# ALERTA TÉCNICA

TLP:WHITE

**MICITT-DGD-DRII-AT-318-2021**

## CISA, FBI y NSA publican un aviso conjunto de ciberseguridad sobre Ransomware Conti

Se les comunica a los Directores (as) /Jefes (as) de Tecnologías de Información y a los enlaces de Ciberseguridad, para que tomen las medidas necesarias.

La Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA), la Oficina Federal de Investigaciones (FBI) y la Agencia de Seguridad Nacional (NSA), han publicado un Aviso de Seguridad Cibernética (CSA) conjunta que alerta a las organizaciones sobre el aumento de los ataques de ransomware Conti.

Los actores cibernéticos maliciosos utilizan el ransomware Conti para robar archivos confidenciales de organizaciones nacionales e internacionales, cifrar los servidores y estaciones de trabajo de las organizaciones objetivo y exigir el pago de un rescate a las víctimas.

**Recomendaciones**

- Tenga una sólida protección del correo electrónico: el correo electrónico sigue siendo el vector de ataque más grande para muchas amenazas cibernéticas porque, desafortunadamente, el phishing funciona. Los correos electrónicos de phishing a menudo contienen enlaces o archivos adjuntos incrustados con malware. La capacitación continua por correo electrónico evitará que los usuarios hagan clic en enlaces y archivos adjuntos sospechosos y les brindará el conocimiento para identificar las señales de una campaña de phishing.

- Utilice una política de privilegios mínimos: otorgue a los usuarios la menor cantidad de privilegios, lo que restringe los derechos de un usuario en la red. Esto puede reducir la capacidad de un usuario para moverse lateralmente a través de la red, ya que luego puede deshabilitar funciones como ejecutar scripts de PowerShell y ejecutar comandos en las solicitudes de comando.
- Haga una copia de seguridad de los datos críticos: este es probablemente el paso más importante ya que el error humano siempre es un riesgo con los pasos anteriores.
- Tener copias de seguridad de sus datos a mano en caso de un ataque de ransomware le permite tener el poder y no verse obligado a pagar el rescate.
- Mantenga actualizados todos sus sistemas tecnológicos, es importante que mantenga todos los equipos, tanto de red como de usuario final, actualizados.
- Implemente la autenticación multifactor (MFA) para cada cuenta. La habilitación de MFA para plataformas de comunicaciones corporativas (como con todas las demás cuentas) proporciona una defensa vital contra este tipo de ataques y, en muchos casos, puede prevenirlos.
- Aumentar los niveles de protección en los equipos que cumplan las funciones de AntiSpam, WebFilter y Antivirus.
- Actualice el software y los sistemas operativos con los últimos parches. Las aplicaciones y los sistemas operativos obsoletos son el objetivo de la mayoría de los ataques. Es importante que mantenga todos los equipos, tanto de red como de usuario final, actualizados.
- Verificar y controlar los servicios de escritorio remoto (RDP).
- Mantener actualizados las protecciones perimetrales de las instituciones.
- Verificar periódicamente los indicadores de compromisos publicados.
- Recuerde segmentar redes
- Desactive los servicios innecesarios en las estaciones de trabajo y los servidores de la institución

- Implementar un sistema de detección de intrusiones, si aún no se ha utilizado, para detectar la actividad en la red potencialmente maliciosa
- Supervise el tráfico web, se recomienda restrinja el acceso de los usuarios a sitios sospechosos o peligrosos.
- Segmentar y segregar redes y funciones con el fin de evitar, en caso de un ataque, que no pueda afectar toda la red
- Contactar al Centro de Respuesta a Incidentes en Seguridad Informática (CSIRT-CR) al correo csirt@micitt.go.cr. Este equipo le brindará ayuda para resolver el incidente y le recomendará cómo actuar para recuperar los archivos si existiera ya algún mecanismo probado

**Referencias**


https://us-cert.cisa.gov/ncas/current-activity/2021/09/22/cisa-fbi-and-nsa-release-joint-cybersecurity-advisory-conti

Aviso de Seguridad Cibernética (CSA)

https://us-cert.cisa.gov/ncas/alerts/aa21-265a

Recurso del gobierno de EE.UU

https://www.cisa.gov/stopransomware


**En caso de alguna duda o consulta, se pueden comunicar al CSIRT-CR por medio del correo electrónico** csirt@micitt.go.cr

MINISTERIO DE CIENCIA, TECNOLOGÍA Y TELECOMUNICACIONES

Firmado digitalmente por JORGE EMILIO MORA FLORES (FIRMA)
Fecha: 2021.09.24 16:25:24 -06'00'

**Jorge Mora Flores**
**Director de Gobernanza Digital**

MINISTERIO DE CIENCIA, TECNOLOGÍA Y TELECOMUNICACIONES

Firmado digitalmente por ROBERTO PAULO LEMAITRE PICADO (FIRMA)
Ubicación: CSIRT-CR
Fecha: 2021.09.27 07:46:47 -06'00'

**Roberto Lemaitre Picado**
**Coordinador CSIRT-CR**