ID: 336565
Sample Name:
CoronaWarnApp.apk
Cookbook:
defaultandroidfilecookbook.jbs
Time: 11:27:45
Date: 06/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

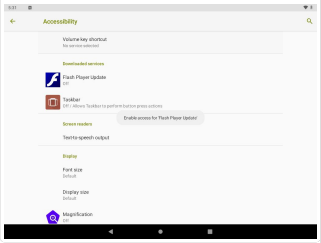
Analysis Report CoronaWarnApp.apk

Overview

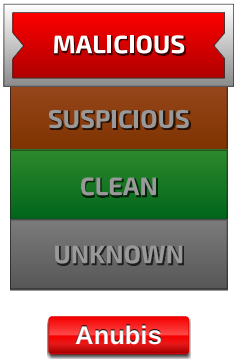
General Information

Sample Name:	CoronaWarnApp.apk
Analysis ID:	336565
MD5:	de2060e42c95d4..
SHA1:	8ebf29e56545925.
SHA256:	0d5ec7d8ea87fc8..

Most interesting Screenshot:



Detection

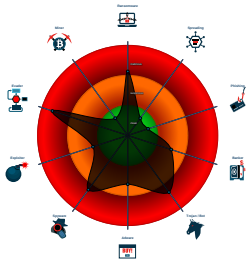


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Detected Anubis BankBot ransomwa…
- Multi AV Scanner detection for subm…
- Deletes other packages
- Found large list of e-Banking applica…
- Found potential keylogger
- Protects itself from removal
- Removes its application launcher (lik…
- Requests to ignore battery optimizat…
- Tries to detect Android x86
- Tries to detect the analysis device (…
- Tries to disable the administrator user

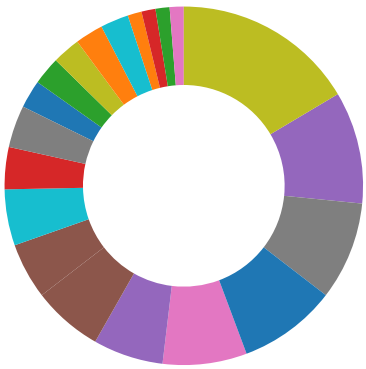
Classification



Yara Overview

No yara matches

Signature Overview



- AV Detection
- Location Tracking
- Privilege Escalation
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- Spam, unwanted Advertisements and Ransom Demands
- Operating System Destruction
- Change of System Appearance
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Found potential keylogger

E-Banking Fraud:

Detected Anubis BankBot ransomware / banking trojan

Found large list of e-Banking application (likely related to e-Banking fraud)

Spam, unwanted Advertisements and Ransom Demands:

Tries to disable the administrator user

Operating System Destruction:

Deletes other packages

System Summary:

Requests to ignore battery optimizations

Hooking and other Techniques for Hiding and Protection:

Protects itself from removal

Removes its application launcher (likely to stay hidden)

Malware Analysis System Evasion:

Tries to detect Android x86

Tries to detect the analysis device (e.g. the Android emulator)

Stealing of Sensitive Information:

Uses accessibility services (likely to control other applications)

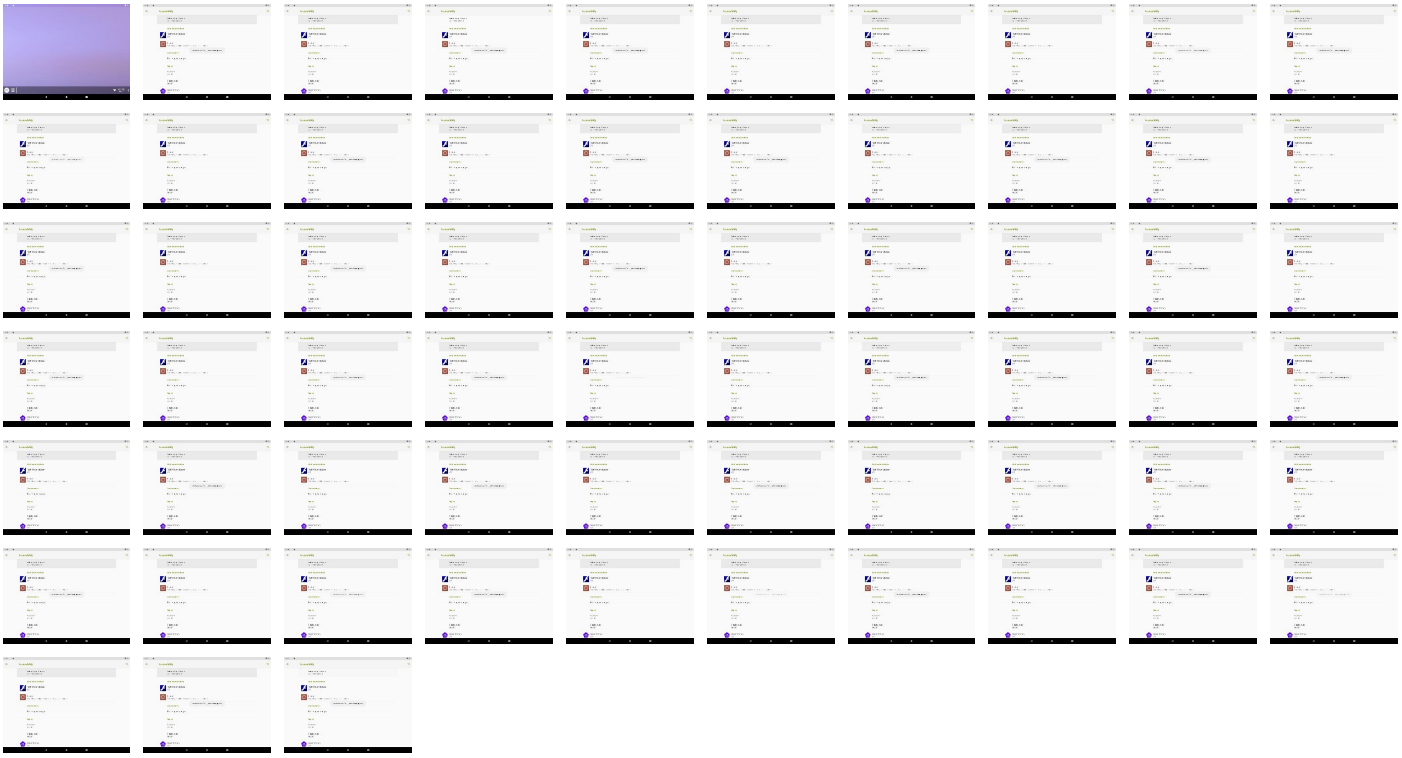
Mitre Att&ck Matrix

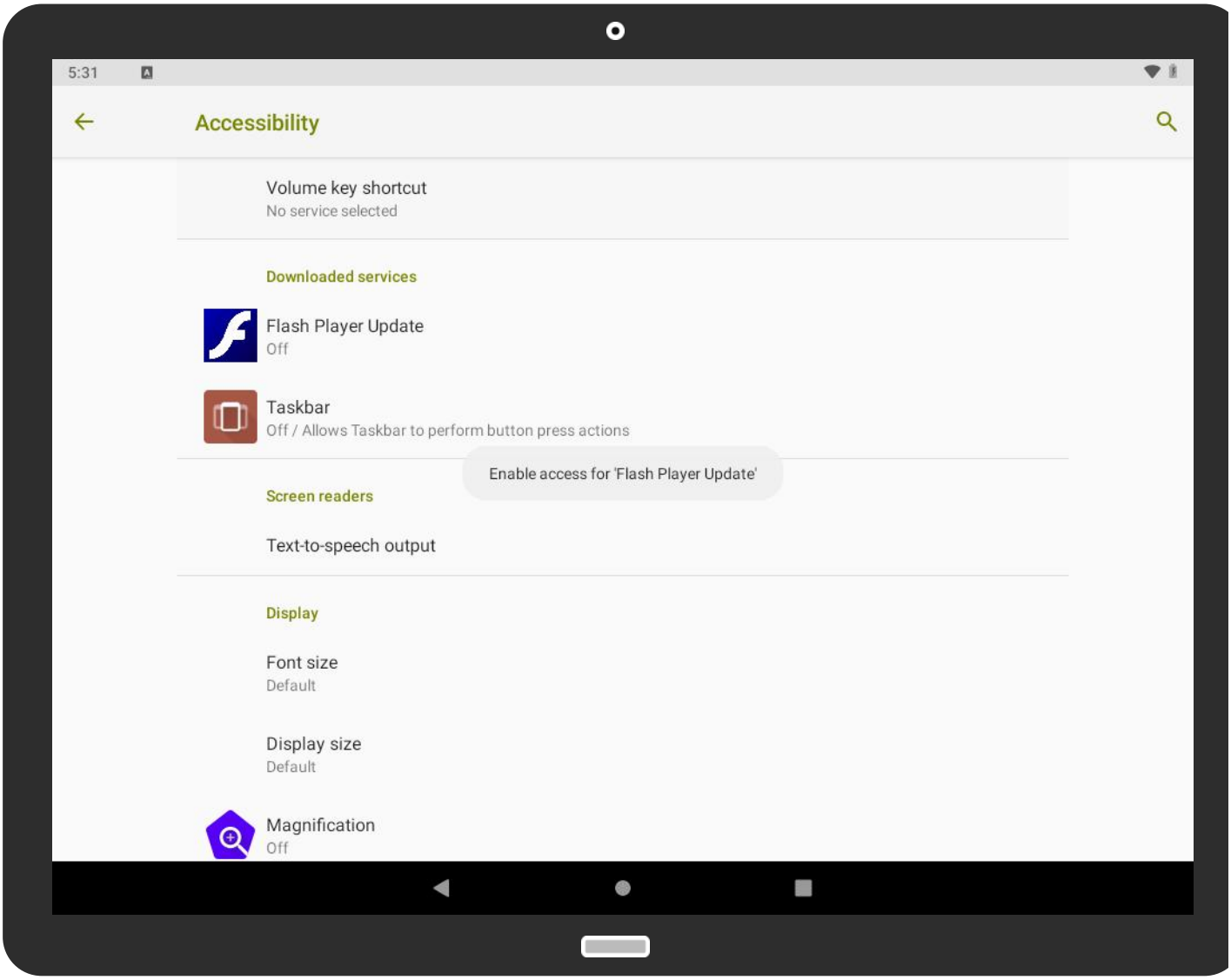
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Application Discovery 2	Input Capture 1	System Network Connections Discovery 1	Remote Services	Access Contact List 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Exploit SS7 to Redirect Phone Calls/SMS 2	Remote Track D Without Authoriz
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	Capture SMS Messages 2	Location Tracking 1 1	Remote Desktop Protocol	Location Tracking 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit SS7 to Redirect Phone Calls/SMS	Remote Wipe Da Without Authoriz
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Application Discovery 2	SMB/Windows Admin Shares	Capture Audio 2 1	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 1	Distributed Component Object Model	Network Information Discovery 1	Scheduled Transfer	Application Layer Protocol 2	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Process Discovery 1	SSH	Input Capture 1	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Owner/User Discovery	VNC	Capture SMS Messages 2	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	

Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
CoronaWarnApp.apk	35%	Virustotal		Browse
CoronaWarnApp.apk	100%	Avira	ANDROID/Svpeng.B.Gen	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://ktosdelaetskrintotpidor.com	5%	Virustotal		Browse
http://ktosdelaetskrintotpidor.com	0%	Avira URL Cloud	safe	
https://app-de-rki.xyz	0%	Avira URL Cloud	safe	
http://101.99.95.109/inj	0%	Avira URL Cloud	safe	
http://sositehuypidarasi.com	4%	Virustotal		Browse
http://sositehuypidarasi.com	0%	Avira URL Cloud	safe	
http://10.0.3.2/injclientup	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
time.android.com	216.239.35.12	true	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.android.com/apk/res/android	classes.dex	false		high
http://schemas.android.com/apk/res-auto	activity_inj.xml	false		high
http://ktosdelaetskrintotpidor.com	classes.dex, android	false	• 5%, Virustotal, Browse • Avira URL Cloud: safe	unknown
https://app-de-rki.xyz	classes.dex	false	• Avira URL Cloud: safe	unknown
https://jsonplaceholder.typicode.com/posts	classes.dex, android	false		high
http://101.99.95.109/inj	classes.dex	false	• Avira URL Cloud: safe	unknown
http://en.utrace.de	classes.dex	false		high
http://sositehuypidarasi.com	classes.dex	false	• 4%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://10.0.3.2/injclientup	classes.dex	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.217.168.67	unknown	United States		15169	GOOGLEUS	false
172.217.168.14	unknown	United States		15169	GOOGLEUS	false
172.217.168.10	unknown	United States		15169	GOOGLEUS	false
8.8.4.4	unknown	United States		15169	GOOGLEUS	false
216.239.35.12	unknown	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	336565
Start date:	06.01.2021
Start time:	11:27:45
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	CoronaWarnApp.apk
Cookbook file name:	defaultandroidfilecookbook.jbs
Analysis system description:	Android 9 (Pie)
APK Instrumentation enabled:	true
Detection:	MAL
Classification:	mal100.rans.troj.spyw.evad.andAPK@0/252@1/0
Warnings:	Show All • Excluded IPs from analysis (whitelisted): 172.217.168.74, 172.217.168.42, 216.58.215.234 • TCP Packets have been reduced to 100 • Excluded domains from analysis (whitelisted): android.googleapis.com, instantmessaging-pa.googleapis.com, play.googleapis.com, auditrecording-pa.googleapis.com • No interacted views • Not all executed log events are in report (maximum 10 identical API calls) • Not all non-executed APIs are in report • Report size exceeded maximum capacity and may have missing disassembly code. • Report size exceeded maximum capacity and may have missing dynamic data code. • VT rate limit hit for: http://10.0.3.2/injclientup

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
172.217.168.67	https://mtv.com	Get hash	malicious	Browse	• www.google.ch/pagead/1p-conversion/950987251/?label=UZjSCJrK4mMQ89O7xQM&guid=ON&script=0&ctc_id=CAIVAgAAAB0CAAAA&ct_cookie_present=false&random=247477394&sscte=1&crd=&is_vtc=1&ocp_id=pa82X_qqBr_E7_UPx4OHmAc&random=277148342&ipr=y
	http://u.to/8cz2Eg	Get hash	malicious	Browse	• fonts.gstatic.com/s/raleway/v12/1Ptrg8zYS_SKggPNwIYqWqZPBg.woff

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://paymentree.ca	Get hash	malicious	Browse	• fonts.gstatic.com/s/opensans/v15/mem8YaGs126MiZpBA-UFVZ0d.woff
	http://www.publishyourarticles.net	Get hash	malicious	Browse	• fonts.gstatic.com/s/ptserif/v9/EJRTQgYoZZY2vCFuvAFT_r21dA.woff
	http://textspeier.de	Get hash	malicious	Browse	• fonts.gstatic.com/s/montserrat/v12/JTURjIg1_i6t8kCHKm45_dJE3gnD-A.woff
	http://trip-suggest.com/fiji/northern/urata/	Get hash	malicious	Browse	• fonts.gstatic.com/s/shadowsintolight/v7/UqyNK9UOIntux_czAvDQx_ZcHqZXBNQzdcD_.woff
	https://urldefense.proofpoint.com/v2/url?u=https-3A__www.e-2Daccess.att.com_abgmas-5Fn_imail_dispatcher-3Faction-3Dsm.unsub-26ct-5Fid-3Dd93e425c959f38a0&d=DwIFAg&c=euGZstcaTDllvimEN8b7jXrwqOf-v5A_CdpgnVfiiMM&r=kOsMS0a61_b_h_foqF1756MSq9w7uqLN5RrsselaQRw&m=VPCss2mfVShNnAVlrIqRm_TqySlhsdqag9KaqHu8cck&s=fhmt5ahwQfahtpQ-YaFUMzShnT6eRLEPWgq7AQHbt18&e	Get hash	malicious	Browse	• www.google.ch/pagead/1p-user-list/1070858700/?value=0&guid=ON&script=0&cdct=2&is_vtc=1&random=3017082205&ipr=y
	https://urldefense.proofpoint.com/v2/url?u=https-3A__www.e-2Daccess.att.com_abgmas-5Fn_imail_dispatcher-3Faction-3Dsm.unsub-26ct-5Fid-3Dd93e425c959f38a0&d=DwIFAg&c=euGZstcaTDllvimEN8b7jXrwqOf-v5A_CdpgnVfiiMM&r=kOsMS0a61_b_h_foqF1756MSq9w7uqLN5RrsselaQRw&m=VPCss2mfVShNnAVlrIqRm_TqySlhsdqag9KaqHu8cck&s=fhmt5ahwQfahtpQ-YaFUMzShnT6eRLEPWgq7AQHbt18&e	Get hash	malicious	Browse	• www.google.ch/pagead/1p-user-list/1070858700/?value=0&guid=ON&script=0&cdct=2&is_vtc=1&random=1387446737&ipr=y
172.217.168.14	CRA-USER-TAX-REFUND.pdf	Get hash	malicious	Browse	• www.youtube.com/
	http://rgho.st/7jXZr4XY6	Get hash	malicious	Browse	• crl.pki.goog/GTSGIAG3.crl
	http://south-floridaattorney.com/indictment-vs-information-in-a-criminal-case/	Get hash	malicious	Browse	• crl.pki.goog/GTSGIAG3.crl

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
time.android.com	575h4N5kNl.apk	Get hash	malicious	Browse	• 216.239.35.8
	zoom-us-zoom.apk	Get hash	malicious	Browse	• 216.239.35.12
	zoom-us-zoom.apk	Get hash	malicious	Browse	• 216.239.35.4
	Truecal9_DZAPK.COM.apk	Get hash	malicious	Browse	• 216.239.35.8
	Truecal9_DZAPK.COM.apk	Get hash	malicious	Browse	• 216.239.35.0
	DualSpace.apk	Get hash	malicious	Browse	• 216.239.35.8
	manager.apk	Get hash	malicious	Browse	• 216.239.35.12
	#U044f#U043d#U0434#U0435#U043a#U0441.apk	Get hash	malicious	Browse	• 216.239.35.8
	#U044f#U043d#U0434#U0435#U043a#U0441.apk	Get hash	malicious	Browse	• 216.239.35.8
	eDevlet.apk	Get hash	malicious	Browse	• 216.239.35.4
	LyI95K8UWt.apk	Get hash	malicious	Browse	• 216.239.35.12
	DMFETQsYWv.apk	Get hash	malicious	Browse	• 216.239.35.0
	_sdcard_Download_install_r3d455.apk	Get hash	malicious	Browse	• 216.239.35.12
	Citrix Workflows for XenMobile_1.10.1.5_apktrending.com.apk	Get hash	malicious	Browse	• 216.239.35.0
	Citrix Workflows for XenMobile_1.10.1.5_apktrending.com.apk	Get hash	malicious	Browse	• 216.239.35.12
	manager.apk	Get hash	malicious	Browse	• 216.239.35.8
	oBlz1VuXEH.apk	Get hash	malicious	Browse	• 216.239.35.4
	oBlz1VuXEH.apk	Get hash	malicious	Browse	• 216.239.35.0

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	iGMtIi8EfC	Get hash	malicious	Browse	• 216.239.35.0
	co.uk.game.mobileapp_2020-09-18.apk	Get hash	malicious	Browse	• 216.239.35.4

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GOOGLEUS	Shipping Document PL and BL003534.ppt	Get hash	malicious	Browse	• 172.217.168.1
	Details!!!!.exe	Get hash	malicious	Browse	• 34.102.136.180
	Inquiry-RFQ93847849-pdf.exe	Get hash	malicious	Browse	• 34.98.99.30
	Order (2021.01.06).exe	Get hash	malicious	Browse	• 34.102.136.180
	W08347.exe	Get hash	malicious	Browse	• 34.102.136.180
	rtgs_pdf.exe	Get hash	malicious	Browse	• 34.102.136.180
	SHIPPING INVOICEpdf.exe	Get hash	malicious	Browse	• 34.102.136.180
	EAd5Xafr5g.exe	Get hash	malicious	Browse	• 216.239.34.21
	SecuriteInfo.com.Trojan.Packed.140.27461.exe	Get hash	malicious	Browse	• 216.239.32.21
	SecuriteInfo.com.Trojan.Packed.140.16756.exe	Get hash	malicious	Browse	• 216.239.36.21
	https://launcher-public-service-prod06.ol.epicgames.com/launcher/api/installer/download/EpicGamesLauncherInstaller.msi?trackingId=65ba5a18455641ffaa1f77c862a78fb2	Get hash	malicious	Browse	• 8.8.8.8
	SecuriteInfo.com.BehavesLike.Win32.Trickbot.gm.exe	Get hash	malicious	Browse	• 216.239.32.21
	mingup.exe	Get hash	malicious	Browse	• 216.239.34.21
	https://firebasestorage.googleapis.com/v0/b/blckaxe.appspot.com/o/general%20page.html?alt=media&token=b4029a1b-78f5-43ff-a7eb-d4555ad6a60e#kymo@willowoodusa.com	Get hash	malicious	Browse	• 216.58.215.225
	http://hoquetradersltd.com/jordanbruce/index.php	Get hash	malicious	Browse	• 216.58.215.225
	https://web.tresorit.com/l/d2q5C#T3PZC5SR6Y1Akp1-8AT_Jg	Get hash	malicious	Browse	• 74.125.140.157
	http://search.hwatchtvnow.co	Get hash	malicious	Browse	• 172.217.168.34
	https://web.tresorit.com/l/d2q5C#T3PZC5SR6Y1Akp1-8AT_Jg	Get hash	malicious	Browse	• 74.125.140.154
	https://nimb.ws/10IXxl	Get hash	malicious	Browse	• 74.125.140.156
	https://www.canva.com/design/DAESYWKuLHs/avvDNRvDuj_tk82H9Q45ZQ/view?utm_content=DAESYWKuLHs&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 74.125.140.155
GOOGLEUS	Shipping Document PL and BL003534.ppt	Get hash	malicious	Browse	• 172.217.168.1
	Details!!!!.exe	Get hash	malicious	Browse	• 34.102.136.180
	Inquiry-RFQ93847849-pdf.exe	Get hash	malicious	Browse	• 34.98.99.30
	Order (2021.01.06).exe	Get hash	malicious	Browse	• 34.102.136.180
	W08347.exe	Get hash	malicious	Browse	• 34.102.136.180
	rtgs_pdf.exe	Get hash	malicious	Browse	• 34.102.136.180
	SHIPPING INVOICEpdf.exe	Get hash	malicious	Browse	• 34.102.136.180
	EAd5Xafr5g.exe	Get hash	malicious	Browse	• 216.239.34.21
	SecuriteInfo.com.Trojan.Packed.140.27461.exe	Get hash	malicious	Browse	• 216.239.32.21
	SecuriteInfo.com.Trojan.Packed.140.16756.exe	Get hash	malicious	Browse	• 216.239.36.21
	https://launcher-public-service-prod06.ol.epicgames.com/launcher/api/installer/download/EpicGamesLauncherInstaller.msi?trackingId=65ba5a18455641ffaa1f77c862a78fb2	Get hash	malicious	Browse	• 8.8.8.8
	SecuriteInfo.com.BehavesLike.Win32.Trickbot.gm.exe	Get hash	malicious	Browse	• 216.239.32.21
	mingup.exe	Get hash	malicious	Browse	• 216.239.34.21
	https://firebasestorage.googleapis.com/v0/b/blckaxe.appspot.com/o/general%20page.html?alt=media&token=b4029a1b-78f5-43ff-a7eb-d4555ad6a60e#kymo@willowoodusa.com	Get hash	malicious	Browse	• 216.58.215.225
	http://hoquetradersltd.com/jordanbruce/index.php	Get hash	malicious	Browse	• 216.58.215.225
	https://web.tresorit.com/l/d2q5C#T3PZC5SR6Y1Akp1-8AT_Jg	Get hash	malicious	Browse	• 74.125.140.157
	http://search.hwatchtvnow.co	Get hash	malicious	Browse	• 172.217.168.34
	https://web.tresorit.com/l/d2q5C#T3PZC5SR6Y1Akp1-8AT_Jg	Get hash	malicious	Browse	• 74.125.140.154
	https://nimb.ws/10IXxl	Get hash	malicious	Browse	• 74.125.140.156
	https://www.canva.com/design/DAESYWKuLHs/avvDNRvDuj_tk82H9Q45ZQ/view?utm_content=DAESYWKuLHs&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 74.125.140.155
GOOGLEUS	Shipping Document PL and BL003534.ppt	Get hash	malicious	Browse	• 172.217.168.1
	Details!!!!.exe	Get hash	malicious	Browse	• 34.102.136.180
	Inquiry-RFQ93847849-pdf.exe	Get hash	malicious	Browse	• 34.98.99.30
	Order (2021.01.06).exe	Get hash	malicious	Browse	• 34.102.136.180
	W08347.exe	Get hash	malicious	Browse	• 34.102.136.180
	rtgs_pdf.exe	Get hash	malicious	Browse	• 34.102.136.180
	SHIPPING INVOICEpdf.exe	Get hash	malicious	Browse	• 34.102.136.180
	EAd5Xafr5g.exe	Get hash	malicious	Browse	• 216.239.34.21

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Trojan.Packed.140.27461.exe	Get hash	malicious	Browse	• 216.239.32.21
	SecuriteInfo.com.Trojan.Packed.140.16756.exe	Get hash	malicious	Browse	• 216.239.36.21
	https://launcher-public-service-prod06.ol.epicgames.com/launcher/api/installer/download/EpicGamesLauncherInstaller.msi?trackingId=65ba5a18455641ffaa1f77c862a78fb2	Get hash	malicious	Browse	• 8.8.8.8
	SecuriteInfo.com.BehavesLike.Win32.Trickbot.gm.exe	Get hash	malicious	Browse	• 216.239.32.21
	mingup.exe	Get hash	malicious	Browse	• 216.239.34.21
	https://firebasestorage.googleapis.com/v0/b/blckaxe.appspot.com/o/general%20page.html?alt=media&token=b4029a1b-78f5-43ff-a7eb-d4555ad6a60e#kymo@willowoodusa.com	Get hash	malicious	Browse	• 216.58.215.225
	http://hoquetradersltd.com/jordanbruce/index.php	Get hash	malicious	Browse	• 216.58.215.225
	https://web.tresorit.com/l/d2q5C#T3PZC5SR6Y1Akp1-8AT_Jg	Get hash	malicious	Browse	• 74.125.140.157
	http://search.hwatchtvnow.co	Get hash	malicious	Browse	• 172.217.168.34
	https://web.tresorit.com/l/d2q5C#T3PZC5SR6Y1Akp1-8AT_Jg	Get hash	malicious	Browse	• 74.125.140.154
	https://nimb.ws/10IXxl	Get hash	malicious	Browse	• 74.125.140.156
	https://www.canva.com/design/DAESYWKuLHs/avvDNRvDuj_tk82H9Q45ZQ/view?utm_content=DAESYWKuLHs&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 74.125.140.155
GOOGLEUS	Shipping Document PL and BL003534.ppt	Get hash	malicious	Browse	• 172.217.168.1
	Details!!!!.exe	Get hash	malicious	Browse	• 34.102.136.180
	Inquiry-RFQ93847849-pdf.exe	Get hash	malicious	Browse	• 34.98.99.30
	Order (2021.01.06).exe	Get hash	malicious	Browse	• 34.102.136.180
	W08347.exe	Get hash	malicious	Browse	• 34.102.136.180
	rtgs_pdf.exe	Get hash	malicious	Browse	• 34.102.136.180
	SHIPPING INVOICEpdf.exe	Get hash	malicious	Browse	• 34.102.136.180
	EAd5Xafr5g.exe	Get hash	malicious	Browse	• 216.239.34.21
	SecuriteInfo.com.Trojan.Packed.140.27461.exe	Get hash	malicious	Browse	• 216.239.32.21
	SecuriteInfo.com.Trojan.Packed.140.16756.exe	Get hash	malicious	Browse	• 216.239.36.21
	https://launcher-public-service-prod06.ol.epicgames.com/launcher/api/installer/download/EpicGamesLauncherInstaller.msi?trackingId=65ba5a18455641ffaa1f77c862a78fb2	Get hash	malicious	Browse	• 8.8.8.8
	SecuriteInfo.com.BehavesLike.Win32.Trickbot.gm.exe	Get hash	malicious	Browse	• 216.239.32.21
	mingup.exe	Get hash	malicious	Browse	• 216.239.34.21
	https://firebasestorage.googleapis.com/v0/b/blckaxe.appspot.com/o/general%20page.html?alt=media&token=b4029a1b-78f5-43ff-a7eb-d4555ad6a60e#kymo@willowoodusa.com	Get hash	malicious	Browse	• 216.58.215.225
	http://hoquetradersltd.com/jordanbruce/index.php	Get hash	malicious	Browse	• 216.58.215.225
	https://web.tresorit.com/l/d2q5C#T3PZC5SR6Y1Akp1-8AT_Jg	Get hash	malicious	Browse	• 74.125.140.157
	http://search.hwatchtvnow.co	Get hash	malicious	Browse	• 172.217.168.34
	https://web.tresorit.com/l/d2q5C#T3PZC5SR6Y1Akp1-8AT_Jg	Get hash	malicious	Browse	• 74.125.140.154
	https://nimb.ws/10IXxl	Get hash	malicious	Browse	• 74.125.140.156
	https://www.canva.com/design/DAESYWKuLHs/avvDNRvDuj_tk82H9Q45ZQ/view?utm_content=DAESYWKuLHs&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 74.125.140.155

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
6ec2896feff5746955f700c0023f5804	zoom-us-zoom.apk	Get hash	malicious	Browse	• 172.217.168.10
	zoom-us-zoom.apk	Get hash	malicious	Browse	• 172.217.168.10
	Truecal9_DZAPK.COM.apk	Get hash	malicious	Browse	• 172.217.168.10
	Truecal9_DZAPK.COM.apk	Get hash	malicious	Browse	• 172.217.168.10
	DualSpace.apk	Get hash	malicious	Browse	• 172.217.168.10
	manager.apk	Get hash	malicious	Browse	• 172.217.168.10
	#U044f#U043d#U0434#U0435#U043a#U0441.apk	Get hash	malicious	Browse	• 172.217.168.10
	#U044f#U043d#U0434#U0435#U043a#U0441.apk	Get hash	malicious	Browse	• 172.217.168.10
	eDevlet.apk	Get hash	malicious	Browse	• 172.217.168.10
	DMFETQsYWv.apk	Get hash	malicious	Browse	• 172.217.168.10
	Citrix Workflows for XenMobile_1.10.1.5_apktrending.com.apk	Get hash	malicious	Browse	• 172.217.168.10
	Citrix Workflows for XenMobile_1.10.1.5_apktrending.com.apk	Get hash	malicious	Browse	• 172.217.168.10
	manager.apk	Get hash	malicious	Browse	• 172.217.168.10
	oBlz1VuXEH.apk	Get hash	malicious	Browse	• 172.217.168.10
	iGMtIi8EfC	Get hash	malicious	Browse	• 172.217.168.10
	co.uk.game.mobileapp_2020-09-18.apk	Get hash	malicious	Browse	• 172.217.168.10
	GAME Reward Mobile App_v14.5_apkpure.com.apk	Get hash	malicious	Browse	• 172.217.168.10
	co.uk.game.mobileapp_2020-09-18 (1).apk	Get hash	malicious	Browse	• 172.217.168.10

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	co.uk.game.mobileapp_2020-09-18.apk	Get hash	malicious	Browse	• 172.217.168.10
	GAME Reward Mobile App_v14.5_apkpure.com.apk	Get hash	malicious	Browse	• 172.217.168.10

Dropped Files

No context

Created / dropped Files

/data/data/anubis.bot.myapplication/files/api0.csv.part	
File Type:	troff or preprocessor input, ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1898
Entropy (8bit):	3.4008133528178877
Encrypted:	false
SSDEEP:	
MD5:	8D6B5771C8CD764DE4FA28E2B5C5EE0E
SHA1:	ED93C40B0AF6653F1C09CEDC44567D5F8797338C
SHA-256:	234D07B361F93BE5F77B79D4163C3F25191C0BEB7D3C781098AEA88C0137588F
SHA-512:	1135F9BCE7792C1C6B8C74650CEA6438F8F321B3FF847062EBF9D1E778BDB9C9768EB52046CFB81E69F4D57683 92F6D4740F22FE15D5A2D0A22B48AD7B92B59
Malicious:	false
Reputation:	low
Preview:	

Static File Info

General

File type:	Zip archive data, at least v2.0 to extract
Entropy (8bit):	7.959180618569579
TrID:	• Android Package (27504/1) 56.12% • Java Archive (13504/1) 27.55% • ZIP compressed archive (8000/1) 16.32%
File name:	CoronaWarnApp.apk
File size:	954008
MD5:	de2060e42c95d4dddbf19d85d6da1cd7
SHA1:	8ebf29e56545925e5d2aa8af413de35cd973eb26
SHA256:	0d5ec7d8ea87fc80887fa6238dd49572182be98c8b02d9c 5dda350a026f16eb7
SHA512:	fe1a4af132831870a5f726fd9baedeadafcce4e1615bf290 7d44efc8f29f8a8235b0e0dc570fd14027bc179e8110a2af 9b101be1363a0d188537e9115fb78771
SSDEEP:	24576:Y74fEOwqCQnuw9lSCWy2Q94IvqHBfEp2Wdr9 m:9EOwqtT5WyJvv0GS
File Content Preview:	PK.....%R..y.4...8O.....AndroidManifest.xml.Z[p...^!.# ...rGEn..... ..LN.(.....m)...S.....N..}p:>.....>w:... m....r.Y..r.9%..s.:{}..k...C9U..6.2ZC+.....?.....f..._._._.... eD..C.A ...2.U.:.3.....\....._.....m.N.....p..

File Icon

Static APK Info

General

Label:	CoronaWarnApp
Minimum SDK required:	21

General

Target SDK required:	28
Version Code:	1
Version Name:	1
Package Name:	anubis.bot.myapplication
Is Activity:	true
Is Receiver:	true
Is Service:	true
Requests System Level Permissions:	false
Play Store Compatible:	true

Activities

Name	Is Entrypoint
anubis.bot.myapplicationcom.google.android.gms.common.api.GoogleApiActivity	
anubis.bot.myapplication.Activity.MainActivity	true
anubis.bot.myapplication.SendSms	
anubis.bot.myapplication.Activity.ActivityPermissions	
anubis.bot.myapplication.API.Screenshot.ActivityScreenshot	
anubis.bot.myapplication.Activity.ActivityInjection	
anubis.bot.myapplication.Activity.ActivityGetNumber	
anubis.bot.myapplication.Activity.ActivityAlert1	
anubis.bot.myapplication.Activity.ActivityGetSMS	
anubis.bot.myapplication.Activity.ActivityAlert2	
anubis.bot.myapplication.Activity.ActivityStartUSSD	
anubis.bot.myapplication.Activity.ActivityPushInjection	
anubis.bot.myapplication.Activity.ActivityOpenURL	
anubis.bot.myapplication.Activity.ActivityScreenLocker	
anubis.bot.myapplication.Activity.ActivityAccessibility	
anubis.bot.myapplication.Activity.ActivityPlayProtect	
anubis.bot.myapplication.Activity.LookScreen	

Receivers

• .Receiver.ReceiverAlarm	
• .Receiver.ReceiverBoot	• Intent: android.intent.action.BOOT_COMPLETED (Priority 999), android.intent.action.QUICKBOOT_POWERON (Priority 999), com.htc.intent.action.QUICKBOOT_POWERON (Priority 999), android.intent.action.USER_PRESENT (Priority 999), android.intent.action.PACKAGE_ADDED (Priority 999), android.intent.action.PACKAGE_REMOVED (Priority 999), android.provider.Telephony.SMS_RECEIVED (Priority 999), android.intent.action.SCREEN_ON (Priority 999), android.intent.action.EXTERNAL_APPLICATIONS_AVAILABLE (Priority 999), android.net.conn.CONNECTIVITY_CHANGE (Priority 999), android.net.wifi.WIFI_STATE_CHANGED (Priority 999), android.intent.action.DREAMING_STOPPED (Priority 999)
• .Receiver.ReceiverMms	• Intent: android.provider.Telephony.SMS_DELIVER
• .Receiver.RecieverPushService	• Intent: android.provider.Telephony.WAP_PUSH_DELIVER

Services

• .API.Screenshot.ServiceScreenshot	
• .API.Screenshot.ServiceSendRequestImageVNC	
• .API.Sound.ServiceRecordSound	
• .API.Sound.ServiceStreamSound	
• .API.Spam.ServiceSenderSpamSMS	
• .API.Spam.ServiceSpamSMS	
• .Alarm.EndlessService	
• .Alarm.JobSchedulerService	
• .LogSrv	
• .ServiceAccessibility	• Intent: android.accessibilityservice.AccessibilityService (Priority 0)
• .ServiceCommands	
• .ServiceCryptFiles	
• .ServiceDeleteSMS	
• .ServiceFindFiles	
• .ServiceGeolocationGPS	
• .ServiceGeolocationNetwork	

• .ServiceHeadlessSmsSend	• Intent: android.intent.action.RESPOND_VIA_MESSAGE (Priority 0)
• .ServiceInjections	
• .ServiceLookScreen	
• .ServiceModuleNotification	
• .ServiceNL	• Intent: android.service.notification.NotificationListenerService (Priority 0)
• .ServicePedometer	
• .ServicePlayProtectToast	
• .ServiceRAT	
• .ServiceToast	
• .StartWhileGlobal	
• .StartWhileRequest	
• .socks.ServiceForwardingTunel	

Permission Requested

- android.permission.ACCESS_FINE_LOCATION
- android.permission.ACCESS_NETWORK_STATE
- android.permission.BIND_ACCESSIBILITY_SERVICE
- android.permission.BIND_JOB_SERVICE
- android.permission.BIND_NOTIFICATION_LISTENER_SERVICE
- android.permission.CALL_PHONE
- android.permission.FOREGROUND_SERVICE
- android.permission.GET_TASKS
- android.permission.INTERNET
- android.permission.PACKAGE_USAGE_STATS
- android.permission.READ_CONTACTS
- android.permission.READ_EXTERNAL_STORAGE
- android.permission.READ_PHONE_STATE
- android.permission.READ_SMS
- android.permission.RECEIVE_BOOT_COMPLETED
- android.permission.RECEIVE_SMS
- android.permission.RECORD_AUDIO
- android.permission.REQUEST_DELETE_PACKAGES
- android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS
- android.permission.SEND_RESPOND_VIA_MESSAGE
- android.permission.SEND_SMS
- android.permission.SYSTEM_ALERT_WINDOW
- android.permission.WAKE_LOCK
- android.permission.WRITE_EXTERNAL_STORAGE
- android.permission.WRITE_SMS

Certificate

Name:	resources.arsc
Issuer:	1.2.840.113549.1.9.1=#1613616e64726f696440616e64726f69642e636f6d,CN=Android,OU=Android,O=Android,L=Mountain View,ST=California,C=US
Subject:	1.2.840.113549.1.9.1=#1613616e64726f696440616e64726f69642e636f6d,CN=Android,OU=Android,O=Android,L=Mountain View,ST=California,C=US

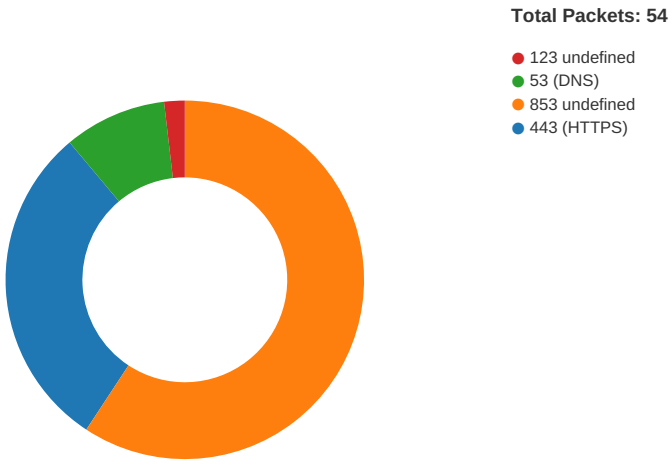
Resources

Name	Type	Size
activity_inj.xml	Android binary XML	464
ic_launcher.png	PNG image data, 512 x 512, 8-bit/color RGB, non-interlaced	65300
resources.arsc	data	25836
notification_icon_background.xml	Android binary XML	436
activity_alert.xml	Android binary XML	392
activity_accessibility.xml	Android binary XML	364
notification_bg_normal_pressed.9.png	PNG image data, 16 x 16, 8-bit colormap, non-interlaced	246
notification_bg_low.xml	Android binary XML	644
notification_action_tombstone.xml	Android binary XML	1340
activity_getsws.xml	Android binary XML	364
AndroidManifest.xml	Android binary XML	20280
notification_bg_normal.9.png	PNG image data, 16 x 16, 8-bit grayscale, non-interlaced	221

Name	Type	Size
notification_bg_low_normal.9.png	PNG image data, 8 x 8, 8-bit grayscale, non-interlaced	215
notification_bg.xml	Android binary XML	644
activity_push_nut.xml	Android binary XML	328
ic_launcher.png	PNG image data, 512 x 512, 8-bit/color RGB, non-interlaced	65300
im.png	PNG image data, 11 x 11, 8-bit colormap, non-interlaced	97
activity_usage_access_settings.xml	Android binary XML	364
ic_launcher.png	PNG image data, 512 x 512, 8-bit/color RGB, non-interlaced	65300
notification_action_background.xml	Android binary XML	1352
notify_panel_notification_icon_bg.png	PNG image data, 14 x 14, 8-bit colormap, non-interlaced	93
qq.jpg	[TIFF image data, big-endian, direntries=4, xresolution=62, yresolution=70, resolutionunit=2], baseline, precision 8, 256x392, frames 3	33221
notification_bg_normal_pressed.9.png	PNG image data, 12 x 12, 8-bit colormap, non-interlaced	229
notification_bg_normal.9.png	PNG image data, 12 x 12, 8-bit grayscale, non-interlaced	212
notification_bg_low_pressed.9.png	PNG image data, 12 x 12, 8-bit colormap, non-interlaced	229
notify_panel_notification_icon_bg.png	PNG image data, 15 x 15, 8-bit colormap, non-interlaced	93
notification_bg_normal_pressed.9.png	PNG image data, 8 x 8, 8-bit colormap, non-interlaced	229
otacert	PEM certificate	1675
CERT.SF	ASCII text, with CRLF line terminators	5501
notify_panel_notification_icon_bg.png	PNG image data, 30 x 30, 8-bit colormap, non-interlaced	99
notification_template_custom_big.xml	Android binary XML	2500
vending.png	PNG image data, 96 x 96, 8-bit/color RGB, non-interlaced	5404
activity_go_adm.xml	Android binary XML	364
CERT.RSA	data	1714
notification_tile_bg.xml	Android binary XML	380
r_l.xml	Android binary XML	328
activity_screen_locker.xml	Android binary XML	328
notification_action.xml	Android binary XML	1164
notification_bg_low_pressed.9.png	PNG image data, 16 x 16, 8-bit colormap, non-interlaced	251
serviceconfig.xml	Android binary XML	508
sendmsg.xml	Android binary XML	372
activity_push_fish.xml	Android binary XML	328
notification_bg_normal.9.png	PNG image data, 8 x 8, 8-bit grayscale, non-interlaced	215
notification_bg_low_normal.9.png	PNG image data, 12 x 12, 8-bit grayscale, non-interlaced	212
notification_template_part_time.xml	Android binary XML	448
activity_main.xml	Android binary XML	464
MANIFEST.MF	ASCII text, with CRLF line terminators	4962
ic_launcher.png	PNG image data, 512 x 512, 8-bit/color RGB, non-interlaced	65300
ic_launcher.png	PNG image data, 512 x 512, 8-bit/color RGB, non-interlaced	65300
notification_template_icon_group.xml	Android binary XML	996
notification_bg_low_normal.9.png	PNG image data, 16 x 16, 8-bit grayscale, non-interlaced	221
activity_play_protect.xml	Android binary XML	464
activity_activ_all_numbers.xml	Android binary XML	364
activity_start_ussd.xml	Android binary XML	364
notification_template_part_chronometer.xml	Android binary XML	448
classes.dex	Dalvik dex file version 035	1217512
notification_bg_low_pressed.9.png	PNG image data, 8 x 8, 8-bit colormap, non-interlaced	229
api0.csv.part.dr	troff or preprocessor input, ASCII text, with very long lines, with no line terminators	1898

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 6, 2021 11:28:02.115653038 CET	41662	443	192.168.2.30	172.217.168.14
Jan 6, 2021 11:28:02.171123028 CET	443	41662	172.217.168.14	192.168.2.30
Jan 6, 2021 11:28:02.370764017 CET	443	41662	172.217.168.14	192.168.2.30
Jan 6, 2021 11:28:02.371448040 CET	443	41662	172.217.168.14	192.168.2.30
Jan 6, 2021 11:28:02.371520996 CET	443	41662	172.217.168.14	192.168.2.30
Jan 6, 2021 11:28:02.373270988 CET	41662	443	192.168.2.30	172.217.168.14
Jan 6, 2021 11:28:12.098742962 CET	41662	443	192.168.2.30	172.217.168.14
Jan 6, 2021 11:28:12.153848886 CET	443	41662	172.217.168.14	192.168.2.30
Jan 6, 2021 11:28:12.172561884 CET	443	41662	172.217.168.14	192.168.2.30
Jan 6, 2021 11:28:12.172875881 CET	443	41662	172.217.168.14	192.168.2.30
Jan 6, 2021 11:28:12.173254967 CET	443	41662	172.217.168.14	192.168.2.30
Jan 6, 2021 11:28:12.174446106 CET	41662	443	192.168.2.30	172.217.168.14
Jan 6, 2021 11:28:16.590878963 CET	48754	443	192.168.2.30	172.217.168.67
Jan 6, 2021 11:28:16.643672943 CET	443	48754	172.217.168.67	192.168.2.30
Jan 6, 2021 11:28:16.643965960 CET	48754	443	192.168.2.30	172.217.168.67
Jan 6, 2021 11:28:18.726811886 CET	55938	853	192.168.2.30	8.8.4.4
Jan 6, 2021 11:28:18.777529001 CET	853	55938	8.8.4.4	192.168.2.30
Jan 6, 2021 11:28:18.777751923 CET	55938	853	192.168.2.30	8.8.4.4
Jan 6, 2021 11:28:18.777780056 CET	55938	853	192.168.2.30	8.8.4.4
Jan 6, 2021 11:28:18.828178883 CET	853	55938	8.8.4.4	192.168.2.30
Jan 6, 2021 11:28:18.837332010 CET	853	55938	8.8.4.4	192.168.2.30
Jan 6, 2021 11:28:18.837408066 CET	853	55938	8.8.4.4	192.168.2.30
Jan 6, 2021 11:28:18.837452888 CET	853	55938	8.8.4.4	192.168.2.30
Jan 6, 2021 11:28:18.837517977 CET	55938	853	192.168.2.30	8.8.4.4
Jan 6, 2021 11:28:18.837563038 CET	55938	853	192.168.2.30	8.8.4.4
Jan 6, 2021 11:28:18.841221094 CET	55938	853	192.168.2.30	8.8.4.4
Jan 6, 2021 11:28:18.892267942 CET	853	55938	8.8.4.4	192.168.2.30
Jan 6, 2021 11:28:18.892457962 CET	55938	853	192.168.2.30	8.8.4.4
Jan 6, 2021 11:28:18.948251009 CET	853	55938	8.8.4.4	192.168.2.30
Jan 6, 2021 11:28:18.965856075 CET	853	55938	8.8.4.4	192.168.2.30
Jan 6, 2021 11:28:18.966118097 CET	55938	853	192.168.2.30	8.8.4.4
Jan 6, 2021 11:28:18.966165066 CET	55938	853	192.168.2.30	8.8.4.4
Jan 6, 2021 11:28:19.016843081 CET	853	55938	8.8.4.4	192.168.2.30
Jan 6, 2021 11:28:19.017057896 CET	55938	853	192.168.2.30	8.8.4.4
Jan 6, 2021 11:28:50.765806913 CET	44518	853	192.168.2.30	8.8.8.8
Jan 6, 2021 11:28:50.813632011 CET	853	44518	8.8.8.8	192.168.2.30
Jan 6, 2021 11:28:50.817920923 CET	44518	853	192.168.2.30	8.8.8.8
Jan 6, 2021 11:28:50.817982912 CET	44518	853	192.168.2.30	8.8.8.8
Jan 6, 2021 11:28:50.865668058 CET	853	44518	8.8.8.8	192.168.2.30
Jan 6, 2021 11:28:50.873450041 CET	853	44518	8.8.8.8	192.168.2.30
Jan 6, 2021 11:28:50.873497009 CET	853	44518	8.8.8.8	192.168.2.30
Jan 6, 2021 11:28:50.873527050 CET	853	44518	8.8.8.8	192.168.2.30
Jan 6, 2021 11:28:50.873596907 CET	44518	853	192.168.2.30	8.8.8.8
Jan 6, 2021 11:28:50.873656988 CET	44518	853	192.168.2.30	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 6, 2021 11:28:50.873667955 CET	44518	853	192.168.2.30	8.8.8.8
Jan 6, 2021 11:28:50.884871006 CET	44518	853	192.168.2.30	8.8.8.8
Jan 6, 2021 11:28:50.932910919 CET	853	44518	8.8.8.8	192.168.2.30
Jan 6, 2021 11:28:50.933697939 CET	44518	853	192.168.2.30	8.8.8.8
Jan 6, 2021 11:28:50.986756086 CET	853	44518	8.8.8.8	192.168.2.30
Jan 6, 2021 11:28:50.992117882 CET	853	44518	8.8.8.8	192.168.2.30
Jan 6, 2021 11:28:50.992453098 CET	44518	853	192.168.2.30	8.8.8.8
Jan 6, 2021 11:28:50.992511988 CET	44518	853	192.168.2.30	8.8.8.8
Jan 6, 2021 11:28:51.040379047 CET	853	44518	8.8.8.8	192.168.2.30
Jan 6, 2021 11:28:51.040642023 CET	44518	853	192.168.2.30	8.8.8.8
Jan 6, 2021 11:29:11.877862930 CET	55942	853	192.168.2.30	8.8.4.4
Jan 6, 2021 11:29:11.928478003 CET	853	55942	8.8.4.4	192.168.2.30
Jan 6, 2021 11:29:11.928692102 CET	55942	853	192.168.2.30	8.8.4.4
Jan 6, 2021 11:29:11.928714991 CET	55942	853	192.168.2.30	8.8.4.4
Jan 6, 2021 11:29:11.979449034 CET	853	55942	8.8.4.4	192.168.2.30
Jan 6, 2021 11:29:11.987597942 CET	853	55942	8.8.4.4	192.168.2.30
Jan 6, 2021 11:29:11.987654924 CET	853	55942	8.8.4.4	192.168.2.30
Jan 6, 2021 11:29:11.987687111 CET	853	55942	8.8.4.4	192.168.2.30
Jan 6, 2021 11:29:11.987745047 CET	55942	853	192.168.2.30	8.8.4.4
Jan 6, 2021 11:29:11.987875938 CET	55942	853	192.168.2.30	8.8.4.4
Jan 6, 2021 11:29:11.991554976 CET	55942	853	192.168.2.30	8.8.4.4
Jan 6, 2021 11:29:12.042865992 CET	853	55942	8.8.4.4	192.168.2.30
Jan 6, 2021 11:29:12.043009043 CET	55942	853	192.168.2.30	8.8.4.4
Jan 6, 2021 11:29:12.097661972 CET	853	55942	8.8.4.4	192.168.2.30
Jan 6, 2021 11:29:12.101699114 CET	853	55942	8.8.4.4	192.168.2.30
Jan 6, 2021 11:29:12.105777025 CET	44164	443	192.168.2.30	172.217.168.10
Jan 6, 2021 11:29:12.142406940 CET	55942	853	192.168.2.30	8.8.4.4
Jan 6, 2021 11:29:12.161056042 CET	443	44164	172.217.168.10	192.168.2.30
Jan 6, 2021 11:29:12.161212921 CET	44164	443	192.168.2.30	172.217.168.10
Jan 6, 2021 11:29:12.162570953 CET	44164	443	192.168.2.30	172.217.168.10
Jan 6, 2021 11:29:12.217796087 CET	443	44164	172.217.168.10	192.168.2.30
Jan 6, 2021 11:29:12.230245113 CET	443	44164	172.217.168.10	192.168.2.30
Jan 6, 2021 11:29:12.230299950 CET	443	44164	172.217.168.10	192.168.2.30
Jan 6, 2021 11:29:12.230329037 CET	443	44164	172.217.168.10	192.168.2.30
Jan 6, 2021 11:29:12.230403900 CET	44164	443	192.168.2.30	172.217.168.10
Jan 6, 2021 11:29:12.230442047 CET	44164	443	192.168.2.30	172.217.168.10
Jan 6, 2021 11:29:12.241508961 CET	44164	443	192.168.2.30	172.217.168.10
Jan 6, 2021 11:29:12.249545097 CET	44164	443	192.168.2.30	172.217.168.10
Jan 6, 2021 11:29:12.249608040 CET	44164	443	192.168.2.30	172.217.168.10
Jan 6, 2021 11:29:12.296941042 CET	443	44164	172.217.168.10	192.168.2.30
Jan 6, 2021 11:29:12.297044992 CET	44164	443	192.168.2.30	172.217.168.10
Jan 6, 2021 11:29:12.305088043 CET	443	44164	172.217.168.10	192.168.2.30
Jan 6, 2021 11:29:12.309974909 CET	443	44164	172.217.168.10	192.168.2.30
Jan 6, 2021 11:29:12.352344036 CET	443	44164	172.217.168.10	192.168.2.30
Jan 6, 2021 11:29:12.448082924 CET	443	44164	172.217.168.10	192.168.2.30
Jan 6, 2021 11:29:12.448138952 CET	443	44164	172.217.168.10	192.168.2.30
Jan 6, 2021 11:29:12.448173046 CET	443	44164	172.217.168.10	192.168.2.30
Jan 6, 2021 11:29:12.448200941 CET	443	44164	172.217.168.10	192.168.2.30
Jan 6, 2021 11:29:12.448240042 CET	443	44164	172.217.168.10	192.168.2.30
Jan 6, 2021 11:29:12.448266983 CET	443	44164	172.217.168.10	192.168.2.30
Jan 6, 2021 11:29:12.448451996 CET	44164	443	192.168.2.30	172.217.168.10
Jan 6, 2021 11:29:27.103746891 CET	55942	853	192.168.2.30	8.8.4.4
Jan 6, 2021 11:29:27.154547930 CET	853	55942	8.8.4.4	192.168.2.30
Jan 6, 2021 11:29:32.123095989 CET	55942	853	192.168.2.30	8.8.4.4
Jan 6, 2021 11:29:32.123179913 CET	55942	853	192.168.2.30	8.8.4.4
Jan 6, 2021 11:29:32.174062014 CET	853	55942	8.8.4.4	192.168.2.30

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 6, 2021 11:28:02.678656101 CET	48850	53	192.168.2.30	8.8.8.8
Jan 6, 2021 11:28:02.735182047 CET	53	48850	8.8.8.8	192.168.2.30
Jan 6, 2021 11:28:12.182918072 CET	49757	53	192.168.2.30	8.8.8.8
Jan 6, 2021 11:28:12.244097948 CET	53	49757	8.8.8.8	192.168.2.30

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 6, 2021 11:28:12.508982897 CET	54101	53	192.168.2.30	8.8.8.8
Jan 6, 2021 11:28:12.576405048 CET	53	54101	8.8.8.8	192.168.2.30
Jan 6, 2021 11:28:17.861713886 CET	59120	53	192.168.2.30	8.8.8.8
Jan 6, 2021 11:28:17.920432091 CET	53	59120	8.8.8.8	192.168.2.30
Jan 6, 2021 11:29:08.839193106 CET	34673	53	192.168.2.30	8.8.8.8
Jan 6, 2021 11:29:08.911892891 CET	53	34673	8.8.8.8	192.168.2.30
Jan 6, 2021 11:29:08.913142920 CET	55301	123	192.168.2.30	216.239.35.12
Jan 6, 2021 11:29:08.961102962 CET	123	55301	216.239.35.12	192.168.2.30

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 6, 2021 11:29:08.839193106 CET	192.168.2.30	8.8.8.8	0x9683	Standard query (0)	time.android.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 6, 2021 11:29:08.911892891 CET	8.8.8.8	192.168.2.30	0x9683	No error (0)	time.android.com		216.239.35.12	A (IP address)	IN (0x0001)
Jan 6, 2021 11:29:08.911892891 CET	8.8.8.8	192.168.2.30	0x9683	No error (0)	time.android.com		216.239.35.8	A (IP address)	IN (0x0001)
Jan 6, 2021 11:29:08.911892891 CET	8.8.8.8	192.168.2.30	0x9683	No error (0)	time.android.com		216.239.35.4	A (IP address)	IN (0x0001)
Jan 6, 2021 11:29:08.911892891 CET	8.8.8.8	192.168.2.30	0x9683	No error (0)	time.android.com		216.239.35.0	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 6, 2021 11:29:12.230329037 CET	172.217.168.10	443	192.168.2.30	44164	CN=upload.video.google.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Nov 10 15:39:49 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Feb 02 15:39:48 CET 2021 Wed Dec 15 01:00:42 CET 2021	771,49195-49196-52393-49199-49200-52392-49161-49162-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13,29-23-24,0	6ec2896feff5746955f700c0023f5804
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

APK Behavior

Installation

Miscellaneous

Simulated Events

Type	Data
boot completed	• -
time tick	• -
incoming sms	• 0123456789 • this is a text message
outgoing sms	• 9876543210 • thank you

Type	Data
location change	• 54.13 • 12.14
motion simulation	• -
incoming call	• 0123456789
outgoing call	• 9876543210
time tick	• -

System Calls

By Permission (executed)

By Permission (non-executed)

Disassembly

0 Executed Methods

0 Non-Executed Methods