Nro. Alerta:	EC-2022-080	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	20-julio-2022	CAMPAÑA DE MALWARE DE CRIPTOMINERÍA DIRIGIDA A SERVIDORES LINUX	V 1.2

I. DATOS GENERALES:

Clase de alerta: Malware
Tipo de incidente: Cryptohacking
Nivel de riesgo: Medio

II. ALERTA

El equipo de seguridad de Microsoft publicó una alerta sobre una campaña de malware ejecutada por un grupo identificado como “8220”. Dicha campaña está dirigida a servidores Linux con el objetivo de instalar criptomineros como parte de una campaña de larga duración.

Figura No. 1: Campaña de malware de criptominería
Fuente: Thehackernews

III. INTRODUCCIÓN

El grupo chino denominado “8220” ha estado activo desde el 2017, y sus ataques se enfocan en campañas de criptominería. Su nombre proviene del puerto 8220 utilizado por el sistema de minería para comunicarse con los servidores “command and control”.

Según los investigadores de Microsoft, para lograr acceso inicial, el grupo “8220” ha lanzado una campaña cuyo objetivo son los sistemas Linux i686 y x86_64 y utiliza el exploit Remote Code Execution (RCE) para el CVE-2022-26134 (Atlassian Confluence) y el CVE-2019-2725 (WebLogic).

Microsoft también ha indicado que después de que el grupo “8220” obtiene acceso al servidor a través del CVE-2022-26134, descarga un “payload” en el

Nro. Alerta:	EC-2022-080	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	20-julio-2022	CAMPAÑA DE MALWARE DE CRIPTOMINERÍA DIRIGIDA A SERVIDORES LINUX	V 1.2

sistema que cambia sus configuraciones para deshabilitar los servicios de seguridad, luego descarga un criptominero, establece persistencia en la red y luego escanea puertos en la red para encontrar otros servidores.

IV. VECTOR DE ATAQUE: Web

V. IMPACTO:

Este tipo de ataques afectan a sistemas Linux i686 y x86_64 afectando dichos sistemas y redes asociadas.

VI. INDICADORES DE COMPROMISO:

En la siguiente tabla, se indican los IOC asociados:

SHA-256	Nombre del paquete
bd3c7a55ee04d5713eaf36dfca291533a544b8f58c1e6e30dcd46e3b58bf38e5	loader script
2bd102ddc0e618d91a7adc3f3fb92fcfb258680f11b904bb129f5f2f918dcc5f	PwnRig miner for i686
ca7fb4ee975499b2b1497fb1be69d0187d0a5cf83a2a646ad2855f4e739c8326 (pwnRig for x86_64)	pwnRig for x86_64

Tabla 1: IOCs
Fuente: Microsoft

VII. RECOMENDACIONES:

El Centro de Respuestas a Incidentes Informáticos de ARCOTEL, EcuCERT, recomienda a su comunidad objetivo y a la ciudadanía lo siguiente:

- Se recomienda proteger los sistemas y servidores, a través de soluciones antivirus, aplicar actualizaciones tanto de software como de hardware, y, utilizar contraseñas distintas y robustas de acceso a nivel de usuario e infraestructura de red.
- Monitoreo continúo de los servidores y la red a fin de determinar comportamientos atípicos.

Dirección: Av. 9 de Octubre N27-75 y Berlín
Código Postal: 170513 / Quito - Ecuador
Teléfono: 593-2 2946 400 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-080	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	20-julio-2022	CAMPAÑA DE MALWARE DE CRIPTOMINERÍA DIRIGIDA A SERVIDORES LINUX	V 1.2

VIII. DESCARGO DE RESPONSABILIDAD

- La información en esta alerta es con fines informativos. El Centro de Respuestas de ARCOTEL, EcuCERT, no respalda ningún producto o servicio comercial, incluidos aquellos sujetos de análisis.
- Cualquier referencia a productos, procesos o servicios comerciales específicos por marca de servicio, marca comercial, fabricante, no constituye ni implica respaldo, recomendación o favorecimiento por parte de EcuCERT.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

- *Palmer, D. (2022, 11 julio). This «evasive» new Linux malware creates a backdoor to steal passwords and more. ZDNet. Recuperado 12 de julio de 2022, de https://www.zdnet.com/article/this-new-evasive-and-persistent-linux-malware-creates-a-backdoor-to-steal-usernames-passwords-and-more/*.

- Paganini, P. (2022, 1 julio). *A long-running cryptomining campaign conducted by 8220 hackers now targets Linux servers*. Security Affairs. Recuperado 12 de julio de 2022, de https://securityaffairs.co/wordpress/132777/cyber-crime/8220-cryptomining-campaign.html#:%7E:text=Microsoft%20Security%20Intelligence%20experts%20are,servers%20to%20install%20crypto%20miners.

- Lakshmanan, R. (2022, 1 julio). *Microsoft Warns of Cryptomining Malware Campaign Targeting Linux Servers*. The Hacker News. Recuperado 12 de julio de 2022, de https://thehackernews.com/2022/06/microsoft-warns-of-cryptomining-malware.html.