

ANDROID STATIC ANALYSIS REPORT



YsxLite (1.45)

File Name:	ysxlite.apk
Package Name:	com.ysxlite.cam
Scan Date:	Oct. 28, 2024, 4:11 p.m.
App Security Score:	36/100 (HIGH RISK)
Grade:	C
Trackers Detection:	10/432

FINDINGS SEVERITY

飛 HIGH	▲ MEDIUM	i INFO	✓ SECURE	Q HOTSPOT
6	16	1	0	3

FILE INFORMATION

File Name: ysxlite.apk **Size:** 54.96MB

MD5: 434c3cd6a91b24380657e7852d5ea950

SHA1: b4ace169a5616dd9e381f86089f69543262b9dec

\$HA256: 149b9467c8c28879a42c99fabc9cc660ea54fb34da9cd314bda4e1de69b060be

i APP INFORMATION

App Name: YsxLite

Package Name: com.ysxlite.cam

Main Activity: com.ysxlite.cam.LauncherAty

Target SDK: 34 Min SDK: 21 Max SDK:

Android Version Name: 1.45

APP COMPONENTS

Activities: 84 Services: 9 Receivers: 10 Providers: 9

Exported Activities: 2 Exported Services: 3 Exported Receivers: 2 Exported Providers: 0

***** CERTIFICATE INFORMATION

Binary is signed v1 signature: True v2 signature: True v3 signature: True v4 signature: False

X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android

Signature Algorithm: rsassa_pkcs1v15 Valid From: 2023-09-13 05:54:36+00:00 Valid To: 2053-09-13 05:54:36+00:00

Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android

Serial Number: 0xdc686c47c1f7146a14cf19ad199b62016f10e382

Hash Algorithm: sha256

md5: dc663c0f5bb4f26d367518a74bdd0448

sha1: 4bad58e28f5cd1049d54502d80aad83b26d09cc3

sha256: 5ab3740bdc2c7d7b8bcd6bcef350b6fe0d3130e081d3dff8413d2c04c47eb32d

sha512: 97ad9ec8e37abdf45ece1feaa5f3497b0f8ec673527108a87a3c6bb5b89e98acbe0692bcd3aa9c96e191d0622049c4ccdd0ee11e8491954ff23a11188cc2b618

PublicKey Algorithm: rsa

Bit Size: 4096

Fingerprint: 0d818abb088a6eadd59b3a46b1718fd809b4b5384ba59278985c0b08d1138b65

Found 1 unique certificates

⋮ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.
android.permission.READ_MEDIA_AUDIO	dangerous	allows reading audio files from external storage.	Allows an application to read audio files from external storage.
android.permission.READ_MEDIA_VIDEO	dangerous	allows reading video files from external storage.	Allows an application to read video files from external storage.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.
android.permission.BLUETOOTH_SCAN	dangerous	required for discovering and pairing Bluetooth devices.	Required to be able to discover and pair nearby Bluetooth devices.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.RECEIVE_USER_PRESENT	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
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.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.FLASHLIGHT	normal	control flashlight	Allows the application to control the flashlight.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.FOREGROUND_SERVICE_MEDIA_PLAYBAC	unknown	Unknown permission	Unknown permission from android reference
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

PERMISSION STATUS		INFO	DESCRIPTION
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.DISABLE_KEYGUARD	normal	disable keyguard	Allows applications to disable the keyguard if it is not secure.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
com.android.launcher.permission.READ_SETTINGS	unknown	Unknown permission	Unknown permission from android reference
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.CHANGE_WIFI_MULTICAST_STATE	normal	allow Wi-Fi Multicast reception	Allows an application to receive packets not directly addressed to your device. This can be useful when discovering services offered nearby. It uses more power than the non-multicast mode.
android.permission.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
android.permission.CHANGE_NETWORK_STATE	normal	change network connectivity	Allows applications to change network connectivity state.
android.permission.USE_FULL_SCREEN_INTENT	normal	required for full screen intents in notifications.	Required for apps targeting Build.VERSION_CODES.Q that want to use notification full screen intents.
android.permission.QUERY_ALL_PACKAGES	normal	enables querying any normal app on the device.	Allows query of any normal app on the device, regardless of manifest declarations.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	dangerous	mount and unmount file systems	Allows the application to mount and unmount file systems for removable storage.

PERMISSION		INFO	DESCRIPTION
android.permission.ACCESS_WIFI_STATE	unknown	Unknown permission	Unknown permission from android reference
android.permission.CHANGE_WIFI_STATE	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.ACCESS_ADSERVICES_TOPICS	normal	allow applications to access advertising service topics	This enables the app to retrieve information related to advertising topics or interests, which can be used for targeted advertising purposes.
com.applovin.array.apphub.permission.BIND_APPHUB_SERVICE	unknown	Unknown permission	Unknown permission from android reference
android.permission.CHANGE_NETWORK_STATE	unknown	Unknown permission	Unknown permission from android reference
com.ysxlite.cam.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference



FILE	DETAILS		
	FINDINGS	DETAILS	
assets/audience_network.dex	Anti Debug Code	Debug.isDebuggerConnected() check	
	Compiler	unknown (please file detection issue!)	
	FINDINGS	DETAILS	
classes.dex	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check network operator name check possible VM check	
	Compiler	r8	

FILE	DETAILS			
	FINDINGS	DETAILS		
classes2.dex	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check SIM operator check network operator name check possible VM check		
	Anti Debug Code	Debug.isDebuggerConnected() check		
	Compiler	r8 without marker (suspicious)		
	FINDINGS	DETAILS		
classes3.dex	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check		
	Compiler	r8 without marker (suspicious)		

FILE	DETAILS			
	FINDINGS	DETAILS		
classes4.dex	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.BOARD check possible Build.SERIAL check SIM operator check network operator name check		
	Anti Debug Code	Debug.isDebuggerConnected() check		
	Compiler	r8 without marker (suspicious)		
	FINDINGS	DETAILS		
	Anti-VM Code	Build.MANUFACTURER check		
classes5.dex	Compiler	r8 without marker (suspicious)		



NO	SCOPE	SEVERITY	DESCRIPTION
1	*	high	Base config is insecurely configured to permit clear text traffic to all domains.
2	*	warning	Base config is configured to trust system certificates.

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 1

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.

Q MANIFEST ANALYSIS

HIGH: 2 | WARNING: 7 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 5.0-5.0.2, [minSdk=21]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.

NO	ISSUE	SEVERITY	DESCRIPTION
2	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
3	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.
4	Service (com.ilnk.llnkService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	Service (com.ilnk.utils.killSelfService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_NOTIFICATION_LISTENER_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
6	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
7	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
8	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
9	Activity (com.amazon.aps.ads.activity.ApsInterstitialActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
10	Activity (com.amazon.device.ads.DTBInterstitialActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	com/apm/insight/h/a.java com/applovin/exoplayer2/l/q.java com/bumptech/glide/load/engine/exec utor/RuntimeCompat.java com/bumptech/glide/util/ContentLengt hlnputStream.java com/bykv/vk/openvk/component/vide o/api/f/c.java com/bytedance/sdk/component/a/i.jav a com/bytedance/sdk/component/embe dapplog/PangleEncryptUtils.java com/bytedance/sdk/component/f/d/f.j ava com/bytedance/sdk/component/f/d/f.j ava com/bytedance/sdk/component/utils/H omeWatcherReceiver.java com/ilnk/utils/IlnkCmdEnc.java com/ilnk/utils/StringUtils.java com/ironsource/environment/c.java com/lzy/okgo/utils/OkLogger.java com/mbridge/msdk/dycreator/a/a.java com/mbridge/msdk/dycreator/e/g.java com/mbridge/msdk/playercommon/ex oplayer2/util/AtomicFile.java com/mbridge/msdk/widget/FeedbackR adioGroup.java com/nicky/framework/utils/SIMCardMg r.java com/nicky/framework/utils/StringUtils.j ava com/yalantis/ucrop/util/EglUtils.java com/yalantis/ucrop/util/ImageHeaderP arser.java com/zxing/common/PlatformSupport

NO	ISSUE	SEVERITY	STANDARDS	Manager.java ឆ្លើងថ្លែស/ads/common/view/AutoNextLi neLinearLayout.java
2	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	com/applovin/exoplayer2/h/z.java com/ilnk/utils/StringUtils.java com/mbridge/msdk/playercommon/ex oplayer2/source/ShuffleOrder.java com/nicky/framework/utils/StringUtils.j ava sg/bigo/ads/common/utils/k.java
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	com/amazon/aps/ads/ApsConstants.jav a com/ilnk/bean/DevUserBean.java com/ilnk/bean/PushBean.java com/ilnk/constants/PushConfig.java com/ironsource/mediationsdk/adqualit y/AdQualityBridgeKt.java com/ironsource/mediationsdk/utils/Iro nSourceConstants.java com/mbridge/msdk/foundation/downl oad/core/DownloadCommon.java com/vungle/ads/internal/Constants.jav a com/vungle/ads/internal/model/Cookie .java com/vungle/ads/internal/task/CleanupJ obKt.java com/ysxlite/cam/constants/PushConfig .java com/zxing/decode/Intents.java
4	Debug configuration enabled. Production builds must not be debuggable.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/bumptech/glide/BuildConfig.java com/bumptech/glide/gifdecoder/Build Config.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/bykv/vk/openvk/component/vide o/api/f/b.java com/bytedance/sdk/component/d/c/c/ c.java com/bytedance/sdk/component/utils/e .java
6	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/applovin/mediation/adapters/ama zonadmarketplace/BuildConfig.java com/applovin/mediation/adapters/byte dance/BuildConfig.java com/applovin/mediation/adapters/goo gle/BuildConfig.java com/applovin/mediation/adapters/goo gleadmanager/BuildConfig.java com/applovin/mediation/adapters/iron source/BuildConfig.java com/applovin/mediation/adapters/iron source/BuildConfig.java com/applovin/mediation/adapters/min tegral/BuildConfig.java com/bytedance/sdk/openadsdk/BuildC onfig.java com/ilnk/bean/WifiSettingBean.java com/ilnk/constants/llnkConstant.java com/jirbo/adcolony/BuildConfig.java com/vungle/mediation/BuildConfig.java
7	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/adcolony/sdk/d1.java com/applovin/impl/sdk/utils/StringUtils .java
8	The file or SharedPreference is World Writable. Any App can write to the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/ironsource/environment/IronSour ceSharedPreferencesUtilities.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/bykv/vk/openvk/component/vide o/a/b/b/d.java

■ NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
----	------------	-------------	---------	-------------

***: *:** ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	14/24	android.permission.VIBRATE, android.permission.SYSTEM_ALERT_WINDOW, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.CAMERA, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.WAKE_LOCK, android.permission.RECORD_AUDIO, android.permission.READ_PHONE_STATE, android.permission.INTERNET, android.permission.ACCESS_WIFI_STATE, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION
Other Common Permissions	8/45	android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, android.permission.FLASHLIGHT, android.permission.FOREGROUND_SERVICE, android.permission.MODIFY_AUDIO_SETTINGS, android.permission.CHANGE_WIFI_STATE, android.permission.CHANGE_NETWORK_STATE, com.google.android.gms.permission.AD_ID

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

• OFAC SANCTIONED COUNTRIES

This app may communicate with the following OFAC sanctioned list of countries.

DOMAIN	COUNTRY/REGION	
www.ysxlite.com	IP: 43.138.210.73 Country: China Region: Beijing City: Beijing	
active.clewm.net	IP: 121.41.108.72 Country: China Region: Zhejiang City: Hangzhou	

Q DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.example.com	ok	IP: 93.184.215.14 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map

DOMAIN	STATUS	GEOLOCATION
outcome-ssp.supersonicads.com	ok	IP: 18.173.205.28 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
www.ysxlite.com	ok	IP: 43.138.210.73 Country: China Region: Beijing City: Beijing Latitude: 39.907501 Longitude: 116.397232 View: Google Map
github.com	ok	IP: 140.82.121.4 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
www.pangleglobal.com	ok	IP: 2.16.1.147 Country: Netherlands Region: Noord-Holland City: Amsterdam Latitude: 52.374031 Longitude: 4.889690 View: Google Map
outcome-crash-report.supersonicads.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
adc-ad-assets.adtilt.com	ok	IP: 192.229.202.78 Country: United States of America Region: New Jersey City: Newark Latitude: 40.735661 Longitude: -74.172371 View: Google Map
ssdk-sg.pangle.io	ok	IP: 212.77.167.240 Country: Germany Region: Bayern City: Regensburg Latitude: 49.014999 Longitude: 12.095560 View: Google Map
outcome-arm-ext-med-ext.sonic-us.supersonicads.com	ok	No Geolocation information available.
ssdk-va.pangle.io	ok	IP: 212.77.167.235 Country: Germany Region: Bayern City: Regensburg Latitude: 49.014999 Longitude: 12.095560 View: Google Map
adc3-launch.adcolony.com	ok	IP: 34.36.45.50 Country: United States of America Region: Texas City: Houston Latitude: 29.941401 Longitude: -95.344498 View: Google Map

DOMAIN	STATUS	GEOLOCATION
lf3-cdn-tos.bytegoofy.com	ok	IP: 47.246.46.225 Country: Italy Region: Lombardia City: Milan Latitude: 45.464272 Longitude: 9.189510 View: Google Map
active.clewm.net	ok	IP: 121.41.108.72 Country: China Region: Zhejiang City: Hangzhou Latitude: 30.293650 Longitude: 120.161423 View: Google Map
p1.i-lnk.com	ok	IP: 174.129.34.188 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map

A TRACKERS

TRACKER	CATEGORIES	URL
AdColony	Advertisement	https://reports.exodus-privacy.eu.org/trackers/90

TRACKER	CATEGORIES	URL
Amazon Advertisement		https://reports.exodus-privacy.eu.org/trackers/92
AppLovin (MAX and SparkLabs)	Advertisement, Identification, Profiling, Analytics	https://reports.exodus-privacy.eu.org/trackers/72
Facebook Ads	Advertisement	https://reports.exodus-privacy.eu.org/trackers/65
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
IAB Open Measurement	Advertisement, Identification	https://reports.exodus-privacy.eu.org/trackers/328
Mintegral	Advertisement, Analytics	https://reports.exodus-privacy.eu.org/trackers/200
Pangle	Advertisement	https://reports.exodus-privacy.eu.org/trackers/363
ironSource	Analytics	https://reports.exodus-privacy.eu.org/trackers/146

▶ HARDCODED SECRETS

POSSIBLE SECRETS "dev_sleep_key": "KeyDown" "dev_wakeup_key": "KeyDown" "dyStrategy.privateAddress": "privateAddress"

POSSIBLE SECRETS
"pppp_status_user_authenticated" : "Logged-in"
"pppp_status_user_authenticating" : "Authenticating"
"session_conn_p2p": "P2P"
"session_conn_rly" : "Relay"
"str_password" : "Password"
"str_session" : "Session"
VXUYBRMamhge5PldHXwCUhQsvqUwyGaK
Q7EHaqXEYxiQEOilyqjopxzkHRhZVKtw
1PTlaN9o47ZvO5QWBq3tjVop340dHl6h
vVWBcEJQjEsfNalmzVe1r7miASaPIW1B
JnlGisJqZLjO7zfwdKKMw91nRUtlhmzE
oaymDZ7pAEcbNFhv7Y0pKv8En2RbSAw
exdb2ky9NstGP6elq11NgBzvOAGjRaxw
BXJhCJIGpStJQsMIN6w6cfyx8EdHGsbw
I8KF2ZVrYmK9QbzsZWlXvJRb7XPAUhEH

POSSIBLE SECRETS
N6xF9rR52YV8YEOBA61RWKACjwLFpOal
GOJ9oRRABJfcwjAA770tm42MgykplS5Q
Mb83VhRFw0YfLpvsGxQ6UEzyZMUp7
9ll84e7XMJCEHu7uA5OKUKZwzRXjipC4
wCPzQVRdLc9fuoZbbzdyTQMs65DUcW8k
FJwhSbR0Dqb1wEJXVBdpfUEyE2PwmXT5
1kYj9up9VehuFRcMC7DoHBWV3d6qFcAR
Un7ie3hNu6oSxsviCElGpaw70qJ7D3pr
6y0uOKezMm2TBG2XREAais4zy5M1tLxd
FDV889hBrMc5nJiB7wS69W2fLt8zA89o
v4tKPq3EceuOa5aRsmEiNo1tTprRM6C7
aad37172d5cdd94b403337275d1087b9619df33290
oK8ltqR6UoxvlOFM7x85SOaiyNHULhPY
iVBORw0KGgoAAAANSUhEUgAAABQAAAAUCAMAAAC6V+0/AAAAIVBMVEUAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
yf08nX9dlZfcKypKRld4zDkH94BCZAU7

POSSIBLE SECRETS

PRV2czZbjjW7Ot8uaJuxnRGNdlXO90ph
jpK43NGJIXClE5ie7D0g7Fa1Rpa7kANX
WM0zVtm2JGvaa9vSTXp0h2YRnQYxQrEK
U1b0Njqb3LWazyJmLiNcKHMDagE8OpYs
Whp7rDnlG0MZliYb9hz51Us4d
les1EbCUxP4xgOdfeUltBKAu87PDHxqp
poMRnmB7rAFaE3bMUxl6O2dxmVQ0Moe
p5EAmOIUOepdn0Id4WtjwtBc6P8vGfuC
W9Yqfcw4l1PfnAsasbj5MfnOF9oeiem1
stwUo5SqMIMCevvnzS9lvu5YLcfkOLDd
f5llxAtAKiBQqbeb00Dlw30sTyOB6Nip
iVBORw0KGgoAAAANSUhEUgAAABAAAAAQCAYAAAAf8/9hAAAAAXNSR0IArs4c6QAAAHRJREFUOBFjYBjygBmHD0SA4puhchdxqMEpLAyUAWn6BsSW0FXhkEDW7IxDDU5 hkOYLQAyymWjNjFDjmID0bSCWB+IrQPwBiPGBx0DJeCD+B9JINUCWF9BtpygQYYYhG0lwGrGFwVugSU5AfByIVWGmDmMaANyNFVTVvpxwAAAAAEIFTkSuQmCC
L0nZjQMyNIt0WlCmUM7oX7gpc1lDkDOo
Pl2vgN3HXqbbKxjZzlk4bg0eix12xhJu

POSSIBLE SECRETS
GuFHMY1Ngi3Kc2EktfHyZFCwamvVcTYP
n5EonvV2d0ynVphuWlfrU3PhJk0DBM6W
jWJWqJI6vm3EcSkucHo8Z2hc4QqQU5eN
kJ80Vw1lOC47iRluFhEDeBzKcKjW1m8D
4d1rNabt9wBbosJplZDA5yWTcQ5bg7DE
o4JUlXa2QWu1MieYLvsMRT696KEqR
AQLjxK2FjJRwwoaJIN65VrZWNOsgzmXU
FcsNCE2HBJuao8xA2rTiJTUxq38jGWif
a1b7a7ea69985aec39f305fb8b08309a0686940e
i1sqGOju2LE8Q92QQNgFTaNu0rUo1z4f
kQTCJIS50BSCbahTVqCDmy8LW1L9RVvG
vKITx3IWvQKkFLmjQGxCBJXBbaEzbyA1
IY1PhTJan2YjTy3m27KNizUeB7qtWqJm
r4XHqvELKUQNiUGngs8vqNM0Mk3b9MGe
qn8tosrMnBeOYh3nA69X7hpHPvfrKSD7

POSSIBLE SECRETS
BjlmtcQqBka41jhChDLZKaESgBphWA9m
b7ab2f95043a05f760c84680
pTWsWF2qz8Xr2QvNaoeX4WQy7B5K1AFD
WI5YCVlpnY9sS2vUV4hGrlGwgmlaf2lo
QXuoBnzEZEqlDLe5TpAidegf9xy2rJp2
dru3glT9ekJ0g4QSSusKvlCYyzfTBGaa
2VeddHnoq1PdFvEHeLIEgk846BKmCK6O
zA4klKNJM0QxWDxEFTSTi5yKhMV68
EvQoHUlErOdPjfZNSaWf5ex2DDXDJXA1
hGyVADXG58acDgE3vlJwpiBKlvJlQGRP
eivXn7WqkaVyJ2amCalRVsu1nM81zzOL
AjQwhKg0BmylW2zY2qnRPlrsdpwDD7xX
UwkWzl2MRtUAPiPmZ2pCt01Egbad
fQADRcl3z4l9sbyUvoxt9O6e4jXdGtkl
2B7qWnr6lboK1kzNzncdoP0B0brMv5Si

POSSIBLE SECRETS
xnB3F8eRzgUElZJXVWbAPi1tu19rGp71
Jjxe8gs2e3QRovgCJLhIxlujBEulNGa6
Kv65PDKGzQbP8opzJD3T0Bs4qFkMuEvW
bCA0WV7g9cnA4ltB5qqjp12FxZMghyDz
2QVULSr2cnp6GdJqlDXRW8b5XXXh3hMX
5xFyhJyAmXwpndJ9EoKqTFqqLl0O0t2g
WzMdgVuSy86surt8IbRNO89xVpYcFvZR
mmPym4lpWgK7OAi14ovsdO61E0NwpnnM
ndgFEZBTUbwthgxyC0k1ffQbXbGUnRaA
Fa9eXDyly4elyWfec912IKE0nqoR5HQV
UwpbEbRNl9IMKeiJ6uSiSZky6ATbVFhh
MZbjV39kBt4hAqLFGwVFLXlTEV84r4gZ
rYxOc7Ypr1bQ7KOGmw9sN058klB7gerB
BNF7ZQJYQPI9GTH2pfcSvMp6af8oi
klaQKGqX2ZTqEjvfJkZOl1WwOBoH9uFY

POSSIBLE SECRETS
LRipwKypnEKMqg6PamR7G8YuQckBwe
a6e46478453c9aeaca5af624
XKBE22ujheeLcTYagdBtfv4d5l35c1GL
B3EEABB8EE11C2BE770B684D95219ECB
zxcvbnmlkjhgfdsaqwertyuiopQWERTYUIOPASDFGHJKLZXCVBNM1234567890
dTodKdBY68fO6HNBSU3LN7qZJ4nOCEpk
9e896LaDKrRwUGEGxpikTCFLA2EDc0Ve
9jmWu3moBjPGR65ZxocrWcXRtVvlqMhB
Llt45BVzQE0lSVvxtilRjadurhGFSSrG
iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAAXNSR0IArs4c6QAAAMRJREFUWAljYBgFoyEw0kOAmYwAcAbqmQbEQkB8igz9FGnxB+r+BcT/gfgPEAsAM d0AsuUgB5yhm81Ai9AtvwUUk6KXAwaV5TcH0ufD03JGLAkJFOdrgJgFKvcWSC8A4i9QPrnUX6DGHUB8Gp8BHEDJD0AMyma0wF+B5qKUHUxAgQEFsGCGOelHkBEPxLSMA lAIEwToeZ+uOQDmulFHDOqQoGtlhCsk6FodY3ME3RskMEeAmmTbgTgXJjBKj4bAaAhQEgIA28ZhUJU6FRwAAAAASUVORK5CYII=
iVBORw0KGgoAAAANSUhEUgAAAAwAAAAMCAQAAAD8fJRsAAAAVkIEQVR4AWMgBNgYJjK8A8KJQBYK6GJ4zBDNEA0kO1ElPgIFQSCK4TWqxBcGczBtDmQhAUuGBCRoChPmZPjF8B8JfoM5QADIQYUC5EowM1xGET6HNygAklo2DuA7sTMAAAAASUVORK5CYII=
1P4e8Svw6pgZkfS1AU7Ku11MIWhAZ0aY
KlezWCwDulS1StSn2NonTUsqgHFd0zlY
7iAt0ZQxlGPQ5tCLEuhHxDXKOxsROBn5

POSSIBLE SECRETS
A9eN1weHgCPL1SkQ3ZXjYtrHuOy08x6Y
xbTSMp8fvBEENljIQe5QRmpFAlAe0spq
sp7WuMlrQg67lklbNPhafgU9zVWwTylU
5zJBssfwfWeqrXRnFZsUzQPBIx8wM7U1
JEnYl3ig6b1G3QZnd7pVPdvbWtuLiuax
GcMaFESaYtqWHDueobHkP3OuSFimx
uaXBHv2Fpyp6t9CjlnIdC1lJtF0IP5s0
8DkF2pCK7gEKj1aPHzeGQpXB8g2QomLh
xZfMamQuDxA6bTypucZ197RYNE4mvlcN
KEGdoxZZnAdDUnYCV96i9ePmYlw0nVcs
dsOpW9WfLYJghusiq4Ru5jQxxgYMnVUV
i2lfi3JYyaWanuhNA9EoVixSZwQkBGPJ
KhrHqa8env5LHobs7dTfjp4HGZPf1i5f
DP3a2sR6Ao5znMBkyRuDzqvSCPyaW43t
6rGRVoRQr925zwi8UOEHhi5JTPDCThCe

POSSIBLE SECRETS
DvSn6PhmC3i7LdpG0vBUuRZmjagS5as7
SocWGKvTrb27mU7l6HYZWtCOqe8vN7We
ErY0P3cLXtwrTQQ8AaevOJsLoOIjf8Vw
ac6c0eb7d1dfb73d9e5cd82f
tZylzHWr5GKf5F95sWHTJWAqY8lomPh4
iVBORw0KGgoAAAANSUhEUgAAABIAAAASCAQAAAD8x0bcAAAAgklEQVR4Ac3KtYECYRgA0UnxAqAALMI72fSrYf8M74jjKGZDOll3l4g36dDFAYXiQKkJH6ygDxMK/WFhoLhg YPGmwM5bhgAMvW1Hjo6FlqSw0Ml5YiGEBIsnOWvuTAnNeLlg44QUdCJhi4lVkMmWiGCVJL89aaWTRqTPH9+C3vRpygZ9roDjp6hXFQAAAABJRU5ErkJggg==
5OO1eWJNP7Y3s5cQVhBQzuf4m1TAFPYu
7XnL499JY0auPeNFsvc8kwtFVWOKtFwM
7lyHNSQ2TJBMgpMVEgH3C5YFRcP1ce7U
bPkhSE8L0qTQU8qqVG5cBeS4akAeFCpX
dejWMVKCcsRHbrwAIECa6aRABNrvRLL1
QDtKUFo4Pv7jZ7qumv108KMzWf6HrSMn
XWwbNIOGXItiEE2sGKxxfB9q5lH48KSv
DtHbWGOE2Bmy5zeMr4BSgc5m3XVIvhqE
3kaHypJVzQjnFbgNDhrnWnyYOdOCg92b

POSSIBLE SECRETS
Xxl4rLnj16XDfkQUiM3437m5W6qonc5R
59L0PM8TZSDfga3AwgwmMzwLrxdyp45T
eS8IZAPFQFjEXoH0I8GlghTr6fGbdCZa
1iDxwsFxF9YiCc2SPrS2klGyrj8KvyqU
tuFyi1rHy9z46G0g3HP9J8Pe4Wglo7s9
1AEGGiZtK9izNwxj0gdNwiRX4yxGSLbl
lPif8zo0BCGymla9nsJJXRn9Vdfcrwfz
1RYqQKBl4tHo2l91LJlKc5yEyLaxvrL0
aVnA9Ux0owpYjW5hlcDkLBlQBKS6Kuco
AkiufmiMzZJvhyS77AiglOXb5e3YRP2V
ccCRkU4tJU1cPhlyS12s2rOBaxNg0sA2
Xt2DRLIKFdB95NsINvyqeyDnMxOOuDLx
p5IIOLlp1B1ZcinDN0X6ynPo7iUU6KYH
xulkP76phNp8oPrFkycOZ9oAWaaFvsfs
5HWyWxmgcaxBLo1LpD3PpaOIjtbRMHJC

POSSIBLE SECRETS
LLxQm2Zb2cHXH3GFymslhrLJVNNE7YVf
k9lbPcfog7a2vud71ZD1yiSptuKC
qcYJgrhXwK3F7gc49b8OJRulLZ0tc
fXviZ9AMoZT5h2KBZwjslTMVylobOTux
PumDfveAcRoz4mAMU1oiRh2l021HXL7u
qXEMgnv7Ct425l7ln8PWxhOPFYVbEYpB
mcSvbra1TWloRdhWTFL80td7BovB7Z6D
u0FGaDlimXxXG0l3UqPLAtx16Sc8Y059
u680PltdmSCtrwUArgQMKOt5dGhFKyFy
XAoGi5mGaFQZFqWDdkVsCV3Av2NgJGYo
pR9Fkr1wWPG0d9ySETcIXHMYi8wcMlk0
9G2r59BoUl91An7yhO6AwlMh4F2sXT3r
Sw9TLHolawUN9KVNZQEO3EMAiDKtc0hD
s90Sw2xfipZOkULUf4YVkqTv1ri2JEFZ
I5FSM6v9D3qkRXnarws6dVsmQqtQoJdF

POSSIBLE SECRETS
MDpcepjwzWMs517m4lh6aUQSJk
DwqRJ6bMYzXyiD2Eugn3dkRE0I23BFLv
EyZhmJMsuDDThnYHJcpUVdPGrs5jP
9PVJQ3IXsUcABNIhPZfYMIRDAFEvqeV3
eeDLrDiwzyZn1GaqUg9DZO06uYqn8isf
9xnRWvfnvAuFWSokCiPir6t5eweLHrnN
2vimyyNbMv6AohadWhJSDQSQPpWOARjH
8HaEwRmcLljD6jWZTmAaPx2QrUAiOCOo
18JvwLOKolmi3RAulpcsWcjyGiEhXJWG
W4gBMubxKiZM5LLivtLPs396PBqN8ReM
Y6chWCHiEHN0DdaKB8VVwvMQijKJ1ylC
YNAb6cApL15ElRgBdl6o6l27RW0RMDqg
THEbbJWzjj3eFDlXZnSzsYrmSmbq8w3u
UFa447OZZwRnjgAwYt6DClQrKKYck
GEphX9PDUn8ir5euMldeMTZrm9gVIFzw

POSSIBLE SECRETS
0vF5Kqqkw0y14nBhXHX4F0aBgr7OScbz
uWFt37UVBdA9eGMxe0FCLaB7SA4moHLj
3teRnM8c4jgHocWnqrQSqB4Xqv7CtSGf
cTyjqlp8UNOQyLJMZAg4XzmxFMTsV66P
O6PB2WDRc4LRgt1IrB9ncLf4vcwP07EY

PGh0bWw+PGhIYWQ+CiAgICA8bWV0YSBuYW1IPSJ2aWV3cG9ydClgY29udGVudD0id2lkdGg9ZGV2aWNILXdpZHRoLCBpbml0aWFsLXNjYWxIPTEiPgogICAgPHN0eWxIPgo glCAglCAglC5jb250YWluZXlgewoglCAglCAglCAglCBmbGV4LWRpcmVjdGlvbjogY29sdW1uOwoglCAglCAglH0KCiAglCAglCAgLMZsZXgtY29udGFpbmVylHsKlCAglCAglCAglCAglCAglC AgZGIzcGxheTogZmxleDsKICAgICAgICAgICAgICAgYWxpZ24taXRlbXM6IGNlbnRlcjsKICAgICAgICAgICAgICAgZmxleC1kaXJIY3Rpb246IGNvbHVtbjsKICAgICAgICAgICAgICAganVzdGImeS1jb sZHMtZWxsaXBzaXMgewoglCAglCAglCAglCAglCBkaXNwbGF5OiBpbmxpbmUtYmxvY2s7CiAglCAglCAglCAglCAglHBvc2l0aW9uOiByZWxhdGl2ZTsKlCAglCAglCAglCAglCAglCAgd2lkdGg6lDg CAgICAgICAgICAgYmFja2dyb3VuZDogI0E3QTdBNzsKICAgICAgICAgICAgYW5pbWF0aW9uLXRpbWluZy1mdW5jdGlvbjogY3ViaWMtYmV6aWVyKDAsIDEsIDEsIDApOwogICA ICAgICAgYW5pbWF0aW9uOiBsZHMtZWxsaXBzaXMyIDAuNnMgaW5maW5pdGU7CiAgICAgICAgICAgICAgICAgICAgICAUGRzLWVsbGlwc2lzIGRpdjpudGgtY2hpbGQoMykgewoglCAglCAglCAglCBsZWZ0OiAzMnB4OwoglCAglCAglCAglCBhbmltYXRpb246IGxkcy1lbGxpcHNpczlgMC42cyBpbmZpbml0ZTsKlCAglCAglCB9CgoglCAglCAglCSsZHMtZWx saXBzaXMgZGl2Om50aC1jaGlsZCg0KSB7CiAglCAglCAglCAglCAglGAlCAglGAlCAglCAglCAglCAglCAglCAglGFuaW1hdGlvbjogbGRzLWVsbGlwc2lzMyAwLjZzlGluZmluaXRlOwogl 5zZm9ybTogdHJhbnNsYXRlKDI0cHgsIDApOwoglCAglCAglCAglCB9CiAglCAglCAglCAgPC9zdHlsZT4KPC9oZWFkPgoKPGJvZHk+CiAglCA8ZGl2IGlkPSJsb2FkaW5nX3dyY XBwZXIiIHN0eWxIPSJkaXNwbGF5OiBmbGV4O2ZsZXgtZGlyZWN0aW9uOiBjb2x1bW47anVzdGlmeS1jb250ZW50OiBzcGFjZS1iZXR3ZWVuO2hlaWdodDogMTAwJTsiPgo8Z Gl2IGNsYXNzPSJjb250YWluZXIgZmxleC1jb250YWluZXIiIHN0eWxlPSIKICAgIGZsZXg6IDE7CiI+CiAgICAgICAgPGRpdiBjbGFzcz0iZmxleC1jb250YWluZXIiIHN0eWxlPSIKICAgI GZsZXg6IDE7CiI+CiAgICAgICAgICAgICAgIDxzdmcgd2lkdGg9IjIzNiIgaGVpZ2h0PSI0NCIgdmlld0JveD0iMCAwIDIzNiA0NCIgZmlsbD0ibm9uZSIgeG1sbnM9Imh0dHA6Ly93d3cud zMub3JnLzIwMDAvc3ZnIj4KlCAglCAglCAglCAglCAglDxwYXRoIGQ9lk0zNy44MDYzIDMwLjI4NTRWMTAuNDI4NUwyMC42MTI5IDAuNVY4LjExNjM2TDI3LjM1MDggMTIuM DA5NUMyNy41OTQ1IDEyLjE0NTUgMjcuNjAwMiAxMi41MjUyIDI3LjM1MDggMTIuNjYxMkwxOS4zNDM1IDE3LjI4NTVDMTkuMDk5OCAxNy40MjcxIDE4LjgxNjQgMTcuND E1OCAxOC41ODk4IDE3LjI4NTVMMTAuNTc2OCAxMi42NjEyQzEwLjMzMzEgMTIuNTI1MiAxMC4zMjc0IDEyLjE0NTUgMTAuNTc2OCAxMi4wMDk1TDE3LjMxNDcgOC4xMjI

wMlYwLjUwNTY2OEwwLjExNTY0NiAxMC40Mjg1VjMwLjl4NTRWMzAuMTk0N1YzMC4yODU0TDYuNzExOTMgMjYuNDc3MlYxOC42OTY1QzYuNzA2MjYgMTguNDE4OCA3 PQSSIBIDE45E0RETES1y4yNzg2MiAxOC4zNzM1TDE1LjI4NiAyMi45OTc3QzE1LjUyOTYgMjMuMTM5NCAxNS42NjU2IDIzLjM4ODcgMTUuNjY1NiAyMy42NDk0VjMyLjg5 NZIDMTUUNICXMyAZMy4xNZU1IDE1LIM0ODMgMZMuMZCZOSAXNS4xMDQ2IDMZLIIVNIVMOC4ZNIY2NyAyOS4ZMZM0TDEUNZCWMZggMZMUMTQXNUWXOC45Nik1IDQZL jA3TDM2LjE2ODUgMzMuMTQxNUwyOS41NjA5IDI5LjMzMzRMMjluODlyOSAzMy4yMjY1QzlyLjU4NDkgMzMuMzY4MiAyMi4yNTA2IDMzLjE4NjkgMjluMjU2MyAzMi44OT c5VjlzLjY0OTRDMjluMjU2MyAyMy4zNzE3lDlyLjQwOTMgMjMuMTl4MSAyMi42MzU5lDlyLjk5NzdMMzAuNjQzMyAxOC4zNzM1QzMwLjg4MTMgMTguMjl2MiAzMS4yMTU 2IDE4LjQxMzIgMzEuMjEgMTguNzAyMlYyNi40ODI5TDM3LjgwNjMgMzAuMjg1NFoilGZpbGw9liM0RDRENEQiPjwvcGF0aD4KlCAglCAglCAglCAglCAglCAglDxwYXRoIGQ9lk0xN S4wOTkgMzMuMjI2Mkw4LjM2MTA2IDI5LjMzM0wxLjc2NDc4IDMzLjE0MTJMMTguOTYzOCA0My4wNjk2VjlxLjMwODZMMC4xMTU3MDcgMTAuNDI4MVYzMC4yODVWM zAuMTk0NFYzMC4yODVMNi43MTE5OSAyNi40NzY5VjE4LjY5NjJDNi43MDYzMiAxOC40MTg1lDcuMDM1lDE4LjIyMDEgNy4yNzg2OCAxOC4zNzMxTDE1LjI4NiAyMi45OTc0 QzE1LjUyOTcgMjMuMTM5IDE1LjY2NTcgMjMuMzg4NCAxNS42NjU3IDIzLjY0OTFWMzIuODk3NUMxNS42NzE0IDMzLjE3NTlgMTUuMzQyNyAzMy4zNzM1IDE1LjA5OSAz My4yMjYyWilgZmlsbD0ilzRDNEM0Qyl+PC9wYXRoPgoglCAglCAglCAglCAglCAgPHBhdGggZD0iTTE4Ljk2MzcgNDMuMDY5NkwzNi4xNjl4lDMzLjE0MTJMMjkuNTYwOSAyO S4zMzNMMjluODIyOSAzMy4yMjYyQzIyLjU4NDkgMzMuMzY3OCAyMi4yNTA1IDMzLjE4NjUgMjluMjU2MiAzMi44OTc1VjIzLjY0OTFDMjluMjU2MiAyMy4zNzE0IDIyLjQwOTI gMjMuMTl3NyAyMi42MzU5lDlyLjk5NzRMMzAuNjQzMiAxOC4zNzMxQzMwLjg4MTlgMTguMjl1OCAzMS4yMTU2lDE4LjQxMjggMzEuMjA5OSAxOC43MDE4Vjl2LjQ4MjVM MzcuODA2MiAzMC4yOTA3VjEwLjQyODFMMTguOTYzNyAyMS4zMDg2VjQzLjA2OTZaliBmaWxsPSJibGFjayI+PC9wYXRoPgogICAgICAgICAgICAgICAgPHBhdGggZD0iTTIwL jYxMjkgMC41VjguMTE2MzZMMjcuMzUwOCAxMi4wMDk1Qzl3LjU5NDUgMTluMTQ1NSAyNy42MDAyIDEyLjUyNTlgMjcuMzUwOCAxMi42NjEyTDE5LjM0MzUgMTcuMjg1 NUMxOS4wOTk4IDE3LjQyNzEgMTguODE2NCAxNy40MTU4IDE4LjU4OTggMTcuMjg1NUwxMC41NzY4IDEyLjY2MTJDMTAuMzMSAxMi41MjUyIDEwLjMyNzQgMTIuMT Q1NSAxMC41NzY4IDEyLjAwOTVMMTcuMzE0NyA4LjEyMjAyVjAuNTA1NjY4TDAuMTE1NjQ2IDEwLjQyODVMMTguOTYzOCAyMS4zMDIMMzcuODExOSAxMC40Mjg1TDIw LjYxMjkgMC41WilgZmlsbD0ilzgwODA4MCI+PC9wYXRoPgoglCAglCAglCAglCAglCAgPHBhdGggZD0iTTU5LjY3NDYgMjMuODUyN0M1OS42NzQ2IDI1Ljg1MzlgNTguNTU4 MiAyNy4yODEyIDU2LjlxNzggMjcuMjgxMkM1My43MyAyNy4yODEyIDUyLjcwNDMgMjUuOTM4MiA1Mi43MDQzIDIzLjkzNzdWMTEuNzA4NUg0Ny42NDk0VjIzLjc2NzdDN DcuNjQ5NCAyOC41MzkzIDUwLjUwNTUgMzEuMzM4NyA1Ni4yMjM0IDMxLjMzODdDNjEuOTA3NCAzMS4zMzg3IDY0Ljc0MDggMjguNDgyNiA2NC43NDA4IDIzLjc2NzdW MTEuNzA4NUg1OS42ODU5VjlzLjg1MjdINTkuNjc0NloiIGZpbGw9ImJsYWNrIj48L3BhdGg+CiAglCAglCAglCAglCAglCAgCABcF0aCBkPSJNNzYuNDcxOSAxNS45MDc4Qzc0LjQ 0MzIgMTUuOTA3OCA3My4wNDM1IDE2Ljc2MzUgNzEuOTU1NCAxOC4zMzIINzEuODcwNFYxNi4zMzg1SDY3LjM4MjJWMzAuOTY0OUg3Mi4wNDA0VjJyLjg3ODJDNzIuMD QwNCAyMS4wNzYxIDczLjA3MTggMTkuNzg5NyA3NC42MTMyIDE5Ljc4OTdDNzYuMTI2MyAxOS43ODk3IDc2Ljg5NyAyMC44NDk0IDc2Ljg5NyAyMi4zOTA4VjMwLjk2NDII ODEuNTU1MIYyMS40NTAxQzgxLjU2MDggMTguMTkxNiA3OS42NzM3IDE1LjkwNzggNzYuNDcxOSAxNS45MDc4WilgZmlsbD0iYmxhY2siPjwvcGF0aD4KICAgICAgICAgICA glCAgIDxwYXRoIGQ9lk04OC42MjE2IDEwLjUzNjllODMuOTYzNFYxNC4zMTFIODguNjlxNlYxMC41MzY5WilgZmlsbD0iYmxhY2siPjwvcGF0aD4KlCAglCAglCAglCAglCAglCAglDx 0aCBkPSJNOTYuODlxNyAxMS43MDg1SDkyLjl3NjhWMTYuMzM4NEg5MC4zMzNWMjAuMTEyNkg5Mi4yNzY4Vjl3LjExMTJDOTluMjc2OCAzMC4yNTY0IDk0LjlyMDYgMzEu MTQwNCA5Ni45MzUgMzEuMTQwNEM5OC4xOTMxIDMxLjE0MDQgOTkuMDc3MSAzMS4wMjcxIDk5LjQ3OTQgMzAuOTEzN1YyNy41MTM2Qzk5LjMwOTQgMjcuNTEzNi A5OC44NTA0IDI3LjU0MTkgOTguNDQ4MSAyNy41NDE5Qzk3LjQ1MDcgMjcuNTQxOSA5Ni44MjE3IDI3Ljl1ODYgOTYuODlxNyAyNi4xMTM4VjlwLjExMjZIOTkuNDc5NFYxN i4zMzg0SDk2LjgyMTdWMTEuNzA4NVoilGZpbGw9lmJsYWNrlj48L3BhdGg+CiAglCAglCAglCAglCAglCA8cGF0aCBkPSJNMTA5LjM5MSAyMi41NjY1QzEwOC45MzlgMjMuOT k0NiAxMDguNTM1IDI1LjkzODMgMTA4LjUzNSAyNS45MzgzSDEwOC40NzIDMTA4LjQ3OSAyNS45MzgzIDEwOC4wMTkgMjMuOTk0NiAxMDcuNTY2IDIyLjU2NjVMMTA1NjVMMTA1LjU2NjVMMTA1NjVMMTANJVMMTANJVMMTANJVMMTANJVMMTANJVMTANJVMTANJVMTANJVMTANJVMTANJVMTANJVMTANJVMTANJVMTANJVMTANJVMTANJVMTANJVMTANJVMTANJVMTANU5NCAxNi4zMzg2SDEwMC42ODFMMTA0Ljk5MyAyNy41OTg4QzEwNS41OTQgMjkuMTQwMiAxMDUuODc3IDMwLjAwMTUgMTA1Ljg3NyAzMC42MjQ5QzEwNS44NzcgNzC42MjQ5QzEwNS44NzcqNzc42MjQ5QzEwNS44NzcqNzc42MjQ5QzEwNS44NzcqNzc42MjQ5QzEwNS44NzcqNzc42MjQ5QzEwNS44NzcqNzc42MjQ5QzEwNS44NzcqNzc42MjQ5QzEwNS44NzcqNzc42MjQ5QzEwNS44NzcqNzc42MjQ5QzEwNS44NzcqNzc42MjQ5QzEwNS44NzcqNzc42MjQ5QzEwNS44NzcqNzc42MjQ5QzEwNS44NzcqNzc42MjQ5QzEwNS44NzcqNzc42MjQ5QzEwNS44NzcqNzc42MjQ5QzEwNS44Nzc42MjQ5QzEwNS44Nzc42MjQ5QzEwNS44Nzc42MjQ5QzEwNS44Nzc42MjQ5QzEwNS44Nzc42MjQ5QzC4MjQ5QzC42MjQ5QzMzEuNjlyMyAxMDUuMzMzIDMyLjE2NjMgMTAzLjk2MiAzMi4xNjYzSDEwMi4zNjRWMzUuNzkzMUgxMDUuMzlDMTA4LjMzMSAzNS43OTMxIDEwOS43MzEgMzQuNTkxNy AxMTAuOTA0IDMxLjE2MzNMMTE1Ljk1OSAxNi4zMzI5SDExMS4zMDFMMTA5LjM5MSAyMi41NjY1WilgZmlsbD0iYmxhY2siPjwvcGF0aD4KlCAglCAglCAglCAglCAglDxwYX RoIGQ9Ik0xMjluNzI1IDMxLjE4MDZWMTluNjA0MUgxMjUuNTI4VjI4Ljc2NzhIMTMzLjk0NVYzMS4xODA2SDEyMi43MjValiBmaWxsPSJibGFjayI+PC9wYXRoPgogICAgICAgIC AgICAgICAgPHBhdGggZD0iTTE0Mi45MyAzMS40NjE4QzE0MS41NTcgMzEuNDYxOCAxNDAuMzc1IDMxLjE2ODUgMTM5LjM4MyAzMC41ODE5QzEzOC4zOTcgMjkuOTg5 MyAxMzcuNjM1IDI5LjE1NzkgMTM3LjA5NyAyOC4wODc1QzEzNi41NjUgMjcuMDExMiAxMzYuMjk5IDI1Ljc1MDQgMTM2LjI5OSAyNC4zMDUxQzEzNi4yOTkgMjluODc4IDE zNi41NjUgMjEuNjIwMiAxMzcuMDk3IDlwLjUzMThDMTM3LjYzNSAxOS40NDMzIDEzOC4zODUgMTguNTkzNyAxMzkuMzQ3IDE3Ljk4M0MxNDAuMzE0IDE3LjM3MjIgMTQ xLjQ0NSAxNy4wNjY4IDE0Mi43MzkgMTcuMDY2OEMxNDMuNTI1IDE3LjA2NjggMTQ0LjI4NyAxNy4xOTY4IDE0NS4wMjUgMTcuNDU2OUMxNDUuNzYzIDE3LjcxNjkgMTQ 2LjQyNSAxOC4xMjUxIDE0Ny4wMTEgMTguNjgxNEMxNDcuNTk4IDE5LjIzNzcgMTQ4LjA2MSAxOS45NjAzIDE0OC4zOTkgMjAuODQ5M0MxNDguNzM4IDIxLjczMjEgMTQ4 LjkwNyAyMi44MDU1IDE0OC45MDcgMjQuMDY5M1YyNS4wMzA4SDEzNy44MzJWMjluOTk5SDE0Ni4yNDIDMTQ2LjI0OSAyMi4yODU0IDE0Ni4xMDQgMjEuNjUzNSAxND

UuODE0IDIxLjEwMzJDMTQ1LjUyNCAyMC41NDY5IDE0NS4xMTYgMjAuMTA4NSAxNDQuNTkgMTkuNzg4QzE0NC4wNjkgMTkuNDY3NSAxNDMuNDU5IDE5LjMwNzMgM FQSS1BJAx SECRETS ZEOMS45OTUgMTkuMzA3MyAxNDEuMzMgMTkuNDk0NyAxNDAuNzYyIDE5Ljg2OTZDMTQwLjE5OSAyMC4yMzg1IDEzOS43NjQgMjAuNzIyMyA xMzkuNDU2IDIxLjMyMDIDMTM5LjE1MyAyMS45MTM1IDEzOS4wMDIgMjluNTU3NSAxMzkuMDAyIDIzLjl1MjlWMjQuODQwM0MxMzkuMDAyIDI1Ljc3MTUgMTM5LjE2N SAyNi41NjM3IDEzOS40OTIgMjcuMjE2OEMxMzkuODI0IDI3Ljg2OTkgMTQwLjI4NyAyOC4zNjg3IDE0MC44OCAyOC43MTM0QzE0MS40NzIgMjkuMDUyIDE0Mi4xNjUgMjku MjlxNCAxNDluOTU3IDI5LjlyMTRDMTQzLjQ3MSAyOS4yMjE0IDE0My45MzkgMjkuMTQ4OCAxNDQuMzYzIDI5LjAwMzdDMTQ0Ljc4NiAyOC44NTI1IDE0NS4xNTlgMjguNjl 4OCAXNDUuNDYgMjguMzMyNUMxNDUuNzY5IDI4LjAzNjEgMTQ2LjAwNSAyNy42NzAzIDE0Ni4xNjggMjcuMjM0OUwxNDguNzM1IDI3LjY5NzVDMTQ4LjUyOSAyOC40NT M0IDE0OC4xNiAyOS4xMTU1IDE0Ny42MjggMjkuNjg0QzE0Ny4xMDlgMzAuMjQ2MyAxNDYuNDQgMzAuNjg0NyAxNDUuNjQyIDMwLjk5OTJDMTQ0Ljg1IDMxLjMwNzYg MTQzLjk0NiAzMS40NjE4IDE0Mi45MyAzMS40NjE4WilgZmlsbD0iYmxhY2siPjwvcGF0aD4KlCAglCAglCAglCAglCAglDxwYXRoIGQ9lk0xNjMuNDM2IDE3Ljl0ODJMMTU4LjM 4MyAzMS4xODA2SDE1NS40ODFMMTUwLjQyIDE3LjI0ODJIMTUzLjMzMUwxNTYuODYgMjcuOTY5NkgxNTcuMDA1TDE2MC41MjQgMTcuMjQ4MkgxNjMuNDM2WilgZmls bD0iYmxhY2siPjwvcGF0aD4KlCAglCAglCAglCAglCAglDxwYXRoIGQ9lk0xNzEuNTE1lDMxLjQ2MThDMTcwLjE0MyAzMS40NjE4lDE2OC45NiAzMS4xNjg1lDE2Ny45NjkgMz Auntgxoumxnjyuotgzidi5Ljk4otmgmty2LjiymSayoS4xntc5idE2nS42odmgmjgumdg3numxnjuumtuxidi3Ljaxmtigmty0Ljg4nSaynS43ntA0idE2nC44odugmj QuMzA1MUMxNjQuODg1IDlyLjg3OCAxNjUuMTUxIDlxLjYyMDlgMTY1LjY4MyAyMC41MzE4QzE2Ni4yMjEgMTkuNDQzMyAxNjYuOTcxIDE4LjU5MzcgMTY3LjkzMiAxNy45 ODNDMTY4LjkgMTcuMzcyMiAxNzAuMDMxIDE3LjA2NjggMTcxLjMyNSAxNy4wNjY4QzE3Mi4xMTEgMTcuMDY2OCAxNzIuODczIDE3LjE5NjggMTczLjYxMSAxNy40NTY5Q zE3NC4zNDggMTcuNzE2OSAxNzUuMDEgMTguMTI1MSAxNzUuNTk3IDE4LjY4MTRDMTc2LjE4NCAxOS4yMzc3IDE3Ni42NDYgMTkuOTYwMyAxNzYuOTg1IDIwLjg0OTND MTc3LjMyMyAyMS43MzIxIDE3Ny40OTMgMjluODA1NSAxNzcuNDkzIDI0LjA2OTNWMjUuMDMwOEgxNjYuNDE4VjlyLjk5OUgxNzQuODM1QzE3NC44MzUgMjluMjg1NCA xNzQuNjkgMjEuNjUzNSAxNzQuNCAyMS4xMDMyQzE3NC4xMDkgMjAuNTQ2OSAxNzMuNzAxIDIwLjEwODUgMTczLjE3NSAxOS43ODhDMTcyLjY1NSAxOS40Njc1IDE3Mi 4wNDQgMTkuMzA3MyAxNzEuMzQzIDE5LjMwNzNDMTcwLjU4MSAxOS4zMDczIDE2OS45MTYgMTkuNDk0NyAxNjkuMzQ3IDE5Ljg2OTZDMTY4Ljc4NSAyMC4yMzg1IDE2 OC4zNSAyMC43MjlzIDE2OC4wNDEgMjEuMzlwOUMxNjcuNzM5IDIxLjkxMzUgMTY3LjU4OCAyMi41NTc1IDE2Ny41ODggMjMuMjUyOVYyNC44NDAzQzE2Ny41ODggMjU uNzcxNSAxNjcuNzUxIDI2LjU2MzcgMTY4LjA3OCAyNy4yMTY4QzE2OC40MSAyNy44Njk5IDE2OC44NzMgMjguMzY4NyAxNjkuNDY1IDI4LjcxMzRDMTcwLjA1OCAyOS4wN TIgMTcwLjc1IDI5LjIyMTQgMTcxLjU0MyAyOS4yMjE0QzE3Mi4wNTcgMjkuMjIxNCAxNzIuNTI1IDI5LjE0ODggMTcyLjk0OCAyOS4wMDM3QzE3My4zNzIgMjguODUyNSAxNz MunzM4IDI4LjYyODggMTc0LjA0NiAyOC4zMzI1QzE3NC4zNTQgMjguMDM2MSAxNzQuNTkgMjcuNjcwMyAxNzQuNzUzIDI3LjIzNDIMMTc3LjMyIDI3LjY5NzVDMTc3LjExN SAyOC40NTM0IDE3Ni43NDYgMjkuMTE1NSAxNzYuMjE0IDI5LjY4NEMxNzUuNjg4IDMwLjI0NjMgMTc1LjAyNiAzMC42ODQ3IDE3NC4yMjcgMzAuOTk5MkMxNzMuNDM1I DMxLjMwNzYgMTcyLjUzMSAzMS40NjE4IDE3MS41MTUgMzEuNDYxOFoilGZpbGw9ImJsYWNrlj48L3BhdGg+CiAglCAglCAglCAglCAglCAgCA8cGF0aCBkPSJNMTgzLjlxNCAxMi 42MDQxVjMxLjE4MDZIMTgwLjUwMIYxMi42MDQxSDE4My4yMTRaIiBmaWxsPSJibGFjayI+PC9wYXRoPgogICAgICAgICAgICAgICAgPHBhdGggZD0iTTE4Ny4wOCAzMS4xO DA2VjEyLjYwNDFIMTkzLjcwMkMxOTUuMTQ3IDEyLjYwNDEgMTk2LjM0NCAxMi44NjcyIDE5Ny4yOTQgMTMuMzkzM0MxOTguMjQzIDEzLjkxOTQgMTk4Ljk1NCAxNC42M zkgMTk5LjQyNSAxNS41NTIxQzE5OS44OTcgMTYuNDU5MSAyMDAuMTMzIDE3LjQ4MTEgMjAwLjEzMyAxOC42MTc5QzIwMC4xMzMgMTkuNzYwOCAxOTkuODk0IDIwLjc 4ODggMTk5LjQxNiAyMS43MDE5QzE5OC45NDUgMjluNjA4OSAxOTguMjMxIDIzLjMyODUgMTk3Ljl3NiAyMy44NjA3QzE5Ni4zMjYgMjQuMzg2OCAxOTUuMTMyIDI0LjY0 OTggMTkzLjY5MyAyNC42NDk4SDE4OS4xMzlWMjluMjczM0gxOTMuNDM5QzE5NC4zNTlgMjluMjczMyAxOTUuMDkzlDlyLjExNjEgMTk1LjY2MSAyMS44MDE3QzE5Ni4yM jkgMjEuNDgxMiAxOTYuNjQ3IDIxLjA0NTggMTk2LjkxMyAyMC40OTU1QzE5Ny4xNzkgMTkuOTQ1MiAxOTcuMzEyIDE5LjMxOTQgMTk3LjMxMiAxOC42MTc5QzE5Ny4zMTI gMTcuOTE2NCAxOTcuMTc5IDE3LjI5MzYgMTk2LjkxMyAxNi43NDk0QzE5Ni42NDcgMTYuMjA1MSAxOTYuMjI2IDE1Ljc3ODggMTk1LjY1MiAxNS40NzA0QzE5NS4wODQg CAgICA8cGF0aCBkPSJNMjA1LjkxMyAxMi42MDQxVjMxLjE4MDZIMjAzLjIwMVYxMi42MDQxSDIwNS45MTNaIiBmaWxsPSJibGFjayI+PC9wYXRoPgogICAgICAgICAgICAgICAg PHBhdGggZD0iTTIxMy42MTYgMzEuNDg5QzIxMi43MzMgMzEuNDg5IDIxMS45MzUgMzEuMzI1NyAyMTEuMjIxIDMwLjk5OTJDMjEwLjUwOCAzMC42NjY2IDIwOS45NDMg MzAuMTg1OSAyMDkuNTI1IDI5LjU1N0MyMDkuMTE0IDI4LjkyODEgMjA4LjkwOSAyOC4xNTcxIDIwOC45MDkgMjcuMjQ0QzlwOC45MDkgMjYuNDU3OSAyMDkuMDYgMj UuODEwOCAyMDkuMzYyIDI1LjMwMjlDMjA5LjY2NCAyNC43OTQ5IDIxMC4wNzMgMjQuMzkyOCAyMTAuNTg3IDI0LjA5NjVDMjExLjEwMSAyMy44MDAyIDIxMS42NzUgMj Muntc2nsayMtiumzegMjmundi1m0myMtiuotQ1idizLji3ndegMjezLju5MiayMy4xntkyIdixnC4yntegMjmumdgwnkMyMtuumdg2idiyLjk4MzkgMje1Ljc2MyAyMi4 5MDUyIDIxNi4yODMgMjluODQ00EMyMTYuODAzIDIyLjc3ODMgMjE3LjE4MSAyMi42NzI0IDIxNy40MTcgMjluNTI3M0MyMTcuNjUyIDIyLjM4MjlgMjE3Ljc3IDIyLjE0NjMgMj E3Ljc3IDIxLjgxOThWMjEuNzU2M0MyMTcuNzcgMjAuOTY0MSAyMTcuNTQ3IDIwLjM1MDQgMjE3LjA5OSAxOS45MTVDMjE2LjY1OCAxOS40Nzk2IDIxNS45OTkgMTkuMjY xOSAyMTUuMTIyIDE5Ljl2MTIDMjE0LjlwOSAxOS4yNjE5IDIxMy40ODkgMTkuNDY0NSAyMTIuOTYzIDE5Ljg2OTZDMjEyLjQ0MyAyMC4yNjg3IDIxMi4wODMgMjAuNzEzMiA yMTEuODg0IDIxLjIwM0wyMDkuMzM1IDIwLjYyMjVDMjA5LjYzNyAxOS43NzU5IDIxMC4wNzkgMTkuMDkyNiAyMTAuNjU5IDE4LjU3MjVDMjExLjI0NiAxOC4wNDY1IDIxMS

45MiAxNy42NjU1IDIxMi42ODIgMTcuNDI5N0MyMTMuNDQ0IDE3LjE4NzggMjE0LjI0NSAxNy4wNjY4IDIxNS4wODYgMTcuMDY2OEMyMTUuNjQyIDE3LjA2NjggMjE2LjIzM BQSSIBLEMSIGCRETSTQgMTcuMjY2NEMyMTcuNDgzIDE3LjM5MzQgMjE4LjA3IDE3LjYyOTIgMjE4LjYxNCAxNy45NzM5QzIxOS4xNjQgMTguMzE4NiAyMTkuNjE1IDE4L igxMTQgMiE5Ljk2NSAxOS40NTI0QzlyMC4zMTYgMjAuMDg3MyAyMjAuNDkyIDIwLjkxMjcgMjIwLjQ5MiAyMS45Mjg2VjMxLjE4MDZIMjE3Ljg0M1YyOS4yNzU4SDIxNy43Mz RDMjE3LjU1OSAyOS42MjY1IDIxNy4yOTYgMjkuOTcxMiAyMTYuOTQ1IDMwLjMwOThDMjE2LjU5NCAzMC42NDg1IDIxNi4xNDQgMzAuOTI5NyAyMTUuNTkzIDMxLjE1Mz RDMjE1LjA0MyAzMS4zNzcxIDIxNC4zODQgMzEuNDg5IDIxMy42MTYgMzEuNDg5Wk0yMTQuMjA2IDI5LjMxMjFDMjE0Ljk1NiAyOS4zMTIxIDIxNS41OTYgMjkuMTYzOSAy MTYuMTI5IDI4Ljg2NzZDMjE2LjY2NyAyOC41NzEzIDIxNy4wNzUgMjguMTg0MyAyMTcuMzUzIDI3LjcwNjZDMjE3LjYzNyAyNy4yMjl4IDIxNy43NzkgMjYuNzA1OCAyMTcuNz c5IDI2LjE1NTVWMjQuMzU5NkMyMTcuNjgzIDI0LjQ1NjMgMjE3LjQ5NSAyNC41NDcgMjE3LjlXNyAyNC42MzE3QzIxNi45NDUgMjQuNzEwMyAyMTYuNjM0IDI0Ljc3OTggMj E2LjI4MyAyNC44NDAzQzIxNS45MzIgMjQuODk0NyAyMTUuNTkgMjQuOTQ2MSAyMTUuMjU4IDI0Ljk5NDVDMjE0LjkyNSAyNS4wMzY4IDIxNC42NDcgMjUuMDczMSAyM TQuNDIzIDI1LjEwMzNDMjEzLjg5NyAyNS4xNjk5IDIxMy40MTcgMjUuMjgxNyAyMTIuOTgxIDI1LjQzODIDMjEyLjU1MiAyNS41OTYyIDIxMi4yMDcgMjUuODIyOSAyMTEuOT Q3IDI2LjExOTJDMjExLjY5MyAyNi40MDk1IDIxMS41NjYgMjYuNzk2NSAyMTEuNTY2IDI3LjI4MDNDMjExLjU2NiAyNy45NTE1IDIxMS44MTQgMjguNDU5NCAyMTIuMzEgMjg SJNMjl1LjMxOSAzNi40MDUyQzIyNC45MTQgMzYuNDA1MiAyMjQuNTQ1IDM2LjM3MiAyMjQuMjEzIDM2LjMwNTVDMjlzLjg4IDM2Ljl0NSAyMjMuNjMyIDM2LjE3ODUgMjl zLjQ2OSAzNi4xMDU5TDIyNC4xMjlgMzMuODgzNkMyMjQuNjE4IDM0LjAxNjcgMjl1LjA1OSAzNC4wNzQxlDIyNS40NDYgMzQuMDU2QzIyNS44MzMgMzQuMDM3OCAyMj YuMTc1IDMzLjg5MjcgMjl2LjQ3MSAzMy42MjA2QzlyNi43NzQgMzMuMzQ4NSAyMjcuMDQgMzIuOTA0IDIyNy4yNjkgMzIuMjg3MkwyMjcuNjA1IDMxLjM2MkwyMjIuNTA3I DE3Lj100DJIMj11LjQxTDIyOC45MzggMjguMDYwM0gyMjkuMDg0TDIzMi42MTIgMTcuMjQ4MkgyMzUuNT10TDIyOS430DIgMzMuMDQwMUMyMjkuNTE2IDMzLjc2NTcgM jl5LjE3NyAzNC4zNzk1lDlyOC43NjYgMzQuODgxNEMyMjguMzU1lDM1LjM4OTMgMjl3Ljg2NSAzNS43NzAzlDlyNy4yOTcgMzYuMDl0M0MyMjYuNzl4lDM2Ljl3ODMgMjl2Lj A2OSAzNi40MDUylDIyNS4zMTkgMzYuNDA1MloilGZpbGw9ImJsYWNrlj48L3BhdGg+CiAglCAglCAglCAglDwvc3ZnPgoglCAglCAglDwvZGl2PgoglCAglCAglDxkaXYgY2xhc3 ·8ZGI2PjwvZGI2PgoglCAglCAglCAglCAgPGRpdj48L2Rpdj4KlCAglCAglCAglCAglDxkaXY+PC9kaXY+CiAglCAglCAglCAglCAglCAglCAgZGI2PjwvZGI2PgoglCAglCAglCAglCAglCAglCAg E3Rpdj/KKjAglC4gK-A8H-ZRpdj-H6E-AglDyvvZGl2Pgo8L2Rpdj4KCgo8L2JvZHk+PC9odG1sPg==

Coel5qxpy1nzBU2HqPuBP2EjNKXl	
9ROYvUVyiX7gohkAn481H2mOSrWfwkEW	
ifP5S9CdlxshggXp37TrbEl199f16GUc	
tyIMHYj4E3EgW4mShNYTh30KqADxMnXY	
9w5E8CzY6m1n4hygXrseg7VRB7EsZT51	
Rp0aJS5Umkn5PDWDdKEfRtTObnscQr7T	
1lDdPMX0zjCtSNVsVcyG9UOAfTksMFfY	
92sHBdTkJGpDSWYr6Ma8vgCUoSk9iZG6	

POSSIBLE SECRETS
rwtSlkdLuH5KaJR0oY6wYi8G8Rc4X5Yb
BEVDZxUetTHXZyMQk8onv0fPj1ZBZ1Qa
uPGJEhgdW6Zw1Sj0lSecSmwhOYLW8VRR
8GKiNnUVprvv3BQA7RRGITYk7sqsrZd2
7a5b85d3ee2e0991ca3502602e9389a98f55c0576b887125894a7ec03823f8d3
UISLjJpxihM79aLvihwYrwdsqCfo0Nro
ZnYv6Dz0eliuCYzsHLE25vrPVm9Ysg64
vBmFH1fuq9MEDYSajFcKFjMjxlndPylT
JMylsM6N3mQ5xBBSQQoIEfTakpln9APf
E7RgkNcVOxUPIMLAnYmg2qDI6nJpawyt
9oUH6lggskzJ9KRnNq9fhlyXZqfLC7qm
dGfRjiYjSJpbyPiyGtO7b0cAlrZw4Mrv
0XKBrb3At6dwoT0wmD89VHK9vq2VdTUa
4ddrBoC1HSiu89JLzfXMV59B74qIm2xJ
7CWVV5CGm74gAvba93StX50LTK78ikzM

POSSIBLE SECRETS
UVmnaLPTsQqsAUFvP4l9eFVdZ5Bnbi11
yCbh3JWABSPWXJzi8IqNfGSw4JUwRc1Z
fc6abssWsZoyWpr8fCHyT3ixVlnX2HG2
Z7tecEc8tS2JrzNmQM0R9CjEnjCb6ksC
MUUz2dKYtP7sZF6Tuk5kEGRgHEx452fJ
el7YtyQobuGYp8qUnEWwGAo9eb5IMR8f
PPqjaOYWzYRlppBEr7ot7ueRFlAfsGXr
mZfo4fllXHQscYR0BkWPKUfaL8c0bByk
1ad75ae72e05dcf4dadbd17a
LtGcJkDv8PpKzGxu4pknm0pyAahoAl9h
jDUjvWDGqsgivCcWfJbzInhujFfNRoy6
Yb4G3rkl5nMioq4UjOOwWhO2qlazlSB5
h73SRN04xx9GKM0Q116IBzLVfoAHdt6S
aJo4Pz0hsbQrFibFt4ypJbnLPuINPYvA
kvUI2sJVOm05aD2rNLnp8ceY2vExoctW

POSSIBLE SECRETS
TZh0Sw2dsxVxMXdj340dFQnUzLECuqag
E1e7Uw5ci0LxHvCHKGZ7MMTImO0krz0e
UW9U9pyLqubavRm8Co8t1ARkgbl4JN3Q
DThvYGttjE9j20qDJ6yVSrG4WY8lD38s



Title: YsxLite

Score: 2.4257426 Installs: 1,000,000+ Price: 0 Android Version Support: Category: Tools Play Store URL: com.ysxlite.cam

Developer Details: xiaowenyin2021, xiaowenyin2021, None, None, 25416287@qq.com,

Release Date: Sep 13, 2023 Privacy Policy: Privacy link

Description:

YsxLite is a virtual and exquisite network client software that is convenient and quick to bind network extensions, directly connect or access network extensions, and realize real-time observation, planning, alarm, real-time video/photography, local and remote video/photo transmission, deletion, download and sharing., providing real-time image parameter settings, secure login and other control functions.

⋮≡ SCAN LOGS

Timestamp	Event	Error
2024-10-28 16:11:22	Generating Hashes	OK

2024-10-28 16:11:22	Extracting APK	ОК
2024-10-28 16:11:22	Unzipping	ОК
2024-10-28 16:11:22	Getting Hardcoded Certificates/Keystores	ОК
2024-10-28 16:11:31	Parsing AndroidManifest.xml	OK
2024-10-28 16:11:31	Parsing APK with androguard	OK
2024-10-28 16:11:31	Extracting Manifest Data	OK
2024-10-28 16:11:31	Performing Static Analysis on: YsxLite (com.ysxlite.cam)	ОК
2024-10-28 16:11:31	Fetching Details from Play Store: com.ysxlite.cam	ОК
2024-10-28 16:11:32	Manifest Analysis Started	OK
2024-10-28 16:11:32	Reading Network Security config from network_security_config.xml	ОК
2024-10-28 16:11:32	Parsing Network Security config	ОК

2024-10-28 16:11:32	Checking for Malware Permissions	ОК
2024-10-28 16:11:32	Fetching icon path	ОК
2024-10-28 16:11:32	Library Binary Analysis Started	ОК
2024-10-28 16:11:32	Reading Code Signing Certificate	ОК
2024-10-28 16:11:35	Running APKiD 2.1.5	ОК
2024-10-28 16:11:40	Updating Trackers Database	ОК
2024-10-28 16:11:40	Detecting Trackers	ОК
2024-10-28 16:11:45	Decompiling APK to Java with jadx	ОК
2024-10-28 16:14:08	Converting DEX to Smali	ОК
2024-10-28 16:14:09	Code Analysis Started on - java_source	ОК
2024-10-28 16:15:20	Android SAST Completed	ОК

2024-10-28 16:15:20	Android API Analysis Started		
2024-10-28 16:15:27	Android Permission Mapping Started		
2024-10-28 16:16:16	Android Permission Mapping Completed		
2024-10-28 16:16:17	Finished Code Analysis, Email and URL Extraction		
2024-10-28 16:16:17	Extracting String data from APK	OK	
2024-10-28 16:16:17	Extracting String data from Code	OK	
2024-10-28 16:16:17	Extracting String values and entropies from Code		
2024-10-28 16:16:17	Performing Malware check on extracted domains		
2024-10-28 16:16:20	Saving to Database	ОК	

Report Generated by - MobSF v4.1.0

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.

© 2024 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.