Recomendaciones para evitar ataques Conti-Ransomeware

ACCIONES PREVENTIVAS

DESARROLLO TECNOLOGICO EMPRESARIAL ADE S. A

19 de abril de 2022

Departamento: Ciberseguridad

Contenido

Página web: https://detecemp.com | Teléfono: **4702-5620 /8753-0128** | Correo: **info@detecemp.com**

ANTECEDENTE

En vista del impacto que ha tenido Conti-Ransomware, tanto en el Ministerio de Hacienda como en el Ministerio de Ciencia y Tecnología, por parte del departamento de seguridad de Desarrollo Tecnológico Empresarial queremos brindarle los siguientes datos y recomendaciones sobre CONTI y como evitar ser víctima de ataques Ransomware.

¿QUÉ ES CONTI?

Descubierto por primera vez en 2020 por investigadores de Carbon Black, Conti es un grupo de ransomware que opera un modelo de ransomware como servicio para implementar el ransomware Conti.

Ransomware-as-a-Service (RaaS) es ofrecido por grupos de ransomware y brinda a los afiliados (ciberdelincuentes que buscan asociarse con grupos de RaaS) acceso a ransomware que está listo para implementarse, así como un libro de jugadas para ayudarlos a guiar sus ataques. Los grupos RaaS toman una pequeña parte de los rescates pagados y proporcionan la mayor parte de las ganancias a los afiliados.

Conti ha saltado a la fama en los últimos dos años, obteniendo $ 180 millones en ganancias de sus ataques, según Chainalysis. También ganó notoriedad por los ataques contra el sector de la salud, incluidas al menos 16 redes de emergencia y salud de EE.UU.

¿CÓMO SE PROPAGA CONTI?

Según algunos reportes, Conti es capaz de obtener acceso inicial sobre las redes de sus víctimas a través de distintas técnicas. Por ejemplo:

- Campañas de phishing especialmente dirigidas que contienen documentos adjuntos maliciosos (como un archivo Word) o enlaces. Estos adjuntos descargan malware como TrickBot, Bazar backdoor o incluso aplicaciones legítimas como Cobalt Strike que son utilizadas de forma maliciosa para realizar movimiento lateral dentro de la red de la víctima y luego descargar el ransomware.
- Explotación de vulnerabilidades conocidas sobre equipos que están expuestos a Internet.
- Ataques sobre equipos con el servicio de RDP expuesto a Internet

RECOMENDACIONES

- **Nunca hagas clic en un vínculo riesgoso**. Evita los vínculos que encuentres en correos no deseados o en sitios web que no conozcas. Si haces clic en un vínculo malicioso, podrías iniciar una descarga automática que, a su vez, podría llevar a una infección.
- **No divulgues información personal**. Si un desconocido te pide datos personales por teléfono, por correo electrónico o por mensaje de texto, haz caso omiso. A veces, cuando los hackers

tienen en mente a su próxima víctima, buscan recabar información personal para adaptar los mensajes engañosos que usarán en el ataque. Si dudas de la veracidad de un mensaje, comunícate directamente con quien te lo haya enviado.

- **Nunca abras un archivo adjunto sospechoso**. Los correos con archivos adjuntos son una de las vías que el ransomware puede usar para ingresar en tu dispositivo. Si dudas de un archivo, no lo abras. Para asegurarte de que un mensaje sea confiable, controla quién te lo envió y verifica que la dirección sea correcta. Nunca abras un archivo adjunto si, para verlo, necesitas habilitar las macros. Si el adjunto está infectado y lo abres, se ejecutará una macro maligna que le dará el mando de tu equipo a un programa malicioso.

- **Nunca uses una memoria USB que no conozcas**. Evita conectar memorias USB u otros dispositivos de almacenamiento si no sabes de dónde provienen. Los ciberdelincuentes pueden dejar unidades infectadas en sitios públicos con la esperanza de que alguien se tiente y las utilice.

- **Mantén al día las aplicaciones y el sistema operativo de tu dispositivo**. Al actualizar periódicamente el sistema operativo y las aplicaciones que hayas instalado, tu dispositivo estará más protegido contra el malware. Cuando descargues un paquete de actualizaciones, asegúrate de que estén incluidos los últimos parches de seguridad. Los parches reducen el riesgo de que un hacker aproveche vulnerabilidades en tus aplicaciones.

- **No descargues archivos de fuentes desconocidas**. Para minimizar el riesgo de introducir ransomware en el dispositivo, nunca descargues aplicaciones o archivos multimedia de sitios que no conozcas. Si vas a descargar algo, hazlo de un sitio confiable y verificado. Los sitios verificados se distinguen por tener un "sello de confianza". Cuando ingreses a una página web, revisa la barra de direcciones del navegador y comprueba que la dirección comience con "**https**" en lugar de "http". Ver un candado o un escudo en esta barra también puede ser una indicación de que el sitio es seguro. Y no olvides mantener la guardia en alto cuando descargues algo en tu dispositivo móvil. Esto varía según el dispositivo, pero el Play Store de Google y el App Store de Apple son dos fuentes en las que puedes confiar.

- **Utiliza un servicio de VPN cuando te conectes a una red Wi-Fi pública**. Para protegerte contra el ransomware, usa el Wi-Fi público con cautela. Cuando te conectas a una red pública, tu dispositivo es más vulnerable de lo normal. Para evitar riesgos, cada vez que uses una red pública, abstente de hacer operaciones confidenciales o utiliza un servicio de VPN.

INDICADORES DE COMPROMISO

Para proteger los sistemas contra el ransomware Conti, CISA, FBI y la Agencia de Seguridad Nacional (NSA) recomiendan implementar las medidas de mitigación descritas en este Aviso, que incluyen requerir autenticación multifactor (MFA), implementar la segmentación de la red y mantener actualizados los sistemas operativos y el software.
Agregar las siguientes IPs a sus listas de bloqueos tanto en los Firewalls como en todas las diferentes plataformas de seguridad con las que cuente la compañía:

- **162.244.80.235**
- **85.93.88.165**
- **185.141.63.120**

Página web: https://detecemp.com | Teléfono: **4702-5620 /8753-0128** | Correo: **info@detecemp.com**

- **82.118.21.1**

Dominios asociados al ransomware

Agregar los siguientes dominios maliciosos a sus listas de bloqueos tanto en los Firewalls como en todas las diferentes plataformas de seguridad con las que cuente la compañía:

Dominios asociados al ransomware				
badiwaw[.]com	fipoleb[.]com	kipitep[.]com	Pihafi[.]com	tiyuzub[.]com
balacif[.]com	Fofudir[.]com	Kirute[.]com	pilagop[.]com	tubaho[.]com
barobur[.]com	fulujam[.]com	kogasiv[.]com	pipipub[.]com	vacio[.]com
baseem[.]com	ganobaz[.]com	kozoheh[.]com	pofifa[.]com	Vegubu[.]com
bimafu[.]com	gerepá[.]com	kuxizi[.]com	radezig[.]com	vigave[.]com
chiste[.]com	gucunug[.]com guafe[.]com	kuyeguh[.]com	raferif[.]com	vipezado[.]com
buloxo[.]com	hakakor[.]com	lipozi[.]com	ragojel[.]com	consentido[.]com
bumoyez[.]com	hejalij[.]com	lujecuk[.]com	rexagi[.]com	vojefe[.]com
bupula[.]com	hepida[.]com	masaxoc[.]com	rimurik[.]com	vonavu[.]com
cajetí[.]com	hesovaw[.]com	mebonux[.]com	Rinutov[.]com	Wezeriw[.]com
cilomum[.]com	hewecas[.]com	mihojip[.]com	rusoti[.]com	anchori[.]com
codasal[.]com	hidusi[.]com	modasum[.]com	sazoya[.]com	wudepen[.]com
comecal[.]com	contrata[.]com	moduwoj[.]com	sidevot[.]com	wuluxo[.]com
Dawasab[.]com	hoguyum[.]com	movufa[.]com	solobiv[.]com	wuvehus[.]com
derotin[.]com	jecubat[.]com	nagahox[.]com	sufebul[.]com	wuvici[.]com

dihata[.]com	jegufe[.]com	nawusem[.]com	suhu como[.]com	wuvidi[.]com
dirupun[.]com	joxinu[.]com	nerapo[.]com	sujaxa[.]com	xegogiv[.]com
dohigu[.]com	kelowuh[.]com	newiro[.]com	tafobi[.]com tepiwo[.]com	xekezix[.]com
dubacaj[.]com	niños[.]com	paxocomprar[.]com	tifiru[.]com	
fecotis[.]com		pazovet[.]com		

OTRAS MEDIDAS DE MITIGACIÓN Y PREVENCIÓN

Utilice la autenticación multifactor.

1. Aplique autenticación multifactor para acceder de forma remota a las redes desde fuentes externas.
2. Implemente la segmentación de la red y filtre el tráfico.
3. Implemente y garantice una segmentación de red robusta entre redes y funciones para reducir la propagación del ransomware. Definir una zona desmilitarizada que elimine la comunicación no regulada entre redes.
4. Filtre el tráfico de red para prohibir la entrada y salida de comunicaciones con direcciones IP maliciosas conocidas.
5. Implemente una lista de bloqueo de URL y / o lista de permitidos para evitar que los usuarios accedan a sitios web maliciosos.
6. Analice en busca de vulnerabilidades y mantenga el software actualizado.
7. Elimine aplicaciones innecesarias y aplique controles.
8. Restrinja las fuentes de origen y exija la autenticación multifactor. Investigue cualquier software no autorizado, en particular el escritorio remoto o el software de monitoreo y administración remotos.
9. Elimine cualquier aplicación que no se considere necesaria para las operaciones diarias. Los actores de amenazas de Conti aprovechan las aplicaciones legítimas, como el software de monitoreo y administración remota y las aplicaciones de software de escritorio remoto, para ayudar en la explotación maliciosa de la empresa de una organización.
10. Implemente la lista de permitidos de aplicaciones, que solo permite a los sistemas ejecutar programas conocidos y permitidos por la política de seguridad de la organización.

Contraseñas de usuario seguras.

- Las contraseñas de usuarios deben tener una longitud mínima de 12 caracteres combinados entre números, mayúsculas, minúsculas y caracteres especiales.
- Se debe cambiar las contraseñas con un tiempo no mayor a 90 días.

Cuentas de usuario seguras.

Página web: https://detecemp.com | Teléfono: **4702-5620 /8753-0128** | Correo: **info@detecemp.com**

- Audite regularmente las cuentas de usuario administrativas y configure los controles de acceso bajo los principios de privilegios mínimos y separación de funciones.
- Audite regularmente los registros para asegurarse de que las nuevas cuentas sean usuarios legítimos.

CONCLUSIÓN

Como ocurre para cualquier clase de malware, hay dos medidas muy importantes para protegerse del ransomware: ejercer la prudencia y usar software de seguridad de primer nivel. En el caso particular del ransomware, también es muy importante contar con copias de seguridad. Son la mejor póliza de seguro si sucede lo peor.

La defensa contra el ransomware requiere que usted aborde proactivamente las fallas antes de que sean aprovechadas en los ataques. Es fundamental ver todas las vulnerabilidades y malas configuraciones en toda su superficie de ataque, predecir que problemas importan con base en inteligencia de amenazas y actuar rápidamente para abordar el riesgo cibernético. Nosotros podemos ayudarle a tener esa visibilidad para que pueda reparar las fallas antes de que se conviertan en problemas que afecten a su negocio y lleguen a los titulares de los medios de comunicación.

Referencias:

- https://www.cisa.gov/uscert/ncas/current-activity/2022/03/09/updated-conti-ransomware
- https://www.cisa.gov/uscert/ncas/alerts/aa21-265a
- https://www.tenable.com/blog/contileaks-chats-reveal-over-30-vulnerabilities-used-by-conti-ransomware-affiliates
- https://www.welivesecurity.com/la-es/2021/11/29/ransomware-conti-principales-caracteristicas/