	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°008	Fecha: 09-01-2024
		Página: 5 de 10

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Nueva campaña de ransomware dirigido a servidores Microsoft SQL en América y Europa		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Investigadores de Securonix han detectado una nueva campaña de distribución de malware de tipo ransomware "Mimic", dirigido a servidores de bases de datos Microsoft SQL de organizaciones en EE. UU., Europa y América Latina. Un ataque exitoso podría permitir a un actor de amenazas secuestrar los datos de una persona o empresa y solicitar un pago (generalmente en criptomonedas) para liberar la información que ha sido comprometida.

2. DETALLES:

El equipo de Securonix Threat Research indicó, que han estado monitoreando una nueva campaña de distribución de malware de tipo ransomware "Mimic" denominado RE#TURGENCE, que explota servidores de bases de datos MS SQL para obtener acceso inicial, está dirigido principalmente a organizaciones en EE. UU., Europa y América Latina.

Como vector de acceso inicial, los actores de amenazas utilizan credenciales administrativas de fuerza bruta para Microsoft SQL Server, seguido de la recolección de credenciales y la habilitación de una función que les permitía ejecutar comandos de shell en el host de la víctima.

Los atacantes ejecutan scripts de PowerShell que conducían a una carga útil de Cobalt Strike muy ofuscada que se carga en el proceso en ejecución actual mediante técnicas de reflexión en memoria (PowerShell en este caso). Según la configuración, la baliza Cobalt Strike está configurada para inyectarse en el proceso nativo de Windows SndVol.exe. Este proceso maneja los controles de volumen y la configuración del sistema.

Los operadores del malware utilizan Cobalt Strike para implementar el software de escritorio remoto legítimo "AnyDesk" y usarlo únicamente para futuras interacciones con los sistemas comprometidos.

Por otro lado, los investigadores indicaron que las actividades de seguimiento incluyeron la implementación de Mimikatz para la recolección de credenciales, el uso de Advanced Port Scanner para el descubrimiento de entornos y el uso de la utilidad psexec de Sysinternals para moverse lateralmente a un controlador de dominio, lo que les permitió acceder a otras máquinas en la red. Después de varios intentos más de movimiento lateral, los actores de amenazas implementaron el ransomware "Mimic" como un archivo autoextraíble. Una vez completado el proceso de cifrado, se distribuyó una nota de rescate en forma de archivo de texto.

El ransomware "Mimic" utiliza la aplicación legítima Everything de VoidTools para consultar y localizar los archivos de destino que serán cifrados. Mimic se detectó en enero de 2023 y eliminará los binarios de Everything utilizados para ayudar en el proceso de cifrado. El cuentagotas Mimic en nuestro caso, "red25.exe", eliminó todos los archivos necesarios para que la carga útil principal del ransomware complete sus objetivos.

Los operadores de malware ejecutaron manualmente el ransomware "Mimic" y lo ejecutaron primero en el servidor MS SQL, un controlador de dominio y otros hosts unidos al dominio.

Igualmente, los atacantes habilitaron la función para compartir portapapeles de AnyDesk, lo que permitió a la empresa de ciberseguridad monitorear los contenidos pegados allí, ya que el host comprometido tenía habilitado el monitoreo del portapapeles. Al analizar el contenido pegado, que estaba en turco, e investigar el identificador "atseverse" que apareció allí, Securonix determinó que al menos uno de los atacantes parece estar ubicado en Turquía.

A. Indicadores de compromiso:

URL:
- seruvadessigen.3utilities[.]com.

Dirección IP:
- 45.148.121[.]87 (Cargas útiles para PYMES de Cobalt Strike).
- 88.214.26[.]3 (Cargas útiles de PowerShell de Cobalt Strike).

Archivo / SHA 256:
- ad.bat - 9F3AD476EDA128752A690BD26D7F9A67A8A4855A187619E74422CC08121AD3D3.
- ps1.ps1 - A222BA1FD77A7915A61C8C7A0241222B4AD48DD1C243F3548CAEF23FE985E9C2.
- 1ED02979B3F312C4B2FD1B9CFDFB6BEDE03CD964BB52B3DE017128FE00E10D3C.
- start.bat - F328C143C24AFB2420964740789F409D2792413A5769A33741ED956FCE5ADD3E.
- Ar3.exe - 1C7B82B084DA8B57FFEEF7BDCA955C2AA4A209A96EC70E8D13E67283C10C12A5.
- gui40.exe - 31FEFF32D23728B39ED813C1E7DC5FE6A87DCD4D10AA995446A8C5EB5DA58615.
- advport.exe - D0C1662CE239E4D288048C0E3324EC52962F6DDDA77DA0CB7AF9C1D9C2F1E2EB.
- red25.exe - E9C63A5B466C286EA252F1B0AA7820396D00BE241FB554CF301C6CD7BA39C5E6.
- red.exe - D6CD0080D401BE8A91A55B006795701680073DF8CD7A0B5BC54E314370549DC4.

3. RECOMENDACIONES:

- No exponer servidores críticos directamente a Internet. En el caso de RE#TURGENCE, los atacantes pudieron ingresar directamente por fuerza bruta al servidor desde fuera de la red principal.
- Limitar el uso del procedimiento xp_cmdshell en servidores de bases de datos MS SQL. Esto habría impedido que los atacantes ejecutaran comandos en la máquina de la víctima.
- Habilitar el registro a nivel de proceso en terminales y servidores para mejorar la telemetría, tanto para las detecciones (como software RMM y/o RAT) como para la búsqueda de amenazas.
- Implementar registros adicionales a nivel de proceso, como registros Sysmon y PowerShell, para obtener cobertura adicional de detección de registros.
- Supervisar la creación de nuevos usuarios locales en los puntos finales, especialmente dentro de entornos de servidores críticos.

Fuente de Información:	• hxxps://www.securonix.com/blog/securonix-threat-research-security-advisory-new-returgence-attack-campaign-turkish-hackers-target-mssql-servers-to-deliver-domain-wide-mimic-ransomware/ • hxxps://www.securonix.com/blog/securonix-threat-labs-security-advisory-threat-actors-target-mssql-servers-in-dbjammer-to-deliver-freeworld-ransomware/ • hxxps://www.bleepingcomputer.com/news/security/mysql-servers-targeted-by-ddostf-ddos-as-a-service-botnet/ • hxxps://www.trendmicro.com/en_ph/research/23/a/new-mimic-ransomware-abuses-everything-apis-for-its-encryption-p.html