CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Amenazas cibernéticas

Fecha: 08/02/2024

Problemática: **Hyundai Motor Europa afectado por ataque de ransomware «BlackBasta»**

Correlativo: AC-0007

Institución / Sector: **Privado**

SITUACIÓN

La división europea del fabricante de automóviles Hyundai, Hyundai Motor Europe, sufrió un ataque de ransomware «BlackBasta». Los actores de la amenaza afirmaron robar 3 terabytes de datos corporativos (información de los departamentos legal, ventas, RRHH, contabilidad, TI y administración. Hyundai Motor Europe confirmó el ataque y trabaja con expertos legales en ciberseguridad para investigar el incidente.

RIESGOS

- Robo de datos confidenciales de los usuarios para cometer fraude, robo de identidad, espionaje y otros delitos.
- Daños a la reputación de la empresa.
- Interrupción de operaciones, generando pérdidas económicas.
- Propagación del ransomware a otras organizaciones que forman parte de la cadena de suministro de Hyundai Motor Europe.

RECOMENDACIONES

- Implementar medidas de seguridad y hacer uso de cortafuegos, antivirus y sistemas de detección de intrusiones.
- Mantener los sistemas actualizados.
- Realizar copias de seguridad regulares para poder restaurar los datos en caso de un ataque.

Nivel de priorización

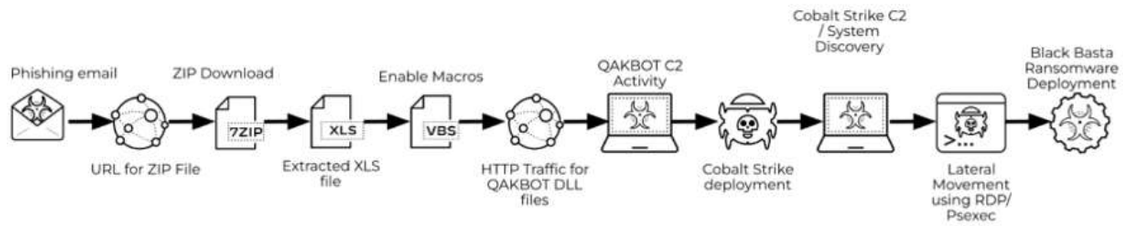
Prioridad Urgente / No Urgente	Actualización Seguimiento/Preventiva/Resiliente
Urgente	Preventiva

Matriz de evaluación

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

ANEXO

Cadena de infección BlackBasta



El ransomware «BlackBasta» se despliega en los equipos de las víctimas, en una primera instancia mediante la ingeniería social con la distribución de phishing por correo electrónico con documentos ofimáticos adjuntos que incorporan macros maliciosas, que una vez ejecutadas proceden con la descarga y uso del troyano Qakbot mediante la explotación de la vulnerabilidad de ejecución remota de código MSDTC, CVE-2022-30190.