BOLETÍN DE ALERTA

Boletín Número: 2021-15 **Fecha de Publicación:** 29/09/2021

Tema: Monitoreo de la actividad del ransomware Cring

SEVERIDAD: CRÍTICA

Descripción:

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

Investigadores de Kaspersky han detectado en el presente año, a diversas empresas atacadas por el ransomware "Cring" reveló que dicho programa malicioso aprovecha una vulnerabilidad en los servidores VPN para infectar a empresas industriales de países europeos.

Detalles:

La cadena de infección funciona de la forma siguiente:

Cring obtiene acceso inicial a través de RDP (Escritorio Remoto) inseguro o comprometido o cuentas válidas, también lo puede hacer a través de exploits, como el abuso de una falla de Adobe ColdFusion (CVE-2010-2861) y en el servidor VPN de FortiGate (CVE-2018-13379).

Para la cosecha de credenciales, los actores que están detrás de "Cring" utilizan herramientas como Mimikatz.

Respecto a movimientos laterales, evasión de defensa y mando y control lo hacen con Cobalt Strike

Mitigación:

- Agregar a una lista negra los indicadores de compromiso en herramientas de seguridad de su infraestructura.
- Mantener el sistema operativo actualizado.
- Sensibilizar al recurso humano de su organización para que evite
- abrir correos y archivos adjuntos de remitentes desconocidos o sospechosos.

Referencia:

https://www.itdigitalsecurity.es/actualidad/2021/05/asi-actua-elransomware-cring-contra-objetivos-industriales
https://www.trendmicro.com/es_mx/research/21/i/examining-thecring-ransomware-techniques.htm
CEDENA-Boletin_84_ransomware_Cring