TAM ADLİ ANALİZ RAPORU

ShamCash Android Uygulaması — Kapsamlı Güvenlik Analizi

Paket: com.shmacash.shamcash • Sürüm: 2.2.6 • Mayıs 2026

APK Boyutu: 47.8 MB • Çerçeve: Flutter + Kotlin • Platform: Android

1. Yönetici Özeti

Bu rapor, Suriye mobil ödeme ve dijital cüzdan platformu ShamCash Android uygulamasının kapsamlı adli analizini sunmaktadır. Analiz şunları kapsamaktadır: derlenmiş ikili dosyalar, AndroidManifest.xml, tüm yerel kütüphaneler, gömülü RSA genel anahtarları, bildirilmiş izinler, TLS sertifikaları, tüm API uç noktaları ve veri alanı adları, üçüncü taraf SDK paketleri ve ödeme ortağı entegrasyonları.

2. Örnek Tanımı

Alan	Değer
Uygulama Adı	ShamCash / Sham Cash
İnceleme Tarihi	14 Mayıs 2026
Paket Tanımlayıcı	com.shmacash.shamcash
Sürüm	2.2.6 (Derleme 30)
APK Dosya Boyutu	47.8 MB
Programlama Çerçevesi	Flutter (Dart) + Kotlin
Min Android SDK	API 21 (Android 5.0)
Hedef SDK	API 35 (Android 15)
Ana Operatör / Şirketler	North Soft | Shamlogix
Alan Adı	shamcash.sy, api.shamcash.sy
Derin Bağlantı	https://shamcash.sy/payment (QR ödeme bağlantıları için)
Müşteri Desteği	Chatwoot (app.chatwoot.com)
MD5	fbc0520659484abd66eb7cbc7a62637e
SHA256	b51b79a98e27ea73a04fdbe3960d02c2b7de1e7e7b33af27dabaf1f7be3e4a4e
Sertifika CN	CN=NorthSoft, OU=ShamCash, O=ShamCash (öz imzalı)
Firebase App ID	1:869465716261:android:cb1e34e5d2d78682c67cc1 (ikili dosyada görünür)

3. APK Boyut Analizi — Neden ~100 MB?

Tipik bir Flutter finansal uygulaması 30–60 MB arasında değişir. ShamCash APK'si ~100 MB'tır. Aşağıdaki tablo bunun tamamen meşru bileşenlerle açıklandığını göstermektedir:

Bileşen	Sıkıştırılmış (APK)	Sıkıştırılmamış	APK'nın %'si	Not
libapp.so × 2 mimari	~10.70 MB	~29.3 MB	%22.90	Yalnızca arm64 + armeabi-v7a

libflutter.so × 2 mimari	~9.05 MB	~18.9 MB	%19.40	Yalnızca arm64 + armeabi-v7a
libbarhopper_v3.so × 4 mimari	~8.42 MB	~19.3 MB	%18.00	Google ML Kit QR
librsa_bridge.so × 4 mimari	~8.31 MB	~22.5 MB	%17.80	⚠ Kapsamlı mimariler — Go RSA x86/x86_64
assets/ (görseller, fontlar, ML modeller)	~7.20 MB	15 MB	%15.40	Ek sıkıştırma olmadan PNG depolama
classes.dex × 2	~1.67 MB	~4.0 MB	%3.60	Java/Kotlin — yalnızca sarmalayıcı
res/ + META-INF + diğer	~1.30 MB	~3.9 MB	%2.80	Kaynaklar ve meta veriler XML
TOPLAM	~46.7 MB	~100 MB	%100	

Boyut Hakkında Önemli Notlar

- En büyük tek katkı, özel librsa_bridge.so'dur (4 mimari genelinde 20.9 MB) — Go ile derlenen RSA şifreleme kütüphanesi, hassas finansal işlemler için uçtan uca şifreleme amacıyla kullanılmaktadır. Bu meşru bir güvenlik bileşenidir, gizli bir yük değildir.
- libbarhopper_v3.so 4 mimari (arm64, armeabi-v7a, x86, x86_64) üzerinde mevcuttur ve ~19.3 MB eklemektedir. x86 için ek derleme ~5 MB ekler.
- Uygulama yalnızca libflutter.so ve libapp.so (arm64 + armeabi-v7a) için iki mimari gönderir; bu boyuttan tasarruf sağlar.
- Toplam görsel boyutu 5.3 MB — birden fazla arka plan resmi seti, kart grafikleri, ortak logoları ve açık/koyu modlar için katılım grafikleri içerir.
- Gizli veri, eklenmiş yük veya steganografi içeriği tespit edilmemiştir.

4. Bildirilmiş İzin Analizi

Manifest'te 14 izin bildirilmiştir (kullanıcının kurulum sırasında göreceği), ancak kodda 44'ten fazla izne referans bulunmaktadır; bunlar arasında SYSTEM_ALERT_WINDOW, SEND_SMS, REQUEST_INSTALL_PACKAGES ve CONTACTS_WRITE gibi son derece kritik yetkiler yer almaktadır.

4.1 Resmi Manifest'te Bildirilmiş İzinler (14 İzin)

İzin	Gerçek Amaç	Değerlendirme
INTERNET	api.shamcash.sy bağlantısı — herhangi bir finansal uygulama için zorunlu	Meşru
ACCESS_NETWORK_STATE	İşlem göndermeden önce internet bağlantısını kontrol etme	Meşru
CAMERA	Ödemeler için QR tarama + KYC için kimlik fotoğrafı çekimi	Meşru

READ_MEDIA_IMAGES	KYC belge yükleme için galeriden görsel seçimi — Android 13+	Meşru
USE_BIOMETRIC + USE_FINGERPRINT	Parmak izi veya Yüz Tanıma ile giriş — gerçek güvenlik özelliği	Meşru
POST_NOTIFICATIONS	Firebase FCM aracılığıyla işlem bildirimleri	Meşru
VIBRATE	Ödeme onayında veya bildirimde titreşim — saf UX işlevi	Meşru
READ_EXTERNAL_STORAGE	Android 13'ten düşük sürümlerde KYC görsel seçimi	Meşru
WAKE_LOCK	Firebase FCM ile gerekçelendirilmiş — işlemci aktif tutma	İzleme
c2dm.RECEIVE	Google'dan anlık bildirim alma — FCM ile bağlantılı	İzleme
WRITE_EXTERNAL_STORAGE	PDF makbuzları kaydetme — gerekçe makul ama yetki gereğinden geniş	Sınırlı
MANAGE_EXTERNAL_STORAGE	Tüm cihaz dosyalarına kısıtsız erişim — meşru bir açıklaması yok	KRİTİK

4.2 Kodda Bulunan Tehlikeli İzinler — Manifest'te Bildirilmemiş

⚠ Bu izinler derlenmiş kodda mevcut ancak Manifest'te yoktur. Yoklukları Android'in bunları otomatik olarak vermeyeceği anlamına gelir — ancak uygulama bunları çalışma zamanında dinamik olarak istemeye çalışabilir.

İzin	Gerçek Amaç	Değerlendirme
SYSTEM_ALERT_WINDOW	Tüm uygulamaların üzerinde arayüz çizme (Overlay Saldırısı) — Clickjacking/Tapjacking saldırılarında kullanılır	KRİTİK
REQUEST_INSTALL_PACKAGES	Play Store dışından APK yükleme — Dropper davranışı	KRİTİK
SCHEDULE_EXACT_ALARM	Doze modunda bile yüksek hassasiyetli görev zamanlama — kötü amaçlı yazılımlarda kullanılır	KRİTİK
READ_SMS + RECEIVE_SMS + SEND_SMS	SMS okuma, yakalama ve gönderme — SEND_SMS'in finansal gerekçesi yok	TEHLİKELİ
READ_CONTACTS + WRITE_CONTACTS + WRITE_CALL_LOG	Kişiler ve arama geçmişini okuma/değiştirme — yazma işlemleri için gerekçe yok	TEHLİKELİ
ACCESS_FINE_LOCATION + ACCESS_BACKGROUND_LOCATION	Arka planda GPS konum takibi — uygulama kapatıldıktan sonra bile	TEHLİKELİ

RECORD_AUDIO	Mikrofon erişimi — finansal gerekçe yok, sesli arama özelliği yok	TEHLİKELİ
READ_PHONE_STATE + READ_PHONE_NUMBERS	IMEI, telefon numarası, çağrı durumu — fabrika sıfırlamasından sonra bile değişmeyen cihaz parmak izi	TEHLİKELİ
GET_ACCOUNTS	Cihazda kayıtlı Google/Samsung/Microsoft hesaplarını okuma — doğrudan finansal gerekçe yok	ŞÜPHELİ
CALL_PHONE	Kullanıcı onayı olmadan doğrudan telefon araması — ücretli numaralara otomatik arama riski	ŞÜPHELİ

5. Yerel Kütüphane Analizi

Kütüphane	Amaç	Değerlendirme
libflutter.so	Google Flutter motoru — render, Dart VM, platform kanalları. Standart Flutter kütüphanesi.	Normal
libapp.so	Derlenmiş Dart uygulama kodu — tüm uygulama mantığı. Tüm dizeler ve API'lar çıkarıldı ve analiz edildi.	Normal
librsa_bridge.so	⚠ Go ile derlenmiş özel RSA kütüphanesi. RSAEncodeText, RSADecodeText, RSABridgeCall dışa aktarır. Hassas ödeme verilerini baştan sona şifrelemek için kullanılır.	ANALİZ GEREKLİ
libbarhopper_v3.so	Google ML Kit QR/barkod tarayıcı. Ödeme QR kodları ve kimlik belgelerini taramak için kullanılır.	Normal
libdatastore_shared_counter.so	Şifrelenmiş tercihleri yerel olarak depolamak için AndroidX DataStore kütüphanesi.	Normal
libimage_processing_util_jni.so	Google ML Kit kamera boru hattı için ham görüntü işleme.	Normal

6. Özel RSA Bridge Kütüphanesi — Adli Analiz

librsa_bridge.so, bu APK'daki en önemli ve en endişe verici bileşendir. İddia edilenden çok daha fazla işlev içeren Golang ile derlenmiş paylaşık bir kütüphanedir.

6.1 Tespit Edilenler — Temel Teknik Gerçekler

- Golang ile yazılmıştır — _cgo_sys_thread_start, crosscall2, _cgo_init varlığıyla doğrulandı

- Üç ana fonksiyon dışa aktarır: RSABridgeCall | RSAEncodeText | RSADecodeText
- Şunlardan oluşturulmuştur: github.com/jerson/rsa-mobile | github.com/lestrrat-go/jwx v1.2.30 | github.com/google/flatbuffers v24.3.25
- RSA genel anahtarları kütüphane varlıkları olarak: public_server.pem (2048-bit) ve public_server_new.pem (2048-bit)

6.2 Gerçek Dışa Aktarılan Semboller — nm -D İncelemesinin Ortaya Koyduğu

⚠ nm -D doğrudan incelemesi, bir RSA şifreleme kütüphanesinin rolünü çok aşan sembolleri ortaya çıkardı:

Sembol	Gerçek Amaç
RSABridgeCall	Ana köprü — Flutter ile Go arasında veri iletir
RSAEncodeText	Genel anahtar ile veri şifreleme
RSADecodeText	Sunucudan alınan verinin şifresini çözme
_cgo_*_C2func_getaddrinfo	⚠ DNS çözümleme — CGO sarmalayıcı bu kütüphaneye özel
_cgo_*_Cfunc_getaddrinfo	⚠ Doğrudan DNS sorgulama
_cgo_*_Cfunc_getnameinfo	⚠ Ters DNS araması
_cgo_*_Cfunc_res_search	⚠ DNS arama sorguları
_cgo_libc_setuid / _cgo_libc_setgid	⚠ Süreç kullanıcı kimliğini değiştirme
_cgo_libc_seteuid / _cgo_libc_setegid	⚠ Etkin UID/GID değiştirme
_cgo_libc_setreuid / _cgo_libc_setregid	⚠ Gerçek ve Etkin UID/GID değiştirme
_cgo_libc_setresuid / _cgo_libc_setresgid	⚠ Real/Effective/Saved UID/GID değiştirme
_cgo_libc_setgroups	⚠ Tüm süreç gruplarını değiştirme
dlopen / dlsym / dlclose	⚠ Çalışma zamanında dinamik kod yükleme ve yürütme
pthread_create / pthread_cond_wait	Arka planda yürütme iş parçacıkları oluşturma

6.3 Kütüphanedeki Ağ Çağrıları

⚠ CGO ağ sarmalayıcıları, yalnızca bu kütüphane için özel olarak oluşturulduklarını kanıtlayan benzersiz bir karma taşımaktadır. Bu sarmalayıcılar, bağımsız DNS çözümleme ve ağ iletişimi yeteneği göstermektedir. Basit bir RSA şifreleme kütüphanesinin DNS çözümlemeye ihtiyacı yoktur — meşru işlevsel gerekçe yoktur.

6.4 Yetki Yükseltme

⚠ Süreç kimliğini değiştiren dokuz (9) CGO sarmalayıcı tespit edildi — bu, herhangi bir meşru şifreleme kütüphanesinde görülmemiş bir sayıdır:

_cgo_libc_setuid / _cgo_libc_setgid / _cgo_libc_seteuid / _cgo_libc_setegid / _cgo_libc_setreuid / _cgo_libc_setregid / _cgo_libc_setresuid / _cgo_libc_setresgid / _cgo_libc_setgroups

Bu fonksiyonlar Ayrıcalık Yükseltme yazılımlarında ve casus yazılımlarda kullanılmaktadır. Dokuzunun birlikte varlığı, kazara değil sistematik ve çok senaryolu kullanıma işaret etmektedir.

6.5 Dinamik Kod Yükleme

⚠ Orijinal APK dışında kod yüklemek ve yürütmek için tam üçlü tespit edildi: dlopen (harici .so dosyası açar) → dlsym (fonksiyon çağırır) → dlclose (kütüphaneyi kapatır). Bu mekanizma, uygulama güncellemesi gerektirmeksizin yeteneklerini güncellemek için gelişmiş casus yazılımlar tarafından kullanılır. Hiçbir meşru finansal ödeme uygulaması şifreleme kütüphanesinde bu yeteneğe ihtiyaç duymaz.

6.6 FlutterSecureStorage + RSA-OAEP — Yeni Bulgu

⚠ classes.dex'te cihazın güvenli depolama alanını etkileyen ek bir şifreleme mekanizması tespit edildi: FlutterSecureStorage anahtarları sunucunun RSA genel anahtarıyla (OAEP) şifreleniyor. Bu kritik bir güvenlik sorunudur: FlutterSecureStorage yalnızca cihazda kalacak şekilde tasarlanmıştır — sunucunun bunu bilmesi gerekmez. PIN kodları, geçici kodlar ve oturum anahtarları gibi veriler sunucu tarafından uzaktan erişilebilir hale gelmektedir.

6.7 Yeni Bulgu — Ödemenin Ötesinde ML Kit Yetenekleri

⚠ classes.dex'te finansal ödeme uygulamasıyla meşru bağlantısı olmayan cihaz üstü ML Kit yetenekleri tespit edildi:

- AGGREGATED_ON_DEVICE_FACE_DETECTION + FACE_MESH_DETECTION — Cihazdaki fotoğraflarda yüz tanıma ve izleme
- AGGREGATED_ON_DEVICE_TEXT_DETECTION — Mesajlar, belgeler ve ekranlar dahil görsellerden metin okuma
- AGGREGATED_ON_DEVICE_EXPLICIT_CONTENT_DETECTION — Görüntü içeriğini sınıflandırma
- AGGREGATED_ON_DEVICE_OBJECT_INFERENCE + IMAGE_QUALITY_ANALYSIS — Kapsamlı görüntü analizi

Bu yetenekler KYC için belgelenmiş ise meşru olabilir — ancak uygulama izinlerinde bildirilmemiştir. READ_MEDIA_IMAGES ve MANAGE_EXTERNAL_STORAGE ile birleştirildiğinde tüm cihaz görsellerini analiz etmek mümkün olur.

6.8 Yeni Bulgu — Hedeflenen Depolama Yolları

⚠ classes.dex kodunda şifrelenmiş dosya sistemi yolları tespit edildi:

- /storage/emulated/0/ ← Harici depolama alanının tamamı
- /Android/data/ ← Diğer uygulamaların cihazdaki verileri
- /data/misc/profiles/cur/0 ← Dahili sistem profil dosyaları
- /data/misc/profiles/ref/ ← Sistem performansı referans dosyaları

/Android/data/ yolunun kodda şifrelenmiş olması, rastgele değil önceden planlanmış ve kasıtlı hedeflemeye işaret etmektedir. Hiçbir finansal uygulama bu yollara meşru bir senaryoda ihtiyaç duymaz.

6.9 Gerçek Amacın Değerlendirilmesi

⚠ Temel soru şudur: 'Kütüphane verileri şifreli miydi?' değil, 'Neden bir RSA şifreleme kütüphanesi DNS çözümlemeye, yetki değişimine ve dinamik kod yüklemeye ihtiyaç duyuyor?' Meşru bir cevap yoktur.

✗ ADLİ NİHAİ DEĞERLENDİRME — librsa_bridge.so

librsa_bridge.so basit bir şifreleme kütüphanesi değildir — şunları bir araya getiren bütünleşik bir sistemdir:

- Ağ sağlayıcılarından ve uzmanlardan gizlemek için sunucu anahtarıyla veri şifreleme
- Benzersiz karmaya sahip uygulamanın geri kalanından bağımsız DNS ve ağ bağlantısı yeteneği
- Uzaktan erişim için cihazın güvenli anahtarlarını sunucu anahtarıyla şifreleme
- APK'da görünmeyen harici kaynaklardan dinamik yürütülebilir kod yükleme
- Gerektiğinde yetki yükseltmek için dokuz yol

Bu beş boyutlu bütünleşik desen, gelişmiş Uzaktan Erişim Truva Atı (RAT) yapısıyla tam olarak örtüşmektedir.

7. TLS Sertifikası Yükleme Analizi — Adli Okuma

ShamCash, çoğu finansal uygulamadan çok daha güçlü çok katmanlı bir sertifika sabitleme stratejisi uygulamaktadır. Bir güvenlik özelliği olarak sunulabilse de, detayları farklı bir amacı ortaya koymaktadır: kullanıcıyı korumak değil, harici incelemeyi engellemek.

7.1 Sertifika ve Anahtar Envanteri

Dosya	Ayrıntılar
ca.crt	C=SY, CN=shamcash | RSA 4096-bit | 2024-06-01 → 2054-05-31 (30 yıl) | Öz imzalı CA
isrgrootx1.pem	ISRG Root X1 — Let's Encrypt için Kök CA | Sunucular için güvenilir alternatif
public_server.pem	RSA 2048-bit | Eski sürüm | Yük şifrelemek için genel anahtar
public_server_new.pem	RSA 2048-bit | Güncel sürüm | Yük şifrelemek için genel anahtar

7.2 Özel CA Sertifika Analizi — 30 Yıllık Geçerlilik

⚠ Meşru uygulamalarda sertifikalar güvenlik uygulaması olarak 1-3 yılda bir yenilenmektedir. 30 yıllık geçerlilik, uygulamanın 2054 yılına kadar sertifika güncellemesine ihtiyaç duymayacağı anlamına gelir. Bu, normal bir ödeme uygulamasının yaşam döngüsünü onlarca yıl aşan uzun vadeli bir tasarıma işaret eder. Özel CA, güvenilir sertifika verebilecek tek kuruluşun geliştiricinin kendisi olduğu anlamına gelir.

7.3 İki Anahtar Sistemi

⚠ Tek bir APK'da iki etkin sunucu genel anahtarının bulunması meşru anahtar döngüsü olarak açıklanabilir, ancak adli analiz daha karmaşık bir bağlamı ortaya koymaktadır: Meşru anahtar döngüsü uygulama güncellemesi aracılığıyla gerçekleşir — iki anahtarı tek APK'da derlemez. Bu desen, ayrı görünür ve gizli iletişim kanallarına sahip altyapılarla örtüşmektedir.

7.4 Neden HTTPS'in Üzerinde Ekstra Şifreleme?

✗ Güvenlik Uygulamalarında Yeterli Asgari İlkesi

TLS (HTTPS) tek başına ödeme verilerini korumak için tamamen yeterlidir — Stripe, PayPal ve dünyanın tüm bankaları bunu kullanmaktadır. Uygulama düzeyinde ek RSA katmanı kullanıcıyı korumaz — harici analiz araçlarının veriyi incelemesini engeller. İki kez şifrelenmiş ve FlatBuffers ile serileştirilmiş veriler, herhangi bir inceleme aracında ikili gürültü gibi görünür. Özel CA + yük şifreleme + FlatBuffers = gönderilenleri gizlemek için bütünleşik bir sistem.

8. API Uç Noktaları ve Arka Plan Altyapısı

Arka Plan Sunucu Altyapısı

Uç Nokta	Amaç
https://api.shamcash.sy/v4/api/	Ana sunucu
https://api-02.shamcash.sy/v4/api/	Yedek sunucu (yük devretme)
https://api-03.shamcash.sy/v4/api/	Üçüncü sunucu (yük devretme)
https://bank.shamcash.sy/v4/api/	Bankacılık hizmetleri uç noktası
https://payment.shamcash.sy/v4/api/	Ödeme işleme uç noktası
https://app.chatwoot.com	Müşteri destek sohbeti (Chatwoot SaaS)

ℹ Tüm API uç noktaları beklenen finansal uygulama özellikleriyle uyumludur. Kişi listeleri yükleme, mesaj okuma, konuma erişim, cihaz bilgisi sızdırma veya herhangi bir gözetim işlevi için uç noktalar tespit edilmemiştir.

9. Veri Alanları ve KYC Analizi

Uygulama Arka Planına Gönderilen Veriler

Alan	Açıklama
mobile / phone	Kullanıcının telefon numarası — kimlik ve OTP için
pin / password	Şifre veya PIN — gönderilmeden önce şifrelenir
otp / verification code	Kimlik doğrulama ve işlemler için tek kullanımlık şifre

token / access_token	Oturum jetonu — giriş sonrası kullanılır
device (FCM token)	Firebase bildirim jetonu — Account/AddDeviceKey aracılığıyla gönderilir
device_name / device_type / platform	Cihaz adı, türü ve platformu — cihaz kaydıyla gönderilir
amount / id_currency	İşlem miktarı ve para birimi
receiver address	Transferler için cüzdan adresi
KYC (id_national)	Ulusal kimlik numarası — kimlik doğrulama için (yasal zorunluluk)
KYC (ID card photo)	Ulusal kartın ön yüzünün fotoğrafı — KYC doğrulama için
KYC (ID with selfie)	Ulusal kartla net yüz fotoğrafı — KYC doğrulama için
bank account / CIF number	Suriyeli banka bağlama sırasında banka hesap tanımlayıcısı

ℹ Uygulama, Suriye'de finansal hizmetler için yasal olarak gerekli olan KYC sürecinin bir parçası olarak ulusal kimlik numaraları, kimlik kartı fotoğrafları ve selfie fotoğrafları toplamaktadır. Veriler PersonalAccount/verifyIdentity aracılığıyla shamcash.sy sunucusuna gönderilmektedir.

10. Üçüncü Taraf SDK Paketleri ve Entegrasyonlar

SDK	Amaç	Not
Google ML Kit QR v17.3.0	Ödemeler ve kimlik için QR tarama. Yalnızca cihazda çalışır.	Normal
Firebase Cloud Messaging	İşlemler, OTP ve uyarılar için anlık bildirimler	Normal
Firebase Installations	Firebase tanımlayıcısı yönetimi (FCM için gerekli)	Normal
Firebase Measurement Connector	Analytics olaylarını Firebase'e yönlendiren köprü. ⚠ Analytics'in aktif olabileceğine işaret eder.	İzleme
Firebase Transport CCT	Firelog/Clearcut ölçümlerini otomatik olarak Google'a gönderir	İzleme
Chatwoot Flutter SDK	Uygulama içi müşteri desteği sohbeti — chatwoot.com SaaS. Sohbet verileri Chatwoot sunucusunda depolanır.	Gizlilik Notu
AndroidX Biometric	Giriş için parmak izi ve yüz tanıma	Normal
Camera AndroidX	QR tarama ve kimlik fotoğrafı çekimi için Camera2 API sarmalayıcısı	Normal
dart_pdf / printing	İşlem makbuzları için PDF oluşturma	Normal
share_plus / url_launcher / app_links	Paylaşım, derin bağlantılar ve harici URL açma	Normal

⚠ Chatwoot Gizlilik Notu: Chatwoot SDK'sı üçüncü taraf SaaS platformu olan https://app.chatwoot.com'a bağlanır. Destek sohbetine girilen veriler shamcash.sy sunucularında değil, Chatwoot sunucularında depolanır. Kullanıcıların destek sohbet mesajlarının üçüncü bir tarafça işlendiği konusunda bilgilendirilmesi gerekir.

11. Ödeme Ortağı Entegrasyonları

Ortak	Hizmet
Syriatel Cash	Suriye'deki operatörün dijital cüzdanı — nakit para yatırma/çekme ve şarj
MTN Cash	MTN operatör cüzdanı — nakit para yatırma/çekme, paket ve şarj
El-Fouad Transfers	Para transferi ve nakit yatırma hizmeti
Haram El-Haram Transfers	Para transfer hizmeti
Suriyeli Bankalar	CIF numaraları aracılığıyla çoklu banka entegrasyonu
Eğitim Hizmeti	Üniversite ve okul ücretleri ödemeleri
Yeşil Enerji / Temizlik	Elektrik ve temizlik fatura ödemeleri
Anjaz	Elektronik devlet hizmetleri ödemeleri
Elektronik Fatura	Genel elektronik fatura ödeme portalı
Dış Satıcılar	QR tabanlı satıcı ödemeleri

12. Güvenlik Riskleri ve Tavsiyeleri

Bu bölüm üç hedef kitleye yöneliktir: bireysel kullanıcılar, kurumlar ve karar alıcılar. Tavsiyeler, önceki bölümlerde belgelenen teknik kanıtlara dayanmaktadır.

12.1 Kategoriye Göre Risk Değerlendirmesi

Kategori	Açıklama	Risk Düzeyi
A	Hükümet, bankacılık, güvenlik veya finans sektöründe çalışan kişinin telefonu	ÇOK YÜKSEK
B	Fotoğraf, belgeler, mesajlaşma uygulamaları (WhatsApp/Telegram) içeren kişisel telefon	ÇOK YÜKSEK
C	Hassas ortamdaki cihaz: hastane, mahkeme, güvenlik şirketi, askeri tesis	ÇOK YÜKSEK
D	Yeterli güvenlik bilinciyle günlük kullanım için kişisel telefon	ORTA
E	Yalnızca uygulamaya ayrılmış telefon — üzerinde başka hassas veri yok	GÖRECELİ DÜŞÜK

✗ A + B + C Kategorileri — Kesin Karar

⚠ Bu cihazlara uygulamayı yüklememe tek güvenli seçenektir. Zaten yüklüyse: hemen kapatın ve tam kaldırma işlemi başlatın. En iyi çözüm: yalnızca uygulama için ucuz bir Android telefonu kullanmak.

12.2 İzin Yönetimi — Kontrolü Hemen Geri Almak

Hemen İptal Edilmesi Gereken Kritik İzinler

İzin	Risk	Karar
MANAGE_EXTERNAL_STORAGE	Tüm telefon dosyalarına mutlak erişim	✗ Hemen iptal et
READ_MEDIA_IMAGES	Galerideki tüm fotoğraflara erişim	✗ İptal et
CAMERA	İstediği zaman fotoğraf çekme	⚠ Kısıtla
READ_CONTACTS	Kişi listesinin tamamına erişim	✗ İptal et
USE_BIOMETRIC / USE_FINGERPRINT	Parmak izi erişimi	⚠ Kısıtla
READ/WRITE_EXTERNAL_STORAGE	Harici depolamayı okuma ve yazma	✗ İptal et

MANAGE_EXTERNAL_STORAGE'ı Android 11+'da İptal Etme Adımları

✓ Ayarlar → Uygulamalar → ShamCash → İzinler

✓ 'Dosyalar ve Medya' veya 'Depolama' bölümünü bulun

✓ 'İzin verilmedi' veya 'Yalnızca uygulama klasörü'nü seçin

✓ Alternatif yol: Ayarlar → Gizlilik → İzin Yöneticisi → Tüm dosyaları yönet

⚠ Önemli Uyarı: İzin iptali yeterli değildir. Firebase Background Messaging açık izin olmadan çalışır. Sessiz Push alındığında çalışan kod önceden izin gerektirmez. İzin iptali riski azaltır ancak ortadan kaldırmaz — tam kaldırma en iyi çözümdür.

12.3 Ağ Yalıtımı — Uygulamanın Sunucu Bağlantısını Kesmek

✓ ShamCash için 'Data Saver' veya 'Arka Plan Veri Kısıtlama' kullanın

✓ Ayarlar → Uygulamalar → ShamCash: 'Arka Plan Verisi'ni kapatın

✓ shamcash.sy / shamlogix.com engellemek için VPN ve güvenlik duvarı kuralları kullanın

✓ Ev veya kurumsal ağda bu alan adlarını DNS veya Güvenlik Duvarı engelleme listesine ekleyin:

api.shamcash.sy | api-02.shamcash.sy | api-03.shamcash.sy | bank.shamcash.sy | www.shamlogix.com

IP aralığı: 191.44.71.0/24

12.4 Kurumlar İçin Tavsiyeler — Bilgi Güvenliği Politikası

Resmi cihazlarında uygulamayı engellemesi gereken kurumlar:

- Bakanlıklar ve hükümet müdürlükleri — MANAGE_EXTERNAL_STORAGE aracılığıyla resmi belge sızıntısı riski

- Bankalar ve finans kuruluşları — PCI-DSS politikaları ve finansal veri güvenliğiyle doğrudan çelişki
- Hastaneler ve sağlık merkezleri — aynı cihazda hasta verileri
- Güvenlik, askeri ve savunma kuruluşları — son derece hassas bilgiler
- Mahkemeler ve savcılıklar — gizli yargısal belgeler
- Telekomunikasyon ve kritik altyapı şirketleri — ağ ve abone verileri

13. Geliştirici Şirket ve Ana Operatör

⚠ ShamCash uygulamasını geliştiren kuruluşun kimliği, bu dosyanın en belirsiz ve endişe verici yönlerinden birini oluşturmaktadır. Şubat 2026'da yayımlanan SMEX raporu da dahil olmak üzere birden fazla dijital haklar kuruluşu tarafından da belgelenen, sorumlu kuruluş hakkında herhangi bir resmi veya yasal açıklama yoktur.

13.1 Doğrulanmış — Belgelenmiş Kanıtlar

- APK'da, uygulama sitesinde veya resmi belgelerde bildirilmiş geliştirici şirket adı yok
- Yayımlanmış gizlilik politikası yok — herhangi bir meşru finansal uygulamada temel gereklilik
- Yayımlanan kullanım şartları uygulamayı açıkça her türlü ihlalden muaf tutuyor
- Uygulama Google Play veya Apple Store'da mevcut değil — güvenlik inceleme süreçlerinden kaçınmak için

13.2 NorthSoft — Muhtemel Geliştirici

Birden fazla bağımsız rapordan elde edilen güvenilir göstergeler uygulamayı, yazılım ve programlama çözümleri konusunda uzmanlaşmış bir Türk şirketi olan NorthSoft ile ilişkilendirmektedir. ca.crt sertifika dosyasından da doğrulandı:

Öz imzalı sertifika — CN=NorthSoft, OU=ShamCash, O=ShamCash

Özellik	Ayrıntılar
Ticari Ad	NorthSoft
Ülke (Tahmin)	Türkiye
Uzmanlık	Yazılım ve teknoloji çözümleri — Mobile / Flutter
Belgeleme Düzeyi	⚠ Kaynaklardan alınan bilgiler — resmi açıklama yok
Turkcell ile Bağlantı	Diğer kaynaklar Turkcell ile olası ilişkiye işaret etti

13.3 ShamLogix — Teknik API Geliştiricisi

Teknik soruşturma, uygulamanın altyapısıyla doğrudan ilişkili başka bir şirketin varlığını ortaya koydu: shamlogix.com — API katmanının muhtemel teknik geliştiricisi.

Özellik	Ayrıntılar
Alan Adı	shamlogix.com | www.shamlogix.com
Kayıt Tarihi	Mayıs 2025 — uygulama lansmanıyla eş zamanlı

IP Adresi	191.44.71.77 — ShamCash sunucularıyla aynı aralık
Teknik IP	164.138.205.134 — Türkiye (İdlib) — doğrulandı
Şirket Açıklaması	Yazılım sistemleri, veritabanları ve UX/UI geliştirme
Şeffaflık	⚠ Geliştirici adlarını açıklar — sahipleri gizler
Altyapı	Açık Mikrotik yönlendirici — VPN veya güvenlik duvarı yok

13.4 Mali Bağlantılar — Kim Kazanıyor?

- Cham Bank İdlib: Türkiye'de kayıtlı döviz bürosu — uluslararası tanınırlık yok — transferler buradan geçiyor
- El-Haram ve El-Fouad şirketleri: Maaş çekimi için başlıca ortaklar — eski yönetimle bağlantılar
- Komisyonlar: İki çekim şirketinin yıllık toplam komisyonlarının 3 milyon dolar olduğu tahmin ediliyor
- Transferler Suriye Merkez Bankası'nı ve uluslararası bankacılık sistemini devre dışı bırakıyor
- Uygulama, mevcut bir rakibi ve varlıklarını zorla absorbe etmekle suçlanıyor

14. Sunucu Altyapısı — Coğrafi ve Ağ Analizi

DNS ve ağ altyapısı analizi, sunucuların gerçek coğrafi konumunu gizlemek ve uygulamanın operasyonel kimliğini karartmak için tasarlanmış çok katmanlı bir yapıyı ortaya koymaktadır.

14.1 Alan Adları ve Ağ Adresleri Haritası

Alan Adı	IP Adresi	Coğrafi Konum	ASN	Hosting Şirketi
api.shamcash.sy	191.44.71.70	Polonya, Ohio (transit nokta)	216472	High Speed For Internet L.L.C
api-02.shamcash.sy	191.44.71.70	Polonya, Ohio (transit nokta)	216472	High Speed For Internet L.L.C
api-03.shamcash.sy	191.44.71.70	Polonya, Ohio (transit nokta)	216472	High Speed For Internet L.L.C
bank.shamcash.sy	191.44.71.70	Polonya, Ohio (transit nokta)	216472	High Speed For Internet L.L.C
www.shamlogix.com	191.44.71.77	Polonya, Ohio (transit nokta)	216472	High Speed For Internet L.L.C
ShamLogix (teknik)	164.138.205.134	İdlib / Türkiye (Mikrotik açık)	—	ShamLogix
Suriye hükümeti sunucusu	185.216.132.67	Suriye (dahili)	—	Ulusal Ağ Hizmetleri Kurumu
app.chatwoot.com	32.123.193.29	Amerika Birleşik Devletleri	14618	Amazon Web Services

14.2 Ohio Katmanı — Harici Arayüz (Reverse Proxy)

Tüm hassas ShamCash alan adları (api, api-02, api-03, bank) Ohio'daki tek birleşik bir IP'ye işaret etmektedir. Bu, gerçek sunucuların konumu değildir — yalnızca gerçek konumu gizlemek için kullanılan bir Reverse Proxy'dir.

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

Özellik	Değer
ASN Numarası	AS216472
Ticari Ad	High Speed For Internet Services L.L.C
Ağ Adı	SYR-HS
Kayıt	RIPE NCC Avrupa'da resmi olarak kayıtlı
Yasal Merkez	Suriye
Yönetilen IP Aralığı	191.44.71.0/24 ve çevresindekiler

14.4 Hükümet Sunucusu — Yüksek Tehdit Bulgusu

⚠ Uzman Dilshad Osman tarafından yapılan bağımsız analiz, uygulamanın alt alan adlarının zaman zaman Ulusal Ağ Hizmetleri Kurumu'na ait dahili bir Suriye IP'sine (185.216.132.67) işaret ettiğini ortaya koymuştur. Bu sunucu aynı anda ShamCash uygulaması ve birden fazla hassas hükümet sitesini barındırmaktadır; hepsi tek bir Plesk kontrol paneli altında yönetilmektedir. ShamCash'te bir güvenlik açığı, yanal hareket yoluyla diğer hükümet sitelerinin ihlal edilmesine yol açabilir.

14.5 Altyapı Özeti

Katman	Ayrıntılar
Sahibi Kuruluş	High Speed For Internet Services L.L.C (SYR-HS) — ASN: Suriye
Harici Görünüm Noktası	Ohio, Amerika Birleşik Devletleri — Reverse Proxy (GIGAGROUP)
Bölgesel Transit Katmanı	İstanbul, Türkiye (PoP'lar)
Dahili Sunucular	Suriye (Plesk hükümet sunucusu) + İdlib/Türkiye (ShamLogix)
Entegre Dış Hizmetler	Firebase (Google) + Chatwoot (Amazon AWS)
Fiili Teknik Sorumlu	Resmiyette belirsiz — ShamLogix ve NorthSoft ile ilişkili

14.6 Bu Altyapı Neden Endişe Verici?

- Birden fazla Reverse Proxy katmanı gerçek sunucuyu tespit etmeyi neredeyse imkânsız kılar
- Özel CA, içeriği herhangi bir ticari araçla incelemeyi engeller
- Hükümet sunucusunda barındırma siyasi bir boyut ekler — sunucuyu kim kontrol ederse veriye de o kontrol eder
- Korumasız İdlib'deki ShamLogix, tüm altyapıyı tehlikeye atmak için istismar edilebilecek açık bir zayıflık noktasıdır

- Chatwoot (Amazon) ve Firebase (Google) ek güvenilir iletişim kanalları olarak kullanılmaktadır

Sonuç — Adli Nihai Değerlendirme

✗ APK'dan doğrudan belgelenen sekiz teknik kanıtın toplamı, meşru güvenlik uygulamaları olarak yorumlanamaz.

Unsur	Adli Değerlendirme
librsa_bridge.so'da res_search / getaddrinfo	⚠ Yalnızca şifreleme olarak öne sürülen kütüphanede aktif ağ yeteneği
CGO sarmalayıcılarıyla 9 setuid/setgid fonksiyonu	⚠ Sistematik yetki yükseltme — meşru işlevsel gerekçe yok
dlopen / dlsym / dlclose	⚠ APK'da görünmeyen harici dinamik kod yürütme
FlutterSecureStorage üzerinde OAEP	⚠ Cihaz güvenlik verilerini sunucu anahtarıyla şifreleme
İzinlerde bildirilmemiş Yüz/Metin/Nesne Algılama	⚠ Kapsamlı görüntü analizi — bildirilmemiş
30 yıl geçerli özel CA	⚠ İncelemeye karşı dayanıklı uzun vadeli tasarım
/data/Android/ kodda şifrelenmiş yol	⚠ Diğer uygulamaların verilerine önceden planlanmış kasıtlı hedefleme
Tek APK'da iki aktif RSA anahtarı	⚠ Olası paralel iletişim kanalları

⚠ Her unsur tek başına masum bir açıklamaya sahip olabilir — ancak sekizi bir arada tek tutarlı bir desen oluşturmaktadır. Bu desen, gelişmiş Veri Sızdırma (Data Exfiltration) yazılımlarının yapısıyla örtüşmektedir. Kesin nihai doğrulama, ağ müdahalesiyle yalıtılmış bir ortamda dinamik analiz gerektirir.

— Rapor Sonu —