



Nro. Alerta:	AL-2023-024	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	 ALERTAS DE SEGURIDAD
TLP:			
Fecha:	05-junio-2023	Vulnerabilidad servidores web de Microsoft Windows IIS	Pág.: 1 of 5

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de incidente: Exfiltración de información y movimiento lateral
Nivel de riesgo: Medio

II. ALERTA

El 23 de mayo de 2023, ASEC (AhnLab Security Emergency Response Center), informó que el grupo Lazarus¹ lleva a cabo ataques contra servidores web de Microsoft Windows IIS, cuando este grupo realiza un análisis y encuentran un servidor web con una versión vulnerable, utilizan la vulnerabilidad adecuada de la versión para instalar un shell web o ejecutar comandos maliciosos.



Figura No. 1.- Ilustración asociada a Lazarus Group
Fuente: https://es.wikipedia.org/wiki/Lazarus_Group



III. INTRODUCCIÓN

Los investigadores del AhnLab Security Emergency Response Center (ASEC) informaron que Lazarus Group está apuntando a versiones vulnerables de servidores Microsoft IIS en una ola reciente de ataques basados en malware.

Una vez descubierto un servidor IIS vulnerable o mal administrados, los atacantes realizan la carga lateral de una DLL maliciosa (msvcr100.dll) para ejecutar una DLL

¹ Grupo Lazarus organización de hackers que se hace llamar Lazarus (o DarkSeoul) y que nació en Corea del Norte en el año 2009



Nro. Alerta:	AL-2023-024	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	 ALERTAS DE SEGURIDAD
TLP:			
Fecha:	05-junio-2023	Vulnerabilidad servidores web de Microsoft Windows IIS	V 1.1 Pág.: 2 of 5

maliciosa (msvcr100.dll) que han colocado en la misma ruta de la carpeta que una aplicación normal (Wordconv.exe), a través del proceso del servidor web de Windows IIS, w3wp.exe. Luego ejecutan la aplicación normal para iniciar la ejecución de la DLL maliciosa. El actor de amenazas ha estado cambiando continuamente el nombre del proceso normal utilizado en la técnica de carga lateral de DLL.

En este documento se cubre la técnica de carga lateral de DLL utilizada durante su proceso de infiltración inicial, así como sus comportamientos de seguimiento.

1. Infiltración inicial:

El actor de la amenaza crea Wordconv.exe, msvcr100.dll y msvcr100.dat a través del proceso del servidor web Windows IIS (w3wp.exe) antes de ejecutar Wordconv.exe. Como se muestra en la siguiente figura, msvcr100.dll está contenido en la lista de DLL de importación de Wordconv.exe, por lo que el primer archivo DLL que se carga cuando se ejecuta Wordconv.exe está determinado por la prioridad de búsqueda de DLL del sistema operativo. Como resultado, el msvcr100.dll malicioso se ejecuta en la memoria del proceso Wordconv.exe.

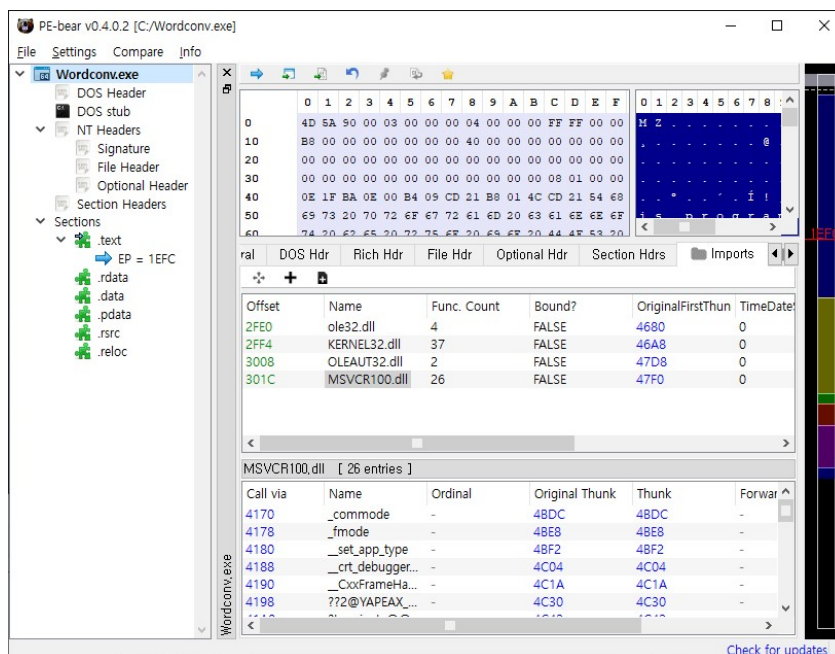




Figura No. 2.- Importar lista de DLL de Wordconv.exe

Fuente: <https://asec.ahnlab.com/en/53132/>

Nro. Alerta:	AL-2023-024	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	 ALERTAS DE SEGURIDAD
TLP:			
Fecha:	05-junio-2023	Vulnerabilidad servidores web de Microsoft Windows IIS	Pág.: 3 of 5

La funcionalidad de msvcr100.dll consiste en descifrar un archivo PE codificado (msvcr100.dat) y la llave que se transmite como un argumento de línea de comandos durante la ejecución de Wordconv.exe, utilizando el algoritmo Salsa20. A continuación, el archivo PE descifrado se ejecuta en la memoria. Posteriormente, se encarga de borrar el módulo DLL malicioso que se cargó mediante la llamada WinAPI de FreeLibraryAndExitThread antes de eliminarse (msvcr100.dll).

Msvcr100.dll es muy similar al malware cylvc.dll cubierto en la publicación del blog de ASEC. “Un caso de infección de malware por parte del grupo de ataque Lazarus que desactiva programas antimalware con la técnica BYOVD”, que se lanzó en 2022. Por lo tanto, los investigadores de ASEC consideran que msvcr100.dll es una variante de malware de cylvc.dll.

De manera similar a msvcr100.dll, cylvc.dll descifra los archivos de datos con la extensión .dat usando el algoritmo Salsa20 antes de ejecutar el archivo PE dentro del espacio de memoria

2. Establecimiento de puntos de apoyo y robo de certificados

Después de la infiltración inicial, el actor de amenazas estableció un punto de apoyo antes de crear malware adicional (diagn.dll) al explotar el "**complemento selector de color**" de código abierto , que es un complemento para Notepad ++.

Diagn.dll es responsable de recibir el archivo PE codificado con el algoritmo RC6 como un valor de argumento de ejecución antes de usar una clave codificada internamente para descifrar el archivo de datos y ejecutar el archivo PE en la memoria, se sospecha que el actor de amenazas ha ejecutado una herramienta de robo de credenciales como Mimikatz.

3. Movimiento lateral

Después de adquirir las credenciales del sistema, el actor de amenazas realiza un reconocimiento interno antes de utilizar el acceso remoto (puerto 3389) para realizar un movimiento lateral hacia la red interna. No se han descubierto más actividades maliciosas por parte del actor de amenazas desde entonces.



<https://www.ecucert.gob.ec>



@EcuCERT_EC

Agencia de Regulación y Control de las Telecomunicaciones

Dirección: Av. Amazonas N40-71 y Gaspar de Villaruel


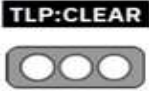
Código postal: 170501 / Quito-Ecuador

Teléfono: 593-2 2271 180

www.arcotel.gob.ec



República del Ecuador

Nro. Alerta:	AL-2023-024	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	 ALERTAS DE SEGURIDAD
TLP:			
Fecha:	05-junio-2023	Vulnerabilidad servidores web de Microsoft Windows IIS	V 1.1 Pág.: 4 of 5

IV. VECTOR DE ATAQUE:

Servidores IIS vulnerables, o mal administrados/configurados.

V. IMPACTO:

Exfiltración de información y el movimiento lateral
 Comportamientos maliciosos a través de w3wp.exe.

VI. INDICADORES DE COMPROMISO

[Detección de archivos]

- Trojan/Win.LazarLoader.C5427612 (2023.05.15.02)
- Trojan/Win.LazarLoader.C5427613 (2023.05.15.03)

[IOC]

- [Ruta del archivo de carga lateral de DLL]
- C:\ProgramData\USOShared\Wordconv.exe
 - C:\ProgramData\USOShared\msvcr100.dll

[MD5]

- e501bb6762c14baafadbde8b0c04bbd6: diagn.dll
- 228732b45ed1ca3cda2b2721f5f5667c: msvcr100.dll
- 47d380dd587db977bf6458ec767fee3d: ? (Variante de malware de msvcr100.dll)
- 4d91cd34a9aae8f2d88e0f77e812cef7: cylvc.dll (Variante de malware de msvcr100.dll)

VII. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo:

- Revisar y analizar las configuraciones de los *servidores web Windows IIS*, es importante protegerlos, para evitar dejarlos vulnerables.
- Utilizar la administración de la superficie de ataque para identificar los activos que podrían estar expuestos a los actores de amenazas y actuar con precaución al aplicar los parches de seguridad más recientes siempre que sea posible.
- Mantener actualizado el software del sistema operativo y las aplicaciones, pero actuar con precaución al aplicar los parches de seguridad, y utilizar los más recientes siempre que sea posible.
- Instalar un software antivirus y mantenerlo actualizado.
- Configurar el firewall del sistema para bloquear el tráfico malicioso.



<https://www.ecucert.gob.ec>



@EcuCERT_EC

Agencia de Regulación y Control de las Telecomunicaciones

Dirección: Av. Amazonas N40-71 y Gaspar de Villaruel



Código postal: 170501 / Quito-Ecuador

Teléfono: 593-2 2271 180

www.arcotel.gob.ec



República del Ecuador

Nro. Alerta:	AL-2023-024	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
Fecha:	05-junio-2023	ALERTAS DE SEGURIDAD	V 1.1
Vulnerabilidad servidores web de Microsoft Windows IIS			Pág.: 5 of 5

- Realizar copias de seguridad de forma periódica.
- Monitorear de manera proactiva las relaciones de ejecución de procesos anormales y tomar medidas preventivas para evitar que el grupo de amenazas lleve a cabo actividades como la exfiltración de información y el movimiento lateral

Con estas recomendaciones de seguridad, se puede minimizar las posibilidades de ser una víctima, las recomendaciones no garantizan la seguridad, pero ayudan a reducir el riesgo.

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:

- Asec. (2023). Warning for MagicLine4NX (Certificate Solution) Vulnerability and Update Recommended. *ASEC BLOG*. <https://asec.ahnlab.com/en/50606/>
- Jcleebobgatenet. (2022). A Case of Malware Infection by the Lazarus Attack Group Disabling Anti-Malware Programs With the BYOVD Technique. *ASEC BLOG*. <https://asec.ahnlab.com/en/40830/>
- Muhan. (2023). Lazarus Group Targeting Windows IIS Web Servers. *ASEC BLOG*. <https://asec.ahnlab.com/en/53132/>
- Muhan. (2023b). Lazarus Group Targeting Windows IIS Web Servers. *ASEC BLOG*. <https://asec.ahnlab.com/en/53132/>
- Paganini, P. (2023, May 25). *North Korea-linked Lazarus targets Microsoft IIS servers*. Security Affairs. <https://securityaffairs.com/146639/hacking/lazarus-targets-microsoft-iis-servers.html>