ALERTA DE SEGURIDAD

CSIRT-RD

Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

FECHA DE PUBLICACIÓN: 22 DE ABRIL 2022

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

ALERTA DE SEGURIDAD

- **TLP** Blanco
- **Tipo de incidente** Ransomware
- **Categoría** Código Malicioso
- **Nivel de peligrosidad CRITICO**

DETALLES DE ALERTA

El Equipo Nacional de Respuesta a Incidentes (CSIRT- RD), comparte los Indicadores de Compromiso (IoC) conocidos del Ransomware **Conti**, el cual funciona a través de diversas TTPs y con ayuda de afiliados.

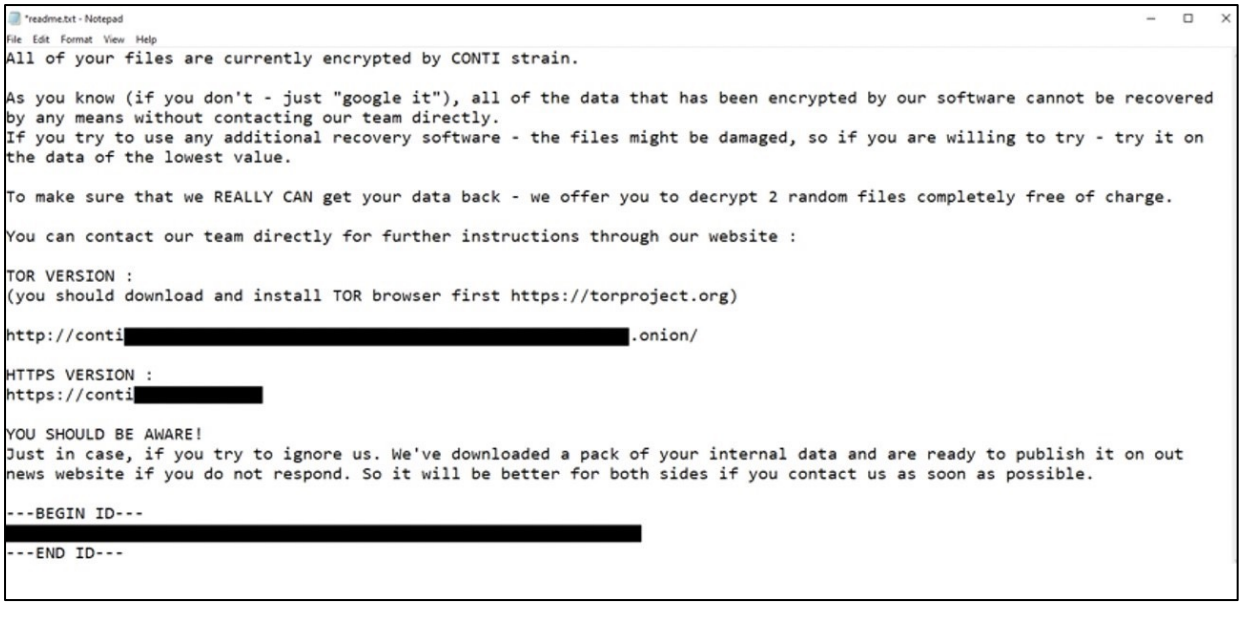
Funcionamiento

Conti es un ransomware que opera bajo el modelo de ransomware as a service y que ha sido entre los distintos grupos de ransomware uno de los que ha tenido mayor actividad recientemente.

Los actores de Conti a menudo obtienen acceso inicial a través de correos de phishing que incluyen adjuntos maliciosos y a través de la explotación de vulnerabilidades o los ataques a servicios RDP expuestos y débilmente configurados.

Mensaje de Rescate

Nota que explica a los usuarios el procedimiento para pagar el rescate de los datos comprometidos:


*readme.txt - Notepad

File Edit Format View Help

All of your files are currently encrypted by CONTI strain.

As you know (if you don't - just "google it"), all of the data that has been encrypted by our software cannot be recovered by any means without contacting our team directly.
If you try to use any additional recovery software - the files might be damaged, so if you are willing to try - try it on the data of the lowest value.

To make sure that we REALLY CAN get your data back - we offer you to decrypt 2 random files completely free of charge.

You can contact our team directly for further instructions through our website :

TOR VERSION :
(you should download and install TOR browser first https://torproject.org)

http://conti[redacted].onion/

HTTPS VERSION :
https://conti[redacted]

YOU SHOULD BE AWARE!
Just in case, if you try to ignore us. We've downloaded a pack of your internal data and are ready to publish it on out news website if you do not respond. So it will be better for both sides if you contact us as soon as possible.

---BEGIN ID---
[redacted]
---END ID---

INDICADORES DE COMPROMISO (IoC)

Dominios

badiwaw[.]com
balacif[.]com
barovur[.]com
basicem[.]com
bimafu[.]com
bujoke[.]com
buloxo[.]com
bumoyez[.]com
bupula[.]com
cajeti[.]com
cilomum[.]com
codasal[.]com
comecal[.]com
dawasab[.]com
derotin[.]com
dihata[.]com
dirupun[.]com
dohigu[.]com
dubacaj[.]com
fecotis[.]com
ipoleb[.]com
fufudir[.]com
fulujam[.]com
ganobaz[.]com
gerepa[.]com
gucunug[.]com
guvafe[.]com
hesovaw[.]com
hewecas[.]com
hidusi[.]com
contrata[.]com
hoguyum[.]com
jecubat[.]com
jegufe[.]com
joxinu[.]com
kelowuh[.]com
kidukes[.]com
kipitep[.]com
kirute[.]com
kogasiv[.]com
kozoheh[.]com
kuxizi[.]com
kuyeguh[.]com
lipozi[.]com
lujecuk[.]com
masaxoc[.]com
mebonux[.]com
mihojip[.]com
modasum[.]com
moduwoj[.]com
movufa[.]com
nagahox[.]com
nawusem[.]com
nerapo[.]com
pazovet[.]com
pihafi[.]com
pilagop[.]com
pipipub[.]com
pofifa[.]com
radezig[.]com
raferif[.]com
ragojel[.]com
rexagi[.]com
rimurik[.]com
rinutov[.]com
rusoti[.]com
sazoya[.]com
sidevot[.]com
solobiv[.]com
sufebul[.]com
suhuhow[.]com
suhuhow[.]com
tafobi[.]com
tepiwo[.]com
tifiru[.]com
tiyuzub[.]com
tubaho[.]com
vafici[.]com
vegubu[.]com
vigave[.]com
vipeced[.]com
vonavu[.]com
wezeriw[.]com
wideri[.]com
wudepen[.]com
wuluxo[.]com
wuvehus[.]com
wuvici[.]com
wuvidi[.]com
xegogiv[.]com
xekezix[.]com
vojefe[.]com
paxobuy[.]com
hejalij[.]com
hakakor[.]com
newiro[.]com
vizosi[.]com

INDICADORES DE COMPROMISO (IoC)

Direcciones IP

- 162.244.80[.]235
- 85.93.88[.]165
- 185.141.63[.]120
- 82.118.21[.]1

RECOMENDACIONES

1. Realizar el análisis correspondiente para el bloqueo a los indicadores de compromiso (IoC) citados en este documento.
2. Recomendamos tener precaución al momento de acceder a enlaces suministrados mediante medios de mensajería.
3. Mantener actualizadas las plataformas y sistemas de información según las recomendaciones del proveedor y en especial priorizar las actualizaciones para aplicaciones externas y servicios de acceso remoto.
4. Realizar contacto inmediato con el Equipo Nacional de Respuesta a Incidentes Cibernéticos (CSIRT-RD), a través del correo incidentes@csirt.gob.do, para reportar cualquier acción sospechosa o posible incidente de ciberseguridad antes de realizar una acción.
5. Reportar los eventos detectados de correos fraudulentos a phishing@csirt.gob.do
6. Realizar campañas de concientización periódica a todos los usuarios de la institución.