BOLETÍN DE ALERTA

Boletín Número: 2021-14 **Fecha de Publicación:** 30/09/2021

Tema: Monitoreo de la actividad del ransomware Conti

SEVERIDAD: CRÍTICA

Descripción:

El Departamento de Ciberseguridad de la DIGETIC/FFAA, informa de la publicación de la Actividad del ransomware Conti de la última semana

La Agencia de Seguridad de Ciberseguridad e Infraestructura (CISA) y la Oficina Federal de Investigaciones (FBI) de los E.U.A., han observado el aumento del uso del ransomware "Conti" en más de 400 ataques contra organizaciones estadounidenses e internacionales.

Detalles:

En los ataques del ransomware "Conti", los actores maliciosos roban archivos, cifran servidores y estaciones de trabajo, exigiendo el pago de un rescate.

Los actores "Conti" obtienen el acceso inicial a las redes a través de alguna de las formas siguientes:

- Campañas de spearphishing utilizando correos electrónicos personalizados que contienen archivos adjuntos maliciosos o enlaces maliciosos.
- Los archivos adjuntos maliciosos de Word a menudo contienen scripts incrustados que se pueden usar para descargar otro malware.
- Credenciales de protocolo de escritorio remoto (RDP) robadas o débiles.
- Llamadas telefónicas.
- Vulnerabilidades comunes en activos externos.
- D. Los actores utilizan herramientas como Windows Sysinternals y
- Mimikatz, para la cosecha de credenciales.

Mitigación:

- Agregar a una lista negra los indicadores de compromiso en herramientas de seguridad de su infraestructura.
- Implementar medidas de mitigación que incluyan requerir autenticación multifactor (MFA).
- Sensibilizar al recurso humano de su organización para que evite abrir correos y archivos adjuntos de remitentes desconocidos o sospechosos.

Referencia:

https://us-cert.cisa.gov/ncas/alerts/aa21-265a ▪
https://thedfirreport.com/2021/09/13/bazarloader-to-contiransomware-in-32-hours/
CEDENA-Boletin_85_Conti.pdf