	EC-2022-044	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	08-marzo-2022	**Acceso no autorizado a NVIDIA y filtración de información**	V 1.1

I. DATOS GENERALES:

Clase de alerta: Información de seguridad de contenidos
Tipo de incidente: Acceso no autorizado a la información
Nivel de riesgo: Alta

II. ALERTA

Actores de amenaza identificados bajo el nombre de Lapsus$ realizaron un ciberataque a NVIDIA[1] sustrayendo credenciales de los empleados e información de dicha corporación.

Figura 1. Ilustración asociada a NVIDIA.

[1] Corporación multinacional que desarrolla: unidades de procesamiento gráfico, tecnologías de circuitos integrados, chips tanto para estaciones de trabajo como para ordenadores personales y dispositivos móviles.

	EC-2022-044	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	08-marzo-2022	**Acceso no autorizado a NVIDIA y filtración de información**	V 1.1

III. INTRODUCCIÓN

En el 2021 NVIDIA con el objetivo de reducir el rendimiento de criptominería introdujo una tecnología en sus controladores llamada Lite Hash Rate, (LHR); de esta manera se pretende que estas unidades de procesamiento gráfico sean menos atractivas para los mineros.

En este sentido, Lapsus$ a través de sus redes de comunicación indican que robaron 1 TB de información; señalando que, luego de los requerimientos planteados a NVIDIA y considerando su negativa; el grupo de extorsión empezó a filtrar en línea dicha información como un chantaje a NVIDIA para que dicha corporación elimine el límite de criptominería de su firmware de GPU.

En la siguiente gráfica, se observa mensajes emitidos por Lapsus$.

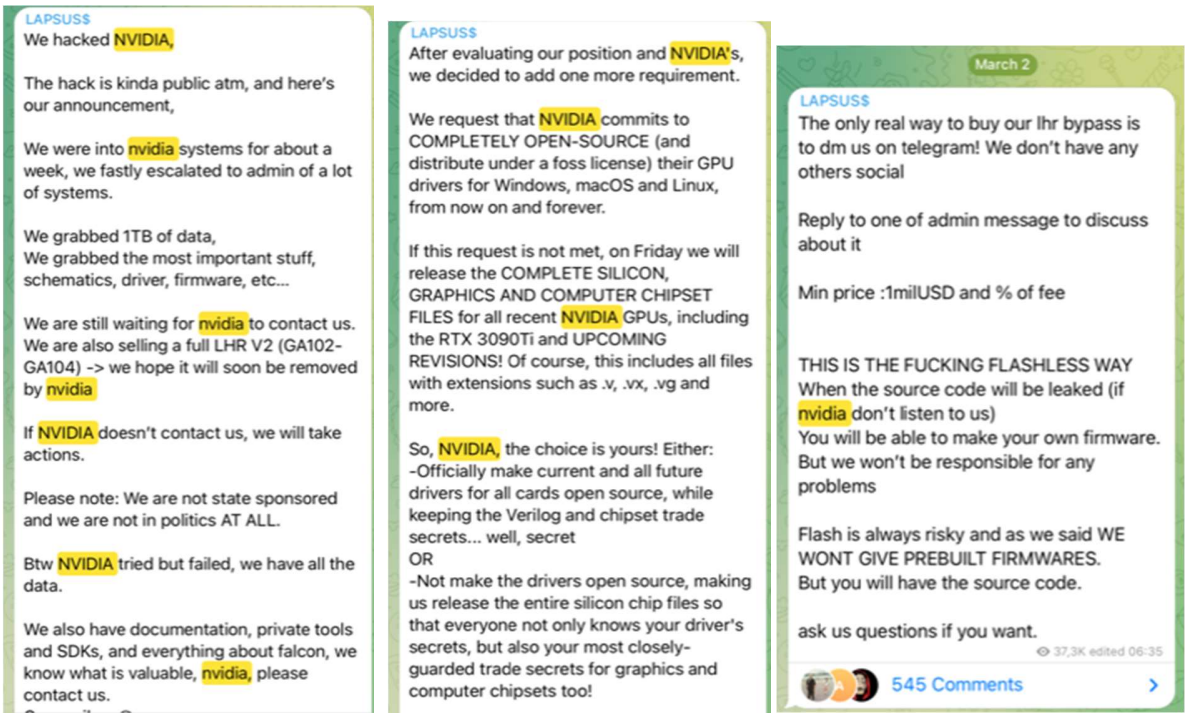

Figura 2. Ilustración asociada a mensajes de Lapsus$
Fuente: Telegram

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

	EC-2022-044	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	08-marzo-2022	**Acceso no autorizado a NVIDIA y filtración de información**	V 1.1

Entre la información sustraída se incluye:

- Más de 70 000 direcciones de correo electrónico de empleados y hashes de contraseñas NTLM[2], muchas de las cuales fueron posteriormente descifradas y distribuidas dentro de la comunidad de hackers
- Datos confidenciales, incluido el código fuente supuestamente asociado con su tecnología Deep Learning Super Sampling (DLSS).
- Dos certificados de firma de código[3]. Los mismos que han caducado (2014, 2018); sin embargo, Windows aún permite que se utilicen para la firma de controladores.

A través de estos ***certificados de firma de código***, los actores de amenaza firman los programas maliciosos haciéndose pasar por legítimos de NVIDIA. Entre los programas maliciosos se tiene balizas Cobalt Strike, Mimikatz, puertas traseras y troyanos de acceso remoto.

Por ejemplo, un actor de amenazas usó el certificado para firmar un troyano de acceso remoto Quasar[4].

En la siguiente gráfica se indica los resultados de análisis de un código malicioso.

[2] El protocolo NTLM estipula que el cliente se autentique con un nombre de usuario y la contraseña correspondiente.
[3] Permite a los desarrolladores firmar digitalmente ejecutables y controladores con el objetivo de que Windows y los usuarios finales puedan verificar el propietario del archivo y si un tercero lo ha manipulado.
[4] Su propósito principal es obtener información confidencial de la mayor cantidad de equipos en una red corporativa

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

	EC-2022-044	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	08-marzo-2022	**Acceso no autorizado a NVIDIA y filtración de información**	V 1.1

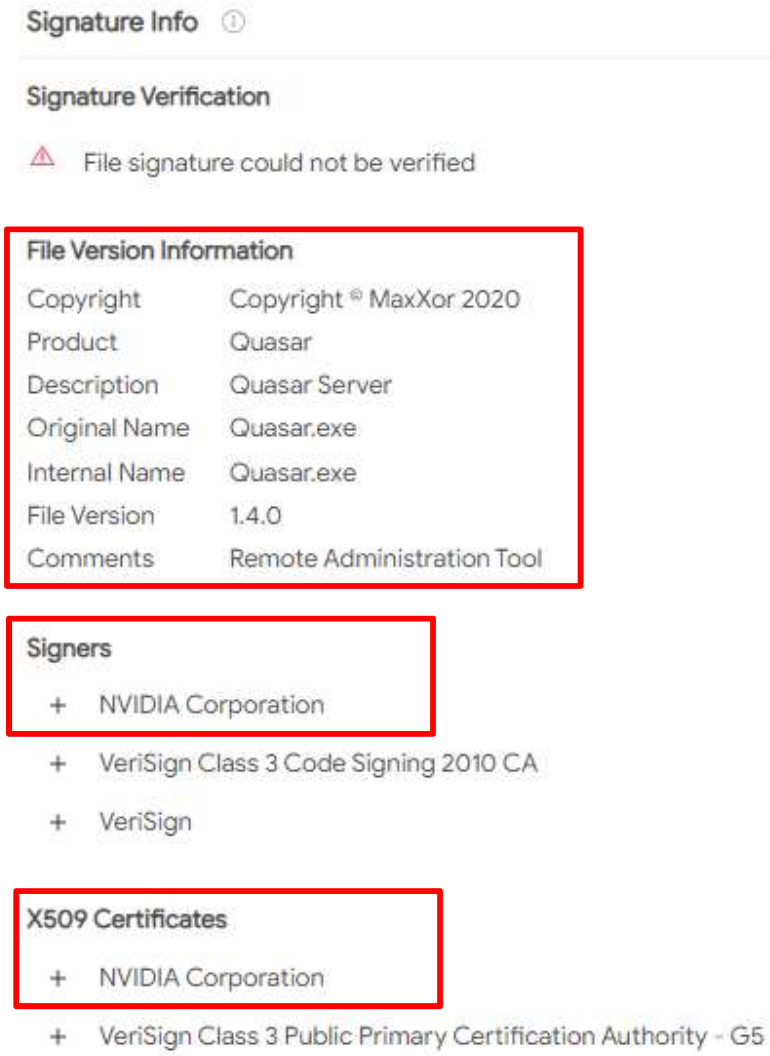

Figura 3. Ilustración asociada a Quasar
Fuente: Virus Total

	EC-2022-044	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	08-marzo-2022	**Acceso no autorizado a NVIDIA y filtración de información**	V 1.1

Finalmente, Lapsus$ afirma que NVIDIA contraatacó con un hackeo no solo al cifrar todos los datos robados, sino también al atacar a los piratas informáticos con ransomware; sin embargo, la información sustraída ha sido filtrada por lo que se considera que Lapsus$ dispone de copia de los archivos.

IV. VECTOR DE ATAQUE:

NVIDIA a través de un comunicado descartó de momento, que el incidente de ciberseguridad que afectó a la Infraestructura de TI tenga relación con el despliegue de un ransomware o que esté relacionado con el conflicto entre Rusia y Ucrania.

V. INDICADORES DE COMPROMISO

A continuación, se mencionan los indicadores de compromiso asociados a los ciberataques.

Ítem	Descripción	Detalle
1	Números de Serie de los certificados	43BB437D609866286DD839E1D00309F5 14781bc862e8dc503a559346f5dcc518

Tabla 1. IOC asociados a ataques entre Rusia y Ucrania
Fuente: Trend Micro

VI. RECOMENDACIONES:

El EcuCert recomienda a su comunidad objetivo:

- Configurar las políticas de control de aplicaciones de Windows Defender para controlar que controladores NVIDIA se pueden cargar.
- Revisar las políticas de seguridad y reglas de filtrado a fin de garantizar de que el código firmado recientemente por el certificado falso se detectado y bloqueado.
- Descargar programas, archivos y actualizaciones, solamente desde fuentes oficiales y verificadas.
- Tener actualizado y utilizar, un software anti-virus.
- Implementar un plan de respuesta a emergencias de la Organización/Institución.

	EC-2022-044	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	08-marzo-2022	**Acceso no autorizado a NVIDIA y filtración de información**	V 1.1

VII. REFERENCIAS:

Abrams, L. (05 de 03 de 2022). *Bleepingcomputer*. Obtenido de Bleepingcomputer: https://www.bleepingcomputer.com/news/security/malware-now-using-nvidias-stolen-code-signing-certificates/

Corfield, G. (05 de 03 de 2022). *The Register*. Obtenido de The Register: https://www.theregister.com/2022/03/05/nvidia_stolen_certificate/

Databreaches. (27 de 02 de 2022). *Databreaches*. Obtenido de Databreaches: https://www.databreaches.net/lapsus-and-the-terrible-horrible-no-good-very-bad-ransom-day1/

Lakshmanán, R. (03 de 03 de 2022). *Thehackernews*. Obtenido de Thehackernews: https://thehackernews.com/2022/03/hackers-who-broke-into-nvidias-network.html

Total, V. (s.f.). *Virus Total*. Obtenido de Virus Total: https://www.virustotal.com/gui/file/065077fa74c211adf9563f00e57b5daf9594e72cea15b1c470d41b756c3b87e1/details