Cyber Security Warning - Preventive

[CTI] Análisis del Troyano Meterpreter: Explorando su Modus Operandi y Potenciales Impactos

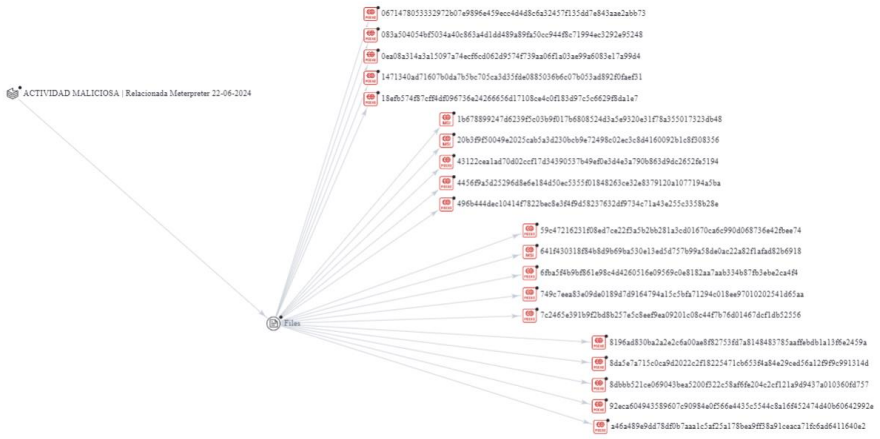
Fecha:	22-06-2024	**TLP:**	Green
Criticidad:	Alto	**Taxonomía:**	Distribución de malware
Tipo de alerta:	Malware, Troyano	**Sectores:**	Empresarial, Financiero, Gobierno, Industrial

Threat Information

Número de IoC:	115	**PAP:**	Green
Familia:	Meterpreter	**Adversario:**	No identificado (bajo seguimiento)

Síntesis

Se ha identificado Meterpreter, un programa malicioso de tipo troyano utilizado por ciberdelincuentes para infiltrarse y tomar control remoto de computadoras infectadas. Una vez que Meterpreter compromete un sistema, permite a los atacantes una variedad de acciones destructivas, como la transferencia furtiva de archivos, la ejecución de comandos maliciosos y la captura de información confidencial como contraseñas y datos financieros. Este malware opera de manera sigilosa en la memoria del sistema, evitando dejar rastros en el disco duro y dificultando su detección por parte de herramientas de seguridad convencionales.



Si requiere verificar el reporte Inicial realizado a esta actividad puede verificarlo aquí.

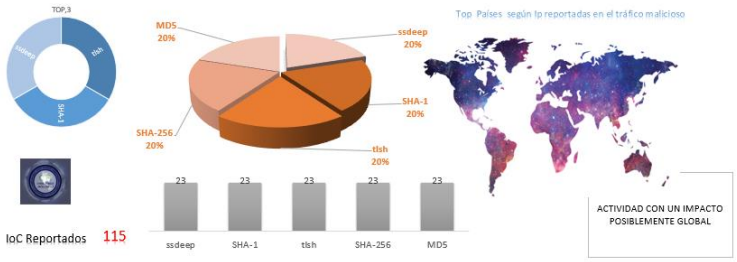
Las fases de acción de Meterpreter, son las siguientes:

1. **Infección inicial:** Meterpreter infecta inicialmente la computadora objetivo a través de métodos como correos electrónicos con documentos maliciosos adjuntos, descargas de software comprometido u otras vulnerabilidades de seguridad explotadas.
2. **Establecimiento de persistencia:** Una vez dentro del sistema, Meterpreter puede establecer mecanismos para asegurar que el malware persista incluso después de reinicios del sistema. Esto puede incluir la modificación de registros, la creación de tareas programadas o la inserción en puntos de inicio del sistema operativo.
3. **Comunicación encubierta:** Utiliza técnicas avanzadas de comunicación, como el cifrado de tráfico, para mantener la comunicación encubierta con el servidor controlado por el atacante, lo que dificulta la detección por parte de herramientas de seguridad.
4. **Control remoto:** Proporciona a los atacantes un control completo sobre la computadora comprometida, permitiéndoles ejecutar comandos arbitrarios, manipular archivos, modificar configuraciones del sistema y realizar otras acciones sin la interacción del usuario.

5. **Captura de información sensible:** Meterpreter puede realizar capturas de pantalla de la computadora infectada y registrar pulsaciones de teclas, lo que permite a los atacantes obtener información confidencial como contraseñas, datos financieros y otra información personal.
6. **Transferencia de archivos:** Facilita la transferencia de archivos entre el sistema comprometido y el servidor controlado por el atacante, lo que permite la descarga e instalación de software adicional, como ransomware u otros tipos de malware.
7. **Explotación de vulnerabilidades:** Meterpreter puede ser utilizado para explotar vulnerabilidades adicionales en el sistema operativo o aplicaciones instaladas, ampliando así el acceso y control sobre la infraestructura de TI de la víctima.

CAPACIDADES (Meterpreter):

- Control remoto completo de computadoras infectadas.
- Transferencia bidireccional de archivos.
- Ejecución de comandos arbitrarios en el sistema comprometido.
- Captura de pantallas del escritorio.
- Registro de pulsaciones de teclas (keylogging).
- Persistencia en el sistema después de reinicios.
- Comunicación cifrada para evitar detección.



NOTA:

Es importante tener en cuenta que esta descripción se basa en la información proporcionada por la fuente inicial y el equipo de CTI mantiene bajo seguimiento continuo este tipo de ataque, tan pronto se tenga mejor o mayor informacion de este su entidad será notificada.

De igual manera, cabe señalar que se debe tener precaución al momento de trabajar con las direcciones IP reportadas en el listado de IoC, ya que podrían pertenecer a algún servicio oficial que se reporta debido a que ha tenido comunicación maliciosa con los Hash relacionados. Si se bloquean en un firewall, podría afectar el funcionamiento de algunos de sus servicios internos.

Dado que no tenemos acceso a sus infraestructuras, no podemos identificar dicha relación. Por lo tanto, se recomienda verificar las IP antes de proceder con el bloqueo.

Técnicas y tácticas identificadas

TÁCTICAS:
TA0001 Initial Access: https://attack.mitre.org/tactics/
TA0002 Execution: https://attack.mitre.org/tactics/
TA0003 Persistence: https://attack.mitre.org/tactics/

TÉCNICAS:
T1056 Input Capture: https://attack.mitre.org/techniques/enterprise/
T1027 Obfuscated Files or Information: https://attack.mitre.org/techniques/enterprise/
T1057 Process Discovery: https://attack.mitre.org/techniques/enterprise/

SUBTÉCNICAS:
T1027.002 - Software Packing: https://attack.mitre.org/techniques/enterprise/
T1027.003 - Steganography: https://attack.mitre.org/techniques/enterprise/
T1027.010 - Command Obfuscation: https://attack.mitre.org/techniques/enterprise/
T1056.001 - Keylogging: https://attack.mitre.org/techniques/enterprise/
T1056.002 - GUI Input Capture: https://attack.mitre.org/techniques/enterprise/
T1056.003 - Web Portal Capture: https://attack.mitre.org/techniques/enterprise/

PLATAFORMAS:
Windows
Linux
MacOS
Network

CÓDIGO CAPEC:
CAPEC-268 Audit Log Manipulation
CAPEC-234 Hijacking a privileged process
CAPEC-109 Object Relational Mapping Injection

CÓDIGO DATA SOURCE:
DS0004 Malware Repository
DS0037 Certificate
DS0023 Named Pipe

Mitigaciones

M1036 - Account Use Policies:
Configurar políticas relacionadas con el uso de cuentas, como bloqueos por intentos de inicio de sesión, horarios específicos de inicio de sesión, etc.

M1049 - Antivirus/Antimalware:
Utilizar firmas o heurísticas para detectar software malicioso.

M1040 - Behavior Prevention on Endpoint:
Utilizar capacidades para prevenir patrones de comportamiento sospechosos en sistemas finales.

M1047 - Audit:
Realizar auditorías o escaneos de sistemas, permisos, software inseguro, configuraciones inseguras, etc.

M1037 - Filter Network Traffic:
Utilizar dispositivos de red para filtrar tráfico de entrada o salida y realizar filtrado basado en protocolos. Configurar software en puntos finales para filtrar tráfico de red.

M1051 - Update Software:
Realizar actualizaciones regulares de software para mitigar el riesgo de explotación.

Impacto y recomendaciones

IMPACTO / ANÁLISIS
La presencia de Meterpreter en un sistema comprometido puede tener consecuencias devastadoras. Los atacantes pueden acceder de manera remota y furtiva al sistema infectado, permitiéndoles robar información sensible como contraseñas, datos financieros y documentos personales. Además, Meterpreter facilita la instalación de malware adicional, como ransomware, exacerbando los daños económicos y reputacionales al cifrar datos críticos y exigir rescates. El control remoto completo otorgado por Meterpreter permite a los atacantes modificar configuraciones del sistema, interrumpir operaciones normales y comprometer redes adicionales dentro de una organización. La capacidad de capturar pantallas y registrar pulsaciones de teclas compromete la privacidad de usuarios y empresas, potencialmente exponiendo datos que podrían ser utilizados para extorsión o chantaje.

MNEMO / DETECCIÓN:

1. Monitoreo de Tráfico de Red: Implementar herramientas de monitoreo que analicen patrones anómalos de tráfico de red, especialmente comunicaciones cifradas sospechosas utilizadas por Meterpreter.
2. Análisis de Comportamiento de Procesos: Utilizar soluciones de análisis de comportamiento para identificar procesos que operan inusualmente en la memoria sin tocar el disco duro, característico de Meterpreter.
3. Auditorías de Acceso y Cambios: Realizar auditorías regulares para detectar cambios no autorizados en configuraciones del sistema y accesos a archivos críticos.
4. Detección de Firmas Maliciosas: Configurar sistemas de detección de intrusos (IDS) y sistemas antivirus para identificar firmas y comportamientos maliciosos asociados con Meterpreter.
5. Análisis Forense de Memoria: Realizar análisis forense de la memoria del sistema para identificar residuos de actividad de Meterpreter, que podrían indicar una infección persistente.

MITRE / MITIGACIÓN:

- Concientización y Capacitación del Usuario: Educar a los usuarios sobre prácticas seguras de navegación web y reconocimiento de correos electrónicos maliciosos que podrían distribuir Meterpreter.
- Políticas de Uso de Dispositivos USB: Implementar políticas que limiten el uso de dispositivos USB no autorizados para prevenir la introducción inadvertida de malware.
- Actualizaciones de Software y Parches: Mantener actualizado el software y aplicar parches de seguridad regularmente para mitigar vulnerabilidades que podrían ser explotadas por Meterpreter.
- Estrategias de Respuesta a Incidentes: Desarrollar y mantener un plan de respuesta a incidentes que incluya la detección temprana y la respuesta rápida a posibles infecciones por Meterpreter.
- Segmentación de Redes: Segmentar la red corporativa para limitar la propagación de Meterpreter en caso de una infección inicial, aislando sistemas críticos y reduciendo el impacto potencial de un compromiso.

Referencias

https://darfe.es/ciberwiki/index.php?title=Meterpreter
https://www.alertasyseguridad.net/
https://www.virustotal.com/
https://otx.alienvault.com/
https://attack.mitre.org/