Boletín informativo
Malware DCRat Adobe

CSIRTSALUD-AV-20251022-08 **TLP: AMBER**

Incidente ID:	0008
Fecha del reporte:	23/10/2025
Entidad:	Todas las Entidades del Ecosistema Digital
Título:	Campaña activa de malware DCRat que afecta sistemas Microsoft Windows en Latinoamérica
Herramienta de detección	N/A
Activo involucrado:	Sistemas Operativos Windows
Tipo de incidente:	Boletín informativo
Nivel de riesgo:	Alto

Objetivo:

Informar a las entidades del ecosistema Digital sobre la campaña activa del malware DCRat que se camufla como instalador de Adobe y está afectando a países como Colombia y Ecuador, describiendo riesgos, productos afectados y las medidas inmediatas de mitigación.

Descripción:

Desde el laboratorio de ESET en Latinoamérica se ha detectado una amenaza que se propaga por la región, con foco en los países de Colombia y Ecuador. Esta amenaza, la cual afecta a sistemas operativos Windows, es detectada por las herramientas de soluciones de seguridad como Win32/Loader.Lycaon.AB.

La amenaza intenta camuflarse de aplicación legítima de Adobe, manipulando los metadatos del archivo ejecutable para aparentar legitimidad. Sin embargo, el archivo carece de firma digital válida, lo que confirma su origen fraudulento.

El objetivo es infectar a las víctimas con el troyano DCRat, una variante de AsyncRAT, un software usado en varias campañas de la región. Si bien no se encontraron los métodos de propagación para llegar hasta sus víctimas, se encontró que la cadena de infección inicia con archivos comprimidos que utilizan nombres que aparentan ser comunicaciones judiciales o gubernamentales como, por ejemplo, “Informe Especial Notificado Nro. 113510000548595265844”, lo cual deja pensar que se trata de una propagación a través de correo electrónico.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Productos afectados:

Los productos afectados corresponden a los sistemas operativos Microsoft Windows, utilizados como plataforma para la distribución y ejecución del malware identificado.

Modo de explotación y cadena de infección

La campaña del malware DCRat se explota principalmente mediante correos de phishing que suplantan entidades legítimas, como proveedores o instituciones oficiales, para inducir al usuario a descargar y ejecutar archivos maliciosos disfrazados de instaladores de Adobe u otros programas. Una vez que la víctima ejecuta el archivo, se activa un *loader* ofuscado que evade mecanismos de seguridad y descarga o inyecta el componente principal del malware en el sistema. Este programa establece persistencia, permitiendo a los atacantes mantener acceso remoto al equipo comprometido, ejecutar comandos, robar credenciales, exfiltrar información y capturar pantallas. DCRat opera bajo el modelo de *Malware-as-a-Service*, lo que facilita su distribución entre distintos actores. Su comunicación con los servidores de comando y control (C2) utiliza dominios dinámicos y técnicas de evasión, lo que dificulta su detección.

Ruta del registro de Windows utilizado para la persistencia

La ruta del registro de Windows utilizado por el Malware para la persistencia es la siguiente:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

La muestra crea los siguientes directorios y archivos

- C:\Users\<NOMBRE_USUARIO> \Documents\KCSoftwares\sdk\
- mdb2db.exe

Indicadores de Compromiso (IoC)

A continuación, se presentan los hashes relacionados con la campaña.

SHA1	Nombre	Detección
758d3c028faaf023c28890f3c4a68cdbce5159e3	AdobeARM.exe	Win32/Loader.Lycaon.AB.gen
adc96ef4fc323a836087b5e53bf7e69be2a9ac9f	AdobeARM.exe	Win32/Loader.Lycaon.AB.gen

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

A continuación, se presenta la IP maliciosa remota relacionada con la campaña.

IP Maliciosa	URL Verificación
154.216.19.63	https://www.virustotal.com/gui/ip-address/154.216.19.63

A continuación, se presenta el dominio relacionado con la campaña

Dominio	URL Verificación
pctrabajonuevo2.casacam.net	https://www.virustotal.com/gui/domain/pctrabajonuevo2.casacam.net

Técnicas MITRE ATT&CK Detectadas:

ID	Nombre
T1056.001	Captura de entrada: registro de teclas (Keylogging)
T1005	Datos del sistema local
T1027.001	Archivos o información ofuscada: relleno binario
T1027.007	Archivos o información ofuscada: resolución dinámica de API
T1027.009	Archivos o información ofuscada: cargas incrustadas
T1027.013	Archivos o información ofuscada: archivo cifrado/codificado
T1036.005	Suplantación (Masquerading): coincidencia con nombre o ubicación de recurso legítimo
T1055.012	Inyección de procesos: hollowing de proceso (Process Hollowing)
T1070.004	Eliminación de indicadores: eliminación de archivos
T1140	Desofuscar/Decodificar archivos o información
T1497.001	Evasión de virtualización/sandbox: comprobaciones del sistema
T1564.003	Ocultar artefactos: ventana oculta
T1622	Evasión de depurador
T1033	Descubrimiento del propietario/usuario del sistema
T1057	Descubrimiento de procesos
T1112	Modificación del registro

T1547.001	Ejecución de inicio automático (Boot/Logon Autostart): claves Run del registro / carpeta de inicio
T1113	Captura de pantalla
T1082	Descubrimiento de información del Sistema
T1571	Puerto no estándar
T1125	Captura de video
T1059.003	Interprete de comandos y scripts
T1106	API nativa
T1041	Exfiltración a través de canal C2

Recomendaciones de mitigación:

- Aplicar de manera inmediata reglas de detección para bloquear la IP y Dominio reportados.
    - pctrabajonuevo2.casacam.net
    - 154.216.19.63
- Evitar la ejecución de archivos desconocidos o descargados desde fuentes no verificadas
- No instalar supuestas actualizaciones o programas que lleguen por correo electrónico o enlaces compartidos.
- Descargar software solo desde los sitios oficiales del proveedor Enlace oficial de Adobe.
    - https://www.adobe.com/co/
- Implementar filtros antiphishing y análisis de adjuntos (sandbox o antivirus de gateway).
- Capacitar a los usuarios para identificar correos sospechosos, especialmente aquellos que simulan ser de entidades gubernamentales, bancos o proveedores.
- Evitar abrir archivos comprimidos protegidos con contraseña si no se ha verificado su procedencia.
- Configurar políticas de grupo (GPO) o herramientas EDR para impedir ejecución de archivos .bat, .vbs, .exe o .ps1 fuera de ubicaciones confiables.
- Activar la característica *Controlled Folder Access* o listas blancas de aplicaciones.
- Asegurar que los equipos cuenten con antivirus/EDR actualizado y análisis en tiempo real.
- Mantener respaldos cifrados y probados regularmente.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Fuentes:

- https://www.welivesecurity.com/es/investigaciones/malware-loader-adobe-dcrat-latinoamerica/

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el CSIRT Salud a través de las líneas telefónicas (+57) 316 8931490 - 3181553570 o mediante el correo electrónico csirtsalud@minsalud.gov.co. Nuestro equipo está disponible para brindar el acompañamiento necesario.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570