Nro. Alerta:	EC-2022-049	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	22-marzo-2022	**Campaña de Amenaza Avanzada Persistente APT-C-36 podría estar presente en Ecuador**	V 1.1

I. DATOS GENERALES:

Clase de alerta: Código Malicioso / Phishing
Tipo de incidente: Malware
Nivel de riesgo: Alta

II. ALERTA

Durante el primer trimestre de 2022, a través del monitoreo realizado por EcuCERT, se ha detectado la presencia de la campaña APT-C-36 (Amenaza Avanzada Persistente) en Ecuador, a través de la que, ciberdelincuentes envían correos electrónicos, haciéndose pasar por Instituciones Públicas de Ecuador, adjuntando archivos de tipo malicioso, los que al ser descargados y ejecutados, instalan malware de tipo RAT/Crypter, con el objetivo de obtener acceso y control remoto a los dispositivos infectados, para posteriormente, apoderarse de información/datos/archivos/contraseñas de carácter sensible, con la finalidad de obtener alguna ganancia económica a través de los mismos.

Figura 1. Ciclo de una Amenaza Avanzada Persistente APT. **Fuente:** B-SECURE

Nro. Alerta:	EC-2022-049	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	22-marzo-2022	**Campaña de Amenaza Avanzada Persistente APT-C-36 podría estar presente en Ecuador**	V 1.1

III. INTRODUCCIÓN

Los ciberdelincuentes, emplean diferentes técnicas y herramientas para captar información de sus víctimas; en este sentido, una APT o Advanced Persistent Attack o Amenaza Avanzada Persistente; utilizan diferentes técnicas de "hacking" continuas y avanzadas para acceder al sistema y robar información. Según las etapas descritas en la Figura Nro. 1.

APT-C-36 también conocido como Blind Eagle / Águila Ciega es un actor de amenaza, probablemente con centro de operaciones en Sur América; ha estado activo desde al menos 2018. El grupo se dirigía principalmente a instituciones gubernamentales colombianas en un inicio; sin embargo, al parecer han empezado a incrementar su actividad en otros países de la región, entre ellos, Ecuador.

Hasta la presente fecha, se ha rastreado como su principal objetivo, la suplantación de identidad de Instituciones ecuatorianas como: La Función Judicial, Fiscalía General del Estado, Procuraduría General del Estado y la Agencia Nacional de Tránsito; podrían estar siendo suplantadas más Instituciones inclusive.

El modo de ataque empleado por APT-C-36, es a través del envío de correos electrónicos de phishing, a través de los que, se adjuntan archivos que contienen código malicioso, o archivos que contienen malware de tipo RAT (troyano de acceso remoto) de naturaleza Crypter (malware especializado cuyo código fuente e encuentra encriptado con el objetivo de evadir sistemas de detección de amenazas), dirigido a varios usuarios/posibles víctimas, con el objetivo de obtener acceso y control remoto de dispositivos, para posteriormente, apoderarse de información y datos personales de carácter sensible, con la finalidad de obtener alguna ganancia económica.

APT-C-36, emplea diferentes tipos de RAT; entre los que se destacan:

- njRAT
- Monitoreo inminente
- Un ProyectoRAT modificado a medida
- RAT de zona de guerra
- RAT asíncrona

- RAT CAL
- RAT Remcos
- BitRAT

IV. VECTOR DE ATAQUE

Phishing

V. IMPACTO

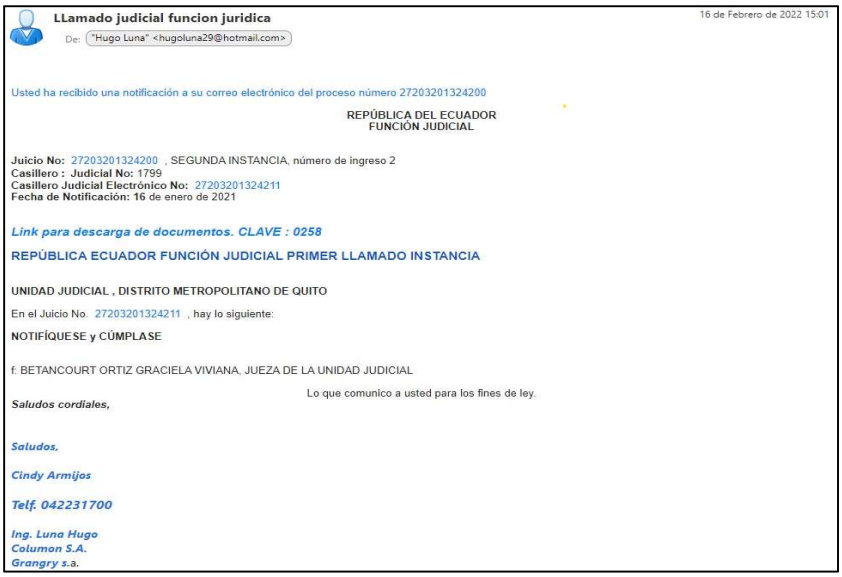
En la actualidad, la campaña de correos electrónicos maliciosos por parte de APT-C-36, para la distribución de malware, circula a nivel nacional. Los actores maliciosos emplean un señuelo en el asunto del correo electrónico; señalando que existe un supuesto “Proceso Judicial Abierto (…)”

En el cuerpo del mensaje, se incluye un anexo en el que supuestamente se encuentra más información del proceso judicial en cuestión; siendo la característica en común, el uso de una clave para descomprimir el archivo adjunto.

Los anexos previamente mencionados, pueden tener extensiones de archivo .VBS (script de ejecución de Visual Basic), .EXE (archivo de ejecución de Windows), entre otros. Archivos que, una vez ejecutados, empiezan a realizar un sin número de procesos y subprocesos en el sistema operativo Microsoft Windows, a nivel de registro, con el objetivo de descargar y ejecutar archivos complementarios para el desarrollo del ciberataque al dispositivo.

En la siguiente figura, se observan las muestras de correo electrónico que incluye archivos maliciosos:

Nro. Alerta:	EC-2022-049	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	22-marzo-2022	**Campaña de Amenaza Avanzada Persistente APT-C-36 podría estar presente en Ecuador**	V 1.1



LLamado judicial funcion juridica 16 de Febrero de 2022 15:01

De: "Hugo Luna" <hugoluna29@hotmail.com>

Usted ha recibido una notificación a su correo electrónico del proceso número 27203201324200

REPÚBLICA DEL ECUADOR
FUNCIÓN JUDICIAL

Juicio No: 27203201324200 , SEGUNDA INSTANCIA, número de ingreso 2
Casillero : Judicial No: 1799
Casillero Judicial Electrónico No: 27203201324211
Fecha de Notificación: 16 de enero de 2021

Link para descarga de documentos. CLAVE : 0258

REPÚBLICA ECUADOR FUNCIÓN JUDICIAL PRIMER LLAMADO INSTANCIA

UNIDAD JUDICIAL , DISTRITO METROPOLITANO DE QUITO

En el Juicio No. 27203201324211 , hay lo siguiente:

NOTIFÍQUESE y CÚMPLASE

f: BETANCOURT ORTIZ GRACIELA VIVIANA, JUEZA DE LA UNIDAD JUDICIAL

Lo que comunico a usted para los fines de ley.

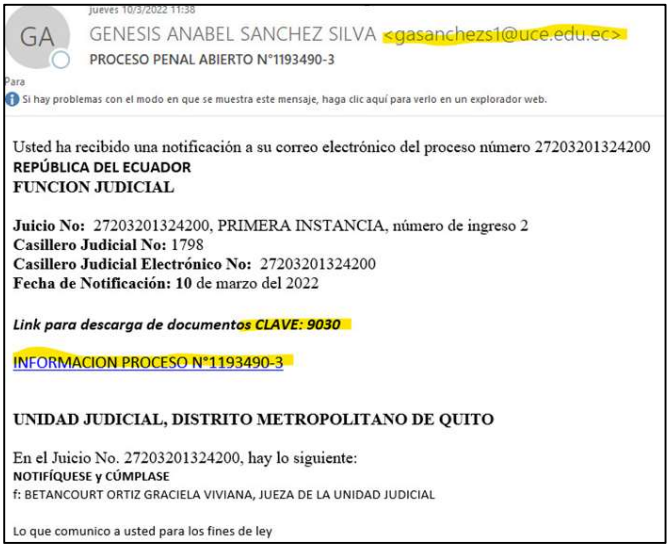
Saludos cordiales,

Saludos,

Cindy Armijos

Telf. 042231700

Ing. Luna Hugo
Columon S.A.
Grangry s.a.



Jueves 10/3/2022 11:38

GA GENESIS ANABEL SANCHEZ SILVA <gasanchezs1@uce.edu.ec>

PROCESO PENAL ABIERTO N°1193490-3

Para

Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.

Usted ha recibido una notificación a su correo electrónico del proceso número 27203201324200
REPÚBLICA DEL ECUADOR
FUNCION JUDICIAL

Juicio No: 27203201324200, PRIMERA INSTANCIA, número de ingreso 2
Casillero Judicial No: 1798
Casillero Judicial Electrónico No: 27203201324200
Fecha de Notificación: 10 de marzo del 2022

Link para descarga de documentos CLAVE: 9030

INFORMACION PROCESO N°1193490-3

UNIDAD JUDICIAL, DISTRITO METROPOLITANO DE QUITO

En el Juicio No. 27203201324200, hay lo siguiente:
NOTIFÍQUESE y CÚMPLASE
f: BETANCOURT ORTIZ GRACIELA VIVIANA, JUEZA DE LA UNIDAD JUDICIAL

Lo que comunico a usted para los fines de ley

Figura 2. Correos Electrónicos posible campaña APT -C -36 que adjuntan archivos maliciosos. **Fuente:** Propia

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

Gobierno del Encuentro | Juntos lo logramos

Nro. Alerta:	EC-2022-049	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	22-marzo-2022	**Campaña de Amenaza Avanzada Persistente APT-C-36 podría estar presente en Ecuador**	V 1.1

A continuación, se procede a realizar el análisis y trazabilidad de lo que ocurre una vez que el documento/archivo adjunto malicioso, es ejecutado en el sistema operativo Windows:

ITEM	MÉTODO DE ENTREGA	DESCRIPCIÓN DEL ARCHIVO ADJUNTO
1	**Muestra Uno** Correo electrónico, el archivo malicioso se adjunta al correo.	**Nombre de Archivo:** DESCARGOS PENALES PROCESO N°1193490-3 **Extensión del Archivo:** .vbs

Tabla 1. Archivo adjunto en distribución de correo electrónico posible APT-C-36. **Fuente:** Propia

Respecto a la muestra número uno, se evidencia que, una vez ejecutado el archivo "DESCARGOS PENALES PROCESO N°1193490-3.vbs", se realizan conexiones a las direcciones IP: 91[.]241[.]19[.]49, y 188[.]114[.]96[.]7 a través de las que, se descargan los archivos "estrellasdll.txt", "estrellasPe.txt" y "va.txt".

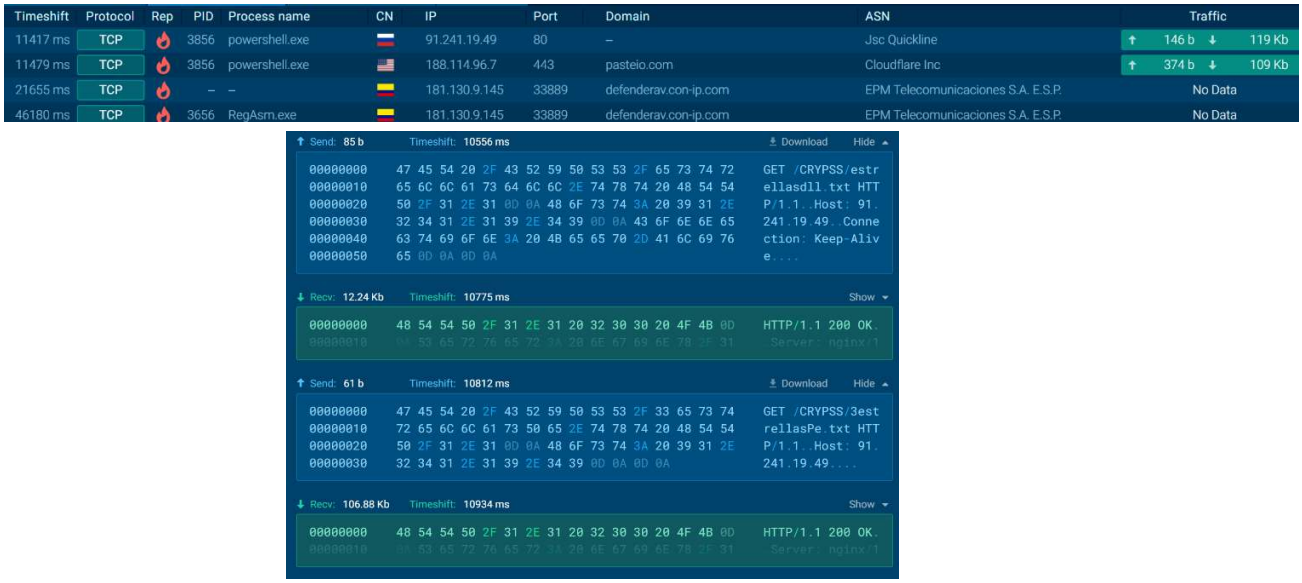
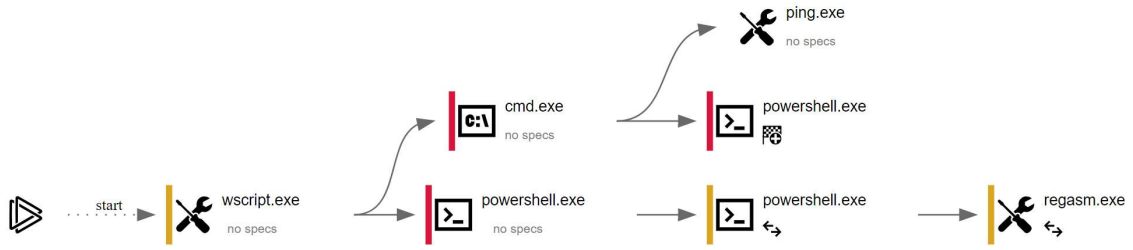


Figura 3. Conexiones y descarga de archivos de tipo malicioso. **Fuente:** Análisis en SandBox AnyRun

Nro. Alerta:	EC-2022-049	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	22-marzo-2022	**Campaña de Amenaza Avanzada Persistente APT-C-36 podría estar presente en Ecuador**	V 1.1

Completa la descarga de lo descrito en la figura Nro. 3, se empiezan a ejecutar siete (7) subprocesos en el sistema Operativo, los que, modifican el sistema a nivel de registro, y, al finalizar, se establece una conexión con la dirección IP 181[.]130[.]9[.]146, a través del puerto 33889, dirección que, podría encontrarse en modo escucha a la espera de una víctima, para conectarse remotamente al equipo, permitiendo al ciberdelincuente acceder al equipo infectado para robar información/datos/contraseñas de carácter sensible.



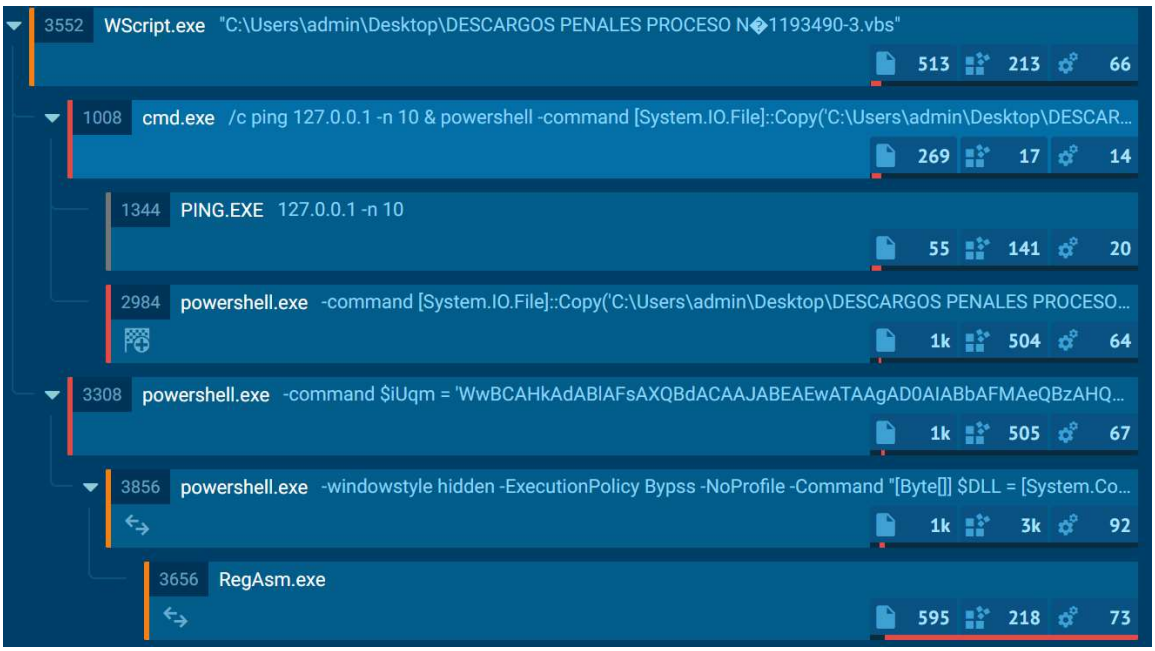


Figura 4. Ejecución a nivel de registro de archivo malicioso. **Fuente:** Análisis en SandBox AnyRun

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:	EC-2022-049	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	22-marzo-2022	**Campaña de Amenaza Avanzada Persistente APT-C-36 podría estar presente en Ecuador**	V 1.1

A continuación, se muestra el diagrama general de conexiones, correspondientes al archivo "DESCARGOS PENALES PROCESO N°1193490-3.vbs": Conexión a tres direcciones IP y descarga de tres archivos de tipo malicioso:

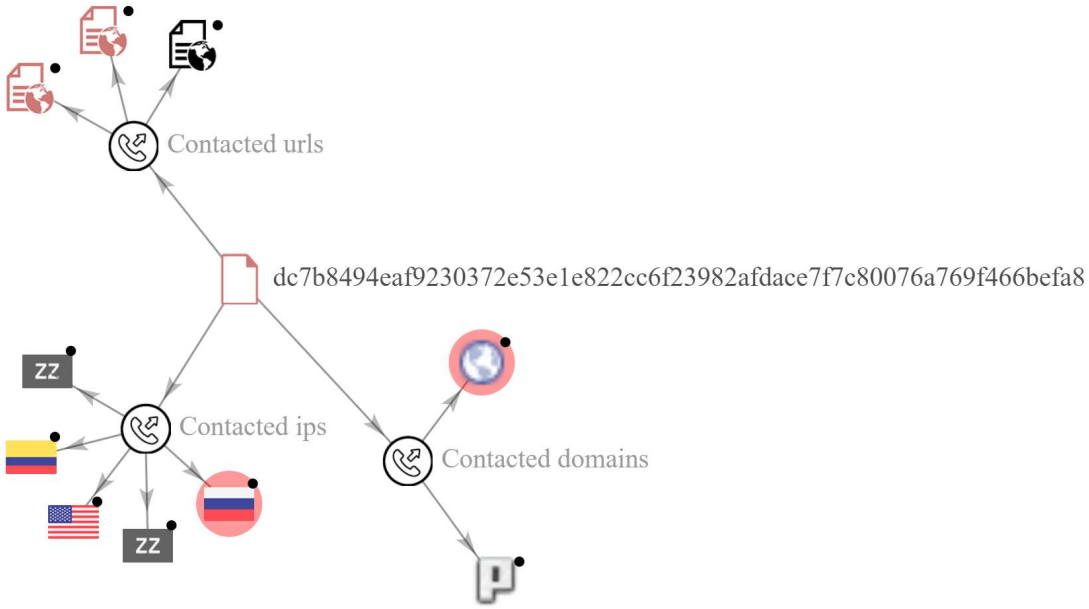


Figura 5. Diagrama de conexiones de archivo malicioso. **Fuente:** Virus Total

ITEM	MÉTODO DE ENTREGA	DESCRIPCIÓN DEL ARCHIVO ADJUNTO
2	**Muestra Dos** Correo electrónico, el archivo malicioso se remite a través de link.	**Link de descarga:** https://drive[.]google[.]com/uc?id=1yD30FbVQBrUyXUN6zxsz-JM8nAM9XPCy&export=download&authuser=0 **Nombre de Archivo:** Citacion Funcion Judicial Republica De Ecuador 2 **Extensión del Archivo:** .exe

Tabla 2. Archivo adjunto en distribución de correo electrónico posible APT-C-36. **Fuente:** Propia

Nro. Alerta:	EC-2022-049	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	22-marzo-2022	**Campaña de Amenaza Avanzada Persistente APT-C-36 podría estar presente en Ecuador**	V 1.1

Respecto a la muestra número dos, correspondiente al archivo “Citación Función Judicial Republica De Ecuador.exe”, el comportamiento es similar; sin embargo, la extensión del archivo está en formato ejecutable, con lo que, una vez ejecutada la aplicación, se conecta a la dirección IP 31[.]42[.]177[.]191, a través de la que, se descargan siete (7) archivos: “versionx64.dll”, “kifoasadx64.exe”, “amsipatcherx64.dll”, “stage1x64.ps1”, “stage1x32.ps1”,” NetCrypter.txt”, “sicv2.ps1”, los mismos que corresponden a la carga útil del archivo malicioso original “Citación Función Judicial Republica De Ecuador.exe”.

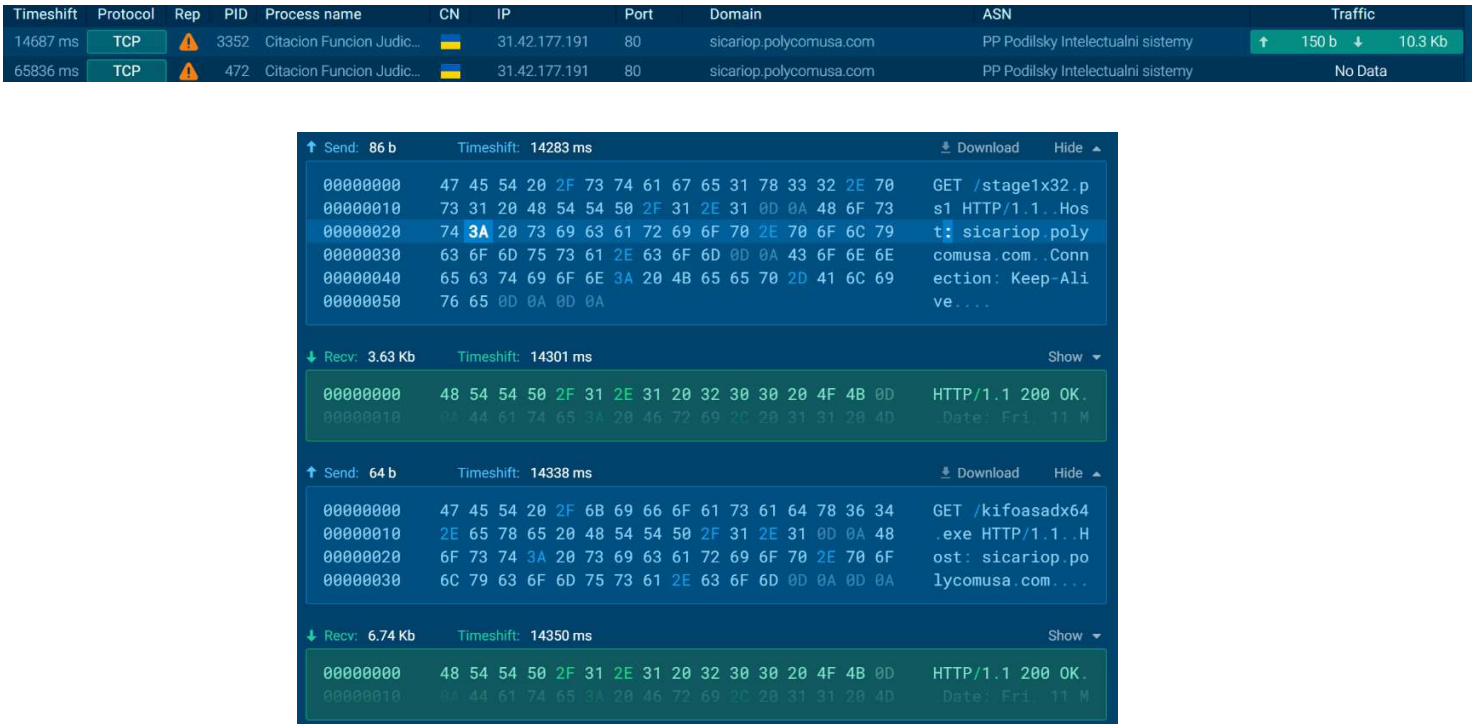


Figura 6. Conexiones y descarga de archivos de tipo malicioso. **Fuente:** Análisis en SandBox AnyRun

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:	EC-2022-049	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	22-marzo-2022	**Campaña de Amenaza Avanzada Persistente APT-C-36 podría estar presente en Ecuador**	V 1.1

Una vez descargados los siete archivos de carga útil mencionados con anterioridad, se proceden a ejecutar subrutinas a nivel de registro de sistema operativo Windows, al igual que el caso de la muestra número 1, se realiza una conexión a la dirección IP: 181[.]130[.]5[.]112, dirección IP que, podría encontrarse en modo escucha a la espera de una víctima, para conectarse remotamente al equipo, permitiendo al ciberdelincuente, acceder al equipo infectado para robar información/datos/contraseñas de carácter sensible.

A continuación, se muestra el diagrama general de conexiones, correspondientes al archivo “Citación Función Judicial Republica De Ecuador.exe”: conexión a dos direccione IP y descarga de siete archivos de tipo malicioso:

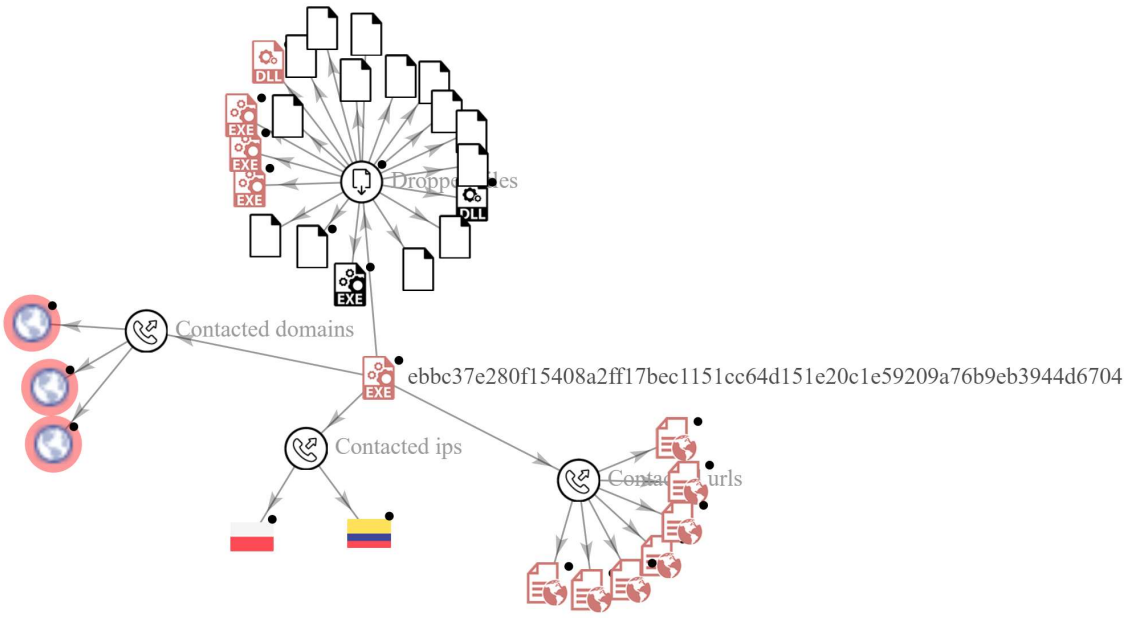


Figura 7. Diagrama de conexiones de archivo malicioso. **Fuente:** Virus Total

Nro. Alerta:	EC-2022-049	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	22-marzo-2022	**Campaña de Amenaza Avanzada Persistente APT-C-36 podría estar presente en Ecuador**	V 1.1

Una vez finalizados los análisis de las muestras números uno y dos, surge la pregunta de ¿Cómo determinar que ambas muestras pertenecen a la amenaza avanzada persistente de APT-C-36?.

El análisis e investigación, a través del que se logró relacionar las muestras expuestas en el presente documento, se desarrolló a través de la indexación en fuentes abiertas de las direcciones IP involucradas, logrando determinar que, archivos maliciosos similares, ya habían sido distribuidos en otros países de la región, entre los cuales resalta Colombia.

A través de una muestra encontrada en el software de sandbox (réplica del área operativa de un computador, sin acceso al resto de la red) Any Run, correspondiente al archivo de nombre "36b25672f.vbs", el que, una vez ejecutado, se conecta a las direcciones IP: 91[.]241[.]19[.]49, 185[.]136[.]171[.]110 y 181[.]130[.]5[.]112, con el objetivo de descargar tres archivos archivos (carga útil del malware): "F3runpe.txt", "33889%20send.txt" y "F3dll.txt"

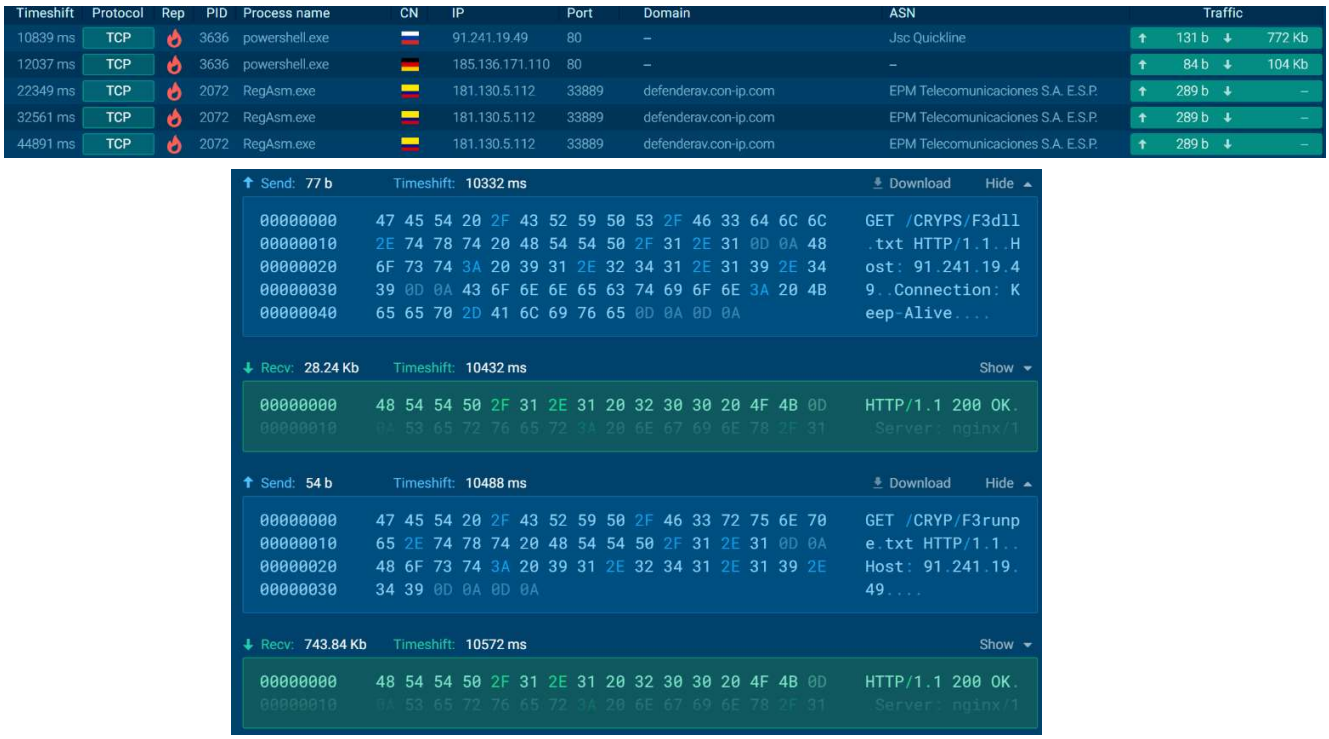


Figura 8. Conexiones y descarga de archivos de tipo malicioso. **Fuente:** Análisis en SandBox AnyRun

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:	EC-2022-049	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	22-marzo-2022	**Campaña de Amenaza Avanzada Persistente APT-C-36 podría estar presente en Ecuador**	V 1.1

Completa la descarga de lo descrito en la figura Nro. 8, se empiezan a ejecutar siete (7) subprocesos en el sistema Operativo, los que, modifican el sistema a nivel de registro, y, al finalizar, se establece una conexión con la dirección IP 181[.]130[.]5[.]112, a través del puerto 33889, dirección que, podría encontrarse en modo escucha a la espera de una víctima, para conectarse remotamente al equipo, permitiendo al ciberdelincuente, acceder al equipo infectado para robar información/datos/contraseñas de carácter sensible.

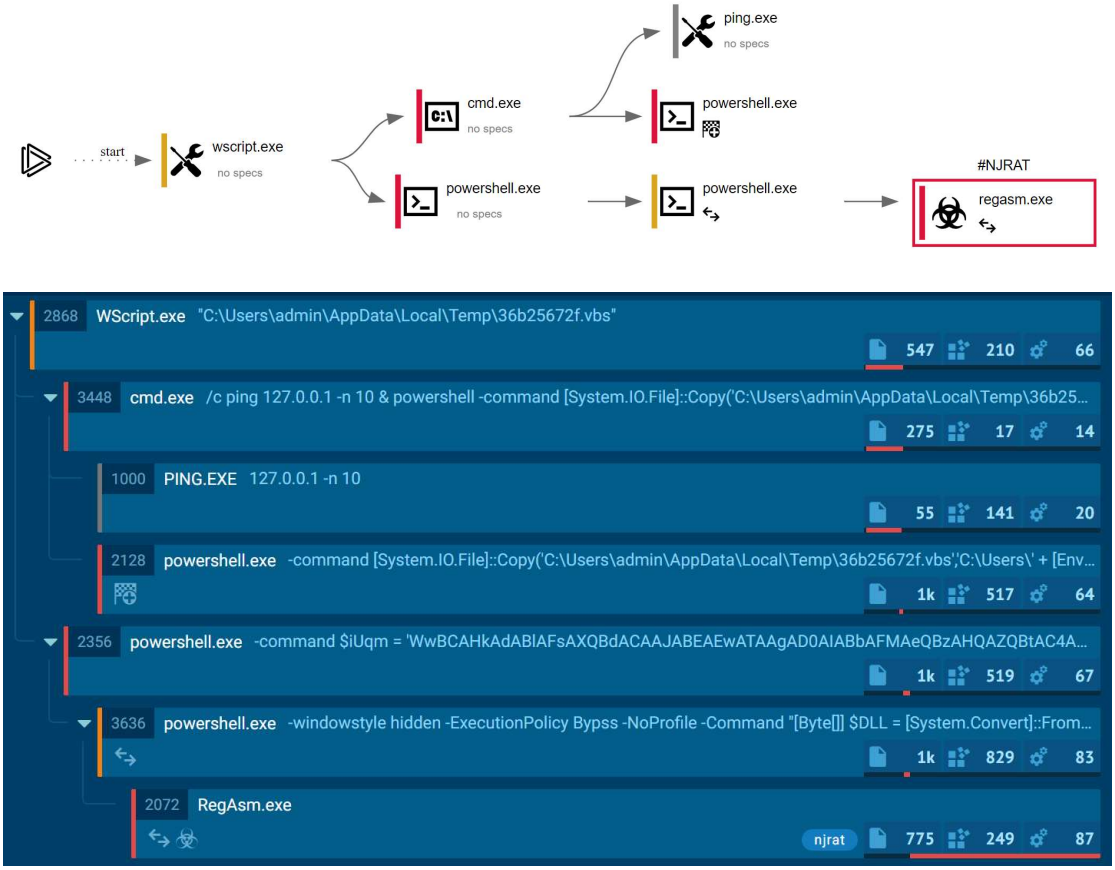


Figura 9. Ejecución a nivel de registro de archivo malicioso. **Fuente:** Análisis en SandBox AnyRun

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:	EC-2022-049	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	22-marzo-2022	**Campaña de Amenaza Avanzada Persistente APT-C-36 podría estar presente en Ecuador**	V 1.1

A continuación, se muestra el diagrama general de conexiones, correspondientes al archivo "36b25672f.vbs": conexión a tres direccione IP y descarga de tres archivos de tipo malicioso.

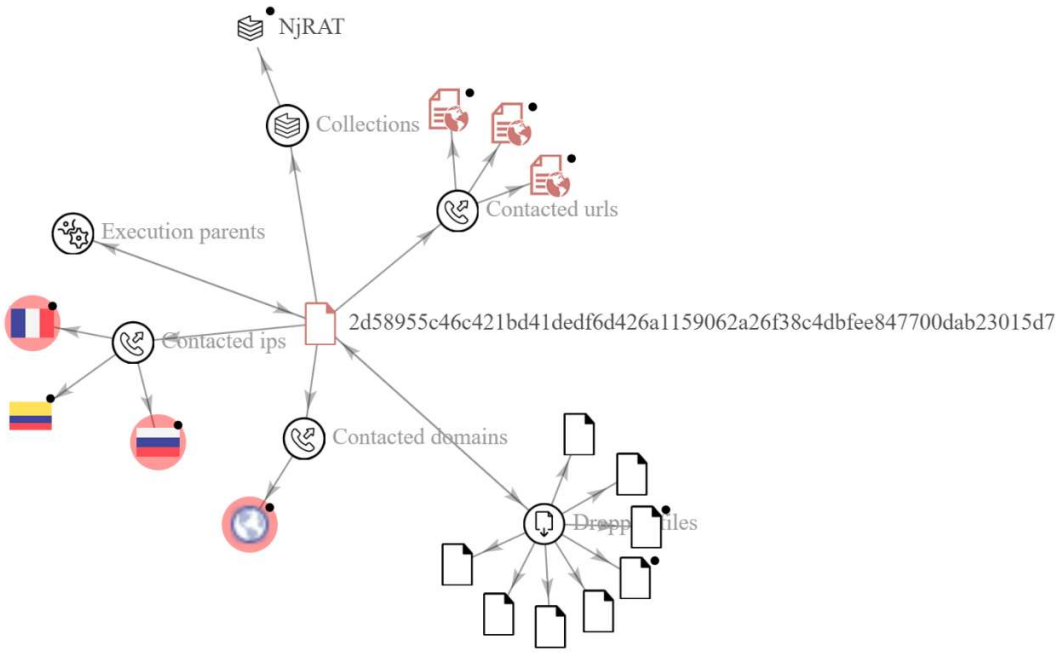


Figura 10. Diagrama de conexiones de archivo malicioso. **Fuente:** Virus Total

En contexto, al tener un archivo de tipo malicioso similar como muestra, se puede evidenciar que las direcciones IP 91[.]241[.]19[.]49 y 181[.]130[.]5[.]112, son el factor común tanto para la muestra número uno "Juicio No 9802201800411 Litigante FUNCION JUDICIAL.vbs", como para la muestra número dos "Citación Función Judicial Republica De Ecuador.exe" respectivamente.

En referencia a lo establecido en el párrafo anterior, podemos evidenciar que se trata del mismo ciberdelincuente, o grupo de ciberdelincuentes, realizando ataques similares, a través de varios métodos de ejecución de malware, ya sea a través de ofuscación de código, o, archivos maliciosos de tipo ejecutable, con el objetivo de no ser detectados.

Nro. Alerta:	EC-2022-049	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	22-marzo-2022	**Campaña de Amenaza Avanzada Persistente APT-C-36 podría estar presente en Ecuador**	V 1.1

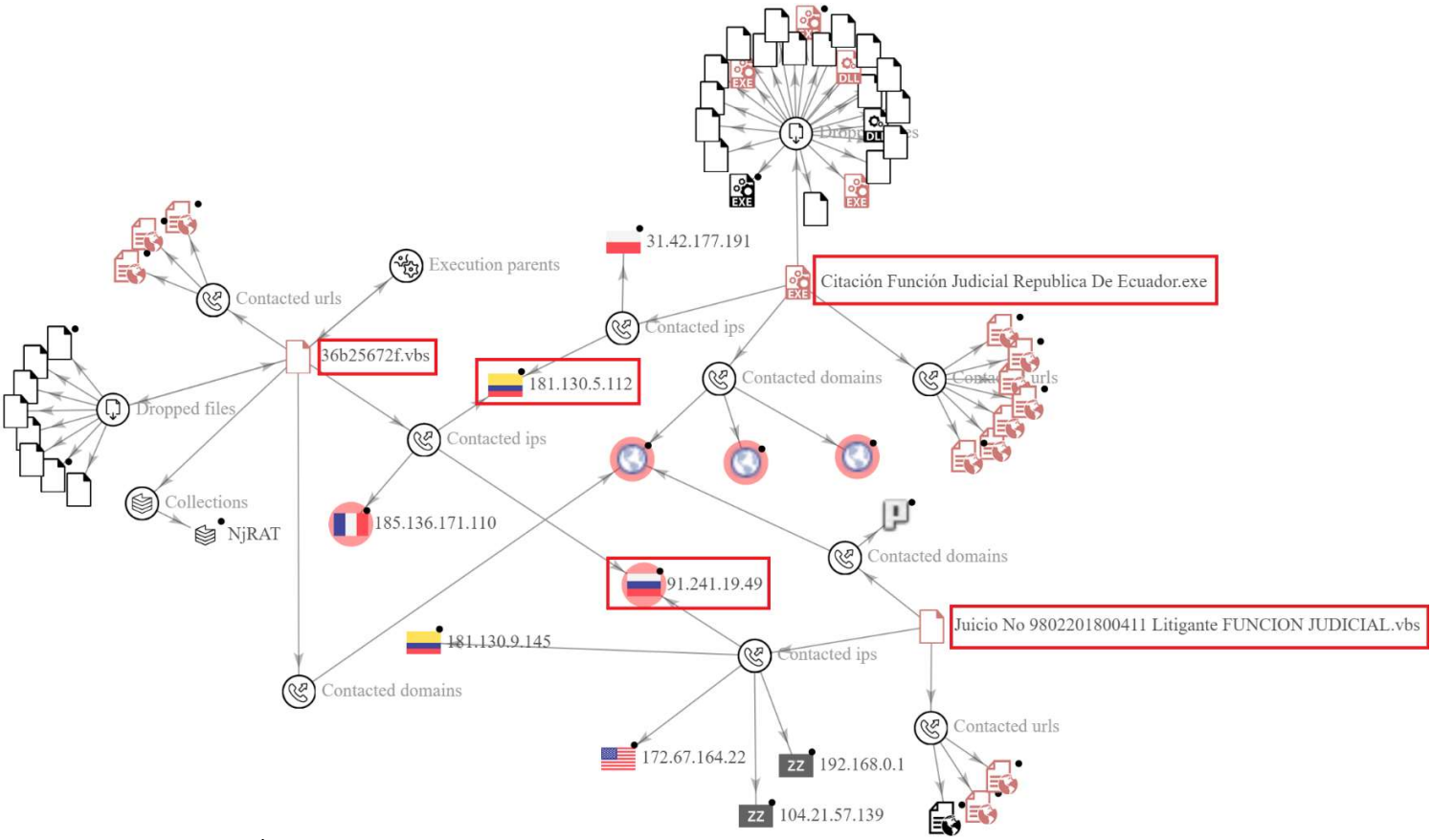
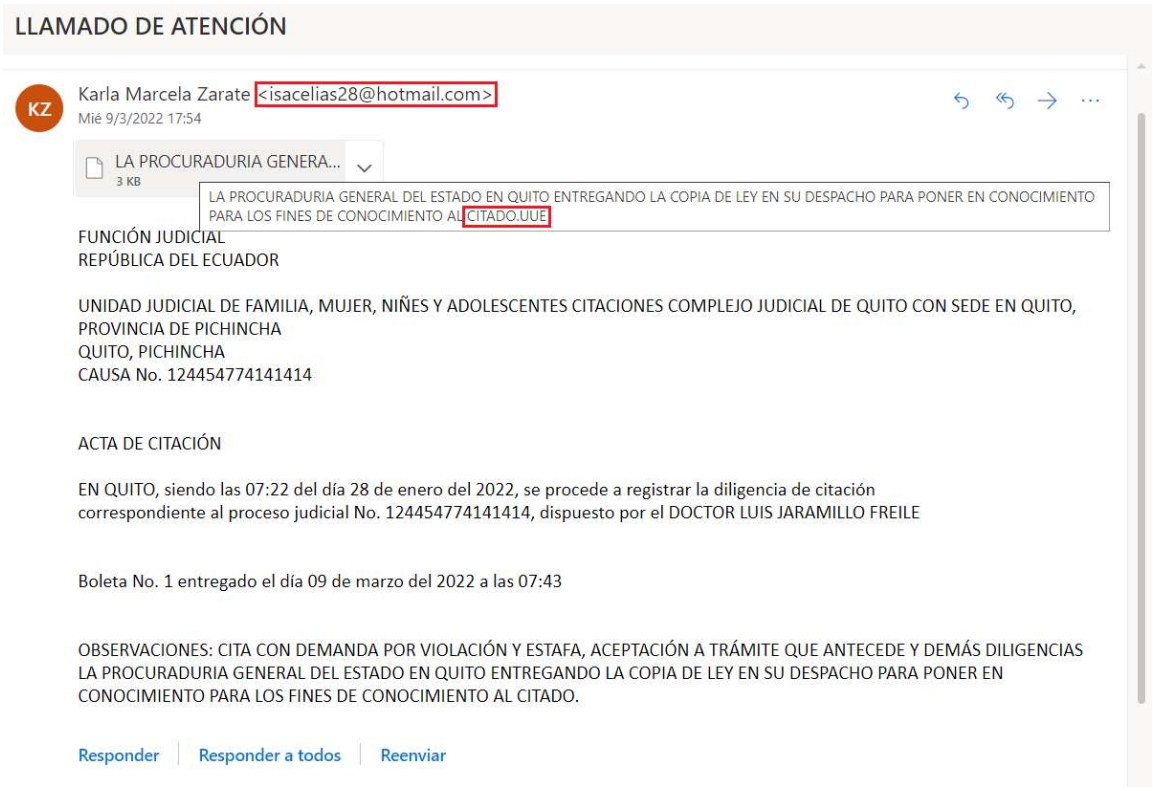


Figura 11. Árbol de conexiones comunes entre muestras uno y dos presentes en Ecuador. **Fuente:** Propia/Virus Total

Adicionalmente, se debe aclarar que, aunque los métodos de ataque sean similares a los presentes por el grupo APT-C-36, se debe considerar que también podría tratarse de un solo individuo, o, conjunto de individuos imitadores del grupo APT-C-36 original, toda vez que el código fuente ofuscado presente en los archivos, pudo haber sido descargado, modificado y adaptado a nuevas funcionalidades.

Nro. Alerta:	EC-2022-049	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	22-marzo-2022	**Campaña de Amenaza Avanzada Persistente APT-C-36 podría estar presente en Ecuador**	V 1.1

A continuación, se adjunta una tercera evidencia de malware de tipo Crypter, es decir, malware especializado, cuyo código fuente se codifica para evitar ser detectados por los diferentes métodos y motores de búsqueda de vulnerabilidades, reportado en Ecuador; corresponde a un correo electrónico de la Procuraduría General del Estado, el mismo que contiene un archivo adjunto de extensión tipo ".UUE", y, una vez ejecutado, se conecta a la dirección IP 212[.]193[.]30[.]240, con el objetivo de realizar la descarga de archivos maliciosos (carga útil), para posteriormente infectar el computador de la víctima. El correo electrónico previamente mencionado, podría también estar relacionado a la misma campaña APT-C-36, toda vez que tiene la misma estructura y comparte la misma relación de dominio Web con la muestra número dos (Tabla Nro. 2): "polycomusa[.]com"


LLAMADO DE ATENCIÓN

KZ Karla Marcela Zarate <isacelias28@hotmail.com>
Mié 9/3/2022 17:54

LA PROCURADURIA GENERA...
3 KB

LA PROCURADURIA GENERAL DEL ESTADO EN QUITO ENTREGANDO LA COPIA DE LEY EN SU DESPACHO PARA PONER EN CONOCIMIENTO PARA LOS FINES DE CONOCIMIENTO AL CITADO.UUE

FUNCIÓN JUDICIAL
REPÚBLICA DEL ECUADOR

UNIDAD JUDICIAL DE FAMILIA, MUJER, NIÑES Y ADOLESCENTES CITACIONES COMPLEJO JUDICIAL DE QUITO CON SEDE EN QUITO, PROVINCIA DE PICHINCHA
QUITO, PICHINCHA
CAUSA No. 124454774141414

ACTA DE CITACIÓN

EN QUITO, siendo las 07:22 del día 28 de enero del 2022, se procede a registrar la diligencia de citación correspondiente al proceso judicial No. 124454774141414, dispuesto por el DOCTOR LUIS JARAMILLO FREILE

Boleta No. 1 entregado el día 09 de marzo del 2022 a las 07:43

OBSERVACIONES: CITA CON DEMANDA POR VIOLACIÓN Y ESTAFA, ACEPTACIÓN A TRÁMITE QUE ANTECEDE Y DEMÁS DILIGENCIAS LA PROCURADURIA GENERAL DEL ESTADO EN QUITO ENTREGANDO LA COPIA DE LEY EN SU DESPACHO PARA PONER EN CONOCIMIENTO PARA LOS FINES DE CONOCIMIENTO AL CITADO.

Responder | Responder a todos | Reenviar

Figura 12. Correo electrónico de PGE posiblemente asociado a APT-C-36. **Fuente:** Twitter

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

Gobierno del Encuentro | Juntos lo logramos

Nro. Alerta:	EC-2022-049	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	22-marzo-2022	**Campaña de Amenaza Avanzada Persistente APT-C-36 podría estar presente en Ecuador**	V 1.1

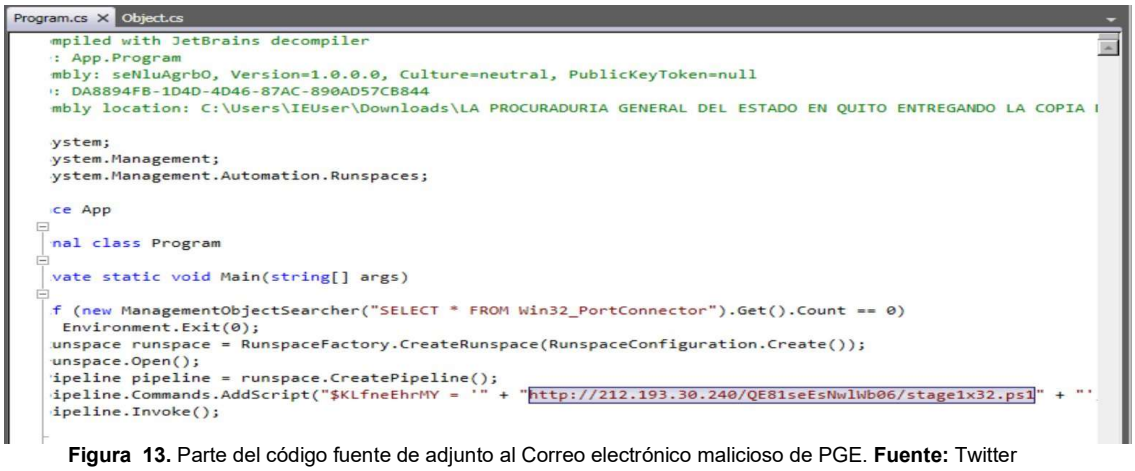


Figura 13. Parte del código fuente de adjunto al Correo electrónico malicioso de PGE. **Fuente:** Twitter

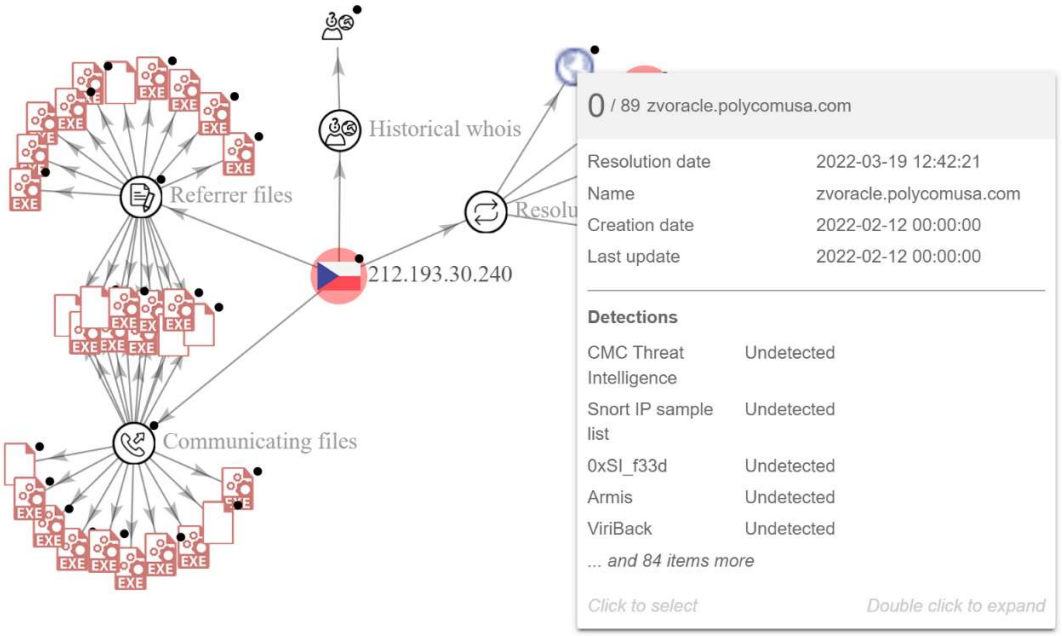


Figura 14. Árbol de conexiones asociado al archivo adjunto del Correo electrónico malicioso de PGE. **Fuente:** Twitter

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

Gobierno del Encuentro | Juntos lo logramos

Nro. Alerta:	EC-2022-049	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	22-marzo-2022	**Campaña de Amenaza Avanzada Persistente APT-C-36 podría estar presente en Ecuador**	V 1.1

VI. INDICADORES DE COMPROMISO:

Ítem	Parámetro	IOC Muestra Uno	IOC Muestra Dos
1	**Nombre de Archivo**	DESCARGOS PENALES PROCESO N°1193490-3	Citación Función Judicial Republica De Ecuador
2	**Descripción**	Juicio No 9802201800411 Litigante FUNCION JUDICIAL.vbs	kifoasad.exe
3	**Nro. de anti virus que detectan**	12 de 53	31 de 70
4	**Threat Name**	njRAT	njRAT
5	**MD5**	852f32efe7a6ecd4ce3b1c93564180ac	216e41dd8889798a65852249394a62ad
6	**SHA-1**	e7362c2ba384a8c15990b0858b89e461f43e022c	606fb46526b2c6187b00a94b2adb288171797127
7	**SHA-256**	dc7b8494eaf9230372e53e1e822cc6f23982afdace7f7c80076a769f466befa8	ebbc37e280f15408a2ff17bec1151cc64d151e20c1e59209a76b9eb3944d6704
8	**Dominios**	defenderav.con-ip[.]com Created: 2014-03-31 IONOS SE	defenderav.con-ip[.]com Created: 2014-03-31 IONOS SE
		pasteio[.]com Created: 2017-07-05 NAMECHEAP INC	polycomusa[.]com Created: 2022-02-12 Registro:--
			sicariop[.]polycomusa[.]com Created: 2022-02-12 Registro:--
9	**IP Traffic**	104[.]21[.]57[.]139 Country: --	31[.]42[.]177[.]191 Country: PL
		172[.]67[.]164[.]22 Country: US	

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:	EC-2022-049	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	22-marzo-2022	**Campaña de Amenaza Avanzada Persistente APT-C-36 podría estar presente en Ecuador**	V 1.1

Ítem	Parámetro	IOC Muestra Uno	IOC Muestra Dos
		181[.]130[.]9[.]145 Country: CO	181[.]130[.]5[.]112 Country: CO
		192.168.0.1 Country: --	
		91[.]241[.]19[.]49 Country: RU	

Tabla 3. IOC de archivos adjuntos de posible APT-C-36. **Fuente:** Análisis en Virus Total.

Considerando la Tabla 3, se observa que el tipo de malware identificado es: **njRAT**; es decir, los actores de amenaza APT-C-36 emplean RATs. En la siguiente gráfica se observa la identificación de la amenaza en los archivos adjuntos:

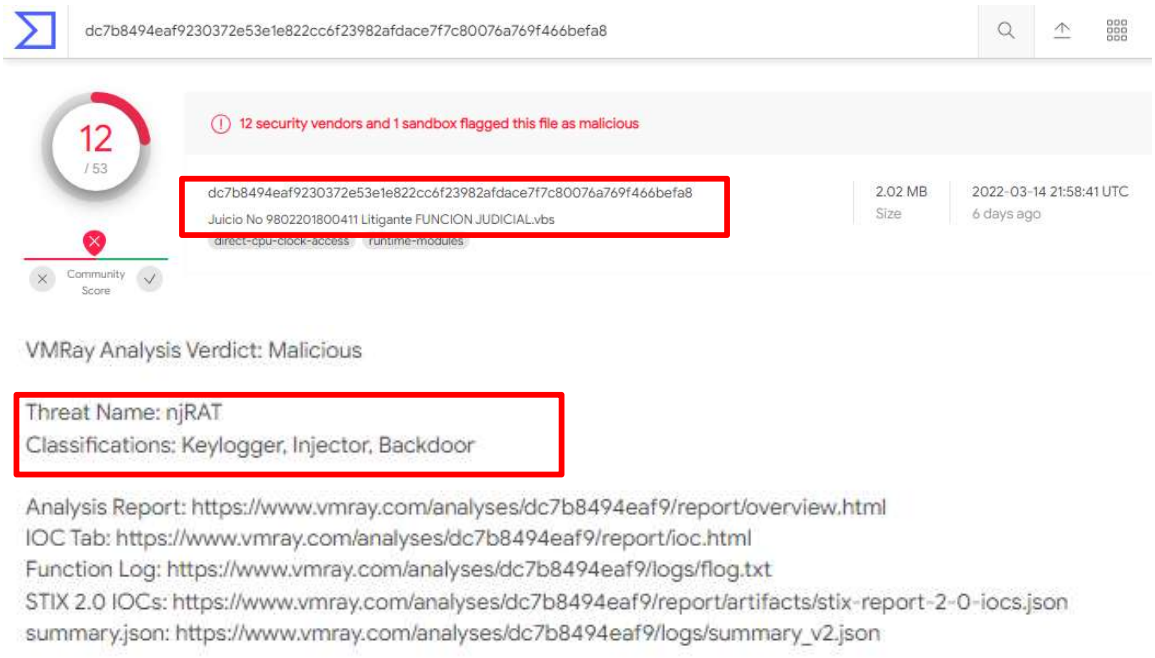


Figura 15. Threat Name de Muestra Uno. **Fuente:** Análisis en Virus Total.

Nro. Alerta:	EC-2022-049	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	22-marzo-2022	**Campaña de Amenaza Avanzada Persistente APT-C-36 podría estar presente en Ecuador**	V 1.1

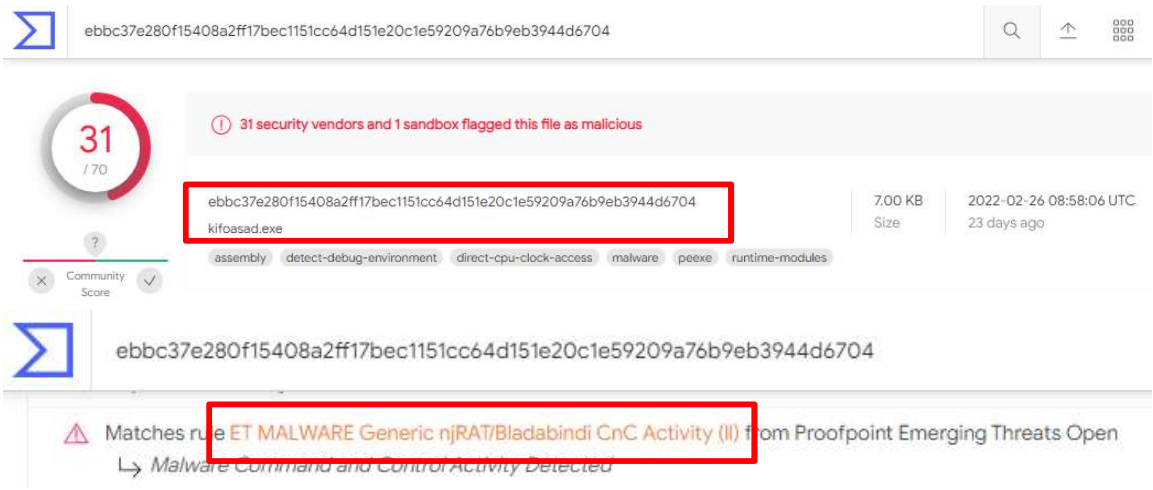


Figura 16. Threat Name de Muestra Dos. **Fuente:** Análisis en Virus Total.

"**njRAT"** es un troyano de accesos remoto (RAT), también conocido como Bladabindi, un programa malicioso que permite a un atacante controlar remotamente un equipo comprometido y realizar diversas acciones. "njRAT" presenta diferentes modificaciones; sin embargo, el troyano original presenta las siguientes características:

- Desarrollado en el lenguaje de programación C#
- Captura de pantalla, captura de cámara y audio
- Captura de pulsaciones de teclado (keylogging)
- Persistencia en el registro de Windows
- Manipulación, descarga, extracción, y ejecución de archivos
- Manipulación del registro de Windows
- Robo de credenciales
- Agrega una excepción en el Firewall de Windows para poder comunicarse
- Conexión al servidor de C&C via Socket TCP y datos codificados en Base64

Nro. Alerta:	EC-2022-049	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	22-marzo-2022	**Campaña de Amenaza Avanzada Persistente APT-C-36 podría estar presente en Ecuador**	V 1.1

VII. RECOMENDACIONES:

El EcuCert recomienda a su comunidad objetivo:

- No abrir, manipular, o interactuar, con correos electrónicos altamente sospechosos que lleguen a las bandejas de correo electrónico personal o Institucional, así como también, mensajes directos en redes sociales, procedente de remitentes desconocidos.
- Implementar técnicas de navegación segura en toda la Institución/Organización, como por ejemplo, utilizar y visitar únicamente sitios Web con certificados SSL, y, de origen no sospechoso.
- Blindar los sistemas de correo electrónico, así como también, el acceso a los mismos, a través de plataformas de autentificación de doble factor, y, uso de contraseñas robustas.
- Monitorear los sistemas de correo electrónico, a través del uso de plataformas de seguridad perimetral, así como también, implementar la correcta configuración a nivel de SPF, DKIM y DMARC de lo mismos, con el objetivo de evitar una posible suplantación de identidad Institucional a nivel de correo electrónico.
- Otorgar privilegios de usuario al mínimo dependiendo del tipo de labor a realizar.
- Descargar programas, archivos y actualizaciones, solamente desde fuentes oficiales y verificadas.
- Implementar y monitorear, plataformas de seguridad perimetral para identificar posible tráfico malicioso tanto a nivel interno como externo la infraestructura de red de la organización/Institución
- Descargar programas, archivos y actualizaciones, solamente desde fuentes oficiales 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.
- 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.

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:	EC-2022-049	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	22-marzo-2022	**Campaña de Amenaza Avanzada Persistente APT-C-36 podría estar presente en Ecuador**	V 1.1

Capacitar a todos los usuarios, mediante la concientización y simulaciones para reconocer e informar sobre intentos de phishing e ingeniería social.

- Tener actualizado y utilizar, un software anti-virus.
- Realizar copias de seguridad regularmente de archivos personales y críticos para la Organización.
- 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. REFERENCIAS:

Fileextension. (s.f.). *File Extension*. Obtenido de File Extension: https://www.file-extension.info/es/format/vbs

Horejsi, J., & Lunghi, D. (13 de 9 de 2021). *TREND MICRO*. Obtenido de TREND MICRO: https://www.trendmicro.com/en_us/research/21/i/apt-c-36-updates-its-long-term-spam-campaign-against-south-ameri.html

IONO, D. G. (s.f.). *Digital Guide IONO*. Obtenido de Digital Guide IONO: https://www.ionos.es/digitalguide/servidores/know-how/archivos-exe/

Malpedia. (s.f.). *Malpedia*. Obtenido de Malpedia: https://malpedia.caad.fkie.fraunhofer.de/details/win.njrat

MALPEDIA. (s.f.). *MALPEDIA*. Obtenido de MALPEDIA: https://malpedia.caad.fkie.fraunhofer.de/actor/apt-c-36

Total, V. (s.f.). *Virus Total*. Obtenido de Virus Total: https://www.virustotal.com/gui/file/ebbc37e280f15408a2ff17bec1151cc64d151e20c1e59209a76b9eb3944d6704/relations

Nro. Alerta:	EC-2022-049	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	22-marzo-2022	**Campaña de Amenaza Avanzada Persistente APT-C-36 podría estar presente en Ecuador**	V 1.1

Total, V. (s.f.). *Virus Total*. Obtenido de Virus Total: https://www.virustotal.com/gui/file/dc7b8494eaf9230372e53e1e822cc6f23982afdace7f7c80076a769f466befa8/relations

WELIVESECURITY. (29 de 09 de 2021). *ESET*. Obtenido de ESET: https://www.welivesecurity.com/la-es/2021/09/29/que-es-njrat-troyano-acceso-remoto-utilizado-cibercriminales/

MALPEDIA. (s.f.). *MALPEDIA*. Obtenido de MALPEDIA: https://www.b-secure.co/recursos/infografias/pasos-de-las-amenazas-persistentes-avanzadas

Sandbox AnyRun. (17 de febrero de 2022). Any Run. Obtenido de Any Run: https://app.any.run/tasks/e3bb8f70-847c-45dc-990a-181b4d29ed7e/

Steck Mera. (18 de marzo de 2022). SteckMera. Obtenido de Twitter: https://twitter.com/SteckMera/status/1504892999498715139/

B-SECURE. (s.f.). B-SECURE. Obtenido de B-SECURE: https://www.b-secure.co/recursos/infografias/pasos-de-las-amenazas-persistentes-avanzadas