Nro. Alerta:	EC-2022-58	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	05-abril-2022	**Malware Verblecon**	Versión 1.0

I. DATOS GENERALES:

Clase de alerta: Malware
Tipo de incidente: Código Malicioso
Nivel de riesgo: Alto

II. ALERTA

El malware Verblecon; es utilizado para cargar malware, permitiendo la instalación de criptomineros en las máquinas de las víctimas.

Figura 1. Ilustración relacionada a malware Verblecon
Fuente: SPRING

III. INTRODUCCIÓN

Verblecon es un cargador de malware que se detectó a principios del 2022, este código malicioso está desarrollado en Java y posee una baja tasa de detección debido a la naturaleza polimórfica[1] del código.

[1] El código de la carga del malware se ve diferente cada vez que se descarga debido al cifrado y la ofuscación.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-58	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	05-abril-2022	**Malware Verblecon**	Versión 1.0

Este código malicioso es usado por los ciberdelincuentes para comprometer dispositivos de víctimas y posteriormente extraer criptodivisas; por ejemplo:

- Instalar software de minería de criptomonedas.
- Robar tokens de Discord[2] y usarlos para publicitar software de videojuegos con troyanos.

Es decir, a través del Malware Verblecon se puede dar inicio a criptojacking (o minería de criptomonedas maliciosa) que se define como el uso no detectado de un dispositivo informático ajeno para extraer monedas digitales. Es la vulneración de un ordenador, smartphone o red de equipos, no para acceder a datos, sino para minar criptomonedas secuestrando recursos de otros

IV. VECTOR DE ATAQUE:

1. El malware verifica si se está ejecutando en un entorno virtual o de espacio aislado; para tal efecto, obtiene la dirección MAC del equipo y verifica los siguientes prefijos:
   - 00:05:69
   - 00:0C:29
   - 00:1C:14
   - 00:50:56
   - 08:00:27
   - 00:16:3E
   - 00:1C:42
   - 0A:00:27
2. Obtiene la lista de procesos en ejecución y compara con su propio catálogo predefinido.
   - A través del comando: **tasklist.exe /fo csv /nh**, obtiene la lista de procesos en ejecución.
3. Se copia a sí mismo en un directorio local de la víctima y crea archivos para usarlos como punto de carga.
4. Una vez que el código malicioso comprueba estos parámetros iniciales; intenta conectarse periódicamente a los siguientes dominios[3]:
   - hxxps://gaymers[.]ax/
   - hxxp://[DGA_NOMBRE][.]tk/
5. Una vez que establece conexión y se obtiene la carga útil se procede a descargar y ejecutar un binario (archivo.BIN)

[2] Aplicación de chat grupal que es particularmente popular entre la comunidad de jugadores.
[3] Para ello emplea DGA (Algoritmo de Generación de Dominio).

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-58	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	05-abril-2022	**Malware Verblecon**	Versión 1.0

V. INDICADORES DE COMPROMISO:

A continuación, se mencionan los IOC relacionados al malware Verblecon.

Ítem	Parámetro	Descripción
1	SHA-256	32a9415daa7f37a93dd0b347461844673c0f5baf0c15c01ee48b147dadf28299 3688c249774cc9a28d2b9b316921cec842bb087c57f4733cf5866226fbe2aeed 5a4f6332ad08b35c055bb5e6dfddc79d2f7905e63fac7595efbedd0b27f12eb8 007f5898c52c3aa1c3dca6d3a30f28f5f72d9789fbb440ae656d88959f68e53e f3f4af5f5eae1a28ad5a01b56d71302a265bce17d2c87ce731edf440612818a6
2	Dominios	hxxps://gaymers[.]ax/ hxxp://[DGA_NOMBRE][.]tk/ hxxp://verble[.]software/styles.jar hxxps://jonathanhardwick[.]me/hardwick.jar hxxps://jonathanhardwick[.]me/hardwick.bin hxxps://jonathanhardwick[.]me/config.txt hxxp://test.verble[.]rocks/dorflersaladreviews.jar hxxp://test.verble[.]rocks/dorflersaladreviews.bin
2	Servidores de comunicación	gaymers[.]hacha 6f3af6ffb074513b51bba688a0b41df7[.]tk

Tabla 1. IOC malware Verblecon
Fuente: Symantec

VI. RECOMENDACIONES:

El EcuCert recomienda a su comunidad objetivo:

- Descargar aplicaciones desde sitios oficiales
- Emplear contraseñas seguras, doble autenticación o certificados electrónicos de encriptación.
- Evita las redes públicas para realizar tus transacciones.
- Evita interactuar con correos electrónicos sospechosos.
- Mantén tus dispositivos protegidos con un sistema anti virus actualizado.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-58	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	05-abril-2022	**Malware Verblecon**	Versión 1.0

VII. REFERENCIAS:

BROADCOM. (29 de 03 de 2022). *BROADCOM*. Obtenido de BROADCOM: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/verblecon-sophisticated-malware-cryptocurrency-mining-discord

Ilascu, I. (29 de 03 de 2022). *BleepingComputer*. Obtenido de BleepingComputer: https://www.bleepingcomputer.com/news/security/verblecon-malware-loader-used-in-stealthy-crypto-mining-attacks/

INTERPOL. (s.f.). *INTERPOL*. Obtenido de INTERPOL: https://www.interpol.int/es/Delitos/Ciberdelincuencia/Cryptojacking

Jessica, L. (29 de 03 de 2022). *The Register*. Obtenido de The Register: https://www.theregister.com/2022/03/29/verblecon_malware_cryptomining/