	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 130	Fecha: 03-06-2023
		Página 12 de 27

Componente que reporta	**CENTRO DE OPERACIONES CIBERESPACIALES**		
Nombre de la alerta	Ransomware del grupo Rhysida atacó red Institucional del Ejercito de Chile		
Tipo de ataque	Ransonware	Abreviatura	Ransonware
Medios de propagación	Correo electrónico, redes sociales, entre otros		
Código de familia	C	Código de subfamilia	C01
Clasificación temática familia	Código Malicioso		

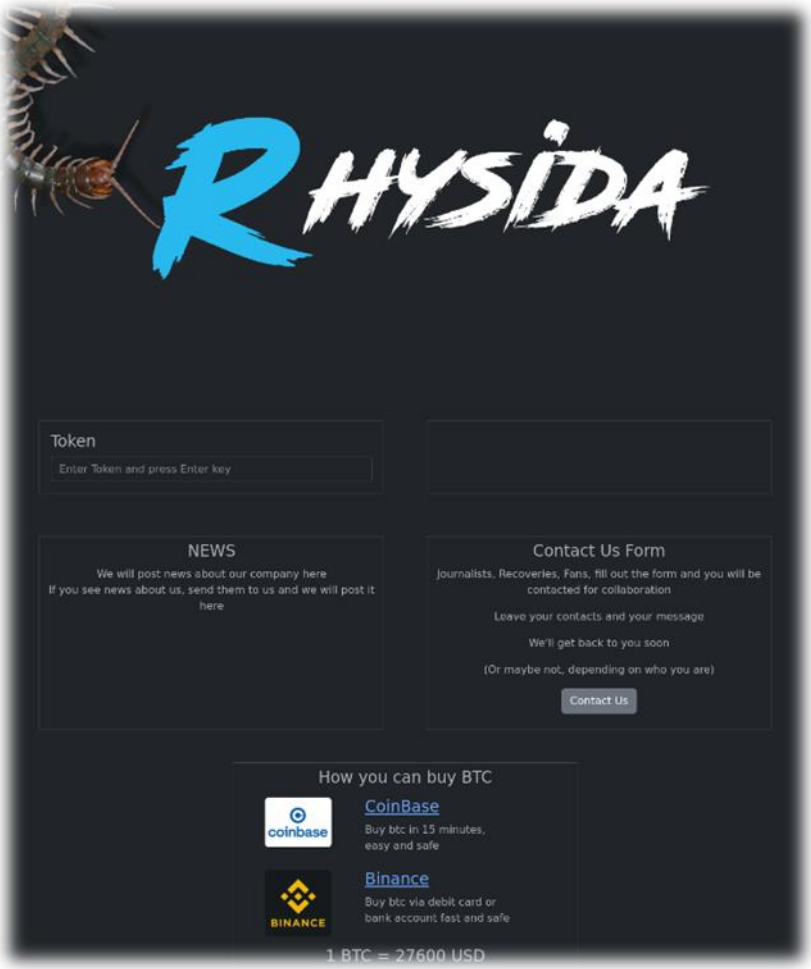
Descripción

1. El día 30 de mayo del 2023, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se tomó conocimiento que, el Ejército de Chile sufrió un ataque informático el 27 de mayo del presente año; a través de un Ransomware operado por el Grupo Rhysida; la cual, viene afectando las redes internas de la institución (Red Intranet Institucional).

   El ransomware operado por el grupo Rhysida; se encarga del secuestro de datos, mediante la encriptación de los archivos y bloqueando los equipos, buscando obtener un beneficio para devolver los documentos obtenidos.

   Cabe mencionar que, debido a los ataques registrados, la institución afectada ordenó a todos los funcionarios no encender sus computadoras y desconectar los cables de Ethernet de los dispositivos, para evitar consecuencias negativas.

   Finalmente, el equipo CSIRT emitió una alerta de seguridad cibernética para solucionar el ataque.



2. Recomendaciones:

- Recomendar al personal encargado del área de informática verificar los equipos informáticos que se encuentren conectados a la red institucional, los cuales deben contar con los programas de protección actualizadas.
- Recomendar a los encargados de administrar dichos equipos informáticos, no apertura páginas emergentes de dudosa procedencia, a fin de evitar ser víctimas de intrusión de software maliciosos.
- Recomendar al encargado de informática verificar los equipos de sus instalaciones asignadas, a fin de evitar incidentes de seguridad digital y se brinden la protección necesaria de los equipos y sistemas informáticos.

Fuentes de información	▪ hxxps://www.13.cl/smart13/articulos/alerta-ejercito-de-chile-sufre-ataque-informatico-en-su-red-interna

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 130	**Fecha: 03-06-2023**
		Página 16 de 27

Componente que reporta	**CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	Nuevo Ransomware Rhysida presente en Latinoamérica		
Tipo de ataque	Ransomware	Abreviatura	Ransomware
Medios de propagación	Correo electrónico, redes sociales y entre otros		
Código de familia	C	Código de subfamilia	C01
Clasificación temática familia	Código Malicioso		

Descripción

ANTECEDENTES:

El 31 de mayo del 2023, a través del monitoreo y búsqueda de amenazas en el Ciberespacio, se tomó conocimiento que, recientemente ha surgido un nuevo grupo de ransomware llamado “Rhysida” en alusión a un tipo de ciempiés que habita en distintas partes del mundo.

DETALLES:

Para el acceso inicial Rhysida utiliza distintos métodos entre los que se han detectado el uso de Cobalt Strike y campañas de phishing dirigidas contra sus objetivos. Al desplegar la carga útil en el equipo víctima aparecerá una ventana de terminal cmd “.” exe para luego ir cifrando los archivos de cada una de las unidades locales descubiertas agregando la extensión ”. rhysida”.

A diferencia de otros ransomware que proporcionan un archivo tipo TXT con las instrucciones para el rescate de la información cifrada, “Rhysida” lo hace con un PDF que se despliega en cada una de las carpetas afectadas, solicitando que las víctimas se pongan en contacto con ellos a través de su portal alojado en la red TOR, es ahí donde les solicitan que se identifiquen utilizando su ID único proporcionado en la misma nota de rescate.
El método de pago utilizado por estos ciber actores es únicamente BTC (Bitcoin), con el objetivo de evadir las transacciones en esta moneda virtual no controlada. Si una víctima decide pagar por el rescate, debe proporcionar su ID y luego completar un formulario adicional en donde se le solicitan más datos con el objetivo de autenticar la información y entregar detalles de contacto. Otro de los hallazgos realizados por los investigadores es que “Rhysida” intenta reemplazar el fondo de escritorio ejecutando distintos comandos.
El tipo de cifrado que utiliza Rhysida es ChaCha20, este cifrado también es utilizado por otros grupos de ciberactores que despliegan ransomware, la particularidad de este cifrado radica en su algoritmo que es de flujo rápido y seguro, su fortaleza está presente en la confidencialidad de los datos de la comunicación y almacenamiento.

Adicionalmente se destaca que “Rhysida” excluye el cifrado de los siguientes directorios:

- $Recycle.Bin
- Boot
- Documents and Settings
- PerfLogs
- Program Files
- Program Files (x86)
- ProgramData
- Recovery
- System Volume Information
- Windows
- $RECYCLE.BIN

Se ha podido identificar los siguientes indicadores de compromiso:

N°	Tipo	indicador
01	SHA256	a864282fea5a536510ae86c77ce46f7827687783628e4f2ceb5bf2c41b8cd3c6
02	SHA1	69b3d913a3967153d1e91ba1a31ebed839b297ed
03	MD5	0c8e88877383ccd23a755f429006b437
04	IP	146.20.132.182
05	IP	146.20.132.183
06	IP	146.20.132.184
07	IP	146.20.132.181

RECOMENDACIONES:

- Usar software antimalware u otras herramientas de seguridad capaces de detectar y bloquear variantes conocidas de ransomware. Estas herramientas pueden usar firmas, heurística o algoritmos de aprendizaje automático para identificar y bloquear archivos o actividades sospechosas.
- Supervisar el tráfico de red y buscar indicadores de compromiso, como patrones de tráfico de red inusuales o comunicación con servidores de comando y control conocidos.
- Realizar auditorías y evaluaciones de seguridad periódicas para identificar las vulnerabilidades de la red y del sistema y garantizar que todos los controles de seguridad estén implementados y funcionen correctamente.
- Educar y capacitar a los empleados sobre las mejores prácticas de seguridad cibernética, incluida la identificación y el informe de correos electrónicos sospechosos u otras amenazas.
- Implementar un plan sólido de respaldo y recuperación para garantizar que la organización tenga una copia de sus datos y pueda restaurarlos en caso de un ataque.

Fuentes de información	▪ hxxps://portal.cci-entel.cl/Threat_Intelligence/Boletines/1603/