Nro. Alerta:	AL-2024-024	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR ALERTAS DE SEGURIDAD	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	29-oct-2024	Malware Beavertail	Pág.: **1** of **4**

I. DATOS GENERALES:

Clase de alerta: Incidente

Tipo de incidente: Malware

Nivel de riesgo: Alto

II. ALERTA

Se descubrió que tres paquetes maliciosos publicados en el registro npm en septiembre de 2024 contenían un malware conocido llamado BeaverTail, un descargador de JavaScript y ladrón de información vinculado a una campaña en curso de Corea del Norte rastreada como Contagious Interview.

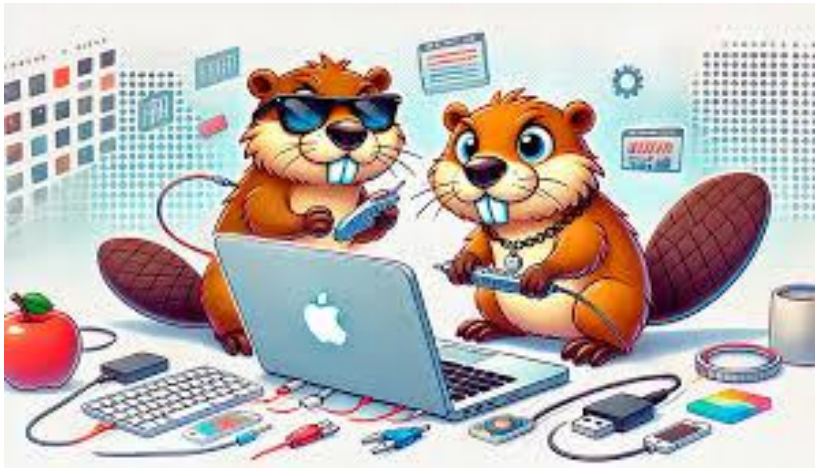

Figura 1.- *Ilustración asociada a Beavertail* ***Fuente: therhackernews***

III. INTRODUCCIÓN

Los especialistas en ciberseguridad de Group-IB descubrieron dos nuevos desarrollos en la familia de malware BeaverTail.

En primer lugar, detectaron una nueva versión de BeaverTail para Windows, ampliando el alcance del malware más allá de sus plataformas anteriores. En segundo lugar, y quizás lo más alarmante, descubrieron una variante JavaScript evolucionada de BeaverTail.

Esta versión circula a través de títulos inocentes. Está construido sobre ReactJS, una biblioteca de JavaScript ampliamente utilizada para juegos populares.

Estas aplicaciones maliciosas están ocultas dentro de paquetes NPM (Node Package Manager) y pueden incluirse fácilmente en múltiples proyectos de desarrollo.

A través de este sofisticado exploit, el grupo Lazarus ha demostrado ser lo suficientemente adaptable en su intento de atacar diferentes sistemas operativos y entornos de desarrollo.

Se ha visto que el malware BeaverTail para Windows se disfraza de una aplicación de conferencia genuina FCCCall.exe.

Esto es similar a una operación anterior de Lazarus donde el grupo troyanizó la aplicación MiroTalk.

Los objetivos principales siguen siendo los mismos para todas las versiones de BeaverTail: obtener información de la billetera de criptomonedas y descargar y ejecutar la carga útil del siguiente paso, InvisibleFerret.

Sin embargo, los desarrolladores del malware ampliaron su alcance, como lo demuestra el creciente número de extensiones de navegador a las que apunta.

IV. VECTOR DE ATAQUE:

Los nombres de los paquetes maliciosos, que ya no están disponibles para descargar desde el registro de paquetes, se enumeran a continuación:

- passpass-js, una copia del pasaporte con puerta trasera (118 descargas)
- bcrypts-js, una copia con puerta trasera de bcryptjs (81 descargas)
- blockscan-api, una copia con puerta trasera de etherscan-api (124 descargas)

Contagious Interview se refiere a una campaña de un año de duración emprendida por la República Popular Democrática de Corea (RPDC) que implica engañar a los desarrolladores para que descarguen paquetes maliciosos o aplicaciones de videoconferencia aparentemente inocuas como parte de una prueba de codificación. Salió a la luz por primera vez en noviembre de 2023.

V. INDICADORES DE COMPROMISO

BeaverTail ahora compromete una gama más amplia de extensiones de navegador, incluidas las mencionadas anteriormente, como kaikas, rabby, argent X y Exodus web3, lo que sugiere que sus operadores tienen la intención de capturar un mayor volumen de activos de criptomonedas de las víctimas.

IoCs

- 185.235.241[.]208:1224
- 95.164.17[.]24:1224
- dc77044fe8d35882015eaa99ca31f826
- b9693b6541a22d01b100b867375279e6
- 8ebca0b7ef7dbfc14da3ee39f478e880
- ed60b3913e6694f4a0ed2fe25551bd1f

VI. IMPACTO:

No es la primera vez que los actores de amenazas utilizan paquetes npm para distribuir BeaverTail. En agosto de 2024, la empresa de seguridad de la cadena de suministro de software Phylum reveló otro grupo de paquetes npm que allanaron el camino para la implementación de BeaverTail y una puerta trasera de Python llamada InvisibleFerret.

Los nombres de los paquetes maliciosos identificados en ese momento eran temp-etherscan-api, ethersscan-api, telegram-con, casco-validate y qq-console. Un aspecto que es común a los dos conjuntos de paquetes es el esfuerzo continuo por parte de

los actores de amenazas para imitar el paquete etherscan-api, lo que indica que el sector de las criptomonedas es un objetivo persistente.

Stacklok detectó una nueva ola de paquetes falsificados (eslint-module-conf y eslint-scope-util) que están diseñados para recolectar criptomonedas y establecer acceso persistente a máquinas de desarrolladores comprometidas.

"Copiar y hacer puertas traseras a paquetes npm legítimos sigue siendo una táctica común de los actores de amenazas en este ecosistema", dijo Datadog. "Estas campañas, junto con Contagious Interview en general, resaltan que los desarrolladores individuales siguen siendo objetivos valiosos para estos actores de amenazas vinculados a la RPDC".

VII. RECOMENDACIONES:

- Aplicar las actualizaciones emitidas por los fabricantes.
- Aplique las últimas actualizaciones de seguridad de Microsoft inmediatamente.
- Priorizar la aplicación de parches en los sistemas conectados a Internet.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta, se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

https://thehackernews.com/2024/10/beavertail-malware-resurfaces-in.html
https://www.cronup.com/feed-de-noticias-de-ciberseguridad-19-08-2024/
https://gbhackers.com/beavertail-malware-weaponized-games-attack/