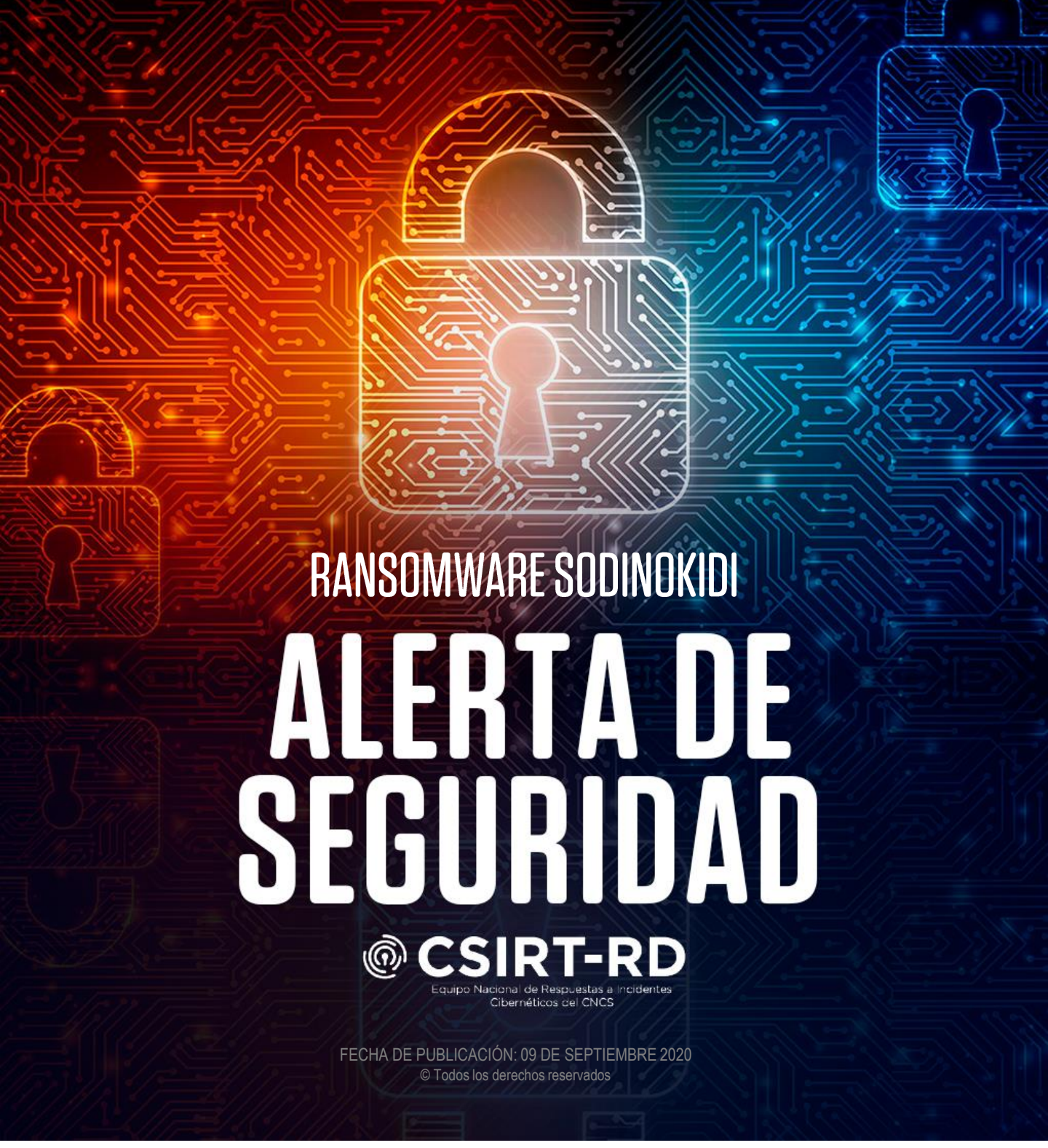


RANSOMWARE SODINOKIDI

ALERTA DE SEGURIDAD

CSIRT-RD
Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

FECHA DE PUBLICACIÓN: 09 DE SEPTIEMBRE 2020

PRESIDENCIA DE LA REPÚBLICA DOMINICANA
MINISTERIO DE LA PRESIDENCIA

CNCS CENTRO NACIONAL DE CIBERSEGURIDAD REPÚBLICA DOMINICANA

CSIRT-RD
Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

El presente documento es propiedad del **Centro Nacional de Ciberseguridad (CNCS),** y fue generado mediante el análisis de varias fuentes de terceras partes y una investigación del equipo CSIRT-RD.

ALERTA DE SEGURIDAD

Las organizaciones están expuestas a diferentes amenazas cibernéticas como consecuencia de la utilización de herramientas digitales tales como páginas web, aplicaciones móviles, correo electrónico, redes sociales, entre otras. Durante los últimos años el **ransomware** se ha convertido en una amenaza relevante para las organizaciones, a pesar de que los números de ataques no son elevados, las victimas continuan suponiendo una fuente importante de ingresos para los ciberdelincuentes, causando grandes perdidas financieras.

El **ransomware** es uno de los mas sofisticados y modernos malware que busca secuestrar datos y pedir un rescate por ellos mediante transferencia de bitcoins.

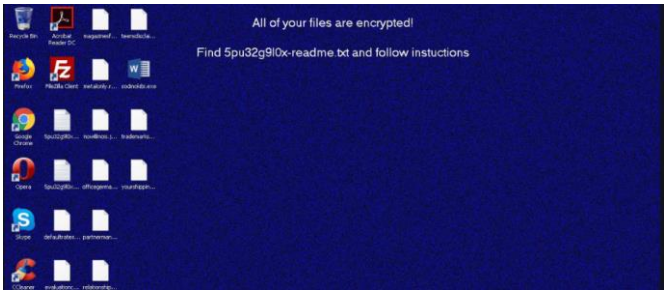
Sodinokibi también conocido como **Revil** es un malware de tipo ransomware para sistemas Windows que sigue el modelo de Ransomware-as-a-service, es decir que permite que cualquier persona que pueda pagar convertirse en operador del virus. Utiliza varias técnicas de ofuscación del servidor de comando y control y puede operar usando el algoritmo de propagación de clave asimétrica, funcionando sin conexión al C&C.

VECTOR DE ATAQUE

Para infiltrarse en las maquinas sodinokibi se aprovecha de varias vulnerabilidades conocidas;

- **CVE-2018-8453**; vulnerabilidad de elevación de privilegios en Windows cuando el componente Win32k no gestiona adecuadamente los objetos en la memoria.

- **CVE-2019-2725**;vulnerabilidad en el componente Oracle WebLogic Server de Oracle Fusion Middleware, fácilmente explotable que podría permitir a un ciberdelincuente no autenticado con acceso a la red mediante HTTP ponga en peligro la funcionalidad del componente



Fondo de pantalla con mensaje de rescate distribuido por Sodinokibi.

VECTOR DE PROPAGACIÓN

La propagación de este malware se ha producido a través de los siguientes vectores:

- El envío de correos maliciosos, mediante **campañas de spam**.
- La **publicidad maliciosa o malvertising**, es decir código malicioso presente en los anuncios que aparecen durante la navegación web, tanto para ser ejecutado directamente en el equipo, como para redirigir a servidores donde se descargan otros ejecutables.

En el ciberespacio dominicano fueron identificadas en los meses de marzo a junio varias conexiones relacionadas al C&C **208.100.26.245** del malware Sodinokibi.

RECOMENDACIONES

1. Mantener los equipos actualizados, tanto sistemas operativos como otros software instalados.
2. Tener precaución en abrir documentos y seleccionar enlaces de correos electrónicos de fuentes desconocidas.
3. Verificar y controlar los servicios de escritorio remoto (RDP).
4. Mantener actualizados las protecciones perimetrales de las instituciones
5. Aumentar los niveles de protección en los equipos que cumplan las funciones de AntiSpam, WebFilter y Antivirus.
6. Verificar el funcionamiento, y si no es necesario, bloquear las herramientas como PsExec y Powershell.
7. Mantener especial atención sobre el tráfico sospechoso que tengan conexiones a los puertos 135TCP/UDP y 445TCP/UDP
8. Verificar periódicamente los indicadores de compromisos publicados.

INDICADORES DE COMPROMISO (IoC)

Lista de IoC relacionadas a este malware;

Dominios (DNS)

boosthybrid.com.au
makeitcount.at
danubecloud.com
takeflat.com
new.devon.gov.uk
huesges-gruppe.de
theclubms.com
hoteledenpadova.it
plastidip.com.ar
zimmerei-fl.de
whittier5k.com
cityorchardhtx.com
greenko.pl
eadsmurraypugh.com
yousay.site
autopfand24.de
artotelamsterdam.com
ftlc.es
waywithwords.net
skanah.com
unetica.fr
rksbusiness.com
simpliza.com
ora-it.de
geekwork.pl
faroairporttransfers.net
microcirc.net
uimaan.fi
peterstrobos.com
wychowanieprzedszkolne.pl
marietteaernoudts.nl
lichencafe.com
withahmed.com
fundaciongregal.org
zervicethai.co.th
zso-mannheim.de
compliancesolutionsstrategies.com
Retroearthstudio.com
corelifenutrition.com
maasreusel.nl
consultaractadenacimiento.com
deprobatehelp.com
effortlesspromo.com
enovos.de
globedivers.wordpress.com
bastutunnan.se
atmos-show.com
surespark.org.uk
radaradvies.nl
em-gmbh.ch
idemblogs.com
iyengaryogacharlotte.com
wien-mitte.co.at
sweering.fr
huehnerauge-entfernen.de
ihr-news.jp
mikeramirezcpa.com
parkcf.nl

INDICADORES DE COMPROMISO (IoC)

sla-paris.com
parkstreetauto.net
sexandfessenjoon.wordpress.com
maratonaclubedeportugal.com
mylovelybluesky.com
connectedace.com
asiluxury.com
wari.com.pe
dutchbrewingcoffee.com
amylendscrestview.com
minipara.com
rocketccw.com
wacochamber.com
anybookreader.de
rimborsobancario.net
heurigen-bauer.at
purposeadvisorsolutions.com
y-archive.com
paulisdogshop.de
navyfederalautooverseas.com
aco-media.nl
spsshomeworkhelp.com
tomaso.gr
upmrkt.co
spacecitysisters.org
drinkseed.com
forskolorna.org
zewatchers.com
fannmedias.com
spd-ehningen.de
ohidesign.com
creative-waves.co.uk
desert-trails.com
troegs.com
abogadoengijon.es
the-virtualizer.com
urmasiimariiuniri.ro
castillobalduz.es
rafaut.com
rollingrockcolumbia.com
dekkinngay.com
restaurantesszimmer.de
mylolis.com
caribdoctor.org
cirugiauretra.es
eglectonk.online
colorofhorses.com
smokeysstoves.com
thewellnessmimi.com
hellohope.com
1team.es
alten-mebel63.ru
dw-css.de
teczowadolina.bytom.pl
tenacitytenfold.com
drugdevice.org
toponlinecasinosuk.co.uk
iwelt.de
thailandholic.com
hkr-reise.de
schlafsack-test.net
mirjamholleman.nl
xn--rumung-bua.online
vannesteconstruct.be
chrissieperry.com
brevitempore.net
nuzech.com
sloverse.com
xn--vrftet-pua.biz
humancondition.com
mooshine.com
alfa-stroy72.com
offroadbeasts.com
americafirstcommittee.org
lapinvihreat.fi

INDICADORES DE COMPROMISO (IoC)

chatizel-paysage.fr
deepsouthclothingcompany.com
allfortheloveofyou.com
rushhourappliances.com
international-sound-awards.com
aodaichandung.com
nandistribution.nl
lebellevue.fr
camsadviser.com
highimpactoutdoors.net
brandl-blumen.de
parking.netgateway.eu
modamilyon.com
cafemattmeera.com
csgospeltips.se
bauertree.com
gratispresent.se
solerluethi-allart.ch
tophumanservicescourses.com
siliconbeach-realestate.com
marketingsulweb.com
hotelzentral.at
hmsdanmark.dk
walter-lemm.de
softsproductkey.com
andersongilmour.co.uk
rota-installations.co.uk
talentwunder.com
boulderwelt-muenchen-west.de
corona-handles.com
euro-trend.pl
syndikat-asphaltfieber.de
kamahouse.net
cuppacap.com
cursoporcelanatoliquido.online
videomarketing.pro
mmgdouai.fr
theduke.de
gastsicht.de
pridoxmaterieel.nl
101gowrie.com
echtveilig.nl
promesapuertorico.com
caribbeansunpoker.com
lorenacarnero.com
romeguidedvisit.com
acomprarseguidores.com
dareckleyministries.com
darrenkeslerministries.com
myzk.site
sotsioloogia.ee
erstatningsadvokaterne.dk
work2live.de
micro-automation.de
cleliaekiko.online
wasmachtmeinfonds.at
airconditioning-waalwijk.nl
podsosnami.ru
micahkoleoso.de
berliner-versicherungsvergleich.de
punchbaby.com
oncarrot.com
kedak.de
fotoscondron.com
themadbotter.com

INDICADORES DE COMPROMISO (IoC)

Hash's

b10d9a62edb6081aa9f7fc865554064bb212555392b1181dc40040e12927f988
c8466c386261facf38ce62e75a8c6414affbfaed439e91fa00e515e079702fe0
bbcaee51155609d365f6bb297d124efea685df0243ec1d4efb5043d9afe5963d
9f79ea51439742e0888abd4273b62bcd247d1c72ea4f729ee870669a13f192c5
9b183afcfccc12af90f82c5f5b8a077bd8c77cf815c62e946a0dfdb4bc78847f
cbf87c3fce4c8608fcc1b1960cc4dc305addfdae889ee3998629d18d8ed2ee1c
1363b70d46c3af4d0794ecf650e3f50ceb3f81302e6059e42d94838e9ada1111
b80b9aa14af3d1af9246b14855d717ef5bd3ad0c26978c312b74323a2da0dbe7
2253f5222ebad25243cd8e3d7ac416939a7cf4f52e991ee3bd6e2f2847d28faf
f1662bfebf68d8da9879fd50b41536078c0c06ed4616dc388ee78a30ce8ccd27
11aaccd9547fd5a71335f33ce8e48ba37381013e16d4e69d01aa4252cfb17a33
31f5e6d1e938023bbb9fe4f760eb068819e6707e0304d3a16a414103ba1c3cd2
63700da4a03a05b362337224c6245f09dd5e9d72312c600ea0b607107bc82ca0
daa70a3c21659eae084f570aaa66fe194d4cbce337815b460c40ab744583c762
2d82bc93b52caad80213eec95e897909c57d75d82a4aec9d1c2fbc204b7104ba
c0faf72bb6e93878eba4b86cac0e949336c971172071a89eb9af3ef768804282
37afe4a36a980dd0609f8e6ccfcfe037aa336d16e1ba811d926eed4050e595ec
d0bf90ab2e04be11a67d7901047a4d0adccc31b436feb4100a09f527a2fe751e
9fb4aca06e67c01e6ae8c11817428cfb8e9206d9bf2fe1126af8bfef3d16835f
da74221e6e6eee961014701cd7f8be3805b324a602264b6801e766c4991906be
443140ef94c80b615eeac17cf63580e85cceb57c6c417273a65872ffe0f712b2
995f0ee67d4fdf4e5182fd09d7d1084f35f863e08ac3989c7cf5174e6fe0333c
4cc16f4d2ae63db6a45e397a134fc8fa23d8ab1ec60610a46142403d40ef6454
bbf341ba4e7aec31155e16f82572f6022c413735e63f0550685846945ec95daf
7c9967af20cf6415b6d581d74efaf9e8f9181da92cba43d7b4056f7fab97c976
b831d550b25956a849594b8e00791edcec7d603ed28948259a8ec62f3ef1b21d
0390701032e3b623a9b43927c6374abcb2c040b343147d934cd0c91f638cf8b8
ed70847aeee2bd0df8f5787c4f580bf7b8e46d7f46b8f6e2bf082c4014c90261
d0fb6f4c608994c787f15ee3b5cc1297180687522ade080c07a708e55ce23de8
09e20223d059891d4712c1fd14423ac5aee9177bcb5e4c7e2d8778415f146499
a3cdb3929b4ad03371335e2cb854e5cfb61816821cd4fcb9807e4fac57f65ea4

Para ver la lista completa de IoC's: https://cncs.gob.do/wp-content/uploads/2020/09/IoC-Sodinokibi.txt