ALERTA DE SEGURIDAD CIBERNÉTICA
AGENT TESLA

El CSIRT de Gobierno informa sobre un prominente RAT, denominado Agent Tesla, sus características y las mejores formas de evitar su accionar sobre los sistemas. Se debe tener en consideración que estas características y modus operandi podrían variar y evolucionar desde la redacción de este documento. De encontrarse indicios de una infección por Agent Tesla o cualquier otro RAT, estos deben ser eliminados de sus sistemas tan rápido como sea posible.

Descripción

Agent Tesla es una amenaza de tipo troyano de acceso remoto, o **RAT**, por su sigla en inglés. También se cuenta dentro del **"Malware as a Service"**, o sea, malware que cualquier ciberdelincuente puede comprar listo para usar e incluso conseguirlo como una suscripción, hasta con soporte 24/7.

Está destinado principalmente a robar información de sus víctimas. Contempla varias capas de ofuscación, lo que le hace difícil de detectar (por ejemplo, puede detectar si está siendo abierta en una sandbox) y además despliega técnicas para ser una amenaza persistente, todas características que explican su extendida popularidad, siendo que data de 2014.

Capacidades

- Una vez desplegado, Agent Tesla realiza numerosas operaciones de espionaje en un equipo:
    - Registra lo que se digita (keylogging).
    - Toma capturas de pantalla.
    - Ve y copia lo que hay en el Portapapeles.
    - Roba contraseñas y cookies de múltiples programas, incluyendo:
        - Decenas de buscadores web, incluyendo Google Chrome, Microsoft Edge, Mozilla Firefox y Opera.
        - VPN como Open VPN y NordVPN.
        - Microsoft Outlook
    - Recopila información como nombre del equipo, sistema operativo, CPU, RAM, TCP hostname, cliente DNS, IP pública, dominio y más.
- Luego de tomar esta información, Agent Tesla la filtra al ciberdelincuente, comunicación que mantiene anónima usando un cliente TOR. Del mismo modo se comunica con su servidor de comando y control.
- También puede comunicarse con el atacante a través del protocolo SMTP de correo electrónico, o incluso por Telegram.

- Persistencia: Agent Tesla puede incorporarse a Registry como programa de inicio para establecer su persistencia, ya que así el RAT se inicia cada vez que se reinicie el equipo.

Técnicas de despliegue

- Se realiza principalmente a través de correos de phishing, los que traen adjuntos de cualquier tipo, incluyendo los más tradicionales, como archivos comprimidos, ejecutables y documentos de Office.
- También pueden descargarse a través de Torrent, páginas web falsas o avisos maliciosos que contengan el troyano.
- Muchas veces el engaño es, irónicamente, la oferta de una actualización o programa de seguridad. Es importante siempre descargar nuestras actualizaciones de los sitios oficiales de los proveedores de software.

Indicadores de Compromiso (IOC)

Sender de Correo

3.133.219.78

9ecf32d40c78a12f43bad7283ac48a98fcdbe1f8dec70fda7df32396f0b69cbf

efac67b547566d4257e435b854da761a1f6892aef4da1c0faed3780c486a25e2

d7dc14b7811f44ecfe82059fcce4300044d34eb9a1e6cba4d25ade821294c809

250dba6f1c65b7e40d352be174ebde12de162ef61ad9be23ac155b6f0a088c5b

7a2a8ba85c73c9b5179cfe2c1598b14b774f7817a935af6d824fb39f2eea1d09

4196ac36c2e960a9c3b602394b6867e9503417a265c48552a8d5c0cfe4d17231

46c460618cb9a10c78dfaedc27e188dcc393589187d751be6e5b1183c5720e70

3d5a618b9509b6a8426aa13d8a32aa4156c4e1aa3b20ac98ab3a0fd449088d66

URL

https://terrazzaitaliana.mx/hrt/Gxuvqbqz_Skhciiey[.]bmp

Recomendaciones

- Mantener todos sus programas y especialmente antivirus, antimalware, firewall y otros software de seguridad actualizados, junto con mantener un esquema de parchados regulares.
- Reforzar todas las protecciones que debemos tener ante el phishing, principalmente nunca hacer clic en enlaces provenientes de mensajes no solicitados de email, SMS o redes sociales.

    - Revisar que el mensaje provenga realmente de quien dice venir y si hay dudas llamar directamente al remitente para saber si el mensaje es real.
    - Fijarse en la extensión del archivo. La última porción es la que determina de qué tipo de archivo se trata. Si dice .pdf.exe, por ejemplo, significa que es un archivo ejecutable.
    - Tampoco ingresar sus credenciales a un sitio abierto desde un enlace. Mejor abrir directamente la página que queremos escribiendo su dirección en el navegador.
- No hacer descargas de archivos sospechosos, como películas o juegos piratas.
- Desactivar los macros en documentos que llegan por email.
- Evitar entregar privilegios de Administrador a usuarios, y solo acceder a como Administrador a los equipos por el tiempo que sea necesario. Evitar abrir documentos mientras se está loggeado como Administrador.

Por otra parte, compartimos regularmente las vulnerabilidades más relevantes en https://www.csirt.gob.cl/vulnerabilidades/. Recomendamos revisar este sitio al menos diariamente.

Fuentes:

- https://www.welivesecurity.com/la-es/2021/04/28/agent-tesla-principales-caracteristicas-este-malware/
- https://attack.mitre.org/software/S0331
- https://blog.qualys.com/vulnerabilities-threat-research/2022/02/02/catching-the-rat-called-agent-tesla
- https://www.riskiq.com/blog/external-threat-management/agent-tesla-trend-analysis/
- https://news.sophos.com/en-us/2021/02/02/agent-tesla-amps-up-information-stealing-attacks/
- https://malpedia.caad.fkie.fraunhofer.de/details/win.agent_tesla

Color	¿Cuándo se debe usar?	¿Cómo se puede compartir?
TLP: ROJO - No es para divulgación, restringida solo a los participantes.	Se debe utilizar "TLP: ROJO "cuando la información está limitada a personas concretas, y podría tener impacto en la privacidad, reputación u operaciones si es mal utilizada.	Los receptores no deben compartir información designada como "TLP: ROJO "con ningún tercero fuera del ámbito donde fue expuesta originalmente. En la mayoría de las circunstancias, TLP:RED debe intercambiarse verbalmente o en persona.
TLP: ÁMBAR - Divulgación limitada, restringida a las organizaciones de participantes.	Se debe utilizar "TLP: AMBAR" cuando la información requiere ser distribuida de forma limitada, pero supone un riesgo para la privacidad, reputación u operaciones si es compartida fuera de la organización.	Los receptores pueden compartir información indicada como "TLP: AMBAR" únicamente con miembros de su propia organización que necesitan conocerla, y con clientes, proveedores o asociados que necesitan conocerla para protegerse a sí mismos o evitar daños. El emisor puede especificar restricciones adicionales para compartir esta información.
TLP: VERDE - Divulgación limitada, restringida a la comunidad.	Se debe utilizar "TLP: VERDE" cuando la información es útil para todas las organizaciones que participan, así como con terceros de la comunidad o del sector	Los receptores pueden compartir la información indicada como "TLP: VERDE" con organizaciones afiliadas o miembros del mismo sector, pero nunca a través de canales públicos.
TLP: BLANCO - La divulgación no está limitada.	Se debe utilizar "TLP: BLANCO" cuando la información no supone ningún riesgo de mal uso, dentro de las reglas y procedimientos establecidos para su difusión pública.	La información "TLP: BLANCO" puede ser distribuida sin restricciones, sujeta a controles de Copyright.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.06.02 11:53:07 -04'00'