DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°208**	**Fecha: 04-09-2023**
		Página: 7 de 14

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Nueva campaña de ransomware FreeWorld dirigido a servidores Microsoft SQL		
Tipo de Ataque	Ransomware	Abreviatura	Ransomware
Medios de propagación	Correo electrónico, redes sociales, entre otros		
Código de familia	C	Código de Sub familia	C01
Clasificación temática familia	Código malicioso		

Descripción

1. ANTECEDENTES:

Investigadores de la empresa de ciberseguridad SecuronixSe, han detectado una nueva campaña de distribución de malware que han denominado "DB#JAMMER", dirigido a servicios expuestos de servidores Microsoft SQL mediante ataques de fuerza bruta, para distribuir cargas útiles de Cobalt Strike y una cepa de ransomware llamada "FreeWorld". Un taque exitoso podría permitir a un actor de amenazas cifrar los datos de la víctima y pedir rescates por descifrarlos.

2. DETALLES:

SecuronixSe indicó que los actores de amenazas están explotando activamente servidores Microsoft SQL vulnerables o sin parchar, para distribuir la carga útil de Cobalt Strike y una cepa de ransomware llamada "FreeWorld".

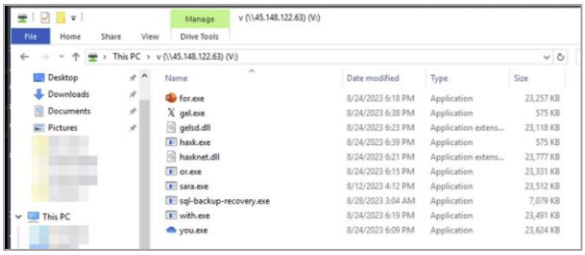
La empresa de ciberseguridad señalo, que la campaña "DB#JAMMER" se destaca por la forma en que se utilizan la infraestructura de herramientas y las cargas útiles del atacante. Algunas de estas herramientas incluyen software de enumeración, cargas útiles RAT, software de explotación y robo de credenciales y, finalmente, cargas útiles de ransomware. La carga útil de ransomware elegida parece ser una variante más nueva de ransomware Mimic llamada "FreeWorld". El texto de FreeWorld estaba presente en los nombres de los archivos binarios, así como en las extensiones de ransomware.

El ransomware "FreeWorld" parece ser una variante de ransomware Mimic, ya que sigue muchos TTP similares para llevar a cabo sus objetivos. Ambas variantes parecen abusar de la aplicación legítima Everything para consultar y localizar archivos de destino que se van a cifrar.

En esta campaña, los actores de amenazas apuntaron a un servidor MS SQL y pudieron obtener un punto de apoyo en la ejecución de código en el host, utilizando la función xp_cmdshell habilitada, presente en el servidor. Una vez explotados, los atacantes enumeran el sistema y ejecutan comandos de shell para debilitar las defensas y desplegar herramientas que ayuden a establecer la persistencia en el equipo de la víctima a través de Ngrok. Ngrok permite eludir el firewall al ejecutar un servicio en el host de la víctima. Se proporciona al atacante una IP pública y un puerto para conectarse.

SecuronixSe, indico que, de acuerdo con el análisis realizado, se determinó que el acceso inicial al equipo de la víctima se logra mediante un ataque de fuerza bruta en el servidor MS SQL, que lo usa para enumerar la base de datos, centrándose especialmente en otras credenciales de inicio de sesión y aprovechar la opción de configuración xp_cmdshell para ejecutar comandos de shell y realizar reconocimiento.

Asimismo, en la siguiente etapa, se trataría de tomar acciones para dañar el firewall del sistema y establecer la persistencia, conectándose para ello a un recurso compartido SMB remoto y transferir archivos hacia y desde el sistema de la víctima, así como instalar herramientas maliciosas como Cobalt Strike. Esto, a su vez, prepara el camino para que la distribución del software AnyDesk impulse en última instancia el ransomware "FreeWorld", no sin antes llevar a cabo un paso de movimiento lateral. AnyDesk es un servicio legítimo que funciona como una RAT.



Contenido de la carpeta compartida SMB

El recurso compartido de red permitió al atacante transferir archivos hacia y desde el sistema víctima, así como instalar herramientas maliciosas.

A. Productos afectados:

- Múltiples versiones de servidores Microsoft SQL.

B. Indicadores de compromiso (IoC):

Nombre del archivo	SHA256
svr.exe	8937A510446ED36717BB8180E5E4665C0C5D5BC160046A31B28417C86FB1BA0F
AD.exe	9D576CD022301E7B0C07F8640BDEB55E76FA2EB38F23E4B9E49E2CDBA5F8422D
n.exe	867143A1C945E7006740422972F670055E83CC0A99B3FA71B14DEABABCA927FE
5000.exe	80BF2731A81C113432F061B397D70CAC72D907C39102513ABE0F2BAE079373E4
FreeWorld.exe	75975B0C890F804DAB19F68D7072F8C04C5FE5162D2A4199448FC0E1AD03690B
DC.exe	C576F7F55C4C0304B290B15E70A638B037DF15C69577CD6263329C73416E490E
Todo.exe	4C83E46A29106AFBAF5279029D102B489D958781764289B61AB5B618A4307405
v.dll	0A2CFFFB353B1F14DD696F8E86EA453C49FA3EB35F16E87FF13ECDF875206897
e3.exe	74CC7B9F881CA76CA5B7F7D1760E069731C0E438837E66E78AEE0812122CB32D
2.exe	947AFAA9CD9C97CABD531541107D9C16885C18DF1AD56D97612DDBC628113AB5
1.exe	95A73B9FDA6A1669E6467DCF3E0D92F964EDE58789C65082E0B75ADF8D774D66
twix.exe	A3D865789D2BAE26726B6169C4639161137AEF72044A1C01647C521F09DF2E16
sara.exe	E93F3C72A0D605EF0D81E2421CCA19534147DBA0DDED2EE29048B7C2EB11B20A
d.dll	CC54096FB8867FF6A4F5A5C7BB8CC795881375031EED2C93E815EC49DB6F4BFF
ahar.exe	68ED5F4B4EABD66190AE39B45FFF0856FBA4B3918B44A6D831A5B9120B48A1E9
sara.exe	42396CE27E22BE8C2F0620EE61611D7F86DFE9543D2F2E2AF3EF5E85613CEE32
italia.dll	F9F6C453DA12C8FF16415C9B696C2E7DF95A46E9B07455CD129CE586B954870D
Egipto.exe	569E3B6EAC58C4E694A000EB534B1F33508A8B5DE8A7AD3749C24727CC878F4D
svr.exe	8937A510446ED36717BB8180E5E4665C0C5D5BC160046A31B28417C86FB1BA0F
Greace.exe	2D27F57B4F193A563443ACC7FE0CBF611F4FF0F1171FCBDF16C3ECEF8F9DBEDB
haxknet.dll	2B68FE68104359E1BC044DB33B4E88B913E4F5BE69DA9FD6E87EA59A50311E6E
gelsd.dll	11259F77F4E477CD066008FBFC7C31D5BBDC9EF708C4B255791EE380999A725C
o.exe	BD1C3303D13CADF8BBD6200597E9D365EC3C05F1F48052CD47DCD69E77C94378
gel.exe	CD5A2EC1A95D754EE5189BFEE6E1F61C76A0A5EE8173DA273E02F24A62FACCFA
para.exe	BEC3F75F638025A5FE3B8D278856FD273999C49AE7543C109205879B59AFC4C3
tu.exe	2AC044936A922455C80E93F76CC3E2CE539FDAB1AF65C0703B57177FEB5326A6
con.exe	FBC9BA3BA7387C38EB9832213B2D87CF5F9FC2BA557E6FDF23556665CA3EF44A
haxk.exe	08F827A63228D7BCD0D02DD131C1AE29BC1D9C3619BE67EA99D8A62440BE57AB

3. RECOMENDACIONES:

- Utilizar contraseñas seguras y complejas, especialmente en servicios expuestos a Internet.
- Limitar el uso del procedimiento almacenado xp_cmdshell, en entornos MS SQL.
- Supervisar los directorios de almacenamiento provisional de malware común, especialmente “C:\Windows\Temp”, que se utilizó en esta campaña de ataque.
- Implementar registros adicionales a nivel de proceso, como registros Sysmon y PowerShell, para obtener cobertura adicional de detección de registros.

Fuente de Información:	• hxxps://www.securonix.com/blog/securonix-threat-labs-security-advisory-threat-actors-target-mssql-servers-in-dbjammer-to-deliver-freeworld-ransomware/