Prevenir ataques de tipo **Ransomware** en tiempos de **pandemia**

El cibercrimen se adapta al mundo que lo rodea y hoy en día en tiempos de pandemia donde los grupos criminales están cambiando cada vez más a señuelos temáticos acorde a la situación del COVID-19, este se ha convertido en un vector de acceso efectivo para el desarrollo de sus actos delictivos.

Descripción

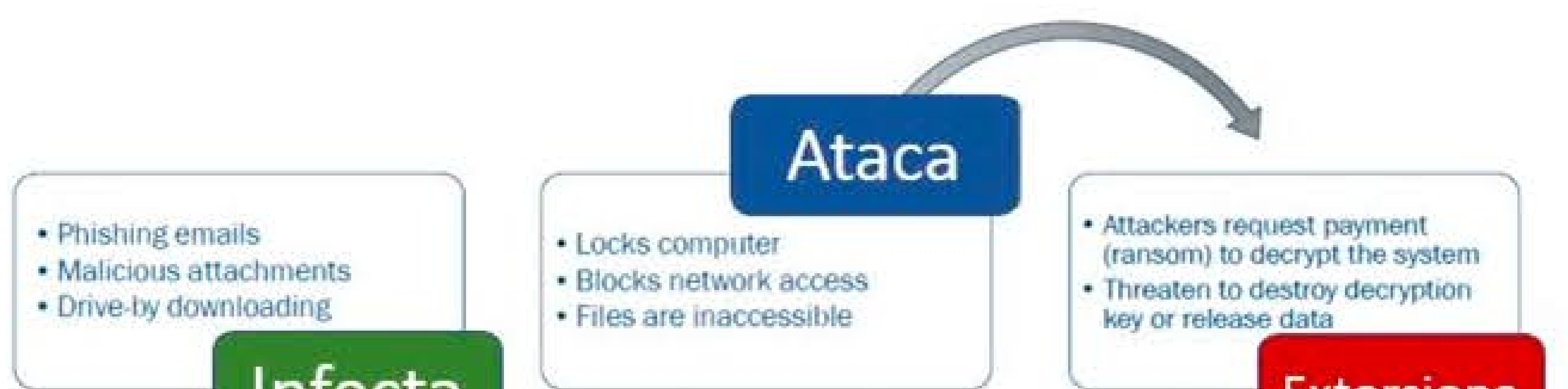
Publicación:
8/06/2020
Importancia:
Alta
Riesgo de explotación:
Media
Tipo de explotación:
Remoto

Fuentes:
DigiSOC

Ante la crisis del COVID-19, en numerosas organizaciones se ha generalizado el uso del teletrabajo como medida preventiva al contagio, sin embargo, esta emergencia se ha caracterizado por un elevado crecimiento de amenazas informáticas a partir de la persuasión humana, así como también accesos a los sistemas de información dada la ausencia de controles de seguridad en la modalidad remota de home-office; es por esto que las empresas deben estar en alerta máxima ante cualquier evento presentado en los puntos más débiles de la compañía (Usuarios remotos), debido a que los actores maliciosos se están aprovechando de la pandemia para lanzar campañas de phishing y ataques de ransomware bajo la ausencia de controles de seguridad.

Un Ransomware es un tipo de software malicioso que accede de forma no autorizada al sistema y realiza un proceso de cifrado de información con el animo de obtener utilidades económicas mediante extorsión

Como funciona:



Durante el ultimo mes las campañas de ransomware se han incrementado exponencialmente en latinoamerica, por esta razón recomendamos fuertemente aplicar las siguientes recomendaciones para su prevención, acciones de contención y recuperación en caso de materializarse el riesgo; de igual manera se aconseja realizar simulacros de planes de continuidad de negocio.

Recomendaciones:

http://	**Nunca abrir enlaces sin verificar** Evite hacer clic en enlaces en correos electrónicos no deseados o en sitios web desconocidos.
	No abrir contenido adjuntos de correos no confiables No abra archivos adjuntos de correo electrónico de remitentes en los que no confía. Mire de quién es el correo electrónico y confirme que la dirección de correo electrónico es correcta
	No conectar dispositivos USB de uso no corporativo Nunca inserte USB u otros dispositivos de almacenamiento de extracción en su computadora si no sabe de dónde provienen.
	Limitar el acceso remoto El acceso remoto a recursos internos de la compañía deben ser estrictamente limitado a lo que el usuario realmente requiera para el desarrollo de sus actividades.
	Copia de seguridad de sus datos Los datos permanecerán seguros si realizas una copia de seguridad de los mismos. Conserva todo lo que has copiado en un disco duro externo, pero asegúrate de no dejarlo conectado al ordenador cuando no lo estés utilizando.
	Cuentas con privilegios No utilizar cuentas con privilegios de administrador. El 86% de las amenazas contra Windows se pueden esquivar en caso de utilizar un usuario común en lugar de un administrador.
	Solo descarga desde sitios de confianza Evita hacer clic en los sitios web desconocidos. Las descargas que se inician al hacer clic en enlaces maliciosos son una forma de infectar el ordenador.
	Mantener actualizados el sistema operativo y aplicativos Mantener el software y el sistema operativo actualizados te ayudará a protegerte del malware. Porque cuando ejecutas una actualización, te aseguras de que te beneficias de los parches de seguridad más recientes, lo que dificulta que los cibercriminales aprovechen las vulnerabilidades de tu software
</>	**Bloqueadores de Javascript** bloquean la ejecución de todo código JavaScript sospechoso de poder dañar el equipo del usuario. Esto ayuda a minimizar la posibilidades de quedar infectado a través de la navegación web.
	Máquinas virtuales Emplear máquinas virtuales para aislar el sistema principal es otra técnica efectiva. En un entorno virtualizado la acción de los ransomware no suele materializarse al confundirlo con herramientas de sandboxing.

Acciones de recuperación ante una infección:

- Pedir ayuda
- Trabajar con expertos
- Aislar la infección
- Cambiar las contraseñas de todos los usuarios
- Revisar todas las conexiones
- Priorizar la recuperación
- No pagar el rescate dado que incentiva y promueve este tipo de campañas.

De acuerdo a nuestras semillas de inteligencia y red señuelos vulnerables desplegados en internet, compartimos los siguientes indicadores de compromisos los cuales presentan actividad reciente en campañas ransomware sobre algunos países de Latinoamérica.

Indicadores de Compromiso

Ransomware activos en Latam

- Pr0lock/Prolock
- MAZE
- CUBA
- DoppelPaymer
- BitPaymer

MD5

```
23d0033fe765242cbc07ceeab7ba3736
f9239348c88b2593814541d33c2df11d
7bb08e3a5e41ade7ad6db8b13771b4bf
83f72b384cffe9b4ee34f32202f35396
ac180806c1b6d9c9d212f1c48a14a8e7
125db77ab046e32ae647d71a00f8f4cd
689e0046ac4ff7f761248af680224994
bdee2a59edb234628048331e19fb4263
7ccb474173438181633cb645bd68b140
2bb758d67ebfb83ebf0a5c737f910774
26f36d027b36f93ee178d91a465d4c22
b3d248808aa72fbb05eff2eee1a127fa
cfdd7599b111c3096d12dcd54f354c8b
6001fb5060f65b28d854d7e24e3b2fbc
4bf9316828eb51d754941d9938cb8a92
b7637ac7a3f365e3129fe5f46db8f3ce
4ae6ebb1a8101c6753e7f94e1e904f3b
44e2e5dcc75befe2eaba0519e07df17d
f7f566c093771c77006dff5c37b08e82
cdf4831134ef0633101c6a0ca752ec6a
fe659d877aed2178ef084e3bf1e40254
ae3aab90f69a05b131bd76abe8a5a988
90cd7b4a952a6c929bd006f74125fb8c
d86fe4358f128b6c739f675da7850a79
b77eae27db59e660f972fab37708807f
90920b069aeef89e811fe56afb08b01b
c579341f86f7e962719c7113943bb6e4
3355ace345e98406bdb331ccad568386
```

SHA1

```
d318737c9116dd181c2ec074c1ffc9e2f42bc31b
0763e80f967822c263d85525d29cb535004e3156
c3f03181f2b69c5644ea93805ae1fd6bb384e534
```

SHA256

```
a0cb6b87c9f5ea12dd8f65c2d3cf3ef62e09995cc76b95c05de647f36c7d49ad
78ce13d09d828fc8b06cf55f8247bac07379d0c8b8c8b1a6996c29163fa4b659
b952e63fe46b25ee4ecb725373bddd1b1776fbc4ba73aee7b7b384a3b0f7f71e
37c26bddf236ab461d7fe9f3ad62a4e8ca44d6145425246cf77e4436fa8091c3
0dcb1897c6b1011a56d863ce4a557e13708bc9981d24d0182233e19350d0f5f1
fdf10c4d6c94ddb63ff5a73bae52fc85cf3c72793eea446a4a60ff4e3a32a62e
d8ca5e798ddf06f8f2b36c1a1b89a789dc7ea3ae1ecf6c3572c8c18bd9414c31
f19fd1647fe3b8a5f03e4d4ab4073b023d48fbcb1c6177e19684e0a1183e5b04
863ff5c8e4ae5d10e35bcae37734d3de5ffcc800871fff780fa773d81a4147c7
5288ced100d4b102f0f61b826720bbffce0ed6338c5a0b46cfae1c67ac1bc765
207f0cb45ac21620a1e1aa2e97dc79662235984e5795a615bcb823c9a5dbf03d
8ec534498fa5cb68b55a29421490db54a2b38bccd31794b2346d6b64472404f6
bed967e3afe31ea0f5b46814863e3f297edb9e1bba1365a7cb78c35f00ddee78
48984f4b5eeb2cc15c34bc52b1626362f685a0c6065e9eeacb4167ec5477396c
d944312406dc8d3d2072b60b12b18ca780d1e516529081f30938c6f6e4913a40
da8bfa2a1b1b8f1047a368e4677f17f7c6f268e774e30b1be68aa46fd7d9a0fb
16fb919e76f8fb66d7464c2764c26b0df90a7d432e8b23539f064e0ff2ddd3e3
1048952aa8f9b3ca3a2d082d3d6940173d81a2a404ba41bf2b7f4af6af2a912a
7cd39eef2f596b18986187f802b5a039773e96dac2e489e8e3ea888704f2303c
0d5ab068a6ba985567167fef7d96619007923164b843e15c7023c9a305435b27
3a45350ec9f63665e39a0d225378ab44980ed23de1815b203bb4831f8ede163a
04b7960c60d0e130d3655b09cb5a5ef88769cd7a8dd41449abe49df583fa6ac4
aeddb640e8bfc7a4e0619ffb756de3b16ccf9b6339b49464740f76e15a977ac8
2581d17c96096a2ff912f4fbf9426be73d6b063a57e68abfcc783aeac55a582e
ca00ed22a0d5db6fdfa102a26c37fd0d420cbc29214eef4d34f2f577c414120d
d3f80ebec40d7c729b87c19bd8f1760a8ec88228839e7d408d571b1577b2b776
059dd7e81265ce033d71a4cfb42549af473d70c5a8d50bc55e741f413b6e94e5
a427f9d287bc907e117535d20e1d3eefbc5587fce8a8f59791e25d915de20982
29b225ac2cb36e9d86a9857a1db08ede52c92aade442069925904d969bbba049
db5e35a5b8d03935ad085b1902f972cf1a2db937279fb9e05d21f3e1018d4253
a6ded68af5a6e5cc8c1adee029347ec72da3b10a439d98f79f4b15801abd7af0
dfbd62a3d1b239601e17a5533e5cef53036647901f3fb72be76d92063e279178
672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1
```

Acciones DigiSOC

El centro de operaciones basado en sus fuentes de inteligencia, mantiene un constante monitoreo de la actividad de fuentes de amenaza y nuevas variantes de ransomware que permiten identificar el accionar de las mismas, haciendo uso de los IoC como parte del servicio de detección y notificación de actividad relacionada.

Red Queen Lab Report | DigiSert | Centro de Investigación e Inteligencia de Amenazas | Digiware

Este comunicado DigiHelp es una alerta de ciberseguridad, incluye información sensible, puede afectar el objetivo del negocio de su compañía. Este contenido que se encuentra en proceso, esta bajo investigación y análisis de las áreas de Digiware, compuestas por DigiSOC, DigiSert y el Centro de investigación e Inteligencia de Amenazas, por lo tanto se desarrollarán << **informes llamados RQL -Red Queen Lab Report** >>, enviados posteriormente por medio de un comunicado oficial.

#Digiware | #DigiwareSuAliado
#DigiwareSecurity | #DigiwareVisionDay