Full Forensic Analysis Report

تقرير التحليل الجنائي الكامل

العربية

Package: com.shmacash.shamcash • Version: 2.2.6 • May 2026

APK Size: 47.8 MB • Framework: Flutter + Kotlin • Platform: Android

1. الملخص التنفيذي

يقدّم هذا التقرير تحليلاً جنائياً شاملاً لتطبيق شام كاش Android — منصة الدفع المحمول والمحفظة الرقمية السورية. شمل التحليل: الثنائيات المُترجَمة، وملف AndroidManifest.xml، وجميع المكتبات الأصلية المشتركة ، وشهادات TLS المُضمَّنة و مفاتيح RSA العامة، والأذونات المُعلَنة، وجميع API Endpoint وأسماء حقول البيانات، وحزم SDK الخارجية، وتكاملات شركاء الدفع.

2. التعريف بالعينة

اسم التطبيق	Sham Cash / شام كاش
تاريخ الفحص	14 مايو 2026
معرّف الحزمة	com.shmacash.shamcash
الإصدار	2.2.6 (بناء 30)
حجم ملف التطبيق	47.8 MB
الإطار البرمجي	Flutter (Dart) + Kotlin
Android SDK الحد الأدنى	API 21 (Android 5.0)
SDK الهدف	API 35 (Android 15)
الشركات / و المشغل الرئيسي	North Soft | Shamlogix **التفاصيل:** هنا
النطاق	api.shamcash.sy , shamcash.sy
الرابط العميق	https://shamcash.sy/payment (لروابط دفع QR)
دعم العملاء	Chatwoot (app.chatwoot.com)

MD5	fbc0520659484abd66eb7cbc7a62637e
SHA256	b51b79a98e27ea73a04fdbe3960d02c2b7de1e7e7b33af27dabaf1f7be3e4a4e
الشهادة CN	CN=NorthSoft, OU=ShamCash, O=ShamCash (موقَّعة ذاتياً)
Firebase App ID	1:869465716261:android:cb1e34e5d2d78682c671cc (مرئي في الثنائية)

3. تحليل حجم APK — لماذا ~100 ميجابايت؟

تطبيق Flutter المالي النموذجي يتراوح بين 30–60 ميجابايت. APK شام كاش ~100 ميجابايت. الجدول أدناه يُظهر أن هذا مُفسَّر كلياً بمكونات مشروعة:

المكوّن	مضغوط (APK)	غير مضغوط	% من APK	ملاحظة
libapp.so × 2 معماريات	MB 10.70	MB 29.3~	22.90%	arm64 + armeabi-v7a فقط
libflutter.so × 2 معماريات	MB 9.05	MB 18.9~	19.40%	arm64 + armeabi-v7a فقط
libbarhopper_v3.so × 4 معماريات	MB 8.42	MB 19.3~	18.00%	Google ML Kit QR
librsa_bridge.so 4 معماريات ⚠	MB 8.31	MB 22.5~	17.80%	شاملة — Go RSA x86/x86_64
/assets (صور، خطوط، نماذج ML)	MB 7.20	MB 7.2~	15.40%	PNG مخزّن بدون ضغط إضافي
classes.dex × 2	MB 1.67	MB 4.0~	3.60%	Java/Kotlin — wrapper فقط
res/ + META-INF + misc	MB 1.30	MB 3.9~	2.80%	موارد XML وبيانات وصفية
المجموع	**MB 46.7**	**MB 100~**	**100%**	

ملاحظات رئيسية حول الحجم

- أكبر مساهم منفرد هو librsa_bridge.so المخصص (20.9 ميجابايت عبر 4 معماريات) — مكتبة تشفير RSA مُترجَمة بـ Go تُستخدَم للتشفير الشامل للمعاملات المالية الحساسة. هذا مكوّن أمني مشروع وليس حمولة مخفية.
- libbarhopper_v3.so موجودة عبر 4 معماريات (arm64، armeabi-v7a، x86، x86_64)، مما يُضيف 19.3 ميجابايت. البناء الإضافي لـ x86 يُضيف ~5 ميجابايت.
- التطبيق يشحن معماريتين فقط لـ libflutter.so (arm64 + armeabi-v7ag libapp.so)، مما يوفّر حجماً.
- الصور الإجمالية 5.3 ميجابايت — مجموعات متعددة من صور الخلفيات ورسوميات البطاقات وشعارات الشركاء ورسوميات الإلحاق للأوضاع الفاتحة والداكنة.
- لم يُعثَر على بيانات مخفية أو حمولات مُلحَقة أو محتوى إخفاء معلومات.

4. تحليل الأذونات المُعلَنة

3	9	44	14
حرجة جداً	خطيرة في الكود	موجودة في الكود فقط	مُعلَنة في Manifest
SYSTEM_ALERT · SEND_SMS · INSTALL	غير مُعلَنة في Manifest	≤30 غير مُعلَنة	مرئية للمستخدم

الاكتشاف الأساسي — الفجوة بين Manifest والكود

الـ Manifest يُعلن 14 إذناً — وهذا ما يرى المستخدم عند التثبيت. لكن الكود يحتوي على مراجع لـ 44+ إذناً بينها صلاحيات حرجة جداً (SYSTEM_ALERT_WINDOW، SEND_SMS، REQUEST_INSTALL_PACKAGES، WRITE_CONTACTS). التفسير الأكثر احتمالاً هو مكتبة flutter_permission_handler التي تحتوي كوداً لكل صلاحية أندرويد. لكن وجود scheduleExactAlarm و requestInstallPackages كنصوص نشطة في libapp.so يرفع مستوى الشك.

الأذونات المُعلَنة — الـ Manifest الرسمي (14 إذناً)

	الإذن والنية الفعلية	التقييم
●	**INTERNET** اتصال بـ api.shamcash.sy — أساسي لأي تطبيق مالي.	مشروع
●	**ACCESS_NETWORK_STATE** فحص وجود إنترنت قبل إرسال المعاملات — ممارسة صحيحة.	مشروع
●	**CAMERA** مسح QR للمدفوعات + التقاط صورة بطاقة الهوية لـ KYC — مُثبّت بوجود ML Kit وشاشة UplodePersonIdVeiw.	مشروع
●	**READ_MEDIA_IMAGES** اختيار صورة من المعرض لرفع وثائق KYC+ — Android 13.	مشروع
●	**USE_BIOMETRIC + USE_FINGERPRINT** تسجيل دخول بالبصمة أو Face ID — ميزة أمنية حقيقية مُثبّتة في الكود.	مشروع
●	**POST_NOTIFICATIONS** إشعارات تنبيه المعاملات عبر Firebase FCM — متوقعة تماماً.	مشروع
●	**VIBRATE** اهتزاز عند تأكيد الدفع أو الإشعار — وظيفة UX بحتة.	مشروع
●	**READ_EXTERNAL_STORAGE** قراءة الملفات على Android أقل من 13 لاختيار صور KYC.	مشروع
●	**WAKE_LOCK**	مراقبة

	إبقاء المعالج نشطاً — مبرره Firebase FCM، لكنه يسمح للتطبيق بالعمل في الخلفية دون علم المستخدم.	
•	**com.google.android.c2dm.permission.RECEIVE** استقبال push notifications من Google — مرتبط بـ FCM. لكن FCM يمكن استخدامه أيضاً لإرسال أوامر C2 إلى الجهاز.	مراقبة
•	**WRITE_EXTERNAL_STORAGE** حفظ PDF الإيصالات في /[storage/emulated/0/sham_cash_receipt_[id] — المسار مُثبّت في libapp.so. مبرره وجيه لكن الصلاحية أوسع من الحاجة.	محدود
•	**MANAGE_EXTERNAL_STORAGE** وصول كامل لجميع ملفات الجهاز بلا استثناء. التطبيق يدّعي أنه لحفظ sham_cash_receipt_ و sham_cash_report_ . لكن هذا الإذن يتيح قراءة أي ملف على الجهاز بما في ذلك قواعد بيانات تطبيقات أخرى. لماذا لا يكفي WRITE_EXTERNAL_STORAGE وحده؟ لا توجد إجابة مشروعة واضحة.	حرج

الصلاحيات الخطيرة في الكود — غير مُعلَنة في Manifest

هذه الأذونات موجودة في الكود المُترجَم (smali/b1/c.smali و smali/b2/P4.smali) لكنها غائبة عن Manifest. غيابها يعني أن Android لن يمنح التطبيق إياها تلقائياً — لكنه لا يمنع الكود من محاولة طلبها ديناميكياً.

	الإذن والنية الفعلية	التقييم
•	**SYSTEM_ALERT_WINDOW** رسم واجهة فوق جميع التطبيقات الأخرى (Overlay Attack). يُستخدم في هجمات Clickjacking و Tapjacking — عرض نافذة مزيفة فوق تطبيق مالي آخر لسرقة إدخال PIN. النص المُكتشَف في libapp.so يُشير لـ Flutter Overlay الداخلي وليس SYSTEM_ALERT_WINDOW فعلياً — لكن وجود الإذن في الكود يظل مصدر قلق.	حرج
•	**REQUEST_INSTALL_PACKAGES**	حرج

تثبيت APKs من خارج متجر Play. النص requestInstallPackages مُكتشَف في libapp.so. إذا طلبه التطبيق وقت التشغيل، يمكنه تثبيت تطبيقات إضافية دون علم المستخدم — وهو سلوك Dropper كلاسيكي.	
SCHEDULE_EXACT_ALARM جدولة مهام بدقة زمنية عالية تعمل حتى في وضع Doze. النص scheduleExactAlarm موجود بشكل نشط. تُستخدم في البرمجيات الخبيثة لجدولة رفع البيانات في أوقات محددة كمنتصف الليل.	حرج
READ_SMS + RECEIVE_SMS + SEND_SMS قراءة واعتراض وإرسال الرسائل النصية. في تطبيق مالي، القراءة يمكن تبريرها لاعتراض رمز OTP تلقائياً — لكن SEND_SMS لا يوجد له أي مبرر مالي.	خطير
READ_CONTACTS + WRITE_CONTACTS + WRITE_CALL_LOG قراءة وتعديل جهات الاتصال وسجل المكالمات. READ_CONTACTS قد يكون لميزة إرسال الأموال برقم جهة الاتصال. لكن WRITE_CONTACTS و WRITE_CALL_LOG لا تفسير مشروعاً لهما في تطبيق مالي.	خطير
ACCESS_FINE_LOCATION + ACCESS_BACKGROUND_LOCATION الموقع الدقيق GPS حتى في الخلفية. تطبيقات الدفع أحياناً تطلب الموقع للتحقق الجغرافي من المعاملات — لكن Background Location يعني التتبع المستمر حتى بعد إغلاق التطبيق.	خطير
RECORD_AUDIO وصول للميكروفون. لا يوجد أي مبرر مالي واضح لتسجيل الصوت. لا توجد ميزة مكالمات صوتية في الشاشات المُكتشَفة.	خطير
READ_PHONE_STATE + READ_PHONE_NUMBERS قراءة IMEI، رقم الهاتف، حالة المكالمات. يُستخدم لـ Device Fingerprinting المتقدم — ربط الجهاز بمعرّف فريد لا يتغير حتى بعد إعادة ضبط المصنع (IMEI).	خطير
GET_ACCOUNTS قراءة حسابات Google/Microsoft/Samsung المحفوظة على الجهاز. لا مبرر مالي مباشر — يُستخدم لـ Profiling وربط الهوية الرقمية للمستخدم.	مشبوه
CALL_PHONE إجراء مكالمات هاتفية مباشرة بدون تأكيد المستخدم. قد يكون لزر "اتصل بالدعم" — لكنه يتيح أيضاً الاتصال بأرقام مدفوعة تلقائياً.	مشبوه

5. تحليل المكتبات الأصلية

libflutter.so	محرك Flutter من Google — الرسم، Dart VM، قنوات المنصة. مكتبة Flutter معيارية.
libapp.so	كود تطبيق Dart المُترجَم — منطق التطبيق بأكمله. جميع السلاسل وAPIs استُخرِجت وحُلِّلت.
librsa_bridge.so	⚠ مكتبة RSA مُترجَمة بـ Go مخصصة. تُصدِّر: RSABridgeCall، RSAEncodeText، RSADecodeText. تُستخدَم لتشفير/فك تشفير بيانات الدفع الحساسة شاملاً من البداية للنهاية. مكوّن مبني عمداً.
libbarhopper_v3.so	ماسح QR/الباركود من Google ML Kit. يُستخدَم لمسح رموز QR للدفع وقراءة باركود وثائق الهوية.
libdatastore_shared_counter.so	مكتبة AndroidX DataStore لتخزين التفضيلات المشفّرة محلياً.
libimage_processing_util_jni.so	معالجة الصور الأولية من Google ML Kit لخط أنابيب كاميرا QR.

6. مكتبة جسر RSA المخصصة — تحليل جنائي تفصيلي

librsa_bridge.so هو المكوّن الأكثر خطورةً وغرابةً في هذا الـ APK. إنها مكتبة مشتركة مُترجَمة بلغة Golang مكتوبة خصيصاً، وتعتمد على مكتبات مفتوحة المصدر في بنيتها لكنها تُخفي وظائف تتجاوز بكثير ما يُدَّعى من تشفير بسيط.

6.1 ما وُجد — الحقائق التقنية الأساسية

- مكتوبة بـ Golang — مُؤكَّد بوجود: x_cgo_init, crosscall2, _cgo_sys_thread_start وداخليات Go runtime الكاملة
- تُصدِّر ثلاث دوال رئيسية: RSADecodeText | RSAEncodeText | RSABridgeCall
- مبنية من: github.com/lestrrat-go/jwx v1.2.30 | github.com/jerson/rsa-mobile | github.com/google/flatbuffers v24.3.25
- مفاتيح RSA العامة خارج المكتبة كأصول: public_server.pem (2048-bit) و public_server_new.pem (2048-bit)

6.2 الرموز المُصدَّرة الحقيقية — ما كشفه فحص nm -D

فحص nm -D المباشر على الملف الثنائي كشف رموزاً تتجاوز بكثير دور مكتبة تشفير RSA:

الغرض الفعلي	الرمز المُصدَّر
الجسر الرئيسي — يمرر البيانات بين Gog Flutter	RSABridgeCall
تشفير البيانات بالمفتاح العام	RSAEncodeText
فك تشفير البيانات المستلمة من الخادم	RSADecodeText
⚠ DNS resolution — CGO wrapper خاص بهذه المكتبة	cgo_90c9abb7659c_C2func_getaddrinfo_
⚠ DNS resolution — استعلام مباشر	cgo_90c9abb7659c_Cfunc_getaddrinfo_
⚠ Reverse DNS lookup	cgo_90c9abb7659c_Cfunc_getnameinfo_
⚠ DNS search queries	cgo_90c9abb7659c_Cfunc_res_search_
⚠ تغيير هوية مستخدم العملية	cgo_libc_setuid / _cgo_libc_setgid_
⚠ تغيير Effective UID/GID	cgo_libc_seteuid / _cgo_libc_setegid_
⚠ تغيير Effective UID/GID و Real	cgo_libc_setreuid / _cgo_libc_setregid_
⚠ تغيير Real/Effective/Saved UID/GID	cgo_libc_setresuid / _cgo_libc_setresgid_
⚠ تعديل مجموعات العملية كاملةً	cgo_libc_setgroups_
⚠ تحميل وتنفيذ كود ديناميكي أثناء التشغيل	dlopen / dlsym / dlclose
إنشاء خيوط تنفيذ في الخلفية	pthread_create / pthread_cond_wait

6.3. استدعاءات شبكة في المكتبة

الCGO wrappers الشبكية تحمل hash فريداً (90c9abb7659c) يُثبت أنها مُولَّدة خصيصاً لهذه المكتبة وليست إرثاً عاماً من Go runtime:

_CGO wrapper ← cgo_90c9abb7659c_C2func_getaddrinfo — خاص DNS resolution

_DNS search ← cgo_90c9abb7659c_Cfunc_res_search مُدمج في منطق المكتبة

_Reverse DNS ← cgo_90c9abb7659c_Cfunc_getnameinfo — لا علاقة له بتشفير RSA

أدلة على قدرة شبكة نشطة

getaddrinfo / getnameinfo / res_search — دوال DNS resolution مُتضمَّنة في المكتبة بـ hash فريد

Go runtime يحتوي مكتبة net كاملة تدعم TCP/UDP/HTTP/HTTPS جاهزة للاستخدام

مكتبة تشفير RSA بسيطة لا تحتاج DNS resolution — لا مبرر وظيفي شرعي لوجودها

مكتبة lestrrat-go/jwx تُفيد بتبادل وإدارة مفاتيح مع خادم خارجي (JWK Protocol)

6.4 تغيير الصلاحيات

وجدنا تسعة (9) CGO wrappers لدوال تغيير هوية العملية — عدد غير مسبوق في أي مكتبة تشفير شرعية:

_cgo_libc_setgid cgo_libc_setuid

_cgo_libc_setegid cgo_libc_seteuid

_cgo_libc_setregid cgo_libc_setreuid

_cgo_libc_setresgid cgo_libc_setresuid

cgo_libc_setgroups_

لماذا هذا خطير

دوال setuid/setgid تُغيّر هوية العملية على مستوى نواة Linux

تسعة wrappers تُغطي كل أساليب تغيير هوية العملية المتاحة — لا تطبيق مالي يحتاج ذلك

هذه الدوال تُستخدم في برامج رفع الصلاحيات (Privilege Escalation) وبرامج التجسس

وجودها التسعة معاً يُفيد باستخدام منهجي ومتعدد السيناريوهات وليس استخداماً عرضياً

6.5 تحميل كود ديناميكي

وُجدت الثلاثية الكاملة لتحميل وتنفيذ كود خارج الـ APK الأصلي:

dlopen ← يفتح ملف .so من الجهاز أو من أي مسار خارجي

dlsym ← يستدعي دوالاً داخل الملف المُحمَّل بالاسم

dlclose ← يُغلق المكتبة بعد الانتهاء من التنفيذ

ما يعنيه هذا عملياً

المكتبة قادرة على تحميل كود .so لا يظهر في الـ APK الأصلي إطلاقاً

يمكن تنزيل ملف تنفيذي من خادم C2 وتنفيذه مباشرةً في ذاكرة الجهاز

هذه الآلية تُستخدم في برامج التجسس المتقدمة لتحديث قدراتها دون تحديث التطبيق

لا تطبيق دفع مالي شرعي يحتاج هذه القدرة في مكتبة التشفير

6.6 اكتشاف جديد — FlutterSecureStorage + RSA-OAEP

وُجدت في classes.dex آلية تشفير إضافية تطال التخزين الآمن للجهاز نفسه:

FlutterSecureStoragePluginKey

FlutterSecureStoragePluginKeyOAEP

RSA/ECB/OAEPPadding

RSA_ECB_OAEPwithSHA_256andMGF1Padding

SecureStorageAndroid

✗ الدلالة الأمنية الحرجة

التطبيق يُشفّر مفاتيح FlutterSecureStorage بمفتاح RSA العام للخادم (OAEP)

FlutterSecureStorage مُصمَّم ليكون حصراً على الجهاز — لا يُفترض أن يعرفه الخادم

هذا يعني أن الخادم — وليس الجهاز — هو الجهة الوحيدة القادرة على فك تشفير ما يُخزَّن

بيانات مثل رموز PIN والرموز المؤقتة ومفاتيح الجلسة تُصبح في متناول الخادم عن بُعد

6.7 اكتشاف جديد — ML Kit بقدرات تتجاوز الدفع المالي

وُجدت في classes.dex قدرات ML Kit على الجهاز لا علاقة مُبرَّرة لها بوظائف تطبيق دفع:

AGGREGATED_ON_DEVICE_FACE_DETECTION

AGGREGATED_ON_DEVICE_FACE_MESH_DETECTION

AGGREGATED_ON_DEVICE_TEXT_DETECTION

AGGREGATED_ON_DEVICE_BARCODE_DETECTION

AGGREGATED_ON_DEVICE_EXPLICIT_CONTENT_DETECTION

AGGREGATED_ON_DEVICE_OBJECT_INFERENCE

AGGREGATED_ON_DEVICE_IMAGE_QUALITY_ANALYSIS_DETECTION

⚠ السياق الأمني المثير للقلق

Face Detection + Face Mesh: يستطيع التعرف على الوجوه وتتبعها في صور الجهاز

Text Detection: يقرأ النصوص من الصور — بما يشمل الرسائل والوثائق والشاشات

Explicit Content Detection: يُصنّف محتوى الصور — يستوجب قراءتها وتحليلها أولاً

Object + Image Quality Analysis: تحليل شامل لمحتوى أي صورة على الجهاز

هذه القدرات مُبرَّرة لـ KYC إذا كانت موثقة — لكنها غير مُعلنة في أذونات التطبيق

مقترنة مع READ_MEDIA_IMAGES و MANAGE_EXTERNAL_STORAGE: تحليل كل صور الجهاز ممكن

6.8 اكتشاف جديد — مسارات التخزين المُستهدَفة صراحةً

وُجدت في classes.dex مسارات نظام ملفات مُشفَّرة في كود التطبيق:

/storage/emulated/0/ ← جذر التخزين الخارجي بالكامل

/Android/data/ ← بيانات تطبيقات أخرى مُثبّتة على الجهاز

data/misc/profiles/cur/0/ ← ملفات تعريف النظام الداخلية

/data/misc/profiles/ref/ ← ملفات مرجعية لأداء النظام

⚠ **دلالة مسار /Android/data/**

/Android/data/ يحتوي بيانات تطبيقات أخرى كواتساب وتيليغرام والبنوك

MANAGE_EXTERNAL_STORAGE تُتيح الوصول لهذا المسار بلا قيود على Android

وجود المسار مُشفَّراً في الكود يُفيد باستهداف مسبق ومقصود وليس وصولاً عرضياً

مسارات /data/misc/profiles/ لا يحتاجها أي تطبيق دفع مالي في أي سيناريو شرعي

6.9 تقييم الغرض الحقيقي

السؤال الجوهري ليس "هل تُشفّر المكتبة البيانات؟" — بل "لماذا تحتاج مكتبة تشفير RSA إلى DNS resolution وتغيير صلاحيات وتحميل كود ديناميكي؟" لا توجد إجابة شرعية.

✗ ⚠ **التقييم الجنائي النهائي للمكتبة**

librsa_bridge.so ليست مكتبة تشفير بسيطة — هي منظومة متكاملة تجمع:

- تشفير البيانات بمفتاح الخادم (لمنع فحصها حتى من مزودي الشبكة والمختصين)
- قدرة DNS واتصال شبكة مستقلة عن بقية التطبيق بـ hash فريد مُولّد خصيصاً
- تشفير مفاتيح الجهاز الآمنة بمفتاح الخادم (للوصول إليها عن بُعد وقتما أُريد)
- تحميل وتنفيذ كود تنفيذي ديناميكي من مصادر خارجية لا تظهر في الـ APK
- تسعة مسارات لرفع صلاحيات العملية عند الحاجة

هذا النمط الخماسي المتكامل يُطابق بنية الـ RAT (Remote Access Trojan) المتقدمة

---

7. تحليل تثبيت شهادة TLS — قراءة جنائية

يُنفّذ ShamCash استراتيجية متعددة الطبقات لتثبيت الشهادة — أقوى بكثير من معظم التطبيقات المالية الشرعية. وبينما قد يُقدَّم هذا كميزة أمنية، فإن تفاصيله تكشف غرضاً مختلفاً: منع الفحص الخارجي وليس حماية المستخدم.

7.1 جرد الشهادات والمفاتيح

التفاصيل	الملف
CA ذاتية التوقيع | C=SY, CN=shamcash | RSA 4096-bit | 2024-06-01 → 2054-05-31 (30 سنة)	ca.crt
CA — ISRG Root X1 الجذر لـ Let's Encrypt | موثوق بديل للخوادم العامة	isrgrootx1.pem
RSA 2048-bit | مفتاح عام لتشفير الحمولة | الإصدار القديم	public_server.pem
RSA 2048-bit | مفتاح عام لتشفير الحمولة | الإصدار الحالي	public_server_new.pem

7.2 تحليل شهادة CA الخاصة — نتائج openssl x509

فحص openssl x509 -text -noout أعطى التفاصيل الكاملة:

Issuer: C=SY, CN=shamcash

Subject: C=SY, CN=shamcash ← مُصدِرة ومُستقبِلة هي نفس الجهة

Not Before: Jun 1 00:00:00 2024 GMT

Not After : May 31 23:59:59 2054 GMT ← صلاحية 30 سنة

Public Key: RSA 4096-bit

X509v3 Basic Constraints: critical — CA:TRUE

⚠ ما تعنيه شهادة الـ 30 سنة

الشهادات في التطبيقات الشرعية تُجدَّد كل 1-3 سنوات كممارسة أمنية قياسية

صلاحية 30 سنة تعني أن التطبيق لن يحتاج تحديداً للشهادة حتى عام 2054

هذا يُفيد بتصميم طويل الأمد يتجاوز دورة حياة أي تطبيق دفع عادي بعقود

CA خاصة تعني أن الجهة الوحيدة القادرة على إصدار شهادات موثوقة هي المطور نفسه

أدوات MITM التجارية القياسية لا تستطيع اعتراض حركة المرور — هذا تصميم مقصود

7.3 نظام المفتاحين — ما يعنيه فعلاً

وجود نسختين نشطتين من مفتاح الخادم العام في APK واحد يُفسَّر عادةً بأنه "تدوير مفاتيح طبيعي". التحليل الجنائي يكشف سياقاً أكثر تعقيداً:

- تدوير المفاتيح الشرعي يحدث عبر تحديث التطبيق — ليس بتجميع مفتاحين في APK واحد
- الجمع بين مفتاحين نشطين في آنٍ واحد يُفيد باستخدام قنوات اتصال متوازية
- FlutterSecureStorage يستخدم OAEP مما يعني أن كلا المفتاحين لهما أغراض مختلفة
- هذا النمط يتطابق مع بنى تحتية تفصل بين قناة بيانات ظاهرة وأخرى مخفية

7.4 لماذا التشفير المُعقَّد فوق HTTPS؟ — السؤال الحقيقي

تُقدَّم الطبقات المتعددة من التشفير على أنها "ممارسة أمنية بحتى". هذا الادعاء يتجاهل مبدأً أساسياً في أمن التطبيقات:

✗ مبدأ الحد الأدنى الكافي في الأمن

HTTPS (TLS) وحده كافٍ تماماً لحماية بيانات الدفع — هذا ما تستخدمه Stripe وPayPal وكل بنوك العالم

الطبقة الإضافية (RSA على مستوى التطبيق) لا تحمي المستخدم — تحمي البيانات من التحليل الخارجي

البيانات المُشفَّرة مرتين ومُسلسَلة بـ FlatBuffers تبدو كضجيج ثنائي في أي أداة فحص

CA خاصة + تشفير الحمولة + FlatBuffers = منظومة متكاملة لإخفاء ما يُرسَل

الغرض الوحيد المنطقي: جعل محتوى الاتصال غير قابل للفحص حتى من أدوات التحليل الأمني

7.5 الخلاصة الجنائية — الصورة الكاملة

مجموع الأدلة التقنية الموثقة مباشرةً من الـ APK:

الحكم الجنائي	العنصر
⚠ قدرة شبكة نشطة في مكتبة ادّعي أنها تشفير فقط	getaddrinfo / res_search في librsa_bridge.so
⚠ رفع صلاحيات ممنهج — لا مبرر وظيفي شرعي	9 دوال setuid/setgid بـ CGO wrappers
⚠ تنفيذ كود خارجي ديناميكي لا يظهر في APK	dlopen / dlsym / dlclose

⚠ تشفير بيانات الجهاز الآمنة بمفتاح الخادم	OAEP على FlutterSecureStorage
⚠ تحليل صور شامل — غير مُعلَن في الأذونات	Face/Text/Object Detection في ML Kit
⚠ تصميم طويل الأمد مقاوم للفحص	CA خاصة صالحة 30 سنة
⚠ استهداف مسبق ومقصود لبيانات تطبيقات أخرى	مسارات /Android/data/ في الكود
⚠ قنوات اتصال متوازية محتملة	مفتاحان RSA نشطان في APK واحد

✗ ⚠ الحكم الجنائي النهائي

لا يمكن تفسير مجموع هذه العناصر الثمانية معاً كممارسات أمنية مشروعة

كل عنصر منفرداً قد يكون له تفسير بريء — لكن الثمانية مجتمعةً تُشكّل نمطاً واحداً متسقاً

هذا النمط يتطابق مع بنية برامج جمع البيانات (Data Exfiltration) المتقدمة

التحقق النهائي القاطع يستلزم تحليلاً ديناميكياً في بيئة معزولة مع اعتراض الشبكة و هذا ما سيتم تأكيده في التقرير الديناميكي

8. API Endpoint وبنية الخلفية

البنية التحتية لخوادم الخلفية

الخادم الأساسي	**https://api.shamcash.sy/v4/api/**
الخادم الثانوي (تجاوز الفشل)	**https://api-02.shamcash.sy/v4/api/**
الخادم الثلثاني (تجاوز الفشل)	**https://api-03.shamcash.sy/v4/api/**
نقطة نهاية الخدمات المصرفية	**https://bank.shamcash.sy/v4/api/**
نقطة نهاية معالجة المدفوعات	**https://payment.shamcash.sy/v4/api/**
دردشة دعم العملاء (SaaS Chatwoot)	**https://app.chatwoot.com**

قائمة نقاط نهاية API الكاملة

تسجيل الدخول مع OTP والتحقق الثنائي	**Authentication/signin / verify / check2fa**
إدارة الحساب والأمان	**Authentication/checkKYC / logout / changePhoneNumber / changeSecurityCode**
استعادة وإعادة تعيين كلمة المرور	**ForgotPassword / ResetPassword**
إعدادات الحساب والأرصدة	**Account/balances / settings / changeLanguage / changePassword**
البحث عن حسابات والاتصال	**Account/getAccountByAddress / editContact / verifyEditContact**
إدارة الجهاز وتعطيل الحساب	**Account/AddDeviceKey / CheckCanDisable / DisableAccount**
إدارة المستلمين المفضّلين	**AccountFavorites/all / new / delete**
إنشاء الحساب الشخصي وKYC	**PersonalAccount/new/v2 / update/v2 / get / verifyIdentity / verifyIdentityCheck**
إدارة أنواع الحسابات التجارية والحكومية والمؤسسية	**CommercialAccounts / GovernmentAccount / OrganizationAccount**
المعاملات والتاريخ	**Transaction/new / logs / history-logs**
التحويلات وخدمات الصرافة	**Exchange/createTransactionToSomeone / createCashInRequest / getServices / Log**
الخدمات المصرفية	**Banks/getBanks / getAccounts / addCif / cashDeposit / cashTransfer / cashWithdraw**
دفع الفواتير	**Billing/getBillingFields / presentment / pay / log**
الدفع الإلكتروني والتعليم والطاقة	**ElectronicPayment / EducationService / Service/GreenEnergy**
محافظ Syriatel وMTN	**MtnWallet / SyriatelWallet (all / cashIn / cashOut / (recharge**
معاملات الجهات الخارجية	**ThirdParty/new / pendingTransaction / changeTransactionStatus**

الإشعارات والجلسات والحسابات الفرعية	**Notification / Session / ManageSubAccount / SubAccount**
السياسات والدعم وإصدار التطبيق	**Static/policy / support / version/new**

i جميع نقاط نهاية API تتوافق مع ميزات التطبيق المالي المتوقعة. لم تُعثَر على نقاط نهاية لرفع جهات الاتصال أو قراءة الرسائل أو الوصول إلى الموقع أو تسريب معلومات الجهاز أو أي وظيفة مراقبة.

9. حقول البيانات وتحليل KYC

ما يُرسَل إلى خلفية التطبيق

رقم هاتف المستخدم — للتعريف والـ OTP	**phone / mobile**
كلمة المرور أو PIN — مشفَّرة قبل الإرسال	**password / pin**
كلمة مرور لمرة واحدة للمصادقة والمعاملات	**otp / verification code**
رمز الجلسة — يُستخدَم بعد تسجيل الدخول	**token / access_token**
رمز إشعار Firebase — يُرسَل عبر Account/AddDeviceKey	**(device (FCM token**
اسم الجهاز ونوعه ومنصته — يُرسَل مع تسجيل الجهاز	**device_name / device_type / platform**
مبلغ المعاملة والعملة	**amount / currency_id**
عنوان المحفظة للتحويلات	**receiver address**
رقم الهوية الوطنية — للتحقق من الهوية (مطلب قانوني)	**(national_id (KYC**
صورة الوجه الأمامي للبطاقة الوطنية — لتحقق KYC	**(ID card photo (KYC**
صورة واضحة للوجه مع البطاقة الوطنية — لتحقق KYC	**(selfie with ID (KYC**
معرّف الحساب المصرفي عند ربط مصرف سوري	**bank account / CIF number**

التحقق من الهوية KYC — نتيجة مهمة

i يجمع التطبيق أرقام الهويات الوطنية وصور بطاقات الهوية وصور السيلفي كجزء من عملية التحقق من الهوية KYC. هذا مطلوب قانونياً للخدمات المالية في سوريا. تُرسَل البيانات إلى PersonalAccount/verifyIdentity على الخادم shamcash.sy .

10. حزم SDK الخارجية والتكاملات

Google ML Kit QR v17.3.0	مسح QR للمدفوعات والهوية. يعمل على الجهاز فقط. تُرسَل قياسات Firelog إلى Google.
Firebase Cloud Messaging (FCM)	إشعارات فورية للمعاملات ورموز OTP والتنبيهات.
Firebase Installations	إدارة معرّف Firebase (مطلوب لـ FCM).
Firebase Measurement Connector v19.0.0	⚠ جسر لتوجيه أحداث Firebase Analytics. يشير إلى أن Analytics قد يكون نشطاً.
Firebase Transport CCT v2.3.3	Clearcut/Firelog من Google — يُرسل قياسات ML Kit إلى Google تلقائياً.
Chatwoot Flutter SDK	دردشة دعم العملاء داخل التطبيق متصلة بـ app.chatwoot.com (منصة SaaS مفتوحة المصدر). بيانات المحادثة تُخزَّن على خادم Chatwoot.
AndroidX Biometric	بصمة الإصبع والتعرف على الوجه لتسجيل الدخول.
AndroidX Camera	مجمّع Camera2 API لمسح QR والتقاط صور الهوية.
dart_pdf / printing	توليد PDF لإيصالات المعاملات.
share_plus / url_launcher / app_links	المشاركة والروابط العميقة وفتح الروابط الخارجية.

Chatwoot — ملاحظة خصوصية مهمة

i يتصل Chatwoot SDK بـ https://app.chatwoot.com — منصة SaaS لدعم العملاء من طرف ثالث. أي بيانات محادثة مُدخَلة في دردشة الدعم تُخزَّن على خوادم Chatwoot، وليس على خوادم shamcash.sy. يجب إبلاغ المستخدمين بأن رسائل دردشة الدعم يتعامل معها طرف ثالث.

11. تكاملات شركاء الدفع

محفظة المشغّل الرقمية في سوريا — إيداع وسحب نقدي وشحن	**Syriatel Cash**
محفظة مشغّل MTN — إيداع وسحب نقدي وباقات وشحن	**MTN Cash**
صرافة وخدمة إيداع نقدي	**الفؤاد للتحويلات المالية**
خدمة تحويل مالي	**هرم الحرام للتحويلات**
ربط مصارف متعددة عبر أرقام CIF	**المصارف السورية**
دفع رسوم الجامعات والمدارس	**الخدمة التعليمية**
دفع فواتير الكهرباء والنظافة	**الطاقة الخضراء / التنظيف**
دفع الخدمات الحكومية الإلكترونية	**أنجز**
بوابة دفع فواتير إلكترونية عامة	**الفاتورة الإلكترونية**
الدفع للجهات الحكومية	**الحسابات الحكومية**
مدفوعات التاجر القائمة على QR	**التجار الخارجيون**

12.المخاطر التوصيات الأمنية:

هذا القسم مُوجَّه لثلاث جهات: المستخدمون الأفراد، والمؤسسات، وصانعو القرار. التوصيات مبنية على الأدلة التقنية الموثقة في الأقسام السابقة وليست تحذيرات نظرية.

12.1 تقييم المخاطر حسب الفئة

مستوى الخطر يتفاوت بحسب طبيعة المستخدم والبيئة:

الفئة	الوصف	مستوى الخطر
A	هاتف موظف حكومي أو مصرفي أو عامل في قطاع أمني أو مالي	بالغ الخطورة
B	هاتف شخصي يحتوي صور، وثائق، تطبيقات مراسلة (واتساب / تيليغرام)	عالٍ جداً
C	جهاز في بيئة حساسة: مستشفى، محكمة، شركة أمنية، مقر عسكري	عالٍ جداً
D	هاتف شخصي للاستخدام اليومي العادي مع وعي أمني كافٍ	متوسط
E	هاتف مخصص للتطبيق فقط — لا بيانات حساسة أخرى عليه	منخفض نسبياً

الفئات A + B + C — حكم قاطع

عدم تثبيت التطبيق على هذه الأجهزة هو الخيار الوحيد المقبول أمنياً

إذا كان مُثبَّتاً بالفعل: أوقف تشغيله فوراً وابدأ إجراء إزالة كاملة (راجع 12.5)

استخدم هاتفاً مخصصاً ورخيصاً للتطبيق فقط — هذا الحل الأمثل للمُلزَمين باستخدامه

12.2 إدارة الأذونات — استرجاع التحكم فوراً

حتى لو كان التطبيق مُثبّتاً، يمكنك تقليص نطاق وصوله بشكل جذري عبر إدارة الأذونات. هذا لا يُلغي الخطر كلياً لكنه يُقلّصه.

أ. الأذونات الحرجة التي يجب سحبها فوراً

الإذن	الخطر	القرار
MANAGE_EXTERNAL_STORAGE	وصول مطلق لكل ملفات الهاتف	✗ اسحبه فوراً
READ_MEDIA_IMAGES	الوصول لكل الصور في المعرض	✗ اسحبه
CAMERA	التقاط صور في أي وقت	⚠ قيّده
READ_CONTACTS	الوصول لجهات الاتصال كاملةً	✗ اسحبه
USE_BIOMETRIC / USE_FINGERPRINT	الوصول لبصمة الإصبع	⚠ قيّده
READ/WRITE_EXTERNAL_STORAGE	قراءة وكتابة التخزين الخارجي	✗ اسحبه

ب. خطوات سحب إذن MANAGE_EXTERNAL_STORAGE تحديداً (الأخطر)

هذا الإذن يحتاج مساراً خاصاً على Android 11+:

1. الإعدادات ← التطبيقات ← شام كاش ← الأذونات
2. ابحث عن 'الملفات والوسائط' أو 'Storage'
3. اختر: 'لا يُسمح' أو 'مجلد التطبيق فقط'
4. مسار بديل: الإعدادات ← الخصوصية ← مدير الأذونات ← إدارة كل الملفات
5. تحقق أن التطبيق لم يعد يظهر في قائمة 'إدارة كل الملفات'

> ⚠ **تحذير مهم — سحب الأذونات ليس كافياً**
>
> **Firebase Background Messaging يعمل حتى بدون أذونات صريحة**
>
> **الكود المُنفَّذ عند استقبال Silent Push لا يحتاج إذناً مسبقاً**
>
> **سحب الأذونات يُقلّص الخطر لكنه لا يُلغيه — الإزالة الكاملة هي الحل الأمثل**

12.3 عزل الشبكة — قطع اتصال التطبيق بالخادم

إذا كنت مُضطراً للإبقاء على التطبيق، عزل اتصاله بالشبكة يُلغي معظم المخاطر المرتبطة بـ C2:

أ. على مستوى الهاتف

- ✓ استخدم 'Data Saver' أو 'تقييد البيانات في الخلفية' لشام كاش
- ✓ في الإعدادات ← التطبيقات ← شام كاش: أوقف 'البيانات في الخلفية' (Background Data)
- ✓ استخدم VPN مع قواعد Firewall لحجب النطاقات: shamcash.sy / shamlogix.com
- ✓ على هواتف Samsung: استخدم 'Smart Manager' لحظر اتصال التطبيق في الخلفية

ب. على مستوى الشبكة المنزلية أو المؤسسية

- ✓ أضف هذه النطاقات لقائمة الحظر في الـ DNS أو Firewall:
  - api.shamcash.sy | api-02.shamcash.sy | api-03.shamcash.sy
  - bank.shamcash.sy | www.shamlogix.com
  - نطاق IP بالكامل: 191.44.71.0/24
- ✓ استخدم Pi-hole أو AdGuard Home لحظر هذه النطاقات على مستوى الشبكة

12.4 الحل الأمثل للمُلزَمين بالاستخدام — هاتف مخصص

الموظفون الحكوميون المُلزَمون باستخدام شام كاش لاستلام رواتبهم يواجهون معضلة حقيقية. الحل العملي الأمثل هو هاتف Android رخيص مخصص للتطبيق فقط.

مواصفات الهاتف المخصص الآمن

- **هاتف Android رخيص (50-100 دولار كافٍ) — لا حاجة لجهاز متطور**
- **لا تُثبّت عليه: واتساب، تيليغرام، تطبيقات بنكية، البريد الإلكتروني، أي صور**
- **لا تُسجّل حساب Google مرتبطاً بهويتك الرئيسية — أنشئ حساباً مخصصاً**
- **أوقف تشغيله بعد الانتهاء من استخدام شام كاش مباشرةً**
- **لا تتصل به بشبكة WiFi المنزلية أو المؤسسية — استخدم بيانات الجوال فقط**
- **لا تُمنحه أي أذون تخزين — ارفض جميع طلبات الأذونات غير الضرورية عند التثبيت**

12.5 توصيات المؤسسات — سياسة أمن المعلومات

أ. الجهات التي يجب أن تحظر التطبيق على أجهزتها الرسمية

- **الوزارات والمديريات الحكومية — خطر تسريب وثائق رسمية عبر MANAGE_EXTERNAL_STORAGE**
- **البنوك والمؤسسات المالية — تعارض مباشر مع سياسات PCI-DSS وأمن البيانات المالية**
- **المستشفيات والمراكز الصحية — بيانات المرضى على نفس الجهاز**
- **المؤسسات الأمنية والعسكرية والدفاعية — معلومات بالغة الحساسية**
- **المحاكم والنيابات العامة — وثائق قضائية سرية**
- **شركات الاتصالات والبنية التحتية — بيانات الشبكة والمشتركين**

13. الشركة المطورة والمشغّل الرئيسي

هوية الجهة المطورة لتطبيق ShamCash تمثّل أحد أكثر جوانب الملف غموضاً وإثارةً للقلق. لا يوجد حتى اللحظة أي إفصاح رسمي أو قانوني عن الكيان المسؤول — وهو ما رصدته منظمات حقوق رقمية متعددة وأكّده تقرير SMEX الصادر في فبراير 2026.

13.1 ما هو مؤكَّد — الأدلة الموثقة

غياب التوثيق الرسمي الكامل

لا يوجد اسم شركة مطوّرة مُعلَن في الـ APK أو موقع التطبيق أو أي وثيقة رسمية

لا سياسة خصوصية منشورة — شرط أساسي في أي تطبيق مالي شرعي

شروط الاستخدام التسعة المنشورة تُعفي التطبيق صراحةً من أي مسؤولية عن الاختراقات

التطبيق غير متاح على Google Play أو Apple Store — تحاشياً لعمليات المراجعة الأمنية

13.2 NorthSoft — المطوّر المُرجَّح

رصدنا من تقارير مستقلة متعددة إشارات موثوقة تربط التطبيق بشركة تركية تُدعى NorthSoft متخصصة في حلول البرمجة و هذا ما اكتشفناه و اكدناه خلال التحليل و ما تم كشفه من ملف الشهادة ca.crt

CN=NorthSoft, OU=ShamCash, O=ShamCash (موقَّعة ذاتياً)

الشهادة ذاتية التوقيع — NorthSoft

- الشهادة غير صادرة من CA موثوقة علناً. موقَّعة ذاتياً من شركة 'NorthSoft' وهي المطوّر.
- أي مستخدم يثبّت APK مباشرة لا يستطيع التحقق من أن الشهادة من مطوّر ShamCash الشرعي.
- نسخة مُعاد تغليفها ضارة يمكن توقيعها بأي شهادة أخرى وتوزيعها عبر قنوات غير رسمية.

الجانب	التفاصيل
الاسم التجاري	NorthSoft
البلد	تركيا (مُرجَّح)
التخصص	حلول برمجية وتقنية — Flutter / Mobile
مستوى التوثيق	⚠ معلومات من مصادر مُطّلعة — لا إفصاح رسمي
الصلة بـ Turkcell	مصادر أخرى أشارت لارتباط محتمل بـ Turkcell

لماذا الغموض مقصود

شركة تطوير مجهولة الهوية تعني: لا جهة قانونية مسؤولة في حال اختراق البيانات

غياب الكيان القانوني يمنع المستخدمين من أي مسار قانوني للتظلم

التطبيق إلزامي لموظفي القطاع العام السوري دون أي شفافية — مئات الآلاف من الأشخاص

13.3 ShamLogix — المطوّر التقني للـ API

التحقيق التقني كشف وجود شركة مرتبطة ارتباطاً مباشراً بالبنية التحتية للتطبيق: shamlogix.com — المطوّر التقني المُرجَّح لطبقة الـ API.

الجانب	التفاصيل
اسم النطاق	shamlogix.com | www.shamlogix.com
تاريخ التسجيل	مايو 2025 — متزامن مع إطلاق التطبيق
عنوان IP	191.44.71.77 — نفس نطاق خوادم ShamCash
IP تقني آخر	164.138.205.134 — تركيا (إدلب — مُؤكَّد)
وصف الشركة	تطوير أنظمة برمجية وقواعد بيانات وUI/UX
الشفافية	⚠ تُعلن أسماء المطورين — لكنها تُخفي أسماء الملّاك
البنية التحتية	Mikrotik router مكشوف — بلا VPN أو جدار حماية

ثلاثة مؤشرات حمراء في ShamLogix

تسجيل النطاق في مايو 2025 متزامن مع إطلاق ShamCash — ليس تزامناً عرضياً

عنوان IP التقني في إدلب (تركيا) مكشوف بلا حماية — Mikrotik router بمنفذ مفتوح عام

الشركة تُفصح عن المطورين لكن تُخفي الملّاك — نمط متعمد لتفادي المساءلة

13.4 الروابط المالية — من يستفيد؟

كشف التحليل المالي ارتباطات تجارية مثيرة للقلق تتجاوز التطبيق نفسه:

- Cham Bank إدلب: مكتب صرافة مسجّل في تركيا — لا اعتراف دولي — التحويلات تمر عبره
- شركتا الحرام والفؤاد: شريكتان رئيسيتان لسحب الرواتب — ارتباطات بالنظام السابق
- العمولات: يُقدَّر مجموع العمولات السنوية لشركتَي السحب بـ 3 ملايين دولار
- التحويلات تتجاوز البنك المركزي السوري والنظام المصرفي الدولي
- امتصاص منصة Sawa: وُجّهت اتهامات للتطبيق باستيعاب منافس قائم وأصوله قسراً

13.5 ملخص هوية المشغّل

i الصورة الإجمالية الموثوقة

المشغّل الرسمي: غير مُعلَن — لا كيان قانوني مسجّل يتحمل المسؤولية

المطوّر التقني المُرجَّح: NorthSoft التركية (مصادر مُطّلعة — دون تأكيد رسمي)

مطوّر الـ API الموثق: ShamLogix — مرتبط بنفس البنية التحتية وأُسس في نفس التوقيت

البُعد الجغرافي: إدلب ← تركيا ← بنية تحتية سورية ← reverse proxy أمريكي

المستفيد المالي المباشر: شركتا الحرام والفؤاد + Cham Bank إدلب

---

14. البنية التحتية للخوادم — التحليل الجغرافي والشبكي

تحليل DNS والبنية التحتية الشبكية يكشف بنية متعددة الطبقات مصمَّمة لإخفاء الموقع الجغرافي الحقيقي للخوادم وتعمية الهوية التشغيلية للتطبيق.

14.1 خريطة النطاقات والعناوين الشبكية

النطاق	عنوان IP	الموقع الجغرافي	ASN	شركة الاستضافة
api.shamcash.sy	191.44.71.70	بولاند، أوهايو (نقطة عبور)	216472	High Speed For Internet L.L.C
api-02.shamcash.sy	191.44.71.70	بولاند، أوهايو (نقطة عبور)	216472	High Speed For Internet L.L.C
api-03.shamcash.sy	191.44.71.70	بولاند، أوهايو (نقطة عبور)	216472	High Speed For Internet L.L.C

bank.shamcash.sy	191.44.71.70	بولاند، أوهايو (نقطة عبور)	216472	High Speed For Internet L.L.C
www.shamlogix.com	191.44.71.77	بولاند، أوهايو (نقطة عبور)	216472	High Speed For Internet L.L.C
[خوادم إدلب]	164.138.205.134	إدلب / تركيا	—	ShamLogix (Mikrotik مكشوف)
[خوادم حكومية سورية]	185.216.132.67	سوريا (داخلي)	—	هيئة خدمات الشبكة الوطنية
app.chatwoot.com	32.193.123.29	الولايات المتحدة	14618	Amazon Web Services
firebaseinstallations.googleapis.com	142.251.211.138	الولايات المتحدة	15169	Google LLC

14.2 طبقة أوهايو — الواجهة الخارجية (Reverse Proxy)

جميع نطاقات ShamCash الحساسة (api, api-02, api-03, bank) تشير لعنوان IP واحد موحَّد في نطاق 191.44.71.x. هذا ليس موقع الخوادم الحقيقية.

i ما هو Reverse Proxy وكيف يعمل

الـ Reverse Proxy هو خادم وسيط يستقبل الطلبات ويُعيد توجيهها للخادم الحقيقي

الغرض المُعلَن: حماية الخوادم من الهجمات المباشرة (WAF / DDoS Protection)

الغرض الأمني الإضافي: إخفاء عنوان IP الخادم الحقيقي عن أي شخص يحلل الشبكة

GIGAGROUP Sp. z o.o. هي شركة الترانزيت الدولية المسؤولة عن نقطة أوهايو

موقع ASN 216472 الرسمي: سوريا — رغم أن نقطة الظهور في أوهايو أمريكا

14.3 ASN 216472 — High Speed For Internet Services L.L.C

هذا هو العنصر الأكثر أهمية في تحليل البنية التحتية. ASN 216472 هو المعرّف الشبكي المستقل العالمي المسؤول عن كافة العناوين والنطاقات المرتبطة بالتطبيق.

الخاصية	القيمة
رقم ASN	AS216472
الاسم التجاري	High Speed For Internet Services L.L.C
الاسم الشبكي	HS-SYR
سجل RIPE	مُسجَّل رسمياً في RIPE NCC الأوروبية
المقر القانوني	سوريا
نطاق IP المُدار	191.44.71.0/24 وما يجاوره

دلالة ASN السوري مع نقطة ظهور أمريكية

الشركة سورية قانونياً — لكن حركة البيانات تمر عبر أوهايو أمريكا كنقطة ظهور

هذا نمط شائع لدى الشركات السورية التي تحتاج اتصالاً دولياً مستقراً وسريعاً

لكنه أيضاً يجعل تتبع الخادم الحقيقي أصعب بكثير من الناحية الجنائية

14.4 طبقة إسطنبول — العمود الفقري الإقليمي

بسبب محدودية الربط المباشر للشبكات السورية بالعمود الفقري العالمي للإنترنت، تعتمد البنية التحتية على نقاط تواجد (PoPs) في إسطنبول تركيا.

- حركة البيانات: المستخدم السوري ← خوادم داخلية ← إسطنبول ← أوهايو ← المستخدم
- PoPs إسطنبول توفر: استجابة منخفضة (Low Latency) واستقرار أعلى للخدمة
- IP إدلب (164.138.205.134): نقطة تطوير تشغيلية تابعة لـ ShamLogix بلا حماية
- Mikrotik router مكشوف في إدلب: منفذ عام مفتوح — بلا VPN أو firewall — ثغرة أمنية فادحة

14.5 الخادم الحكومي السوري — اكتشاف بالغ الخطورة

كشف تحليل مستقل أجراه الخبير ديلشاد عثمان أن نطاقات التطبيق الفرعية تشير أحياناً لعنوان IP سوري داخلي (185.216.132.67) تابع لهيئة خدمات الشبكة الوطنية.

خطورة الاستضافة على الخادم الحكومي

هذا الخادم يستضيف في آنٍ واحد: تطبيق ShamCash + مواقع حكومية حساسة متعددة

جميعها تحت إدارة لوحة تحكم Ple sk الواحدة — بابٌ واحد لكل شيء

ثغرة في ShamCash = lateral movement محتمل لاختراق مواقع حكومية أخرى

الخبير عثمان حدّد ثغرة فعلية تُتيح هذا الانتقال الجانبي بين المواقع

المستخدمون التجاريون والحكوميون معاً على نفس البنية التحتية الضعيفة

14.6 رسم البنية التحتية — التسلسل الكامل

مسار البيانات من الجهاز للخادم الحقيقي:

[جهاز المستخدم]

↓ HTTPS مُشفَّر بـ CA خاصة

[نقطة أوهايو — 191.44.71.70] ← Reverse Proxy / WAF

↓ TLS داخلي

[PoPs إسطنبول] ← Transit عبر تركيا

↓

[185.216.132.67] ← خادم سوري حكومي (Plesk)

أو

[164.138.205.134] ← ShamLogix إدلب (Mikrotik مكشوف)

لماذا هذه البنية مثيرة للقلق أمنياً

طبقات متعددة من الـ Reverse Proxy تجعل تحديد الخادم الحقيقي شبه مستحيل

CA خاصة تمنع اعتراض الاتصال وفحص محتواه بأي أداة تجارية

استضافة على خادم حكومي تُضيف بُعداً سيادياً — من يتحكم بالخادم يتحكم بالبيانات

ShamLogix في إدلب بلا حماية = نقطة ضعف مكشوفة يمكن استغلالها لاختراق البنية كلها

Chatwoot) Amazon) وFirebase) Google) كطبقات خدمات إضافية — قناتا اتصال موثوقتان مُستغَلَّتان

14.7 الخلاصة الجغرافية

تلخيص البنية التحتية

الجهة المالكة للـ ASN: High Speed For Internet Services L.L.C — سوريا (HS-SYR)

نقطة الظهور الخارجية: أوهايو، الولايات المتحدة — Reverse Proxy) GIGAGROUP)

طبقة الترانزيت الإقليمية: إسطنبول، تركيا (PoPs)

الخوادم الداخلية: سوريا (خادم حكومي Plesk) + إدلب/تركيا (ShamLogix)

الخدمات الخارجية المُدمَجة: Amazon AWS (Chatwoot) + Google Firebase

المسؤول التقني الفعلي: غير مُحدَّد رسمياً — يرتبط بـ NorthSoftg ShamLogix