D149F76DB8DCA058AE	com.softedu.sieumaytinh	FastMath
E5490690A5F50F26BB6D252E4449C7F10CF6D8CC149A8DACED113C41637A8A1E	com.dlsoft.video.fb	Easy Download Video FB
41B515259E29D031440CBB4A32A2795278317E7F5AE9D038BD04EB3A5EE76044	com.babydragon.downloader.photo.video	Downloader for Insta
7B7590875E16FAA28EAC46D1600B465EDB2D2BF5349EE0661DD2CDA8C3418A1C	com.appx.tool.smart.compass	Compass
355F6196B0E40BC8E04A6A79B8BFEC5F788CF4BF5A9F082E87745EB5977E4F3F	com.bitfree.app.compass	Compass
D2CE55590156C8A1CDBDE1109D81D4A5A2CFBC7348BE87DCE6020788E694AD43	com.ghostteam.cleannerbooster	Cleaner Booster Pro
8C34B7D233868811AF12364FF783FB9CDDBD8D900B6FEE7285723F4190E9721C	com.azmobile.chessmaster	Chess Master

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