MOBSF

ANDROID STATIC ANALYSIS REPORT

Covid Check (4.0.0)

File Name:	ch.admin.bag.covidcertificate.verifier.apk
Package Name:	ch.admin.bag.covidcertificate.verifier
Scan Date:	May 9, 2022, 4:13 p.m.
App Security Score:	70/100 (LOW RISK)
Grade:	A

FINDINGS SEVERITY

HIGH	WARNING	INFO	SECURE
0	5	1	2

FILE INFORMATION

File Name: ch.admin.bag.covidcertificate.verifier.apk
Size: 20.78MB
MD5: d63dfa07074c1f125ddb9e951fb1aba1
SHA1: 249d3b08426a8c76db8fb29a9f0c986358f91c4a
SHA256: ac1c8930a263002e14fb2df28ead7301f22ea6a3000cd12a628ad8a7452a5b36

APP INFORMATION

App Name: Covid Check
Package Name: ch.admin.bag.covidcertificate.verifier
Main Activity: ch.admin.bag.covidcertificate.verifier.MainActivity
Target SDK: 31
Min SDK: 23
Max SDK:
Android Version Name: 4.0.0
Android Version Code: 4000000

APP COMPONENTS

Activities: 2
Services: 1
Receivers: 0
Providers: 1
Exported Activities: 0
Exported Services: 0
Exported Receivers: 0
Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=CH, ST=Bern, L=Bern, O=Bundesamt für Gesundheit BAG
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-05-22 13:25:32+00:00
Valid To: 2120-04-28 13:25:32+00:00
Issuer: C=CH, ST=Bern, L=Bern, O=Bundesamt für Gesundheit BAG
Serial Number: 0x3d416dd5
Hash Algorithm: sha256
md5: 27cb9202677e490dee0c3340fb1e1828
sha1: 66db2743cd38bb2fd93531bd436a742b891ac998
sha256: a573c85457e02ee99004735d7445ab4418d07287a8fac057915416332a3c7c63
sha512: 2d3e03819ae995afe11df4297f2a92567b79b166f7b5ba3ab638db3503dabfe4615417f4e56a07d256b26dae64a28ddf4eca08a422db0ee133ba127a6b502cfe
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 6d5243bc4fed234e18756e70977c16dc4a29d1628ec93c1c7188e018ff228635

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.

APKID ANALYSIS

FILE	DETAILS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	ch/admin/bag/covidcertificate/sdk/android/net/RetrofitFactory.java ch/admin/bag/covidcertificate/sdk/android/net/CertificatePinning.java ch/admin/bag/covidcertificate/common/net/ConfigRepository.java
2	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	ch/admin/bag/covidcertificate/sdk/android/verification/CertificateVerificationController$refreshTrustList$3.java ch/admin/bag/covidcertificate/sdk/android/metadata/ProductMetadataController$refreshProductsMetadata$3.java ch/admin/bag/covidcertificate/sdk/android/verification/CertificateVerificationController$processTask$2.java ch/admin/bag/covidcertificate/common/util/SingleLiveEvent.java ch/admin/bag/covidcertificate/sdk/android/data/FileStorage.java COSE/ASN1.java ch/admin/bag/covidcertificate/sdk/android/utils/EncryptedSharedPreferencesUtil.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	io/jsonwebtoken/JwsHeader.java
4	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	net/i2p/crypto/eddsa/EdDSASecurityProvider.java
5	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	j$/util/concurrent/ThreadLocalRandom.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_RBG_EXT.1.1	Security Functional Requirements	Random Bit Generation Services	The application implement DRBG functionality for its cryptographic operations.
2	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
3	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application implement asymmetric key generation.
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['camera', 'network connectivity'].
5	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
6	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.
7	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application leverage platform-provided functionality to encrypt sensitive data in non-volatile memory.
8	FMT_MEC_EXT.1.1	Security Functional Requirements	Supported Configuration Mechanism	The application invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.
9	FTP_DIT_EXT.1.1	Security Functional Requirements	Protection of Data in Transit	The application does encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.
10	FCS_RBG_EXT.2.1,FCS_RBG_EXT.2.2	Selection-Based Security Functional Requirements	Random Bit Generation from Application	The application perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using Hash_DRBG. The deterministic RBG is seeded by an entropy source that accumulates entropy from a platform-based DRBG and a software-based noise source, with a minimum of 256 bits of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
11	FCS_CKM.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Asymmetric Key Generation	The application generate asymmetric cryptographic keys not in accordance with FCS_CKM.1.1(1) using key generation algorithm RSA schemes and cryptographic key sizes of 1024-bit or lower.
12	FCS_CKM.1.1(3),FCS_CKM.1.2(3)	Selection-Based Security Functional Requirements	Password Conditioning	A password/passphrase shall perform [Password-based Key Derivation Functions] in accordance with a specified cryptographic algorithm..
13	FCS_COP.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Operation - Encryption/Decryption	The application perform encryption/decryption not in accordance with FCS_COP.1.1(1), AES-ECB mode is being used.
14	FCS_COP.1.1(2)	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services in accordance with a specified cryptographic algorithm SHA-1/SHA-256/SHA-384/SHA-512 and message digest sizes 160/256/384/512 bits.
15	FCS_COP.1.1(3)	Selection-Based Security Functional Requirements	Cryptographic Operation - Signing	The application perform cryptographic signature services (generation and verification) in accordance with a specified cryptographic algorithm RSA schemes using cryptographic key sizes of 2048-bit or greater.
16	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
17	FCS_HTTPS_EXT.1.3	Selection-Based Security Functional Requirements	HTTPS Protocol	The application notify the user and not establish the connection or request application authorization to establish the connection if the peer certificate is deemed invalid.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
18	FIA_X509_EXT.1.1	Selection-Based Security Functional Requirements	X.509 Certificate Validation	The application invoked platform-provided functionality to validate certificates in accordance with the following rules: ['The application validate a certificate path by ensuring the presence of the basicConstraints extension and that the CA flag is set to TRUE for all CA certificates', 'The application validate the revocation status of the certificate using the Online Certificate Status Protocol (OCSP) as specified in RFC 2560 or a Certificate Revocation List (CRL) as specified in RFC 5759 or an OCSP TLS Status Request Extension (i.e., OCSP stapling) as specified in RFC 6066'].
19	FIA_X509_EXT.1.2	Selection-Based Security Functional Requirements	X.509 Certificate Validation	The application treat a certificate as a CA certificate only if the basicConstraints extension is present and the CA flag is set to TRUE.
20	FIA_X509_EXT.2.1	Selection-Based Security Functional Requirements	X.509 Certificate Authentication	The application use X.509v3 certificates as defined by RFC 5280 to support authentication for HTTPS , TLS.
21	FIA_X509_EXT.2.2	Selection-Based Security Functional Requirements	X.509 Certificate Authentication	When the application cannot establish a connection to determine the validity of a certificate, the application allow the administrator to choose whether to accept the certificate in these cases or accept the certificate ,or not accept the certificate.
22	FCS_CKM.1.1(2)	Optional Security Functional Requirements	Cryptographic Symmetric Key Generation	The application shall generate symmetric cryptographic keys using a Random Bit Generator as specified in FCS_RBG_EXT.1 and specified cryptographic key sizes 128 bit or 256 bit.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.cc-a.bit.admin.ch	ok	**IP:** 108.156.22.76 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
www.gl.ch	ok	**IP:** 193.135.58.32 **Country:** Switzerland **Region:** Thurgau **City:** Frauenfeld **Latitude:** 47.558159 **Longitude:** 8.898540 **View:** Google Map
javax.xml.xmlconstants	ok	No Geolocation information available.
www.lu.ch	ok	**IP:** 194.40.144.142 **Country:** Switzerland **Region:** Luzern **City:** Luzern **Latitude:** 47.050480 **Longitude:** 8.306350 **View:** Google Map
covid19-vac-check.ch	ok	**IP:** 185.48.147.44 **Country:** Switzerland **Region:** Vaud **City:** Bussigny **Latitude:** 46.551102 **Longitude:** 6.555970 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
vd.ch	ok	**IP:** 145.232.192.197 **Country:** Switzerland **Region:** Vaud **City:** Lausanne **Latitude:** 46.515999 **Longitude:** 6.632820 **View:** Google Map
bag-coronavirus.ch	ok	**IP:** 34.65.60.252 **Country:** Switzerland **Region:** Zurich **City:** Zurich **Latitude:** 47.366669 **Longitude:** 8.550000 **View:** Google Map
tools.ietf.org	ok	**IP:** 4.31.198.62 **Country:** United States of America **Region:** California **City:** San Jose **Latitude:** 37.339390 **Longitude:** -121.894958 **View:** Google Map
www.ar.ch	ok	**IP:** 185.17.69.20 **Country:** Switzerland **Region:** Luzern **City:** Luzern **Latitude:** 47.050480 **Longitude:** 8.306350 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.jura.ch	ok	**IP:** 193.246.28.145 **Country:** Switzerland **Region:** Jura **City:** Delemont **Latitude:** 47.364929 **Longitude:** 7.344530 **View:** Google Map
www.cc.bit.admin.ch	ok	**IP:** 108.156.22.89 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
www.sz.ch	ok	**IP:** 193.135.58.23 **Country:** Switzerland **Region:** Thurgau **City:** Frauenfeld **Latitude:** 47.558159 **Longitude:** 8.898540 **View:** Google Map
www.ge.ch	ok	**IP:** 160.53.252.106 **Country:** Switzerland **Region:** Geneve **City:** Geneva **Latitude:** 46.202221 **Longitude:** 6.145690 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
gesundheit.tg.ch	ok	**IP:** 161.78.13.64 **Country:** Switzerland **Region:** Thurgau **City:** Frauenfeld **Latitude:** 47.558159 **Longitude:** 8.898540 **View:** Google Map
www.zh.ch	ok	**IP:** 194.247.8.174 **Country:** Switzerland **Region:** Zurich **City:** Aussersihl **Latitude:** 47.377522 **Longitude:** 8.521270 **View:** Google Map
itunes.apple.com	ok	**IP:** 184.50.200.24 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map
www.gsi.be.ch	ok	**IP:** 159.144.56.20 **Country:** Switzerland **Region:** Bern **City:** Bern **Latitude:** 46.948090 **Longitude:** 7.447440 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
ofsp-coronavirus.ch	ok	**IP:** 34.65.60.252 **Country:** Switzerland **Region:** Zurich **City:** Zurich **Latitude:** 47.366669 **Longitude:** 8.550000 **View:** Google Map
www.baselland.ch	ok	**IP:** 193.47.168.16 **Country:** Switzerland **Region:** Basel-Landschaft **City:** Liestal **Latitude:** 47.484550 **Longitude:** 7.734460 **View:** Google Map
www.be.ch	ok	**IP:** 159.144.56.20 **Country:** Switzerland **Region:** Bern **City:** Bern **Latitude:** 46.948090 **Longitude:** 7.447440 **View:** Google Map
ufsp-coronavirus.ch	ok	**IP:** 34.65.60.252 **Country:** Switzerland **Region:** Zurich **City:** Zurich **Latitude:** 47.366669 **Longitude:** 8.550000 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.corona-impfung-zug.ch	ok	**IP:** 3.126.202.50 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
sh.ch	ok	**IP:** 178.250.24.196 **Country:** Switzerland **Region:** Zurich **City:** Zurich **Latitude:** 47.366669 **Longitude:** 8.550000 **View:** Google Map
www.ai.ch	ok	**IP:** 159.100.250.129 **Country:** Switzerland **Region:** Vaud **City:** Lausanne **Latitude:** 46.515999 **Longitude:** 6.632820 **View:** Google Map
www.coronaimpfzentrumbasel.ch	ok	**IP:** 34.252.100.94 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
foph-coronavirus.ch	ok	**IP:** 34.65.60.252 **Country:** Switzerland **Region:** Zurich **City:** Zurich **Latitude:** 47.366669 **Longitude:** 8.550000 **View:** Google Map
www.bl.ch	ok	**IP:** 193.47.168.16 **Country:** Switzerland **Region:** Basel-Landschaft **City:** Liestal **Latitude:** 47.484550 **Longitude:** 7.734460 **View:** Google Map
www.ow.ch	ok	**IP:** 195.65.10.20 **Country:** Switzerland **Region:** Zurich **City:** Zurich **Latitude:** 47.366669 **Longitude:** 8.550000 **View:** Google Map
www.bit.admin.ch	ok	**IP:** 162.23.129.87 **Country:** Switzerland **Region:** Bern **City:** Bern **Latitude:** 46.948090 **Longitude:** 7.447440 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
youtu.be	ok	**IP:** 142.250.74.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.ur.ch	ok	**IP:** 195.65.10.20 **Country:** Switzerland **Region:** Zurich **City:** Zurich **Latitude:** 47.366669 **Longitude:** 8.550000 **View:** Google Map
www.fr.ch	ok	**IP:** 52.29.81.245 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
www.bag.admin.ch	ok	**IP:** 108.156.22.45 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
apache.org	ok	**IP:** 151.101.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.vs.ch	ok	**IP:** 193.247.117.21 **Country:** Switzerland **Region:** Valais **City:** Sion **Latitude:** 46.229080 **Longitude:** 7.359420 **View:** Google Map
covid19.impf-check.ch	ok	**IP:** 185.48.147.42 **Country:** Switzerland **Region:** Vaud **City:** Bussigny **Latitude:** 46.551102 **Longitude:** 6.555970 **View:** Google Map
www.ag.ch	ok	**IP:** 193.47.122.80 **Country:** Switzerland **Region:** Aargau **City:** Aarau **Latitude:** 47.392540 **Longitude:** 8.044220 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.nw.ch	ok	**IP:** 195.65.10.26 **Country:** Switzerland **Region:** Zurich **City:** Zurich **Latitude:** 47.366669 **Longitude:** 8.550000 **View:** Google Map
www.cc-d.bit.admin.ch	ok	**IP:** 108.156.22.113 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
www.ti.ch	ok	**IP:** 193.246.181.24 **Country:** Switzerland **Region:** Ticino **City:** Bellinzona **Latitude:** 46.192780 **Longitude:** 9.017030 **View:** Google Map
www.gr.ch	ok	**IP:** 193.247.16.45 **Country:** Switzerland **Region:** Graubunden **City:** Chur **Latitude:** 46.849861 **Longitude:** 9.532870 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
github.com	ok	**IP:** 140.82.121.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.ne.ch	ok	**IP:** 148.196.30.27 **Country:** Switzerland **Region:** Neuchatel **City:** Neuchatel **Latitude:** 46.991791 **Longitude:** 6.931000 **View:** Google Map
www.sg.ch	ok	**IP:** 193.238.142.3 **Country:** Switzerland **Region:** Sankt Gallen **City:** Wil **Latitude:** 47.461521 **Longitude:** 9.045520 **View:** Google Map
so.ch	ok	**IP:** 193.135.80.188 **Country:** Switzerland **Region:** Solothurn **City:** Solothurn **Latitude:** 47.207909 **Longitude:** 7.537140 **View:** Google Map

HARDCODED SECRETS

POSSIBLE SECRETS
"language_key" : "en"
"wallet_add_certificate" : "Add"
"language_key" : "de"
"wallet_add_certificate" : "Hinzufügen"
"wallet_certificate" : "Covid-Zertifikat"
"language_key" : "fr"
"wallet_add_certificate" : "Ajouter"
"language_key" : "it"
"wallet_add_certificate" : "Aggiungere"
"language_key" : "rm"
"wallet_add_certificate" : "Agiuntar"

PLAYSTORE INFORMATION

Title: COVID Certificate Check

Score: 4.25 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** 6.0 and up **Category:** Health & Fitness **Play Store URL:** ch.admin.bag.covidcertificate.verifier

Developer Details: Federal Office of Public Health FOPH, Federal+Office+of+Public+Health+FOPH, None, https://www.bag.admin.ch/bag/de/home/krankheiten/ausbrueche-epidemien-pandemien/aktuelle-ausbrueche-epidemien/novel-cov/covid-zertifikat.html, covid-zertifikat@bag.admin.ch,

Release Date: May 31, 2021 **Privacy Policy:** Privacy link

Description:

COVID Certificate Check is the official app for checking COVID certificates in Switzerland. It is developed by the Federal Office of Information Technology, Systems and Telecommunication FOITT on behalf of the Federal Office of Public Health. The app allows you to check whether a COVID certificate issued in Switzerland or the EU is valid in Switzerland. How the app works A button on the home screen activates the smartphone camera and the app is ready to capture the QR code. Simply position the QR code on the paper or on the mobile phone shown with a holder app in the square displayed and the QR will be captured automatically. Immediately afterwards, the system performs an automatic check concerning Swiss validity rules. A tick and a green background indicate that the presented certificate is valid. An exclamation mark and a red background indicate that the presented certificate is not valid. A question mark and an orange background indicate that the check failed. In addition, the full name and date of birth of the certificate holder are displayed. These details are to be compared with the identification document presented. Data protection is a top priority The data concerning COVID certificates and checking processes is not stored. COVID certificates are protected by a digital signature and are thus forgery-proof. The use of the app is limited to Switzerland and is subject to Swiss law.

Report Generated by - MobSF v3.5.1 Beta

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.