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

Lima, 25 de julio de 2022

N° 200-2022-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° 200	Fecha: 25-07-2022
		Página 04 de 14

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Amenaza de código malicioso de tipo Ransomware RaaS: LokiLocker		
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

Según un informe de BlackBerry Threat Intelligence, el grupo emergente de ciberdelincuencia está ejecutando el modelo probado y verdadero de ransomware-as-a-service (RaaS).

- **Actor de amenazas:** Ransomware RaaS: LokiLocker
- **Tipo de amenaza:** Código malicioso, malware, ransomware.

ANTECEDENTES:

- LokiLocker es un ransomware como servicio (RaaS) que surgió por primera vez en agosto de 2021.
- Se distribuyó inicialmente en herramientas especializadas de piratería de fuerza bruta que atacaban las cuentas de los consumidores en servicios como Spotify y PayPal.
- El grupo se expandió y ahora incluye aproximadamente 30 afiliados que ahora apuntan a los sistemas Windows de habla inglesa dentro de las empresas, el cual encripta archivos y deja inutilizable su máquina si no se paga el rescate.
- Blackberry mencionó: "Algunas de las herramientas de craqueo utilizadas para distribuir las primeras muestras de LokiLocker parecen haber sido desarrolladas por un equipo de craqueo iraní llamado AccountCrack. Además, al menos tres de los afiliados conocidos de LokiLocker usan nombres de usuario únicos que se pueden encontrar en los canales de piratería iraníes".

DETALLES:

- Ransomware as a Service (RaaS) es un término en inglés que hace referencia a un modelo de negocio en el cual los desarrolladores de un malware tipo ransomware es ofertado a otros a actores de amenaza interesados.
- Es conocido que los actores de amenaza pueden contratar la creación de malware como un servicio o la posibilidad de sumarse a través de un programa de afiliados.
- El modelo de Ransomware as a Service (RaaS) funciona de la siguiente manera:
  1. Los ciberdelincuentes escriben el código del ransomware.
  2. Los afiliados compran o alquilan el código para ejecutar los ataques. Existen suscripciones mensuales o de tarifas únicas, y los paquetes cuentan con guías detalladas que explican cómo deben ejecutarse los programas.
  3. Una vez adquirido el paquete de ransomware, se busca que la víctima descargue el programa. Ante esto, los ciberdelincuentes apelan a la credibilidad y utilizan técnicas como el phishing o el smishing para cometer su delito.
  4. Luego el ciberdelincuente cifra los archivos de la víctima en unidades locales y recursos compartidos de red con una combinación estándar de AES para el cifrado de archivos y RSA para la protección de claves.
  5. Por último, se le pide a la víctima que envíe un correo electrónico a los atacantes para obtener instrucciones sobre cómo pagar el rescate y liberar los datos.

Nota: LokiLocker cuenta con una función de limpieza opcional: si la víctima no paga en el plazo especificado por el atacante, todos los archivos que no sean del sistema se eliminarán y el MBR se sobrescribirá, borrando todos los archivos de la víctima y dejando el sistema inutilizable.

Fondo de escritorio de LokiLocker

A continuación, se brinda los Indicadores de compromiso (IoC):

0684437b17ae4c28129fbb2cfe75b83cc8424ba119b9ca716ad001a284d62ead	SHA256
15d7342be36d20ce615647fac9c2277f46b6d19aa54f3cf3d99e49d6ce0486d0	SHA256
1a4a3bfb72f3a80e4b499ecebe99f53a2b7785eace7f612b3e219409d1e1ffc7	SHA256
2a7f01d924a4fc38c9fad586634eccbc28de07d97531c4a02eb6085359093a45	SHA256
37702b94f9fc14a406312a2a392ad9553cf05c4b6870d94b5cf4781c02c29414	SHA256
4215b5ce91deb97011cba2dd94d5bac1a745d6d55f6938b86e209eaaf8e655df	SHA256
52c045b57e24585467be13454c5db551987fd23bfa931a7f6ab41e6f11b8a7ec	SHA256
55da12a82c8e0b9fda5dbba6612627c0ee5d13d55e3bcc1df2ca9785c97caf64	SHA256
5ccee068daf8a672d0e63e334e00985aa7fe56aa26b6c036d562728fdf968237	SHA256
6205056cd92c75579f56bd0ce7159fae9f360d4c183beb10743330952bf22056	SHA256
630e24cc1c4c95321965ad967e77e1888c48c4b1f653d800c7df08e879814787	SHA256
75a5d27c77cf8515cff84d789f0e8f849b37e15b9b5f1c0801bab414061048a6	SHA256
78a530f35d1cc89fc757b7661cbd57b2e9e46aeed53e2e66247db66c214a2ba0	SHA256
7f23ea1e5ab087ba2c4e0ea251d680ef5190d49181efcc222702075b276d5990	SHA256
8630df622ee773c3d9c934fe9d925c019b43232e8f2810ee651dcf5f3ec79893	SHA256
88acae18f2cf7de7bb76784d45d9612561c8890872ea3629f0608577928745a5	SHA256
8de5b9332556da8f401c5cbf3cea1dbc1e1ba277c0efa85dce8cd36310c2936c	SHA256
8f78555f0f62b4f280a77109dbaa4aeb5c347d1ea38b521f98c57a7acea8087e	SHA256
8f8cf6b8cd0c789d3f67f6291bb7c0c5416e27320631c852152a63513185941e	SHA256
a1e30ea263ba21d656717f7f7824ecb2dc90896f55eae134afaf7691209979fd	SHA256
ac1b326f23e17726a2b90ce8a9d29c6e44a2cb37b431e2b94734bdd17618ae26	SHA256
adacbc5402326f87c76cc7737ad924ce5bd7394400ef86a48fa754af9d22da66	SHA256
b01a96892f3efdaa6682078339b23d8954d571c27ee15a4ce9ef8ad6c415f06d	SHA256
b8996e435ba229837d13f9837f6c0451f50a5767b0d1f1bb715670c802a1d564	SHA256
c3fe7ee5451108c16d7730d0bf589f70b841f3846908c1761d827a70f3462ef0	SHA256
c80513aaff11a2a2914d3a674737f63fbc04c6d5de7fda6f8b6e07df580664cf	SHA256
c8e8599e8d86ff7daf02ea9c01d31f4cdcf829314c76b84d1b1b8a982d1299c5	SHA256
cb17673f3cde6e542db3ff5facee2a01fdec462be275e9274c512038470009d1	SHA256
da0a82d322502cd6d156649dee1e0a45348df0dce272b6ae2dd81af25f774c62	SHA256
df24b04f6ff0ac50fbf1c01ee02f809c1c3f9fbe9d14eefc3306b1b586bf943e	SHA256

e28b0a93649010788bbeda883a08254fefe3710700fc2c5a8dea94ec39402ec3	SHA256
f2da3d1410c5058720a4307acf5fec7fc2b54285be9dd89eae108cce368dcde7	SHA256
fe930861d5eec95a3ea1239e7a8f4182a2cf5b094ac3a48c4cb2f0ef39facd05	SHA256
fffcf4be17e732aa3a5387e747290236d0f75ff3a24cb43eca793668d7772ddd	SHA256
4e6471c4574152d0eb2d2c608e540e505f3db41b50997d1f06c47e587a355d80	SHA256
7c890018d49fe085cd8b78efd1f921cc01936c190284a50e3c2a0b36917c9e10	SHA256
9ab1694c978f11521c6bca73d40256e4b433f3279792db8ae1fecc5e0ad174c9	SHA256
ebc955f12b0a2b588efca6de0af144dd00e33ead80185a887bf7c97329b28ec6	SHA256
1e6ecdb54224eea50476be03d5a48083deae15301f26ba3519e0c0a5eb77b1f4	SHA256
268c2924d45c0c7be9b67b85f03ddf5df97f2bc8963faefe1bec244e0cb95225	SHA256
36b5fe49cd81393f8c60c70c941a1e6aaf181775b0614f1c4a142f38c7af1a81	SHA256
42088f0e3e9c70b7d1d238f7e3b03a3ca177748ba2568adba9104bbed2827734	SHA256
6d1ecc48069eae14a831af05d29d2d25c0fa9f7c62f1f51c44d0d70fb014a590	SHA256
84d9ef8cb92d57b178cce655f3f7808c6f5cf42f15c468f741b253f37ffc39fc	SHA256
bb382bbc0756832748b33f0d7f7ec218d570afa031937259e69237df4945d074	SHA256
ca478cb334360bef31d394438cba1449dfe0b8d751cc8eb679f09e12e5068d1a	SHA256
e9e80fd3fe71d133609f5bc75081b13123e4f9a5ed1920050727955185f3ce52	SHA256
fe40e5c6244c7e0a256689b6ea0881998fef897cece79a2add3ba8f7a23f4f2b	SHA256
8cb1e9c99ad716a2541697a6d4ada32433b56e11dfe6aa1cb7c4fbc72b4bad2e	SHA256
c1e8c720da2297aa4432364441b341ec85e6f7f571cf6348ffdc51f4ae96418a	SHA256
loki-locker[.]one	Dominio C2
194.226.139[.]3	C2 IP
91.223.82[.]6	C2 IP
Software\Loki\public	Valor de registro
Software\Loki\full	Valor de registro
Software\Loki\timer	Valor de registro
Software\Microsoft\CurrentVersion\Run\Michael Gillespie	Valor de registro
%ProgramData%\winlogon.exe	Ejecutable
%ProgramData%\config.Loki	Archivo de configuración
<malware_path>\loki.txt	Archivo de configuración
<malware_path>\logs.txt	Archivo de registro
Restore-My-Files.txt	Archivo Léame
Info.Loki	Archivo HTA
Cpriv.Loki	Archivo de datos
Loki/1.0	Agente de usuario
.Loki	Extensión de archivo
.Adair	Extensión de archivo
.Boresh	Extensión de archivo
.Rainman	Extensión de archivo
.Spyro	Extensión de archivo

Nombres de afiliados conocidos

AbolSpyro	Miracle	hijack
AdairFile	Miveh_sabzikosher	jhnvjfygbjdhf
Ahmad_C4	Roxlock	mjid4MB
Darwin	Shadow	mr_noobx
Fardinyps	ShreAzm0	numbervpss
Fuck3r_life	Sirer	optimus982
Helpmezeus	darkages	pf9922
John	darkkiller	qazw
Kingbo	arkwave	sidewinder
LokiBlack	ghost	
Mindnear	h33shmat	

Direcciones de correo electrónico conocidas

BlackSpyro[at]mailfence[.]com	filemanager[at]cock[.]li
BlackSpyro[at]tutanota[.]com	jesushelp01[at]techmail[.]info
DecNow[at]MsgSafe[.]io	jesushelp02[at]mailfence[.]com
DecNow[at]TutaMail[.]Com	kingbo[at]tutanota[.]com
Decoder[at]firemail[.]cc	kingboo[at]mailfence[.]com
Decryptfiles[at]goat[.]si	kingvps1[at]mailfence[.]com
Filemanager[at]mailfence[.]com	kingvps[at]mailfence[.]com
Helpingdecode[at]tutanota[.]com	lockirswsuppurt[at]mailfence[.]com
Miiracle11[at]yandex[.]com	lockteam[at]cock[.]li
Miracle11[at]keemail[.]me	lockteam[at]keemail[.]me
PayForDecrypting[at]gmail[.]com	loki.black[at]mailfence[.]com
PayForDecrypting[at]outlook[.]com	loki.black[at]msgsafe[.]io
Rdpmanager[at]airmail[.]cc	loki.help[at]bingzone[.]net
RoxLock[at]keemail[.]me	loki.help[at]mailfence[.]com
RoxLock[at]mailfence[.]com	loki.support01[at]techmail[.]info
Shadow0[at]mailfence[.]com	loki.support02[at]mailfence[.]com
Shadow11[at]mailfence[.]com	loki01[at]keemail[.]me
Skydancerf5[at]cock[.]li	loki02[at]mailfence[.]com
Sapphire01[at]keemail[.]me	lordpdx[at]tutanota[.]com
Sapphire02[at]mailfence[.]com	mrcrypt2[at]mailfence[.]com
Unlockpls.dr01[at]protonmail[.]com	mrcrypt[at]msgsafe[.]io
Unlockpls.dr01[at]yahoo[.]com	mrrobot13[at]cock[.]li
adairfile[at]mailfence[.]com	pf2536[at]protonmail[.]com
adairfile[at]tutanota[.]com	pf2536[at]tutanota[.]com
admindec[at]rape[.]lol	puffcrypt[at]gmail[.]com
anoniran[at]protonmail[.]com	rain.man13[at]mailfence[.]com
badlamadec[at]msgsafe[.]io	rain_man13[at]keemail[.]me
d4rkw4ve[at]tutanota[.]com	skydancerf5[at]tutanota[.]com
dark4wave[at]yandex[.]com	tran9ino00[at]protonmail[.]com
dark.killer[at]mailfence[.]com	wannayourdata[at]gmail[.]com
darkkiller[at]cock[.]li	xmaster22[at]tutanota[.]com
decryptyourfiles[at]firemail[.]cc	xmagic22[at]tutanota[.]com
decsup[at]tuta[.]io	xmaster22[at]tutanota[.]com
falcon9[at]cyberfear[.]com	

CONCLUSIÓN:

- Los ciberdelincuentes se vienen aprovechando de las campañas de extorsión. El modelo de negocio del ransomware se ha ido incrementando al pasar de los años, pero se ha hecho presente mucho más durante los dos últimos años.

RECOMENDACIONES:

- Implementar los indicadores de compromisos (IoC) en sus plataformas de seguridad digital.
- Mantener copias de seguridad (backup) al día y realizar pruebas de recuperación de las mismas.
- Concientizar al equipo de trabajo en todos los niveles de la institución.
- Contar con directrices vigentes de autenticación multifactor en los sistemas de información.
- Contar con soluciones de ciberseguridad vigentes y actualizadas.
- Contar con un plan de respuesta ante incidentes.

Fuentes de información	▪ hxxps://blogs.blackberry.com/en/2022/03/lokilocker-ransomware ▪ hxxps://www.techtarget.com/searchsecurity/news/252514720/LokiLocker-ransomware-crew-bursts-onto-the-scene ▪ hxxps://encyclopedia.kaspersky.com/glossary/ransomware-as-a-service-raas/ ▪ Análisis propio de fuentes abiertas.

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 200	Fecha: 25-07-2022
		Página 08 de 14

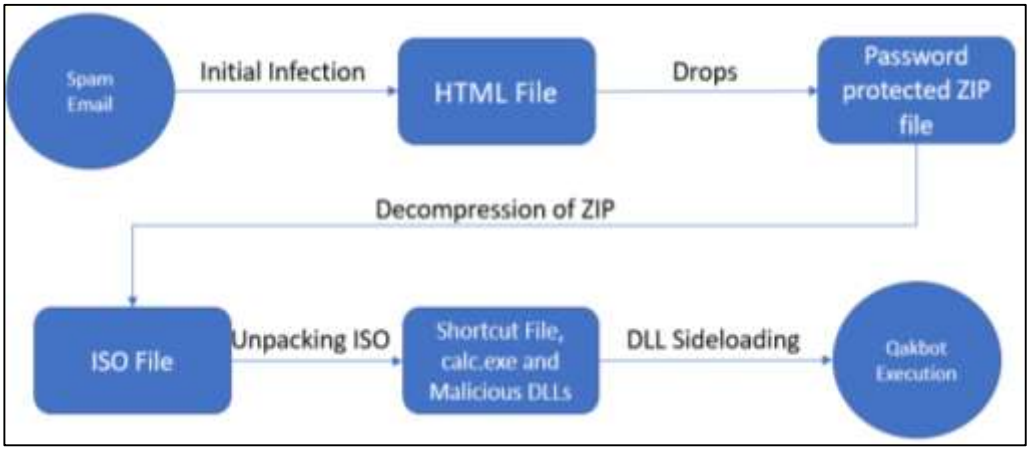
Componente que reporta	**CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	Nueva campaña de spam masivo de correo electrónico distribuye malware “QBot”		
Tipo de ataque	Malware	Abreviatura	Malware
Medios de propagación	Correo electrónico, redes sociales, entre otros		
Código de familia	C	Código de Subfamilia	C01
Clasificación temática familia	Código Malicioso		

Descripción

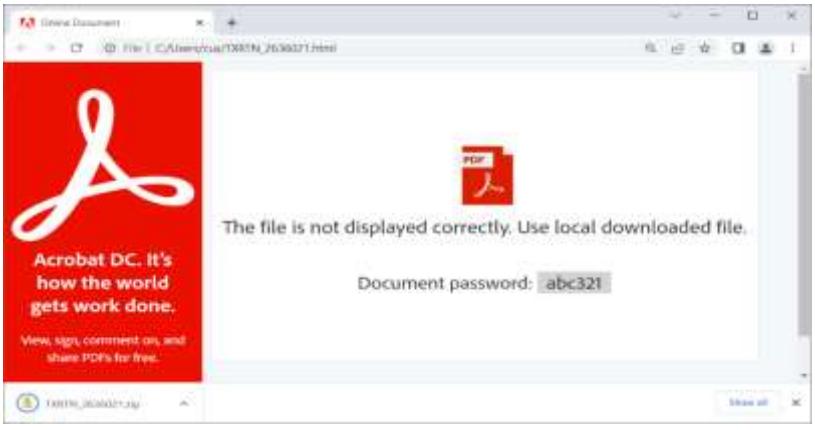
A través del monitoreo y búsqueda de amenazas en el ciberespacio del día 24 de Julio del 2022, se tomó conocimiento la nueva campaña de phishing que distribuye malware “QBot” y usa la calculadora de Windows para descargar la carga útil maliciosa en las computadoras infectadas.

ANTECEDENTES:

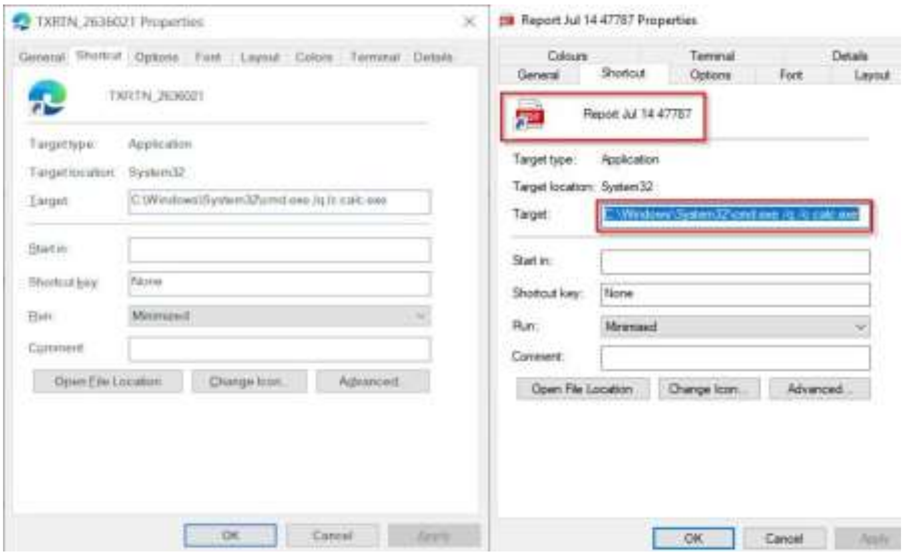
- QBot, también conocido como Qakbot, es una variedad de malware de Windows que comenzó como un troyano bancario, pero evolucionó hasta convertirse en un potente malware, y las pandillas de ransomware lo utilizan en las primeras etapas del ataque.
- Para la infección inicial, Qakbot utiliza una campaña de spam masivo de correo electrónico.
- En esta campaña, el correo electrónico no deseado contiene un archivo “.zip” protegido con contraseña que contiene un archivo “ISO”. Cuando está montado, este archivo ISO muestra un archivo “.lnk” disfrazado de archivo “PDF”. Si la víctima abre el archivo “.lnk”, el sistema está infectado con el malware Qakbot.



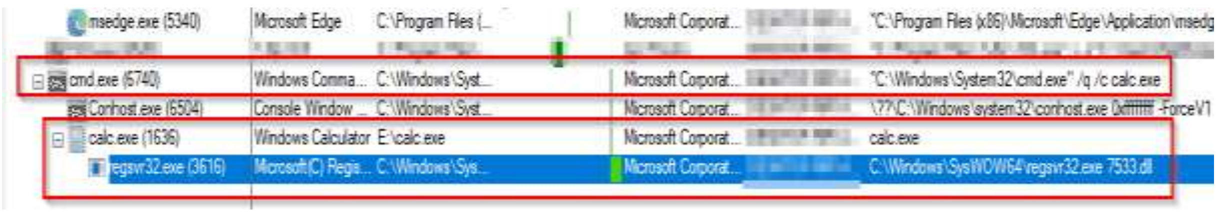
- Los correos electrónicos utilizados en la última campaña llevan un archivo HTML adjunto que descarga un archivo ZIP protegido por contraseña con un archivo “ISO” dentro.
- La contraseña para abrir el archivo ZIP se muestra en el archivo HTML y el motivo para bloquear el archivo es evitar la detección antivirus.
- La “ISO” contiene un archivo “.LNK”, una copia de “calc.exe” (calculadora de Windows) y dos archivos “DLL”, “WindowsCodecs.dll” y una carga llamada “7533.dll”.



- Cuando el usuario monta el archivo "ISO", solo muestra el archivo ".LNK", que está disfrazado para parecer un PDF que contiene información importante o un archivo que se abre con el navegador Microsoft Edge.
- Sin embargo, el acceso directo apunta a la aplicación Calculadora en Windows, como se ve en el cuadro de diálogo de propiedades de los archivos.



- Hacer clic en el acceso directo desencadena la infección al ejecutar "Calc.exe" a través del símbolo del sistema.
- Los actores de amenazas se aprovechan de esta falla al crear su propio archivo "WindowsCodecs.dll" malicioso que inicia el otro archivo "[numerado].dll", que es el malware "QBot".
- Al instalar "QBot" a través de un programa confiable como la Calculadora de Windows, es posible que algunos programas de seguridad no detecten el malware cuando se carga, lo que permite que los actores de amenazas eludan la detección.
- Árbol del proceso de ejecución de Qakbot.



RECOMENDACIONES:

- No abrir correos electrónicos de remitentes desconocidos o irrelevantes.
- Evite abrir enlaces y archivos adjuntos de correo electrónico que no sean de confianza sin verificar primero su autenticidad.
- Utilizar soluciones antivirus de renombre en sus dispositivos conectados, incluidos PC, portátiles y dispositivos móviles.
- Tener actualizado el Sistema Operativo.

Fuentes de información	▪ https://www.bleepingcomputer.com/news/security/qbot-phishing-uses-windows-calculator-sideloading-to-infect-devices/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 200	Fecha: 25-07-2022
		Página 10 de 14

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad crítica de Inyección SQL en productos SonicWall		
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:

Los investigadores, H4lo y Catalpa de Hatlab DBappSecurity, han reportado una vulnerabilidad de severidad CRÍTICA de tipo inyección SQL (SQLi) que afecta a afecta a Analytics On-Prem y Global Management System (GMS). La explotación exitosa de esta vulnerabilidad podría permitir a un atacante no autenticado visualizar, agregar, modificar o eliminar información en la base de datos de back-end.

2. Detalles:

- La vulnerabilidad de severidad **crítica** identificada como CVE-2022-22280 de la neutralización inadecuada de elementos especiales utilizados en un comando SQL en SonicWall GMS y Analytics, podría ocasionar una vulnerabilidad de inyección SQL por parte de un atacante no autenticado. Un atacante remoto podría enviar declaraciones SQL especialmente diseñadas, lo que podría permitirle ver, agregar, modificar o eliminar información en la base de datos de back-end.
- Esta vulnerabilidad se puede usar para alterar la lógica de consulta para eludir los controles de seguridad, o para insertar declaraciones adicionales que modifican la base de datos de back-end, posiblemente incluyendo la ejecución de comandos del sistema. La probabilidad de explotación podría reducirse mediante la incorporación de un firewall de aplicaciones web (WAF) para bloquear los intentos de SQLi.
- La vulnerabilidad de tipo inyección SQL, se debe a que el software construye todo o parte de un comando SQL utilizando la entrada influenciada externamente desde un componente ascendente, pero no neutraliza o neutraliza incorrectamente elementos especiales que podrían modificar el comando SQL previsto cuando se envía a un componente descendente.

3. Productos afectados:

- GMS, versiones 9.3.1-SP2-Hotfix1 y anteriores;
- Analytics, versiones 2.5.0.3-2520 y anteriores.

4. Solución:

SonicWall recomienda actualizar los productos afectados a la siguiente versión parcheada de software disponibles de inmediato:

- GMS, versión 9.3.1-SP2-Hotfix-2;
- Analytics, versión 2.5.0.3-2520-Hotfix1.

Fuentes de información	▪ hxxps://www.incibe-cert.es/alerta-temprana/avisos-seguridad/inyeccion-sql-productos-sonicwall ▪ hxxps://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0007 ▪ hxxps://www.sonicwall.com/support/notices/security-notice-sonicwall-gms-sql-injection-vulnerability/220613083124303/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 200	Fecha: 25-07-2022
		Página 11 de 14

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Red Hat lanza actualizaciones de seguridad en varios de sus productos		
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:

Red Hat ha reportado múltiples vulnerabilidades de severidad ALTA de tipo validación de entrada incorrecta en varios de sus productos. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante no autenticado obtener acceso a información confidencial, manipular datos y comprometer el sistema afectado.

2. Detalles:

- La vulnerabilidad de severidad **media** identificada como CVE-2022-21540 de validación de entrada incorrecta podría permitir a un atacante remoto no autenticado obtener acceso a información confidencial. La vulnerabilidad existe debido a una validación de entrada incorrecta dentro del componente Hotspot en Oracle GraalVM Enterprise Edition. Un atacante remoto no autenticado puede aprovechar esta vulnerabilidad para obtener acceso a información confidencial.
- La vulnerabilidad de severidad **media** identificada como CVE-2022-21541 de validación de entrada incorrecta podría permitir a un atacante remoto no autenticado manipular datos. La vulnerabilidad existe debido a una validación de entrada incorrecta dentro del componente Hotspot en Oracle GraalVM Enterprise Edition. Un atacante remoto no autenticado puede aprovechar esta vulnerabilidad para manipular datos.
- La vulnerabilidad de severidad **alta** identificada como CVE-2022-34169 de validación de entrada incorrecta podría permitir a un atacante remoto no autenticado comprometer el sistema afectado. La vulnerabilidad existe debido a un problema de truncamiento de enteros al procesar hojas de estilo XSLT maliciosas. Un atacante remoto no autenticado puede pasar datos especialmente diseñados a la aplicación para corromper los archivos de clase de Java generados por el compilador XSLTC interno y ejecutar bytecode de Java arbitrario.

3. Productos afectados:

- Red Hat Enterprise Linux Server para Power LE: servicios de actualización para soluciones SAP 8.1 ppc64le;
- Red Hat Enterprise Linux para x86_64 - Servicios de actualización para soluciones SAP 8.1 x86_64;
- Java-1.8.0-openjdk (paquete de Red Hat): anteriores a la versión 1.8.0.342 b07-1.el8_1;
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions: 9.0;
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support: 9.0;
- Red Hat Enterprise Linux for ARM 64: 9;
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support: 9.0;
- Red Hat Enterprise Linux for Power, little endian: 9;
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support: 9.0;
- Red Hat Enterprise Linux for IBM z Systems: 9;
- Red Hat Enterprise Linux for x86_64 - Extended Update Support: 9.0;
- java-11-openjdk (Red Hat package): 11.0.15.0.10-1.el9_0;
- Red Hat Enterprise Linux for x86_64: 9.

4. Solución:

Red Hat recomienda actualizar los productos afectados con la última versión de software disponible que corrige estas vulnerabilidades.

Fuentes de información	▪ hxxps://access.redhat.com/errata/RHSA-2022:5701 ▪ hxxp://access.redhat.com/errata/RHSA-2022:5695 ▪ http://access.redhat.com/errata/RHSA-2022:5687

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 200	Fecha: 25-07-2022
		Página 12 de 14

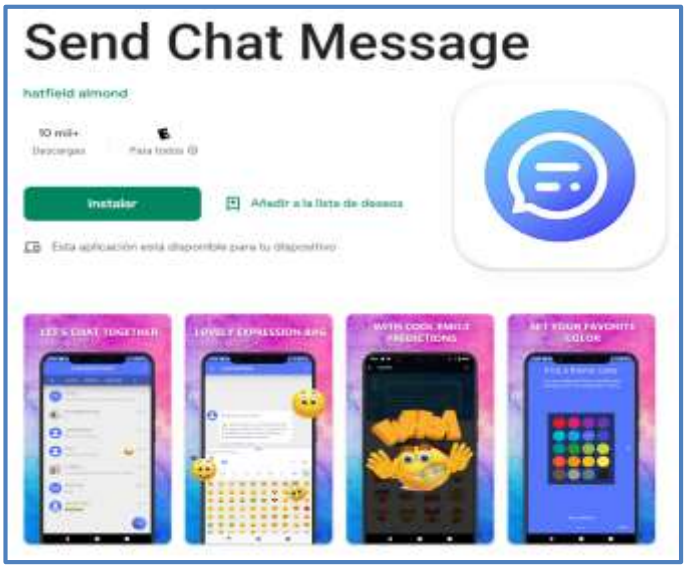
Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Propagación de Troyano Joker a través del aplicativo móvil SEND CHAT MESSAGE.		
Tipo de Ataque	Troyano	Abreviatura	Troyano
Medio de Propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Subfamilia	C01
Clasificación temática familia	Código malicioso		

Descripción

1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se tomó conocimiento que actores de amenazas vienen realizando una campaña de propagación del troyano Joker a través del aplicativo gratuito denominado **SEND CHAT MESSAGE**, que se encuentra disponible en la plataforma de distribución digital de aplicaciones móviles para los dispositivos con sistema operativo Android Google Play Store.

2. El aplicativo **SEND CHAT MESSAGE**, es una aplicación de mensajería y tiene la finalidad que el usuario realice comunicación digital (SMS, MMS) a través de la red de internet.

3. ***APLICATIVO MÓVIL***



4. ***DETALLES DEL APLICATIVO MÓVIL:***

- Versión : 1.0.3
- Tamaño de archivo : 23 MB.
- Nombre del paquete : com.ital.message.sdt
- Actualizado : 22JUL2022
- Precio : Gratis

5. ***PERMISOS SOLICITADOS:***

- Acceso a la galería de fotos y archivos multimedia.
- Acceso a cámara y video
- Acceso al almacenamiento del dispositivo móvil
- Información de contactos del dispositivo
- Información sobre las conexiones de red
- Información del ID del dispositivo móvil

6. ***PROVEEDORES DE SEGURIDAD INFORMÁTICA ALERTAN COMO MALICIOSO AL APLICATIVO DE ANÁLISIS***.

TROJAN/ANDROID-JOKER: Es una aplicación maliciosa que se ejecuta en segundo plano en un dispositivo móvil sin que el usuario lo sepa. Espera silenciosamente las órdenes de un servidor de Comando y Control (C&C). Estos comandos pueden, desde robar y enviar información personal a servidores remotos, hasta actuar como bots DDoS contra las víctimas objetivo.

7. ***INDICADORES DE COMPROMISO (IoC)***

- MD5 : 20db1513f8d26da3a8d4e874874ef13e
- SHA-1 : f630557c4402b30c7d684b501b1ac44dca96db92
- SHA-256 : 542962ff3ef4ee7cd8d36261d39f705c42a1ea23e88ea2b9a2f8128aceaea411

8. ***OTRAS DETECCIONES***

9. Que los actores de amenazas a través de la plataforma de distribución digital de aplicaciones móviles para dispositivos con sistema Android "**Google Play Store**", vienen propagando troyanos, siendo el caso del aplicativo denominado **SEND CHAT MESSAGE**, lo que ocasiona un riesgo a la seguridad de los dispositivos móviles, toda vez que los ciberdelincuentes pueden ejecutar software espías, tomar el control y comando (C&C) o simplemente robar información sensible de las víctimas; lo que se recomienda lo siguiente:

- Desinstalar el aplicativo de análisis.
- Analizar los permisos que otorgan a las aplicaciones móviles.
- No abrir archivos sospechosos.
- Instalar y mantener actualizado el antivirus.
- Actualizar el sistema operativo del dispositivo móvil.

Fuentes de información	▪ Análisis propio de redes sociales y fuente abierta

Índice alfabético