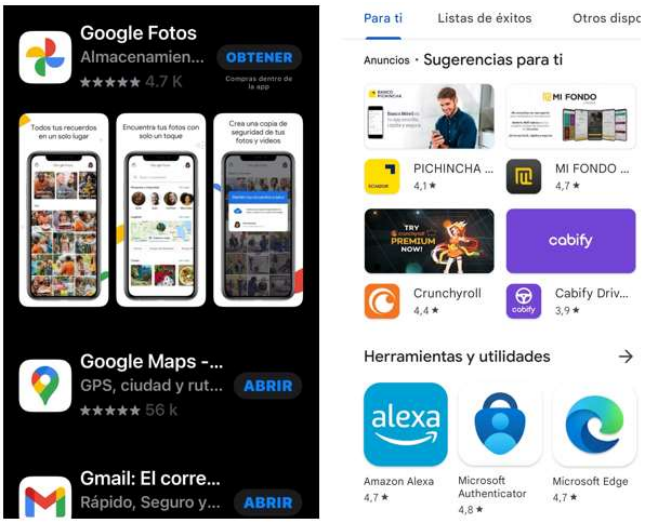
| | | | |
|---|---|---|---|
| Nro. Alerta: | **AL-2023-04** | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR<br><br>**ALERTAS DE SEGURIDAD** | ecucert |
| TLP: | TLP:BLANCO | | |
| Fecha: | 19-enero-2023 | **Android: SpyNote Malware** | V 1.1 |

## I. DATOS GENERALES:

**Clase de alerta:** Malware
**Tipo de incidente:** Remote Acces Trojan (RAT)
**Nivel de riesgo:** Alta
**Plataforma:** Android

## II. INTRODUCCIÓN




**Gráfica 1.- SpyNote, malware RAT compromete la seguridad de teléfonos móviles**

SpyNote es un malware de la categoría de troyanos de acceso remoto (RAT) de Android.

La herramienta de creación SpyNote RAT se puede utilizar para desarrollar aplicaciones maliciosas con la funcionalidad del malware.

Un troyano de acceso remoto (RAT) es un tipo de malware que controla un sistema a través de una conexión de red remota. Una RAT generalmente se instala sin el conocimiento de la víctima, a menudo como carga útil de un programa de caballo de Troya, e intentará ocultar su funcionamiento a la víctima y al software de seguridad y otro software antivirus.

Una RAT permite a sus operadores realizar muchas actividades en el dispositivo comprometido (por ejemplo, controlar la cámara de un dispositivo, acceder a su almacenamiento, interceptar llamadas y mensajes de texto, etc.). Todo esto se hace a través de una aplicación fácil de usar alojada en un servidor de comando y control.



**Dirección:** Av. Amazonas N40-71 y Gaspar de Villaroel
**Código postal:** 170501 / Quito-Ecuador
**Teléfono:** 593-2 2271 180 - www.arcotel.gob.ec

| | | | |
|---|---|---|---|
| Nro. Alerta: | **AL-2023-04** | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR<br><br>**ALERTAS DE SEGURIDAD** | ecucert |
| TLP: | TLP:BLANCO | | |
| Fecha: | 19-enero-2023 | **Android: SpyNote Malware** | V 1.1 |

En el último trimestre de 2022, los investigadores de ThreatFabric observaron un gran aumento en el volumen de muestras pertenecientes a la familia SpyNote Malware. Esta familia, también conocida como SpyMax, es un spyware único y efectivo diseñado para observar en secreto la actividad del usuario en un dispositivo Android. El malware SpyNote puede monitorear, administrar y modificar los recursos y funciones del dispositivo junto con las capacidades de acceso remoto.

SpyNote tiene varias variantes distintas: la más reciente, SpyNote.C, se rastrea y rastrea de forma rutinaria en las operaciones diarias, y compensa la mayoría de las muestras de spyware que ThreatFabric observó desde octubre de 2022.

Una de las principales diferencias entre las primeras variantes, SpyNote.A y SpyNote.B, y la última, SpyNote.C, es el objetivo de la campaña. SpyNote.C ha sido la primera variante en apuntar abiertamente a las aplicaciones bancarias, haciéndose pasar por una gran cantidad de instituciones financieras acreditadas como HSBC, Deutsche Bank, Kotak Bank, BurlaNubank, así como otras aplicaciones conocidas como WhatsApp, Facebook y Google Play. .

SpyNote tiene la capacidad de actualizarse, descargar e instalar nuevas aplicaciones, ver mensajes SMS, acceder a la cámara, contactos, última ubicación GPS; incluso puede escuchar y grabar audio desde el micrófono del dispositivo, escuchar llamadas, hacer llamadas, recuperar listas de contactos.

SpyNote puede acceder a detalles técnicos como el número IMEI del dispositivo, la dirección MAC de Wi-Fi y la información del operador.

SpyNote utiliza los Servicios de accesibilidad para dificultar a los usuarios la desinstalación de la aplicación, la instalación de nuevas versiones y la instalación de otras aplicaciones. Sin ninguna intervención del usuario, SpyNote puede hacer clic en los botones "instalar" y "actualizar" gracias a los servicios de accesibilidad:

La última variante de esta familia de malware, SpyNote.C, fue desarrollada y vendida a actores individuales a través del canal de Telegram por su desarrollador, bajo el nombre de CypherRat.

El actor de amenazas ofreció a la venta CypherRat utilizando el sistema de pago Sellix, que utiliza criptomonedas para evitar el seguimiento. Estas ventas se desarrollaron desde agosto de 2021 hasta octubre de 2022, acumulando más de 80 clientes separados



**Dirección:** Av. Amazonas N40-71 y Gaspar de Villaroel
**Código postal:** 170501 / Quito-Ecuador
**Teléfono:** 593-2 2271 180 - www.arcotel.gob.ec

| | | | |
|---|---|---|---|
| Nro. Alerta: | **AL-2023-04** | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR<br><br>**ALERTAS DE SEGURIDAD** | ecucert |
| TLP: | TLP:BLANCO | | |
| Fecha: | 19-enero-2023 | **Android: SpyNote Malware** | V 1.1 |

| Icon / App name / Package name | Malware family | Malware variant | Malware types |
|---|---|---|---|
| Play Store (com.warned.moon)<br>7f3b84a0fa394b66422fddf729d7f9ba3000f4dcdcd61eb394005462264595fb | SpyNote | SpyNote.C | RAT<br>Spyware |
| Sistem Bildirimleri (com.marble.physicians)<br>08463529d7d681246a0dd1d24a59fa50d354568f04673642bb44cc613a824be9 | SpyNote | SpyNote.C | RAT<br>Spyware |
| CypherRat (splash.app.main)<br>0dcd025c20d7f5e4b503d40034b5d4b8cf2661df235bcfc7f6e67230765 0a62f | SpyNote | SpyNote.C | RAT<br>Spyware |
| Google Play Protect (cmf0.c3b5bm90zq.patch)<br>71ec22035d5499a89dad13911cc84d17c9021ba40f241702c31dce443ee3d8c4 | SpyNote | SpyNote.A | Spyware |

**Gráfica 2.- SpyNote haciéndose pasar por aplicaciones genéricas. Fuente:**
**https://www.threatfabric.com/blogs/spynote-rat-targeting-financial-institutions.html**

## III. ALERTA

En octubre de 2022, el código fuente estuvo disponible como código abierto a través de GitHub, luego de una filtración y algunos incidentes de estafa en foros de piratería, donde los actores se hacían pasar por el actor de amenazas original para robar dinero de otros delincuentes. El creador original había cambiado su enfoque a un nuevo proyecto de spyware, CraxsRat, como una aplicación paga con capacidades similares al proyecto original.

Según MITRE ATT&CK, SpyNote tiene las siguientes características:

ID: S0305
Tipo: Malware
Plataforma: Android
Version: 1.2
Creado: 25 October 2017
Última Modificación: 24 de octubre de 2022

Técnicas usadas:

| Nro. Alerta: | **AL-2023-04** | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR<br><br>**ALERTAS DE SEGURIDAD** | ecucert |
|---|---|---|---|
| TLP: | TLP:BLANCO | | |
| Fecha: | 19-enero-2023 | **Android: SpyNote Malware** | V 1.1 |

| Dominio | ID | | Nombre | Uso |
|---|---|---|---|---|
| Móvil | T1429 | | Captura de audio | SpyNote RAT puede activar el micrófono de la víctima |
| Móvil | T1533 | | Datos del sistema local | SpyNote RAT puede copiar archivos desde el dispositivo al servidor C2 |
| Móvil | T1624 | .001 | Ejecución activada por eventos: receptores de difusión | SpyNote RAT utiliza un receptor de transmisión de Android para iniciarse automáticamente cuando se inicia el dispositivo. |
| Móvil | T1430 | | Seguimiento de ubicación | SpyNote RAT recopila la ubicación del dispositivo. |
| Móvil | T1636 | .003 | Datos Protegidos del Usuario: Lista de Contactos | SpyNote RAT puede ver contactos. |
| | | .004 | Datos de usuario protegidos: mensajes SMS | SpyNote RAT puede leer mensajes SMS |

**Tabla 1.- Técnicas usadas por SpyNote, malware de la categoría de troyanos de acceso remoto (RAT) de Android**

SpyNote sigue el modus operandi de otro malware bancario al solicitar permisos a los servicios de accesibilidad para extraer códigos de autenticación de dos factores (2FA) de Google Authenticator y registrar las pulsaciones de teclas para desviar las credenciales bancarias.

Además, SpyNote incluye funcionalidades para saquear las contraseñas de Facebook y Gmail, así como para capturar el contenido de la pantalla aprovechando la API MediaProjection de Android. La iteración más reciente de SpyNote (llamada SpyNote.C) es la primera variante que afecta a las aplicaciones bancarias, así como a otras aplicaciones conocidas como Facebook y WhatsApp.

SpyNote se hace pasar por el servicio oficial de Google Play Store y otras aplicaciones genéricas que abarcan fondos de pantalla, productividad y categorías de juegos. Una lista de algunos de los artefactos de SpyNote, que se entregan principalmente por medio de ataques de smishing, es la siguiente:

- Bank of America Confirmation (yps.eton.application)
- Burla Nubank (com.appser.verapp)
- Conversations_(com.appser.verapp)
- Current Activity (com.willme.topactivity)



**Dirección:** Av. Amazonas N40-71 y Gaspar de Villaroel
**Código postal:** 170501 / Quito-Ecuador
**Teléfono:** 593-2 2271 180 - www.arcotel.gob.ec

- HSBC UK Mobile Banking (com.employ.mb)
- Kotak Bank (splash.app.main)
- Virtual SIM Card (cobi0jbpm.apvy8vjjvpser.verapchvvhbjbjq)

## IV. VECTOR DE ATAQUE

- Smishing
- Pishing

## V. IMPACTO:

- Usando los privilegios solicitados en la captura de pantalla, esta variante de SpyNote se puede usar para rastrear mensajes SMS, llamadas, videos y grabaciones de audio, además de actualizar su versión e incluso instalar nuevas aplicaciones.

- Las versiones más recientes de SpyNote no solo son extremadamente poderosas, sino que también incluyen una variedad de funciones de seguridad, desde la simple ofuscación de cadenas hasta el uso de empaquetadores comerciales. Esto hace que sea mucho más difícil de analizar, lo que lo convierte en una herramienta potente para los actores de amenazas.

- El análisis de la muestra de SpyNote indica que los actores de amenazas detrás de la campaña de vigilancia tenían un amplio control sobre los dispositivos de las víctimas. Este malware no solo tiene una lista considerable de funciones, sino que también es altamente personalizable, evade la detección y engaña a las víctimas para que descarguen, instalen y proporcionen acceso completo a sus dispositivos.

## VI. INDICADORES DE COMPROMISO:

En la siguiente Tabla se indican IoC de este malware.

| Ítem | Parámetro | Descripción |
|---|---|---|
| 1 | Tipo de archivo | Android |
| 2 | Nombre | sicurezza-posteitaliane.apk |
| 3 | Tamaño | 744.09 kB |
| 3 | FUNCIÓN HASH | MD5: 4fe2d12c67a7f5360dd6d57ce2402e6a |
| | | SHA-1: 88f57f24bd29231d6e5d6ac6c326168503afb51b |

| Nro. Alerta: | **AL-2023-04** | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR<br><br>**ALERTAS DE SEGURIDAD** | ecucert |
|---|---|---|---|
| TLP: | TLP:BLANCO | | |
| Fecha: | 19-enero-2023 | **Android: SpyNote Malware** | V 1.1 |

| Ítem | Parámetro | Descripción |
|---|---|---|
| | | SHA-256: c3ee6bc6f4e23981757b452c7b0236048a48b9c875f4d5e25266f8262fe208c5 |
| 4 | Direcciones IP contactadas: | 13.58.157.220<br>142.250.31.106<br>3.142.81.166<br>3.19.130.43<br>159.203.126.35<br>154.211.96.78 |

**Tabla 2. IoC de malware Spy Note**

## Análisis de proveedores de seguridad

| | | | |
|---|---|---|---|
| Ad-Aware | Trojan.GenericKD.50090802 | AhnLab-V3 | Spyware/Android.Agent.888518 |
| Alibaba | TrojanSpy:Android/SpyNote.bb513723 | Antiy-AVL | Trojan/Generic.ASMalwAD.372 |
| Avast | Android:SpyMax-D [Spy] | Avast-Mobile | Android:Evo-gen [Trj] |
| AVG | Android:SpyMax-D [Spy] | Avira (no cloud) | ANDROID/Banker.FAAR.Gen |
| BitDefender | Trojan.GenericKD.50090802 | BitDefenderFalx | Android.Trojan.SpyNote.A |
| Comodo | Malware@#28omzbaexgv12 | Cynet | Malicious (score: 99) |
| Cyren | AndroidOS/Banker.L | DrWeb | Android.Spy.982.origin |
| Emsisoft | Trojan.GenericKD.50090802 (B) | eScan | Trojan.GenericKD.50090802 |
| ESET-NOD32 | A Variant Of Android/Spy.Agent.BAT | Fortinet | Android/SpyNote.ANltr.spy |
| GData | Trojan.GenericKD.50090802 | Ikarus | Trojan.AndroidOS.SpyNote |
| K7GW | Trojan ( 0001140e1 ) | Kaspersky | HEUR:Trojan-Spy.AndroidOS.SpyNote.an |
| Kingsoft | Android.Troj.idevreg.ac.(kcloud) | Lionic | Trojan.AndroidOS.SpyNote.C!c |
| MAX | Malware (ai Score=100) | MaxSecure | Android.spynote.j |
| McAfee | Artemis!4FE2D12C67A7 | McAfee-GW-Edition | Android/Tripoli |
| Microsoft | Trojan:AndroidOS/Multiverze | NANO-Antivirus | Trojan.Android.Mlw.ffkkg |
| QuickHeal | Android.Spy.GEN27587 | Sangfor Engine Zero | Malware.Android-Script.Save.557766d0 |
| Sophos | Andr/Spy-AZW | Symantec | Trojan.Gen.2 |
| Symantec Mobile Insight | Trojan:Spymax | Tencent | A.privacy.SpyInfoRATs |
| Trellix (FireEye) | Trojan.GenericKD.50090802 | TrendMicro | TROJ_FRS.0NA103D822 |
| TrendMicro-HouseCall | TROJ_FRS.0NA103D822 | Trustlook | Android.Malware.Spyware |
| VirIT | Android.Trj.Backdoor.BAJ | Yandex | Trojan.Mober.bSzBF9.5 |

**Gráfica 2.- Análisis de proveedores de malware Spy Note – Fuente: https://www.virustotal.com**



**Dirección:** Av. Amazonas N40-71 y Gaspar de Villaroel
**Código postal:** 170501 / Quito-Ecuador
**Teléfono:** 593-2 2271 180 - www.arcotel.gob.ec

| | | | |
|---|---|---|---|
| Nro. Alerta: | **AL-2023-04** | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR<br><br>**ALERTAS DE SEGURIDAD** | ecucert |
| TLP: | TLP:BLANCO | | |
| Fecha: | 19-enero-2023 | **Android: SpyNote Malware** | V 1.1 |

## VII. RECOMENDACIONES:

El EcuCert recomienda a su comunidad objetivo:

- Instalar actualizaciones disponibles en medios oficiales del proveedor, previo análisis del impacto que podría provocar en los servicios críticos para el negocio de la organización.
- Realizar copias de respaldo de seguridad periódicas, de la información crítica para evitar la pérdida de la misma.
- Actualizar el sistema operativo de los equipos a las últimas versiones.
- No abrir, manipular, o interactuar, con correos electrónicos altamente sospechosos que lleguen a las bandejas de correo o mensaje en redes sociales.
- Otorgar privilegios de usuario al mínimo dependiendo del tipo de labor a realizar.
- Implementar técnicas de navegación segura en toda la Institución/Organización, como por ejemplo visita únicamente de sitios con certificados SSL, y, de origen no sospechoso.
- Bloquear el acceso de usuarios, a dispositivos de almacenamiento externo, ajenos a la Institución/Organización, a través de políticas de seguridad adecuadas.
- Implementar y monitorear, plataformas de seguridad perimetral para identificar posible tráfico malicioso tanto a nivel interno como externo a la infraestructura de red de la organización/Institución
- Descargar programas, archivos y actualizaciones, solamente desde fuentes oficiales y verificadas.
- Cerrar todo tipo de conexión/protocolo de acceso remoto a infraestructuras críticas en la Organización/Institución, en el caso de requerir su implementación, realizarlo bajo estrictas normas de seguridad apalancados en plataformas de seguridad perimetral y, uso de una VPN.
- Tener actualizado y utilizar, un software anti-virus
- Mantener actualizados, y, bajo licenciamiento, (ya sea a nivel de software libre o de paga, de ser el caso), todos y cada uno de los sistemas y subsistemas de software y hardware de toda la infraestructura de IT y OT de la Institución, esto es, incluido a nivel de Firmware de todos los componentes.
- Diseñar una política de revisión de logs, que permita detectar comportamientos fuera de lo normal en procesos legítimos del sistema.



**Dirección:** Av. Amazonas N40-71 y Gaspar de Villaroel
**Código postal:** 170501 / Quito-Ecuador
**Teléfono:** 593-2 2271 180 - www.arcotel.gob.ec

- Mantener listas de control de acceso para las unidades mapeadas en red restringiendo los privilegios de escritura. Con esto podrá identificar el impacto generado por el cifrado de archivos, entendiendo que el secuestro de información se producirá en todas las unidades de red mapeadas en el equipo víctima.
- Capacitar a todos los usuarios, mediante la concientización y simulaciones para reconocer e informar sobre intentos de phishing e ingeniería social. Seguir las normativas internacionales tales como ISO 27001:2013 en su control A.7.2.2 “Concienciación con educación y capacitación en seguridad de la información” o NIST PR.AT-1: “Todos los usuarios se encuentran entrenados e informados”, a fin de tener bases para divulgar campañas educativas orientadas a nivel de usuarios respecto al correcto uso de las herramientas tecnológicas
- Implementar un plan de respuesta a emergencias de la Organización/Institución.
- En el caso de sufrir un ataque de proporciones mayores, contacte a las Autoridades competentes en base a la Normativa Legal Vigente a nivel Nacional.

## VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona "tal cual" solo con fines informativos. EcuCERT no respalda ningún producto o servicio comercial, incluidos los sujetos de análisis.
- Cualquier referencia a productos, procesos o servicios comerciales específicos por marca de servicio, marca comercial, fabricante o de otro modo, no constituye ni implica respaldo, recomendación o favorecimiento por parte del EcuCERT.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

## IX. BIBLIOGRAFÍA.


- **Threat Fabril. (2023).** *SpyNote: Spyware with RAT capabilities targeting Financial Institutions*; recuperado el 05 de enero de 2023 de: https://www.threatfabric.com/blogs/spynote-rat-targeting-financial-institutions.html#appendix

- **Teknomers. (2023).** *SpyNote ataca de nuevo: spyware de Android dirigido a instituciones financieras*; recuperado el 05 de enero de 2023 de: https://teknomers.com/es/spynote-ataca-de-nuevo-spyware-de-android-dirigido-a-instituciones-financieras/

| Nro. Alerta: | **AL-2023-04** | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR<br><br>**ALERTAS DE SEGURIDAD** | ecucert |
|---|---|---|---|
| TLP: | TLP:BLANCO | | |
| Fecha: | 19-enero-2023 | **Android: SpyNote Malware** | V 1.1 |


- **Masterhacks Blog. (2023).** *Detectan nuevos ataques de SpyNote, un spyware para Android dirigido a instituciones financieras.* recuperado el 05 de enero de 2023 de: https://blogs.masterhacks.net/noticias/hacking-y-ciberdelitos/detectan-nuevos-ataques-de-spynote-un-spyware-para-android-dirigido-a-instituciones-financieras/

- **MITRE ATT&CK (2023).** *SpyNote RAT*, recuperado el 05 de enero de 2023 de: https://attack.mitre.org/software/S0305/

- **Shivang, D. (2017)**. *SpyNote RAT posing as Netflix app*. Recuperado el 05 de enero de 2023 de https://www.zscaler.com/blogs/security-research/spynote-rat-posing-netflix-app