CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Amenaza Cibernética

Fecha: **27/10/2022**

Problemática: **Comando Conjunto de las Fuerzas Armadas de Ecuador bajo ataque cibernético**

Correlativo: **AA-0060**

Institución / Sector: **Instituciones Públicas y Privadas**

CONTEXTO

El Comando Conjunto de las Fuerzas Armadas de la República del Ecuador se encuentra bajo ataque cibernético que interrumpió los servicios tecnológicos de la institución. Los actores de amenaza identificados como "ALPHV/BlackCat" por medio de sus canales oficiales se atribuyeron la actividad maliciosa.

Nivel de priorización

Prioridad Urgente / No Urgente	Actualización Seguimiento/Preventiva/Resiliente
Urgente	**Preventiva**

Matriz de Evaluación

Riesgo Alto/ Medio/ Bajo	Nivel de Afectación		
	Integridad	Disponibilidad	Confidencialidad
Alto	**Alto**	**Alta**	**Alta**

SITUACIÓN

De acuerdo a la información obtenida por el Centro Estratégico de Monitoreo – CEM, Los actores de amenaza identificados como "ALPHV/BlackCat" se encuentran perpetrando ataques cibernéticos en contra de la institución en mención, logrando como objetivo la interrupción de los servicios tecnológicos.

A continuación, se muestran las Tácticas y Técnicas utilizadas por este actor de amenazas según MITRE ATT&CK

Táctica	Técnica	Identificación
Ejecución	Intérprete de comandos y secuencias de comandos	T1050
Comando y control	Servicio Web	T1102
Acceso inicial	Aprovechar la aplicación orientada al público	T1212
Persistencia	Servicios remotos externos	T1133
Acceso a Credenciales	Volcado de credenciales del sistema operativo	T1003
Movimiento lateral	Secuestro de sesión de servicio remoto	T1563.001
	Usar material de autenticación alternativo: pasar el hash	T1550.002
Exfiltración	Exfiltración a través del servicio web	T1567
Impacto	Datos cifrados por impacto	T1486

Hasta el momento no se cuenta con información del estado y magnitud del ciberataque

RECOMENDACIONES

- Active las funciones de actualización automática de software en computadoras, teléfonos móviles y otros dispositivos conectados siempre que sea posible y pragmático.
- Actualizar regularmente los sistemas operativos, el hardware y el software de los dispositivos.
- Llevar a cabo una rutina periódica de actualización y parcheo de los sistemas operativos, clientes de correo electrónico y programas ofimáticos.
- Implementar planes de recuperación ante desastres de TI que contengan procedimientos para realizar y probar regularmente copias de seguridad de datos que se pueden usar para restaurar datos de la organización.
- Implemente un proceso de gestión de vulnerabilidades basado en riesgos para la infraestructura de TI a fin de identificar y priorizar las vulnerabilidades críticas y las configuraciones incorrectas de seguridad para su corrección.

Considere implementar:

- Firewall perimetral
- Servicios de Antivirus/Antimalware.
- Herramientas de Prevención de Intrusiones en la red (IDS)
- Herramientas de Detección y Respuesta de Amenazas de Puntos Finales (EDR)
- Herramientas de Detección y Respuesta Extendidas (XDR)

ÁREA PARA DEFINICIONES

REFERENCIAS

1. https://www.socinvestigation.com/blackcat-alphv-ransomware-as-a-service-raas-had-compromised-at-least-60-entities-worldwide/ https://attack.mitre.org/versions/v11/techniques/T1598/002/
2. https://attack.mitre.org/versions/v11/techniques/T1050/
3. https://attack.mitre.org/versions/v11/techniques/T1102/
4. https://attack.mitre.org/versions/v11/techniques/T1212/
5. https://attack.mitre.org/versions/v11/techniques/T1133/
6. https://attack.mitre.org/versions/v11/techniques/T1003
7. https://attack.mitre.org/versions/v11/techniques/T1563/001/
8. https://attack.mitre.org/versions/v11/techniques/T1550/002/
9. https://attack.mitre.org/versions/v11/techniques/T1567/
10. https://attack.mitre.org/versions/v11/techniques/T1486/

DICCIONARIO DE DATOS

- Atacante (ciberdelincuente, actor de amenazas): Persona que realiza actividades delictivas en la red contra personas o sistemas informáticos, pudiendo provocar daños económicos o reputacionales mediante robo, filtrado de información.
- Cifrado: Proceso de codificación de información para poder evitar que esta llegue a personas no autorizadas.

ÁREA PARA DEFINICIONES