Alerta

Técnica

Spyware móvil dirigido a aplicaciones de mensajería

COLCERT AL-20251127 - 084

TLP:CLEAR

Resumen Ejecutivo

El incremento en el uso de *spyware* comercial dirigido a dispositivos móviles representa una amenaza creciente para usuarios de aplicaciones de mensajería como **Signal**, **WhatsApp** y **Telegram**, especialmente en sectores críticos y actores de alto valor. Los ciberdelincuentes, incluidos grupos estatales y operadores de *spyware* avanzado, **explotan vulnerabilidades** de vinculación de dispositivos, ***phishing*** con QR y **suplantación de aplicaciones**, permitiendo la **exfiltración de comunicaciones cifradas**. Aunque estas campañas son a nivel global, se ha identificado que usuarios en Colombia también han sido expuestos a contenidos, enlaces y artefactos asociados, de acuerdo con reportes abiertos. No obstante, hasta el momento no existe evidencia que indique compromisos directos a entidades del Estado. La probabilidad de impacto es alta, dada la amplia adopción de estas plataformas y la sofisticación de los actores, generando riesgos potenciales de espionaje político, corporativo y militar. La consecuencia inmediata es la exposición de información sensible y la erosión de la confianza en sistemas de comunicación seguros.

NIVEL DE RIESGO

ALTO

Contexto

El aviso emitido por CISA alerta que múltiples actores de amenazas, incluidos grupos con motivaciones financieras, espionaje estatal y redes criminales, **están utilizando *spyware* comercial para comprometer dispositivos móviles y obtener acceso a información sensible en aplicaciones de mensajería**. Estas herramientas permiten a los atacantes evadir defensas tradicionales y operar de manera encubierta en los sistemas afectados. Se identifican varias familias de *spyware* comerciales, entre ellas:

- **LANDSLIDE / LANDFALL**: un *spyware* comercial para Android con capacidades avanzadas de acceso remoto, exfiltración de datos y vigilancia persistente.
- **CLAYRAT**: utilizado en campañas que distribuyen aplicaciones falsas de Telegram y páginas de phishing para comprometer dispositivos Android.
- **Pegasus / NSO Group**: aunque sujeto a restricciones, sigue siendo uno de los ejemplos emblemáticos de *spyware* avanzado en investigaciones sobre abuso de plataformas de mensajería.
- **Campañas de suplantación de Signal y ToTok**: que distribuyen variantes recientes de *spyware* móvil diseñadas para capturar mensajes y metadatos.
- ***Spyware* usado por actores vinculados a Rusia contra Signal**: herramientas personalizadas para monitorear comunicaciones cifradas de aplicaciones seguras.

Estas familias comparten técnicas comunes de vigilancia, como lectura de mensajes, grabación de pantalla, acceso a archivos, seguimiento de ubicación y captura de credenciales, con el objetivo de comprometer la privacidad del usuario y evadir los mecanismos de cifrado de extremo a extremo.

Las campañas descritas han afectado a un amplio espectro de víctimas: periodistas, defensores de derechos humanos, funcionarios gubernamentales, personal diplomático, organizaciones de tecnología, y también usuarios comunes. Las plataformas más afectadas son principalmente Android, dada la facilidad de instalación de aplicaciones desde fuentes externas, aunque en casos específicos también se han observado compromisos en iOS mediante técnicas más sofisticadas. El uso de estas herramientas permite a los atacantes interceptar comunicaciones privadas directamente en el dispositivo, antes o después del cifrado, lo que representa un riesgo crítico tanto para la seguridad individual como organizacional.

Vectores de ataque identificados

- Las investigaciones evidencian que los actores de amenazas están utilizando múltiples técnicas para lograr la instalación y operación del spyware en dispositivos móviles. Entre los principales vectores identificados se encuentran:

- ***Phishing* dirigido (*spearphishing*):** actores distribuyen enlaces maliciosos a través de correo electrónico, SMS, mensajería instantánea o redes sociales para inducir al usuario a instalar aplicaciones manipuladas o entregar permisos excesivos.

- **Suplantación de aplicaciones legítimas**: variantes reportadas incluyen aplicaciones falsas que imitan a **Signal**, **Telegram**, **WhatsApp** o **ToTok**, engañando al usuario para instalarlas desde sitios externos.

- **Instalación de aplicaciones APK fraudulentas o modificadas**: los ciberdelincuentes publican paquetes APK fuera de tiendas oficiales, en sitios de descarga, dominios ***typosquatting*** o páginas clonadas que distribuyen versiones adulteradas con *spyware* incorporado.

- **Uso de códigos QR maliciosos**: campañas detectadas utilizan QR falsificados que redirigen a portales no oficiales, descargan aplicaciones manipuladas o vinculan el dispositivo a cuentas controladas por el atacante.

- **Enlaces maliciosos dentro de aplicaciones de mensajería**: los atacantes aprovechan la confianza del usuario dentro de chats para enviar enlaces que redirigen a la descarga de *spyware*, páginas de *phishing* o actualizaciones "obligatorias" falsas.

- **Explotación de vulnerabilidades**: algunos actores aprovechan fallas de seguridad en sistemas Android o en aplicaciones como WhatsApp o Telegram para ejecutar código sin interacción del usuario, permitiendo la instalación silenciosa del spyware.

- **Perfiles móviles falsos o configuración remota**: incluye perfiles MDM (*Mobile Device Management*) fraudulentos o configuraciones que otorgan control extendido sobre el dispositivo, especialmente observados en ataques más dirigidos contra personal gubernamental o diplomático.
- La mayoría de las campañas recientes emplean infraestructuras rotativas, donde los atacantes utilizan dominios desechables, hospedaje en VPS de bajo costo y enlaces que cambian constantemente para evadir reputación, listas negras y mecanismos de filtrado.

Las investigaciones citadas por CISA identifican la participación de múltiples actores de amenaza estatales y grupos asociados, principalmente vinculados a operaciones de espionaje móvil dirigidas a usuarios de aplicaciones de mensajería segura como **Signal**, **WhatsApp** y **Telegram**. Entre los actores confirmados se encuentran:

- **UNC5792** (Alineado con Rusia): actor especializado en comprometer usuarios de **Signal** mediante invitaciones falsas a grupos y redirección hacia enlaces manipulados que permiten vincular dispositivos adicionales a la cuenta de la víctima.
- **UNC4221** (Alineado con Rusia): grupo que emplea kits de *phishing* diseñados específicamente para **Signal**, utilizando sitios web falsos y códigos QR maliciosos que vinculan la cuenta del objetivo con un dispositivo bajo control del atacante.
- **APT44** (Sandworm / Seashell Blizzard - Rusia): actor estatal de alto nivel que ha realizado operaciones de espionaje móvil avanzadas, incluyendo compromiso físico o de proximidad (*close access*) y manipulación del proceso de vinculación de dispositivos en **Signal**. Es uno de los actores más sofisticados implicados en esta campaña.
- **Turla** (Rusia): grupo de inteligencia asociado al Servicio Federal de Seguridad de Rusia (FSB), mencionado en investigaciones relacionadas por su participación en campañas de espionaje digital contra dispositivos y comunicaciones móviles, incluyendo la exfiltración de datos desde aplicaciones de mensajería.
- **UNC1151** (Bielorrusia): actor alineado con el gobierno de Bielorrusia, vinculado previamente a operaciones de monitorización de comunicaciones, phishing avanzado y espionaje contra activistas y funcionarios.

- **Clay RAT Operators** (Medio Oriente - atribución en análisis): según SecurityAffairs, campañas recientes han distribuido Android *spyware* aprovechando señuelos como **Telegram** y servicios de mensajería alternos. Si bien la atribución no es definitiva, se ha observado que comparte infraestructura y patrones operativos similares a los empleados históricamente por actores en Oriente Medio.
- **Operadores de "Landfall" Spyware** (Comercial – Origen no confirmado): **Landfall** es un *spyware* distribuido a través de campañas que imitan aplicaciones legítimas de comunicación. La infraestructura utilizada muestra características propias de operadores con capacidad técnica y recursos sostenidos, típicos de actores privados especializados en vigilancia digital o grupos que operan bajo contrato.
- **Actores vinculados a NSO Group** (Israel): aunque no forman parte directa de esta campaña, CISA incluye como referencia la restricción legal impuesta por cortes de EE. UU. a **NSO** por el uso de *spyware* contra usuarios de WhatsApp, reforzando el contexto general de espionaje móvil comercial.

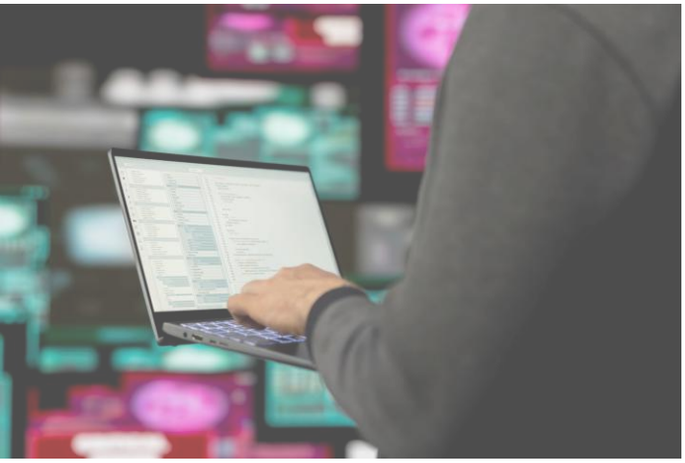
Técnicas MITRE ATT&CK asociadas

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Collection	Command and Control	Exfiltration
T1660: Phishing	T1398: Boot or Logon Initialization Scripts	T1404: Exploitation for Privilege Escalation	T1407: Download New Code at Runtime	T1417: Input Capture	T1420: File and Directory Discovery	T1429: Audio Capture	T1437: Application Layer Protocol	T1646: Exfiltration Over C2 Channel
	T1541: Foreground Persistence		T1541: Foreground Persistence		T1430: Location Tracking	T1533: Data from Local System	T1521: Encrypted Channel	
					T1418: Software Discovery	T1417: Input Capture	T1521.001: Symmetric Cryptography	
					T1426: System Information Discovery	T1430: Location Tracking		
					T1421: System Network Connections Discovery	T1636: Protected User Data		
						T1636.003: Contact List		
						T1636.004: SMS Messages		
						T1513: Screen Capture		
						T1409: Stored Application Data		

Mitigaciones MITRE

MITIGACIÓN	CÓDIGO	RELEVANCIA
Formación y orientación a usuarios	**M1011**	Enseña a los usuarios a identificar y rechazar *spearphishing movil*, enlaces, QR maliciosos y solicitudes de permisos peligrosos.
Enterprise Policy	**M1012**	Permite aplicar controles centrales como listas de aplicaciones permitidas, bloquear instalación desde orígenes no autorizados, controlar la vinculación de dispositivos, prohibir perfiles de configuración no aprobados.
Antivirus / Antimalware	**M1058**	Soluciones antimalware para móviles pueden detectar comportamientos típicos de spyware (privilegios anómalos, exfiltración, persistencia, módulos descargados) y bloquear o aislar el endpoint.
Aplicar parches y actualizaciones	**M1001**	Mantener el sistema operativo y aplicaciones actualizadas mitiga vulnerabilidades explotables.

Impacto para Colombia y la región



- **Sectores afectados**: Hay mayor riesgo para entidades de gobierno, defensa, salud, financiero, TIC y educación debido al uso extendido de aplicaciones de mensajería en sus operaciones, aunque la afectación es general.

- **Riesgo alto**: El riesgo se considera alto debido a la naturaleza de la amenaza (spyware comercial avanzado, técnicas de vinculación remota, phishing dirigido y suplantación de aplicaciones). Aunque no se han confirmado compromisos directos en Colombia, estos vectores representan un riesgo significativo para usuarios de mensajería ampliamente utilizada en el país.

Posibles consecuencias:

- Intercepción de comunicaciones sensibles.
- Suplantación de identidad mediante la toma de cuentas o dispositivos vinculados.
- Acceso a información personal y corporativa que puede favorecer campañas de fraude, extorsión o chantaje digital.
- Espionaje estatal o corporativo, dirigido a funcionarios, diplomáticos, empresas de energía, telecomunicaciones y finanzas.
- Compromiso de operaciones en sectores críticos (salud, gobierno, defensa), debido a la filtración de información estratégica.
- Riesgos para la integridad física de activistas, defensores de DD.HH. o periodistas a través del |rastreo y vigilancia de sus comunicaciones.

- **Implicaciones en seguridad digital**:
  - Incremento de campañas de ingeniería social sofisticadas, especialmente usando enlaces, QR y APK personalizadas.
  - Debilitamiento de la confianza en aplicaciones de mensajería utilizadas para coordinación operativa en entidades gubernamentales y privadas.
  - Necesidad urgente de políticas de uso seguro de mensajería, incluyendo restricciones a la vinculación de dispositivos y verificación de QR
  - Exposición de infraestructura de comunicaciones ante actores con capacidades avanzadas, lo que exige monitoreo reforzado en redes corporativas y gubernamentales.
  - Aumento en la demanda de medidas de protección móvil, como EDR para móviles, MTD (Mobile Threat Defense), listas de aplicaciones permitidas y endurecimiento de sistemas Android/iOS.

Recomendaciones

- Actualizar el sistema operativo y todas las aplicaciones de mensajería a la última versión disponible para garantizar que se corrijan vulnerabilidades conocidas que podrían ser explotadas por spyware o módulos maliciosos.

- Instalar soluciones de seguridad móviles, como Mobile Threat Defense (MTD) o antivirus confiables, que detecten comportamientos sospechosos, acceso no autorizado a datos, escalamiento de privilegios y conexiones a infraestructura de comando y control.

- Configurar políticas de seguridad mediante herramientas MDM/EMM (Mobile Device Management / Enterprise Mobility Management) para permitir únicamente aplicaciones de fuentes confiables, bloquear instalaciones desde orígenes desconocidos y restringir funciones críticas como accesibilidad y administración del dispositivo.

- Capacitar a los usuarios sobre la identificación de *phishing*, enlaces maliciosos, códigos QR sospechosos y solicitudes de permisos excesivos en aplicaciones de mensajería, fomentando prácticas de seguridad como verificar remitentes y no escanear códigos no verificados.

- Cifrar la información sensible almacenada en los dispositivos, incluyendo bases de datos de aplicaciones de mensajería, contactos y archivos, para que, en caso de infección, los datos exfiltrados no sean fácilmente explotables.

- Eliminar permisos innecesarios y revisar regularmente los privilegios otorgados a cada aplicación, reduciendo el riesgo de que un spyware utilice funcionalidades de accesibilidad, administrador de dispositivo o lectura de notificaciones para robar información.

- Implementar autenticación multifactor (MFA) en cuentas de mensajería y servicios críticos para minimizar el impacto de posibles compromisos de credenciales a través de spyware, reduciendo la probabilidad de accesos no autorizados derivados de intentos de vinculación remota.

- Revisar detenidamente los indicadores de compromiso (IOC) proporcionados, los cuales pueden ser integrados en los sistemas de seguridad perimetral. Se sugiere realizar la validación correspondiente para asegurar que su implementación no afecte la disponibilidad operativa ni la continuidad de los servicios.

TIPO	VALOR
MD5	1d5d2bbbb510d0e7d84860878847127d
SHA1	30fa53d7ec7e7fccfc58789d5fbc0f883901d68a
SHA256	b21a2162c5bc9340671840618f236d2655d1107bdc2a203a2ad6f2a00df0081e
MD5	e1f890c6b61d791757246265efe8cb46
SHA1	2ef00ef624020a775b846d5d121bc25d568cd441
SHA256	30b19c656844a188082a01f9545a59c1e074df6018fa36bfd7167723c7f3fe7c
MD5	20ef5078b4d0bda24c97d1e5b4c24222
SHA1	118a846224609d7e538f8ba7c946d46315f29b6d
SHA256	e791d7007a58f7b8d336f9e2b1bd8fc8c7e120b610b857b6e7a7121c86c3909f
MD5	4f27140d7ff3c5009791bec1e0e42bde
SHA1	50ae0c93a16518eda6e2116ba04573eceafa386b
SHA256	bc2fc09b00a25ff10b1ec85653d1b628e138a22b26cf69095a458434733900c2
MD5	e88a147c25a595dda4a56067869a2d03
SHA1	fd173697b29e1e81933b4bd9e6a125eec7fa8a55
SHA256	9d2c1f2c9fe90a06fa9278d9f6656696df6177d8bf89cafcd94f768606923 1f7
MD5	84cc2ddd81588a0319992f3a24b07d4d
SHA1	6b144b92c6cf8ed3d07410514d3bdf5f8956ede4
SHA256	ac2c0b4a338622b4d3a16929d4071dba7ca229032b7d31f233cc97aef11910c0
MD5	39f618e31c6d23b19b2defb860b54976
SHA1	ae38ea029cb19d22f2760d96a281508592f5cce7
SHA256	82fbac89e82e00af9409cb231c1da284e5506cd7644b7ae9a05a96145f3105d8
MD5	c782e27008a2b578fd153a9de37c8241
SHA1	27e1d36a3cd9220c4262f17aa3192eb1ec797bf6
SHA256	9de3a9a8dfa4c04293b3544c90fc242a7f87931ce71e31405b59227bdea589dc
MD5	f8d142f4e1a258fe328acb8e49c9eae7
SHA1	e8cdf03066e115415be8bb528bc9a80fa7451fff
SHA256	1796708dd67570c30d8dc9ea2a10a2bc8a7d8d2cea9c5c2103486e6f5b7ed7ad

TIPO	VALOR
MD5	b6b591d66f601cecfeef72cc526b0163
SHA1	c73d7a6f11d5d6f4bf883238257b396e75d146b0
SHA256	2808e5c6d33d6d38bfa4f5c9d108bdf9e89d1c68e81f033311859b1d273c60c9
DOMINIO	youtubeplusandroid[.]ru
DOMINIO	antiradar[.]life
DOMINIO	noblico[.]net
DOMINIO	ai-messenger[.]co
DOMINIO	spiralkey[.]co
DOMINIO	store.latestversion[.]ai

Fuentes

CISA, 24/11/2025, 26/11/2025, Spyware allows cyber threat actors to target users of messaging applications, Aviso oficial.
https://www.cisa.gov/news-events/alerts/2025/11/24/spyware-allows-cyber-threat-actors-target-users-messaging-applications#note1

CISA, 24/11/2025, 26/11/2025, Mobile communications best practices, Guía oficial.
https://www.cisa.gov/sites/default/files/2025-11/guidance-mobile-communications-best-practices-20251124_508c.pdf

Google Cloud, 05/02/2025, 26/11/2025, Russia targeting Signal Messenger, Blog corporativo.
https://cloud.google.com/blog/topics/threat-intelligence/russia-targeting-signal-messenger/

Palo Alto Networks Unit 42, 18/08/2025, 26/11/2025, Landfall is new commercial-grade Android spyware, Blog corporativo.
https://unit42.paloaltonetworks.com/landfall-is-new-commercial-grade-android-spyware/

The Hacker News, 15/08/2025, 26/11/2025, WhatsApp issues emergency update for users amid spyware threat, Medio de noticias.
https://thehackernews.com/2025/08/whatsapp-issues-emergency-update-for.html

Bleeping Computer, 20/08/2025, 26/11/2025, Android spyware campaigns impersonate Signal and ToTok messengers, Medio de noticias.
https://www.bleepingcomputer.com/news/security/android-spyware-campaigns-impersonate-signal-and-totok-messengers/

Security Affairs, 22/08/2025, 26/11/2025, ClayRat campaign uses Telegram and phishing sites to distribute Android spyware, Blog de seguridad.
https://securityaffairs.com/183169/malware/clayrat-campaign-uses-telegram-and-phishing-sites-to-distribute-android-spyware.html

Reuters, 23/06/2025, 26/11/2025, WhatsApp banned on US House representatives' devices: memo, Medio de noticias.
https://www.reuters.com/world/us/whatsapp-banned-us-house-representatives-devices-memo-2025-06-23/

The Record, 12/06/2025, 26/11/2025, Judge bars NSO from targeting WhatsApp users, lowers damages, Medio de noticias.
https://therecord.media/judge-bars-nso-from-targeting-whatsapp-users-lowers-damages

The Record, 10/07/2025, 26/11/2025, Researchers report spyware infections in UAE, Medio de noticias.
https://therecord.media/researchers-spyware-uae-infections

WeLiveSecurity (ESET), 05/09/2025, 26/11/2025, New spyware campaigns target privacy-conscious Android users in UAE, Blog corporativo.
https://www.welivesecurity.com/en/eset-research/new-spyware-campaigns-target-privacy-conscious-android-users-uae/

Zimperium, 12/09/2025, 26/11/2025, ClayRat: a new Android spyware targeting Russia, Blog corporativo.
https://zimperium.com/blog/clayrat-a-new-android-spyware-targeting-russia