Informe

Coyuntural

Suplantación a la Fiscalía usada para propagar DcRAT

COLCERT IN-20251010-025

TLP:CLEAR

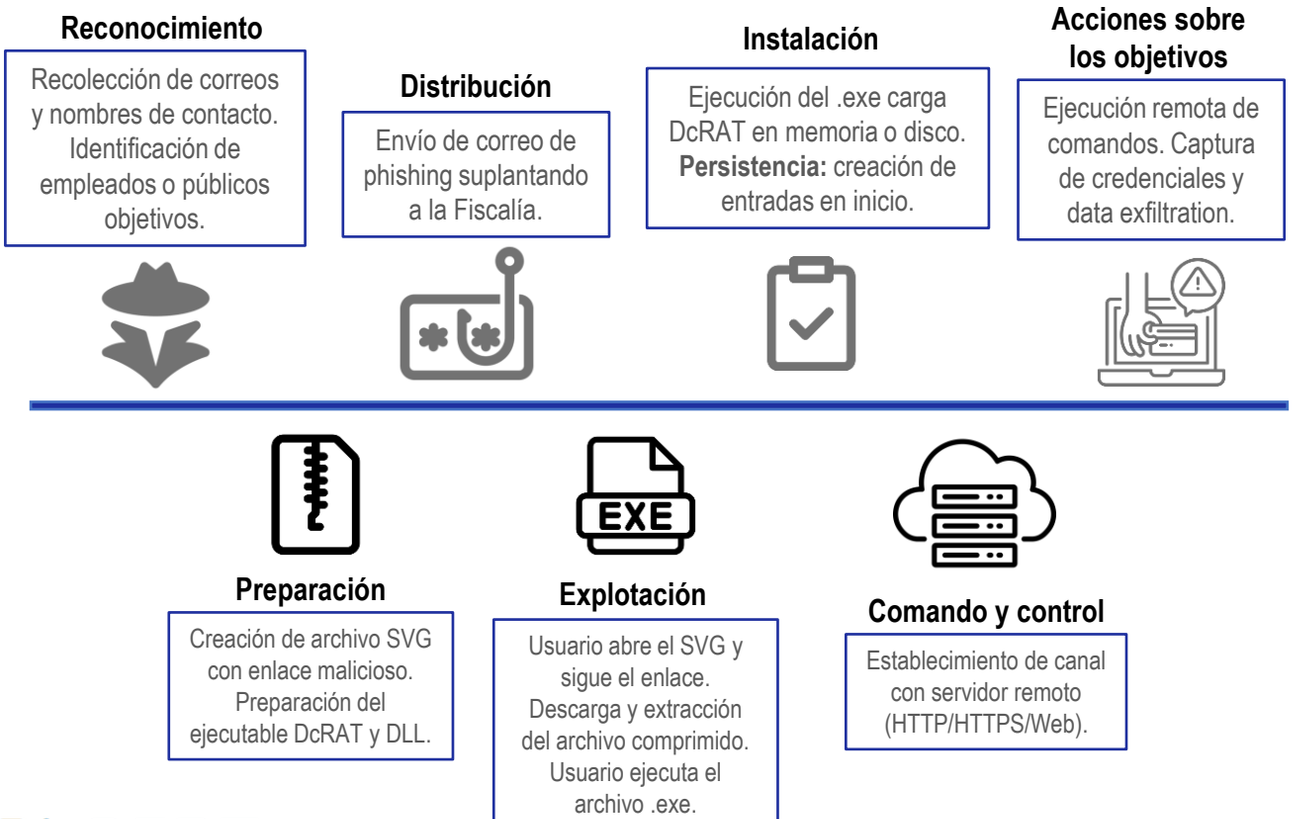
Resumen ejecutivo:

Durante la última semana se identificó una campaña de phishing dirigida a usuarios en Colombia, en la que los actores de amenaza suplantan a la Fiscalía General de la Nación con el objetivo de inducir a las víctimas a descargar y ejecutar un archivo malicioso. El correo electrónico distribuido en esta campaña contenía un archivo adjunto en formato SVG, el cual, al ser abierto, redirigía a un repositorio en línea donde se alojaba un archivo comprimido que contenía cinco componentes: un archivo ejecutable, dos bibliotecas dinámicas (DLL) y dos archivos de tipo desconocido.

Tras ejecutar el archivo principal, se determinó que este correspondía a una muestra del troyano de acceso remoto (RAT) conocido como DcRAT, una amenaza desarrollada en C# que otorga al ciberdelincuente control total sobre el sistema comprometido. DcRAT es capaz de ejecutar comandos de forma remota, registrar pulsaciones de teclado, capturar pantallas, extraer información confidencial y desplegar módulos adicionales, lo que representa un riesgo significativo para la confidencialidad, integridad y disponibilidad de los datos del usuario o de la organización afectada.

La cadena de infección evidencia un uso de técnicas de ingeniería social y suplantación institucional para generar confianza en el destinatario y facilitar la ejecución del código malicioso. Este tipo de campañas refuerza la necesidad de fortalecer las estrategias de concienciación y detección temprana frente a correos con adjuntos inusuales, así como mantener actualizados los controles de seguridad que permitan identificar comportamientos anómalos asociados a comunicaciones con servidores de comando y control.

Siguiendo el modelo de **Cyber Kill Chain**, se clasifica el modo de ataque de los actores de amenaza de la siguiente manera:



Análisis estático de la muestra

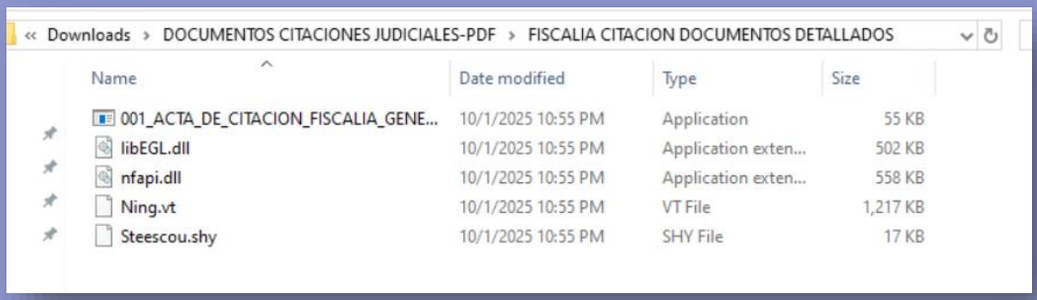
Se ha detectado una campaña de distribución de DcRAT en Colombia, la cual se propaga mediante mensajes de correo electrónico de tipo phishing. A partir de esta actividad, se identificó el archivo malicioso involucrado y se realizó su respectivo análisis.

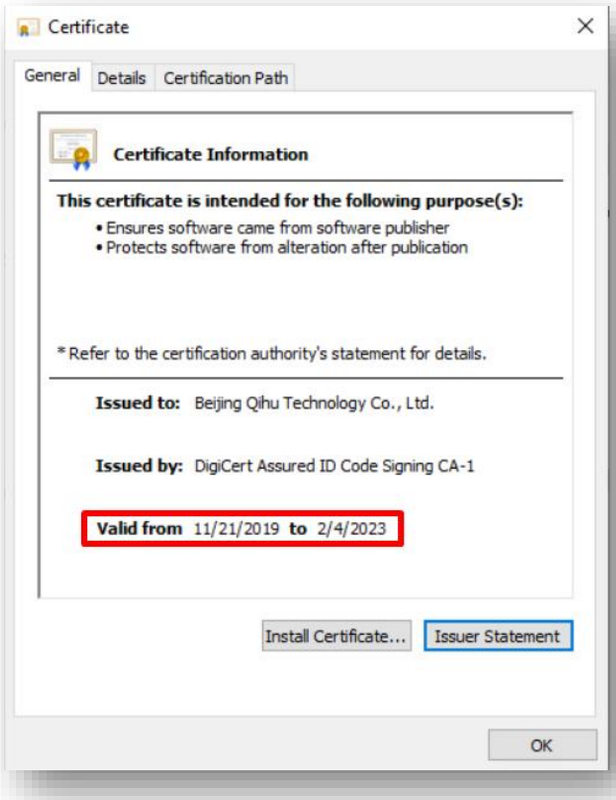
INFORMACIÓN DE LA CARGA ÚTIL INICIAL	
MD5	c9d2e690f222e8d86d4ef601598228b0
SHA1	d699f28897775e7d75e7ac3c88ec8b1256a87a7d
SHA256	9ecce36b93d62587f260be904ed2302b173b74056147733dcea13702f2257391
FILE NAME	Boleta de citacion fiscalia general radicado No 2025-6632-996636-PDF.svg
FILE TYPE	SVG
FILE SIZE	2.12 MB (2227118 bytes)
SSDEEP	3072:TZiWk9+VwUokCPjsOftMa1za6H2PjoAo+/+UfEMTT:TZiWGhBoOftMQULoWFEMn
TLSH	T188A5AE71CDB28E1607925A6B48DF33D59D7DB3B346FC84FB2092AA53F1729A2C2C9105

Se evidenció una campaña de correos electrónicos fraudulentos que, aunque presentan variantes, persiguen el mismo objetivo: la distribución de un troyano de acceso remoto. Los mensajes suplantan a la Fiscalía e incluyen archivos adjuntos en formato SVG que contienen enlaces a un repositorio desde el cual se descarga un archivo comprimido, presentado como documentación relacionada con una supuesta demanda.

En este caso, el artefacto descargado corresponde a un archivo comprimido en formato LZH, identificado como “DOCUMENTOS CITACIONES JUDICIALES-PDF”, que se obtiene desde el servicio de almacenamiento en la nube Koofr.

Al descomprimir el archivo, se identificó la presencia de cinco componentes: un archivo ejecutable, dos bibliotecas dinámicas (DLL) y dos archivos adicionales de tipo desconocido. Estos elementos conforman el conjunto de archivos utilizado por los ciberdelincuentes para ejecutar la carga maliciosa, evidenciando una posible estructura diseñada para la instalación y funcionamiento del troyano de acceso remoto.

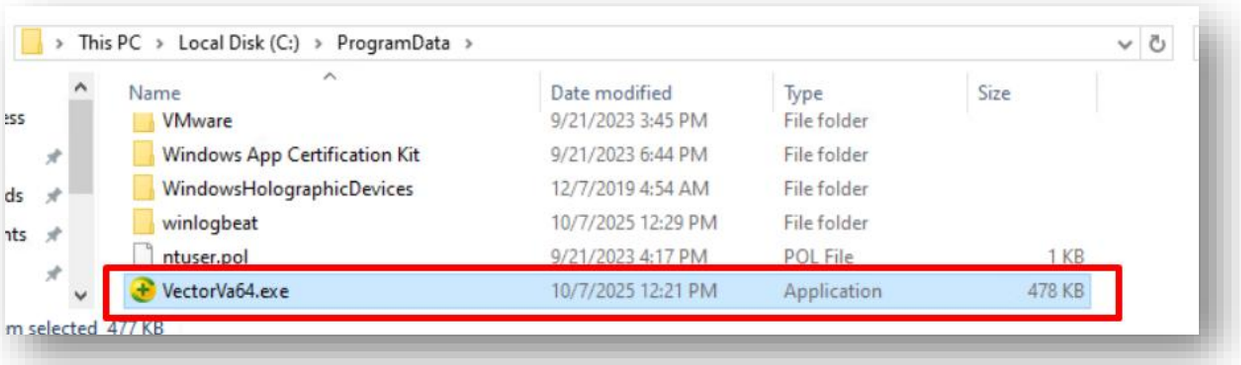


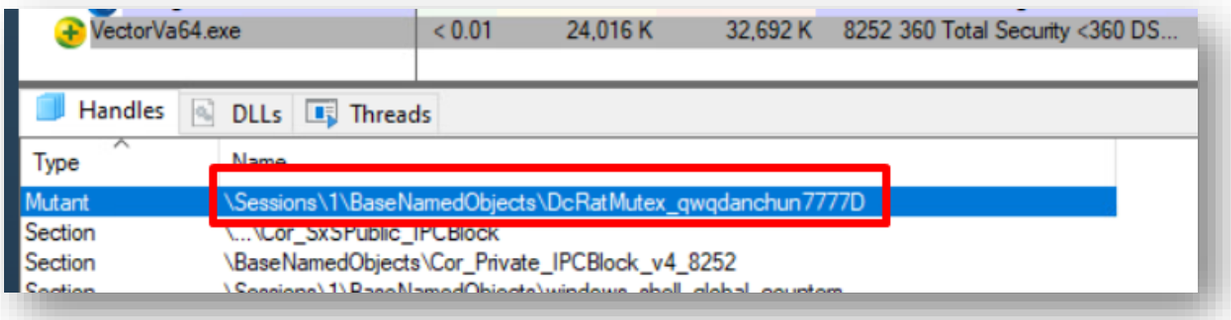


Al verificar el archivo ejecutable denominado “001_ACTA_DE_CITACION_FISCALIA_GENERAL_DETALLES-PDF.exe”, se identificó que estaba firmado digitalmente con un certificado emitido por la autoridad certificadora **DigiCert Assured ID Code Signing CA-1**, a nombre de **Beijing Qihoo Technology Co., Ltd**. El certificado presentaba un período de validez comprendido entre el 21 de noviembre de 2019 y el 4 de **febrero de 2023**.

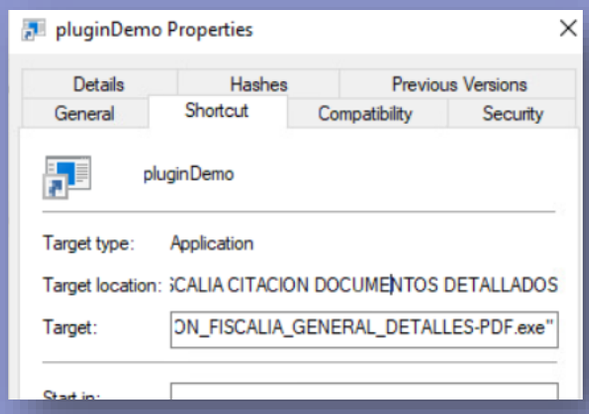
No obstante, dicha firma no garantiza la legitimidad del ejecutable, ya que los actores maliciosos suelen reutilizar o falsificar certificados caducados o comprometidos para aparentar autenticidad y evadir mecanismos de detección.

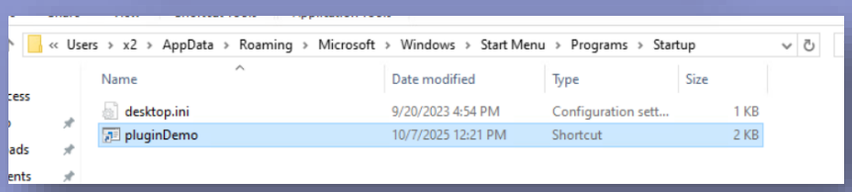
Al ejecutar el archivo "**001_ACTA_DE_CITACION_FISCALIA_GENERAL_DETALLES-PDF.exe**", se observó la creación automática de un nuevo archivo ejecutable en la ruta "C:\ProgramData" denominado **VectorVa64.exe**, el cual fue posteriormente ejecutado en el sistema. Durante el análisis del proceso activo, se identificó la presencia de un handle asociado a un *mutex* denominado "**DcRatMutex_qwqdanchun7777D**", elemento característico y empleado por la familia de troyanos de acceso remoto **DcRAT** para evitar la ejecución simultánea de múltiples instancias del mismo agente en un dispositivo comprometido. Este comportamiento confirma la actividad del RAT y su capacidad de persistencia dentro del entorno afectado.



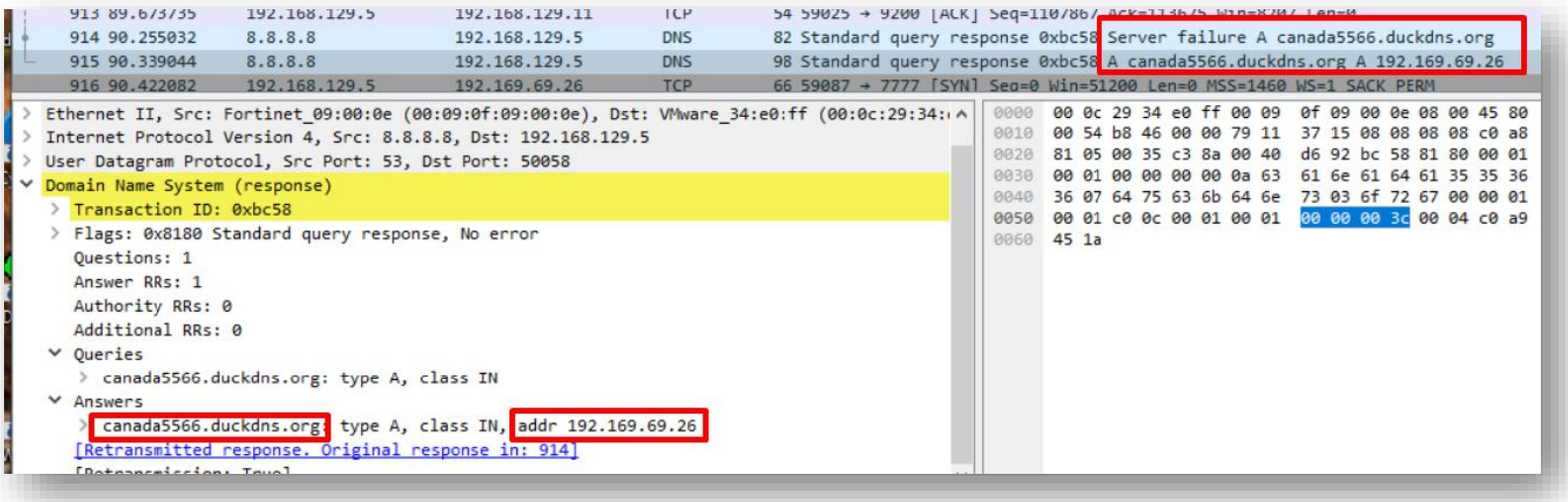


Con el objetivo de garantizar persistencia en el sistema, se creó un acceso directo (.lnk) denominado "pluginDemo" dentro de la carpeta de inicio automático del usuario (Startup). Este atajo está configurado para ejecutarse en cada inicio de sesión, lo que asegura que la carga maliciosa se vuelva a lanzar tras reinicios o cierres de sesión. La ruta objetivo del .lnk apunta directamente al ejecutable inicial 001_ACTA_DE_CITACION_FISCALIA_GENERAL_DETALLES-PDF.exe, lo que confirma que el acceso directo actúa como mecanismo de autostart.

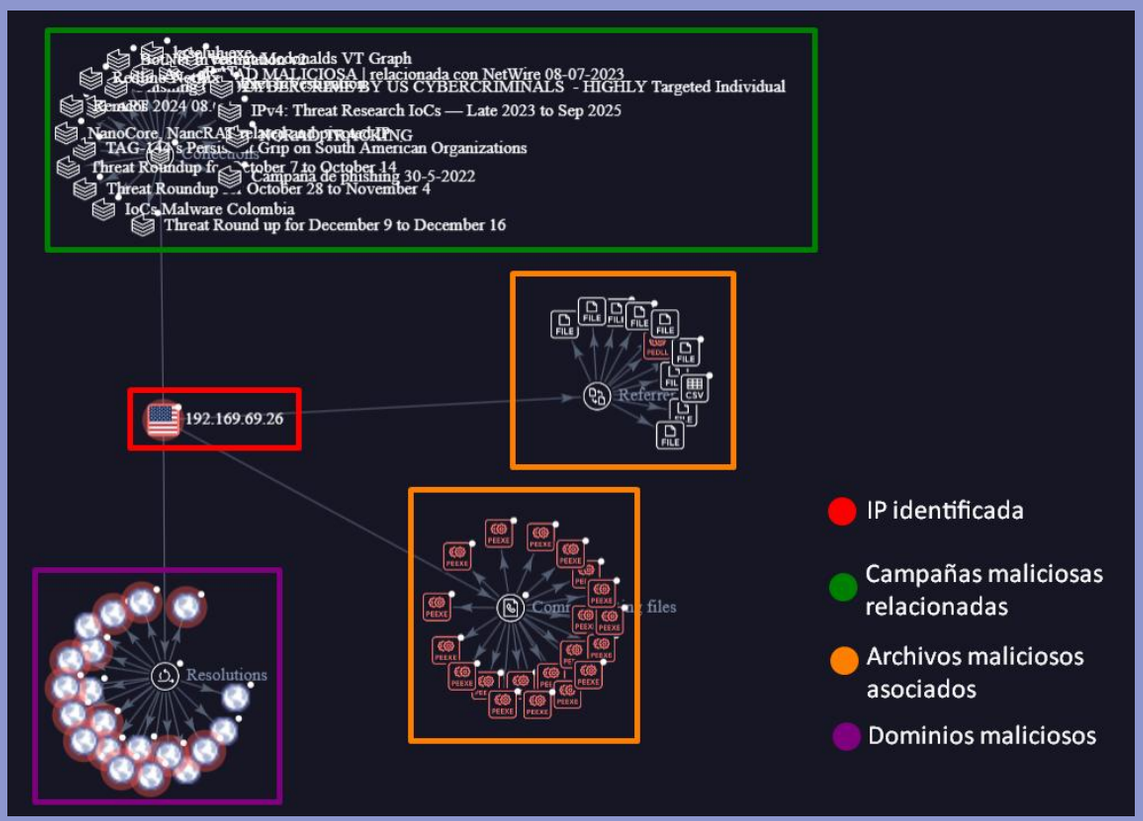




Al inspeccionar la actividad de red del equipo comprometido, se observó que la muestra estableció una conexión saliente hacia el nombre de dominio **canada5566.duckdns[.]org**, el cual resolvió a la dirección IP **192[.]169.69.26**. El dominio pertenece a un servicio de DNS dinámico (DuckDNS), frecuentemente utilizado por actores maliciosos para mantener infraestructura de comando y control (C2) con direcciones IP cambiantes. La correlación entre la resolución DNS y las comunicaciones salientes sugiere que dicha infraestructura actuó como servidor C2 para **DcRAT**.



Tanto el subdominio como la dirección IP fueron catalogados como indicadores maliciosos. El análisis de la dirección IP reveló que se encuentra geoposicionada en Estados Unidos y presenta antecedentes de uso en múltiples campañas de distribución de malware dirigidas a Colombia y otros países de la región latinoamericana.



Técnicas MITRE ATT&CK asociadas

NOMBRE TÉCNICA	ID TÉCNICA	DESCRIPCIÓN
Phishing: Spearphishing Attachment	T1566.001	Envío de correos con adjuntos maliciosos para inducir a la víctima a descargar o extraer un paquete que contiene la carga útil.
User Execution: Malicious File	T1204.002	Ejecución dependiente de la acción del usuario, mecanismo responsable de activar la carga inicial en el equipo.
Ingress Tool Transfer	T1105	Transferencia o descarga de herramientas o archivos desde infraestructura externa (repositorios o servicios de almacenamiento en la nube) hacia el entorno víctima.
Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	T1547.001	Persistencia mediante entradas en claves Run del registro o accesos directos en la carpeta Startup, que aseguran la ejecución después de reinicios o inicios de sesión.

Mitigaciones MITRE

MITIGACIÓN	ID MITIGACIÓN	RELEVANCIA
User Training (Capacitación de usuarios)	M1017	Reduce el éxito de campañas de *spearphishing* con adjuntos (SVG) al mejorar la capacidad de los usuarios para reconocer y reportar correos y archivos sospechosos; contribuye a disminuir la ejecución involuntaria de la carga.
Restrict Web-Based Content (Restringir contenido web)	M1021	Permite bloquear o filtrar descargas desde servicios de almacenamiento y restringir tipos de archivos peligrosos, reduciendo la probabilidad de descargas automáticas desde enlaces contenidos en el SVG.
Execution Prevention (Aplicación de control / whitelisting)	M1038	Implementar AppLocker/WDAC o políticas de control de ejecución evita que binarios no aprobados se ejecuten, mitigando la activación del RAT incluso si el archivo llega al equipo.
Restrict Registry Permissions (Restringir permisos del Registro)	M1024	Limitar quién puede modificar claves del Registro y carpetas de inicio dificulta la creación de entradas Run / acceso directo (.lnk) en Startup usadas para persistencia, complicando que el atacante mantenga ejecución automática tras reinicios.

Recomendaciones

- Implementar políticas de control de aplicaciones que limiten la ejecución de archivos descargados desde ubicaciones no confiables o temporales, evitando así la instalación de binarios potencialmente maliciosos.
- Configurar reglas avanzadas en el firewall perimetral y en los sistemas de seguridad endpoint (EDR) para bloquear conexiones salientes hacia dominios o direcciones IP sospechosas que no estén asociadas a operaciones legítimas.
- Monitorear continuamente la creación y modificación de claves de registro, tareas programadas y servicios del sistema operativo, con el fin de identificar intentos de persistencia o ejecución automática de programas no autorizados.
- Actualizar y parchear todos los sistemas operativos, navegadores, complementos y aplicaciones utilizadas, minimizando la explotación de vulnerabilidades que permitan la ejecución remota de código.
- Restringir privilegios administrativos solo al personal estrictamente necesario, aplicando el principio de mínimo privilegio y controlando el uso de herramientas del sistema como PowerShell, MSBuild o regsvr32 que suelen ser abusadas por actores maliciosos.
- Capacitar periódicamente a los usuarios sobre los riesgos asociados con la descarga y ejecución de archivos adjuntos o enlaces desconocidos, fortaleciendo la conciencia en ciberseguridad y reduciendo la superficie de ataque inicial.

COLCERT

Indicadores de compromiso

IOC IDENTIFICADOS EN ESTA CAMPAÑA	
MUTEX	DcRatMutex_qwqdanchun7777D
URL	hxxps://app[.]koofr[.]net/links/c6602426-64ee-4c66-ab03-e7f360ed5b68?id=8027ad11-9012-4489-a23c-15dffcedd7c9
MD5	c9d2e690f222e8d86d4ef601598228b0
MD5	a58dcaa2b7cd265ca1b63cf4fa42cdb4
MD5	f2b85341a241bc9a8249f467ed3b6473
MD5	c27ac80a56f7bfcfca384fe0ab33ba3e
MD5	9befe1d20b4fe190e37f097e84506597
MD5	6edca0741eec689b33cdb8c2a1bad987
MD5	917d64d1c08216c0a4a3fd2c137aed84
MD5	570b90edff265636b424c1c2594adedc
SHA1	d3cea0170107566700ad9f2c1c9dcd6488cc9e8c
SHA1	e48fb705ea6f6729d5d4a77ba1c94a96f9c07779
SHA1	44ed925e2d3ba3d68f89104e1062aee1c81fa6f9
SHA1	7432dfef4b6f2f7dbd75959ea6eb50f1044b4512
SHA1	79df099da695e6407a76b629c2ef9b4e5922c49b
SHA1	80f60bf52f0c35ccd975d8cb499b07f66801d2cd
SHA1	d699f28897775e7d75e7ac3c88ec8b1256a87a7d
SHA1	e8df3ec9d201af860ae700a9a249264d180facb6
SHA256	22dbc084969a9bd61593ff342aa74ff00356a20d3a5607df88dadad90b04cf95
SHA256	52fe0a9e8e623023d3b0c3f1c36c151155faeebef443301e009c48485205c791
SHA256	6e1a27ac594d9143e2a9832d799bfe52bd0eb04e672e827c6dfcb0bb9145ddb8
SHA256	a70978d0cb43ca85b2f91ca022f678d38ec04b8ddef895355c934777e1c7c673
SHA256	3641afbd01782f19b560744f9bbc87f066e737e08fec258111f03af295090de1
SHA256	dcfedf6e12b086ac39022d75d3cbd9e1cc0000536b763a4ccb9ef7b20020ddcf
SHA256	62bdbd0d9fa330bbe0e75b3a7f0d80eb663dab4f081fc2d4f46932fe3c36ef5b
SHA256	9ecce36b93d62587f260be904ed2302b173b74056147733dcea13702f2257391
DOMINIO	canada5566.duckdns[.]org
IP	192.169.69[.]26