Conti-Ransomware | Acciones Preventivas

Blue Team Ops:
Soluciones especiales.

Contenido

Antecedentes 3

¿Cómo se propaga Conti? 3

Recomendaciones 3

Indicadores de compromiso (IOCs) 4

IPs de los servidores C2 (comando y control). 4

Dominios asociados al ransomware 5

Otras medidas de mitigación y prevención 6

Utilice la autenticación multifactor. 6

Contraseñas de usuario seguras. 7

Cuentas de usuario seguras. 7

1. Antecedentes

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 equipo de ATTICYBER se recomienda proactivamente acatar las indicaciones aquí descritas.

Los actores de amenazas cibernéticas de Conti permanecen activos e informaron que los ataques de ransomware de Conti contra organizaciones estadounidenses e internacionales han aumentado a más de 1,000. La Agencia de Seguridad de Ciberseguridad e Infraestructura (CISA) y la Oficina Federal de Investigaciones (FBI) han observado el aumento del uso del ransomware Conti contra organizaciones estadounidenses e internacionales. En los ataques típicos de ransomware Conti, los actores cibernéticos maliciosos roban archivos, cifran servidores y estaciones de trabajo, y exigen un pago de rescate.

2. ¿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

3. Recomendaciones

A. **Limite el acceso a los recursos a través de la red, especialmente restringiendo RDP (Remote Desktop Protocol):** Después de evaluar los riesgos, si rdp se considera operacionalmente necesario.

B. **Hacer backups de la información de manera periódica:** validar que se cuente con respaldos recientes de todos los servidores críticos con el fin de evitar una pérdida económica o reputacional.

C. **Mostrar las extensiones de los archivos que por defecto vienen ocultas, para evitar abrir archivos maliciosos:** Abrir solamente archivos que provengan de fuentes confiables.

D. **No abrir archivos adjunto ni enlaces en un correo si no conoces a la persona que lo envió:** Habilite filtros de spam fuertes para evitar que los correos electrónicos de phishing lleguen a los usuarios finales, filtre los correos electrónicos que contienen archivos ejecutables para evitar que lleguen a los usuarios finales.
E. **Implementar una solución EDR (Endpoint Detection and Response) o XDR(Extended detection and response):** Sobre todo en activos críticos o con una alta exposición, para realizar análisis periódicos de los activos de red y así detectar posibles anomalías.
F. **Mantener los equipos actualizados, tanto el Sistema Operativo como las aplicaciones que se utilicen:** Actualice el software y los sistemas operativos, las aplicaciones y el firmware en los activos de red de manera oportuna. Considere la posibilidad de utilizar un sistema centralizado de administración de parches.
G. **Capacitar al personal de la empresa para que sea consciente de los riesgos a los que estamos expuestos en Internet:** Implemente un programa de capacitación de usuarios para disuadir a los usuarios de visitar sitios web maliciosos o abrir archivos adjuntos maliciosos.
H. **Se recomienda a los equipos de TI mantenerse atentos ante cualquier anomalía** En caso de actividad sospechosa dar aviso inmediato al equipo de ATTICYBER.

4. Indicadores de compromiso (IOCs)

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.

IPs de los servidores C2 (comando y control).

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
- 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				
badiwaw[.] com	fipoleb[.] com	kipitep[.] com	pihafi[.] com	tiyuzub[.] com
balacif[.] com	fofudir[.] com	kirute[.] com	pilagop[.] com	tubaho[.] com
barovur[.] com	fulujam[.] com	kogasiv[.] com	pipipub[.] com	vafici[.] com
basisem[.] com	ganobaz[.] com	kozoheh[.] com	pofifa[.] com	vegubu[.] com
bimafu[.] com	gerepa[.] com	kuxizi[.] com	radezig[.] com	vigave[.] com
bujoke[.] com	gucunug[.] com guvafe[.] com	kuyeguh[.] com	raferif[.] com	vipeced[.] com
buloxo[.] com	hakakor[.] com	lipozi[.] com	ragojel[.] com	vizosi[.] com
bumoyez[.] com	hejalij[.] com	lujecuk[.] com	rexagi[.] com	vojefe[.] com
bupula[.] com	hepide[.] com	masaxoc[.] com	rimurik[.] com	vonavu[.] com
cajeti[.] com	hesovaw[.] com	mebonux[.] com	rinutov[.] com	wezeriw[.] com
cilomum[.] com	hewecas[.] com	mihojip[.] com	rusoti[.] com	wideri[.] com
codasal[.] com	hidusi[.] com	modasum[.] com	sazoya[.] com	wudepen[.] com
comecal[.] com	hireja[.] 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	suhuhow[.] com	wuvidi[.] com
dirupun[.] com	joxinu[.] com	nerapo[.] com	sujaxa[.] com	xegogiv[.] com
dohigu[.] com	kelowuh[.] com	newiro[.] com	tafobi[.] com tepiwo[.] com	xekez[.] com
dubacaj[.] com	kidukes[.] com	paxobuy[.] com	tifiru[.] com	
fecotis[.] com		pazovet[.] com		

5. Otras medidas de mitigación y prevención

Utilice la autenticación multifactor.

A. Aplique autenticación multifactor para acceder de forma remota a las redes desde fuentes externas.
B. Implemente la segmentación de la red y filtre el tráfico.
C. 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.
D. Filtre el tráfico de red para prohibir la entrada y salida de comunicaciones con direcciones IP maliciosas conocidas.
E. Implemente una lista de bloqueo de URL y / o lista de permitidos para evitar que los usuarios accedan a sitios web maliciosos.
F. Analice en busca de vulnerabilidades y mantenga el software actualizado.
G. Elimine aplicaciones innecesarias y aplique controles.
H. 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.
I. 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.
J. 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. Implemente políticas de restricción de

software (SRP) u otros controles para evitar que los programas se ejecuten desde ubicaciones comunes de ransomware, como carpetas temporales compatibles con navegadores de Internet populares o programas de compresión / descompresión.

Contraseñas de usuario seguras.

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

Cuentas de usuario seguras.

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

Referencias: Updated: Conti Ransomware | CISA, Conti Ransomware | CISA