PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno y Transformación Digital

Siempre con el pueblo

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Centro Nacional de Seguridad Digital

asbanc
ASOCIACIÓN DE BANCOS DEL PERÚ

Lima, 06 de mayo de 2022

N° 124-2022-CNSD

La presente **Alerta Integrada de Seguridad Digital** corresponde a un análisis técnico periódico realizado por el Comando Conjunto de las Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aérea del Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en el marco de la Seguridad Digital del Estado Peruano.

El objetivo de esta alerta **es informar a los responsables de la seguridad digital de las entidades públicas y las empresas privadas sobre las amenazas en el entorno digital** para advertir las situaciones que pudieran afectar la continuidad de sus servicios en favor de la población.

Las marcas y logotipos de empresas privadas y/o entidades públicas se reflejan para ilustrar la información que los ciudadanos reciben por redes sociales u otros medios y que atentan contra la confianza digital de las personas y de las mismas empresas **de acuerdo con lo establecido por el Decreto de Urgencia 007-2020**.

La presente Alerta Integrada de Seguridad Digital es información netamente especializada para informar a las áreas técnicas de entidades y empresas.

Contenido

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 124	Fecha: 06-05-2022
		Página 4 de 10

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Incidente de Malware en el fabricante estadounidense de maquinaria agrícola AGCO		
Tipo de ataque	Malware	Abreviatura	Malware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de subfamilia	C02
Clasificación temática familia	Código Malicioso		

Descripción

I. DATOS GENERALES:

AGCO, uno de los principales productores de maquinaria agrícola con sede en EE. UU., ha anunciado que se vio afectado por un ataque de ransomware que afectó a algunas de sus instalaciones de producción.

II. EVIDENCIA:

- AGCO anunció que el día 05/05/2022 sufrió un ataque de ransomware que afectó algunas de las instalaciones de producción de la empresa, el incidente fue anunciado por la empresa el día de hoy 06/05/2022.
- Si bien AGCO no proporciona ningún detalle sobre la causa de la interrupción, es probable que la empresa apague partes de sus sistemas de TI para evitar la propagación del ataque.
- En un comunicado de prensa, la empresa afectada se ha manifestado:

"AGCO aún está investigando el alcance del ataque, pero se prevé que sus operaciones comerciales se verán afectadas negativamente durante varios días y potencialmente más tiempo para reanudar por completo todos los servicios, dependiendo de la rapidez con la que la empresa pueda reparar sus sistemas. La empresa proporciona actualizaciones a medida que avanza la situación"

- Como explica el comunicado, la investigación aún está en curso y se espera que el impacto de este ciberataque dure un período considerable mientras restauran los sistemas.

III. TEMA:

- AGCO es un gigante en el sector, tiene ingresos de más de $9 mil millones, emplea a 21,000 personas y posee marcas como Fendt, Massey Ferguson, Challenger, Gleaner y Valtra.
- Como tal, cualquier interrupción de la producción causada por el ataque de ransomware podría tener un impacto significativo en la cadena de suministro en la producción y entrega de equipos.
- El FBI advirtió recientemente que los ataques de ransomware estaban dirigidos al sector agrícola en los Estados Unidos, destacando dos casos notables en 2022.
- La agencia había emitido un aviso similar en septiembre de 2021, seguido de ataques de ransomware de alto impacto contra dos grandes cooperativas de agricultores, NEW Cooperative y Crystal Valley.

IV. CONCLUSIÓN:

- Todas las entidades directamente vinculadas a la producción y el suministro nacional de alimentos se consideran infraestructura crítica y están destinadas a obtener ganancias masivas.
- En la situación actual, dadas las tensiones políticas, este ciberataque podría tener motivos de represalia, con el objetivo de interrumpir la producción de la firma.

V. RECOMENDACIÓN:

- Concientizar al equipo de trabajo en todos los niveles de la institución.
- Contar con soluciones de ciberseguridad vigentes y actualizadas.
- Contar con un plan de respuesta ante incidentes.

Fuentes de información	▪ hxxps://www.bleepingcomputer.com/news/security/us-agricultural-machinery-maker-agco-hit-by-ransomware-attack/

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 124**	**Fecha: 06-05-2022**
		Página 5 de 10

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad en Metasys de Johnson Controls		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. Resumen:

Johnson Controls, Inc., ha reportado una vulnerabilidad de severidad ALTA de tipo cambio de contraseña no verificado en los servidores Metasys ADS/ADX/OAS. La explotación exitosa de esta vulnerabilidad podría permitir que un usuario autenticado bloquee a otros usuarios fuera del sistema y se haga cargo de sus cuentas.

2. Detalles:

- La vulnerabilidad de cambio de contraseña no verificado se debe a que, al configurar una nueva contraseña para un usuario, el producto no requiere el conocimiento de la contraseña original ni el uso de otra forma de autenticación. Esto podría ser utilizado por un atacante para cambiar las contraseñas de otro usuario, obteniendo así los privilegios asociados con el usuario.
- La vulnerabilidad identificada como CVE-2022-21934 de cambio de contraseña no verificado, podría permitir que un usuario autenticado bloquee a otros usuarios fuera del sistema y hacerse cargo de las cuentas.

3. Productos afectados:

Johnson Controls informa que esta vulnerabilidad afecta a los siguientes servidores Metasys ADS/ADX/OAS:

- Servidores Metasys ADS/ADX/OAS: versión 10 y 11.

4. Solución:

Johnson Controls recomienda actualizar el producto afectado a la siguiente versión disponible:

- Actualice todas las Metasys ADS/ADX/OAS v10 con el parche 10.1.5;
- Actualice todas las Metasys ADS/ADX/OAS v11 con el parche 11.0.2.

Fuentes de información	▪ hxxps://www.incibe-cert.es/alerta-temprana/avisos-sci/vulnerabilidad-metasys-johnson-controls-inc-0 ▪ hxxps://www.cisa.gov/uscert/ics/advisories/icsa-22-125-01 ▪ hxxps://www.johnsoncontrols.com/-/media/jci/cyber-solutions/product-security-advisories/2022/jci-psa-2022-09.pdf

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 124**	**Fecha: 06-05-2022**
		Página 6 de 10

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades en QNAP QTS, QuTS hero y QuTScloud		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. Resumen:

Se ha reportado múltiples vulnerabilidades de severidad ALTA de tipo inyección de comando, seguimiento del enlace, Cross-site Scripting y redirección de URL a un sitio que no es de confianza que afecta a QNAP QTS, QuTS hero y QuTScloud. La explotación exitosa de estas vulnerabilidades podría permitir que un atacante remoto ejecute comandos arbitrarios en el sistema de destino, comprometa el sistema de destino, realice ataques de secuencias de comandos entre sitios (XSS) y redirija a sus víctimas a una URL maliciosa.

2. Detalles:

- La vulnerabilidad identificada como CVE-2021-44051 podría permitir que un atacante remoto ejecute comandos arbitrarios en el sistema de destino. La vulnerabilidad existe debido a una validación de entrada incorrecta. Un atacante remoto no autenticado puede pasar datos especialmente diseñados a la aplicación y ejecutar comandos arbitrarios en el sistema de destino. La explotación exitosa de esta vulnerabilidad puede resultar en un compromiso completo del sistema vulnerable.
- La vulnerabilidad identificada como CVE-2021-44052 podría permitir que un atacante remoto comprometa el sistema de destino. La vulnerabilidad existe debido a un problema de seguimiento de enlaces. Un atacante remoto puede atravesar el sistema de archivos a ubicaciones no deseadas y leer o sobrescribir archivos.
- La vulnerabilidad identificada como CVE-2021-44053 podría permitir a un atacante remoto realizar ataques de secuencias de comandos entre sitios (XSS). La vulnerabilidad existe debido a una desinfección insuficiente de los datos proporcionados por el usuario. Un atacante remoto puede engañar a la víctima para que siga un enlace especialmente diseñado y ejecute código HTML y script arbitrario en el navegador del usuario en el contexto de un sitio web vulnerable. La explotación exitosa de esta vulnerabilidad puede permitir que un atacante remoto robe información potencialmente confidencial, cambie la apariencia de la página web, realice ataques de phishing y de descarga oculta.
- La vulnerabilidad identificada como CVE-202144054 podría permitir que un atacante remoto redirija a las víctimas a una URL arbitraria. La vulnerabilidad existe debido a la sanitización inadecuada de los datos proporcionados por el usuario. Un atacante remoto puede crear un enlace que lleve a un sitio web de confianza; sin embargo, cuando se hace clic, redirige a la víctima a un dominio arbitrario. La explotación exitosa de esta vulnerabilidad puede permitir que un atacante remoto realice un ataque de phishing y robe información potencialmente confidencial.

3. Productos afectados:

- QNAP QTS: antes del 5.0.0.1986 20220324, 4.5.4.1991 20220329, 4.3.6.1965 20220302, 4.3.4.1976 20220303, 4.3.3.1945 20220303, 4.2.6 20220304;
- QuTS hero: antes de h5.0.0.1986 Compilación 20220324, h4.5.4.1971 Compilación 20220310;
- QuTScloud: antes de c5.0.1.1998.

4. Solución:

Se recomienda actualizar los productos afectados a la última versión disponible que corrige estas vulnerabilidades.

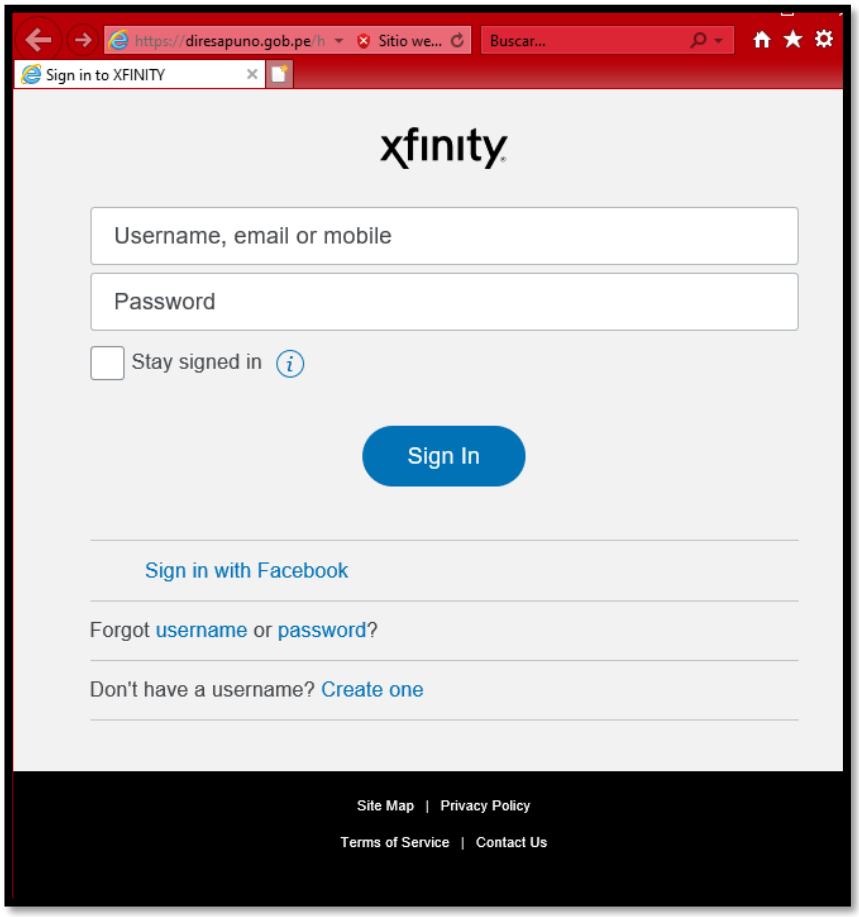
Fuentes de información	▪ hxxps://www.qnap.com/en/security-advisory/qsa-22-16 ▪ hxxps://www.cybersecurity-help.cz/vdb/SB2022050605

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 124	Fecha: 06-05-2022
		Página 7 de 10

Componente que reporta	COMANDANCIA DE CIBERDEFENSA DE LA MARINA DE GUERRA DEL PERÚ		
Nombre de la alerta	Ataque cibernético a sitios web con dominio “.gob.pe”		
Tipo de ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Correo Electrónico		
Código de familia	G	Código de subfamilia	G03
Clasificación temática familia	Fraude		

Descripción

1. El día 06 de mayo de 2022, a través del monitoreo y búsqueda de amenazas en el ciberespacio se identificó una página web con dominio "gob.pe" (xxxxs://diresapuno.gob.pe/hohh/), estaría siendo usada para realizar ataques tipo phishing.



2. Recomendaciones:
   a. Evitar ingresar a enlaces de dudosa procedencia.
   b. Mantener los equipos protegidos, con el software actualizado.

Fuentes de información	▪ Comandancia de Ciberdefensa de la Marina, Osint

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 124	Fecha: 06-05-2022
		Página 8 de 10

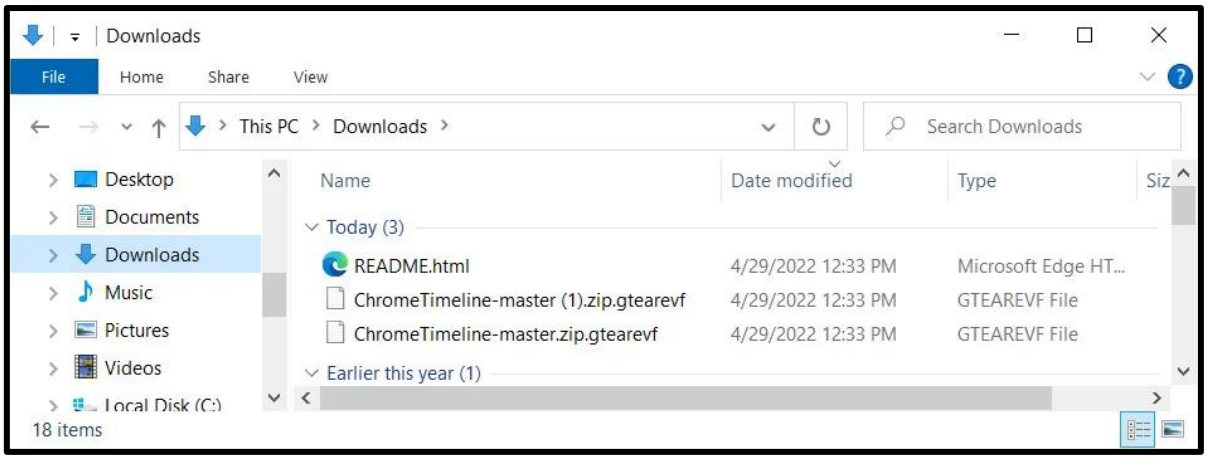
Componente que reporta	COMANDANCIA DE CIBERDEFENSA DE LA MARINA DE GUERRA DEL PERÚ		
Nombre de la alerta	Nuevo ransomware Magniber		
Tipo de ataque	Ransomware	Abreviatura	Ransomware
Medios de propagación	Correo electrónico, redes sociales, entre otros		
Código de familia	C	Código de subfamilia	C09
Clasificación temática familia	Código malicioso		

Descripción

1. El 6 de mayo del 2022, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que un grupo de ciberdelincuentes están expandiendo una variedad de ransomware a través de falsas actualizaciones del sistema operativo Windows 10. Se trata del ransomware Magniber que logra introducirse en los equipos mediante enlaces de descarga de Windows disponibles en páginas web ilegales.

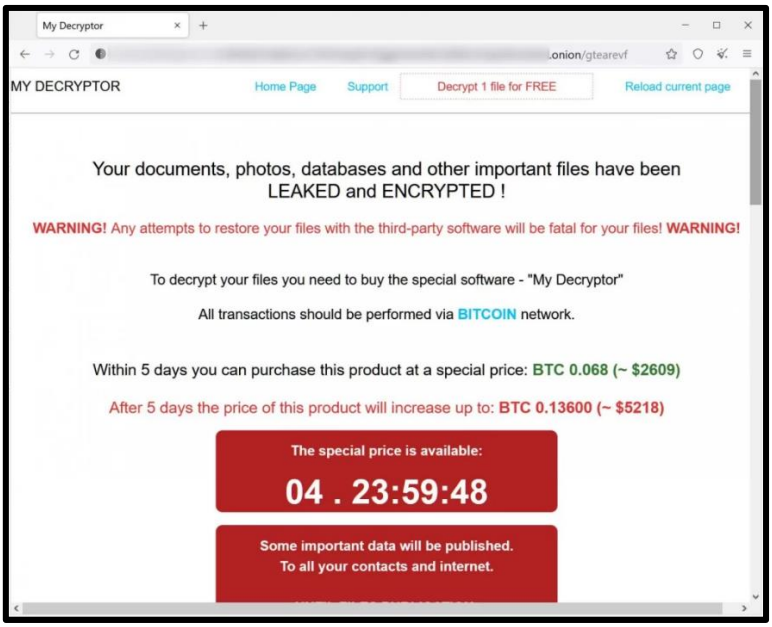
Sistema Operativo de Windows 10

2. Al momento de instalar el ransomware Magniber en el ordenador, éste eliminará las copias de volumen y luego cifrará los archivos. Al realizar esta acción, el ransomware agregará una extensión aleatoria de 8 caracteres como:
   - 'Win10.0_System_Upgrade_Software.msi'
   - 'Security_Upgrade_Software_Win10.0.msi'.
   - 'System.Upgrade.Win10.0-KB47287134.msi'
   - 'System.Upgrade.Win10.0-KB82260712.msi'
   - 'System.Upgrade.Win10.0-KB18062410.msi'
   - 'System.Upgrade.Win10.0-KB66846525.msi'.



Archivos en el paquete del Ransomware Magniber

3. Asimismo, tiene una nota de rescate con el nombre Readme.html en cada carpeta con instrucciones precisas de cómo realizar el pago a través de Magniber Tor. El pago de Magniber se titula "**My Decryptor"** y permitirá a la víctima descifrar un archivo de forma gratuita, ponerse en contacto con el soporte o determinar el monto del rescate y la dirección de bitcoin que los afectados deben realizar.



La forma de pago mediante "My Decrytor"

4. Adicionalmente, se tiene más detalles de este ransomware:

MD5 Hash	59EF984C16A5C1723D9958FBEB1B7450
SHA-1 Hash	A7BCD0188E3FD0F16226AB44477A04662A5C5450
SHA-256 Hash	2E6F9A48D854ADD9F895A3737FA5FCC9D38D082466765E550CCA2DC47A10618E
Posibles sistemas a afectar	Microsoft Windows 7 Enterprise Edition Service Pack 1 (build 7601, version 6.1.7601), 64-bit Internet Explorer version: 8.0.7601.17514 Microsoft Office version: 2003 PDF Reader version: 9.0 Flash player version: 11.2.202.228 No Flash player plugin installed Platform Version 4.4.0.9 Detection Package Version 4.4.0.180402

5. Por último, el ransomware se considera seguro el cual no contiene ninguna debilidad que pueda explotarse para recuperar archivos de forma gratuita, sin embargo; esta campaña se dirige principalmente a estudiantes y consumidores en lugar de víctimas empresariales, lo que hace que la demanda de rescate sea demasiado costosa para muchos usuarios.

6. Recomendaciones:

- Mantener los equipos con los últimos parches de seguridad para asegurar que las vulnerabilidades conocidas no puedan ser explotadas.
- Bloquear los indicadores de compromiso (IOC) mostrados, en los dispositivos de seguridad de su infraestructura.
- No abrir correos electrónicos de dudosa procedencia (remitente desconocido), ni dar clic en enlaces, ni descargar archivos adjuntos desconocidos.
- Utilizar solo fuentes de descarga conocidas.
- Asegurar de hacer copias de los archivos importantes periódicamente.
- Mantener el sistema operativo actualizado.

Fuentes de información	▪ Comandancia de Ciberdefensa de la Marina, Osint

Índice alfabético