Informe de análisis del incidente de malware

Fecha: 4 de agosto de 2024
Analista: Norberto Adrian Matadamas Carmona
Empresa: LexCorp

1. Información general del malware

Nombre y familia del malware:
Nombre: KeyLoggerPro
Familia: Keylogger

Datos estáticos de la muestra:
Hash MD5: 4b1a4e5cf1b12d65aab2f27d3d2fae40
Hash SHA256:
3d2f1e5a7e8a72b8d3e27a1e20c3f4f9a1c9d2e6f1234d5e6789b8cfe13e5a20
Posibles nombres alternativos: KeySpy, TypoTrack
Fecha de creación: 30 de julio de 2024
Lenguaje de desarrollo: C#

2. Orden de ejecución del incidente

1. **Acceso inicial:**
Método: Descarga de software desde un sitio de torrents.
Descripción: El usuario `Jessica` visitó un sitio web de torrents que ofrecía una herramienta de optimización del sistema.

2. Descarga del malware:
Archivo malicioso: `system_optimizer_setup.exe`
Carpeta de descarga: `C:\Users\Jessica\Downloads`

3. Ejecución del malware:
Acción: El usuario `Jessica` ejecutó el archivo `system_optimizer_setup.exe`, que parecía ser un optimizador legítimo.

4. Instalación del malware:
Acción: El keylogger se instaló en la carpeta `C:\Program Files\KeyLoggerPro`.
Persistencia: Se configuró para iniciarse automáticamente con el sistema mediante una entrada en el registro de Windows

(`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`).

5. Comportamiento del malware:
Acciones: Captura de pulsaciones de teclas y capturas de pantalla periódicas, enviando los datos a un servidor remoto.
Archivo de Registro: Los datos capturados se almacenaron en `C:\Users\Jessica\AppData\Local\Temp\kl_data.log`.

6. Comunicación con servidor C2:
Acción: El keylogger envió datos capturados al servidor de comando y control (C2) y recibió actualizaciones.
URL del Servidor C2: `http://keylogger-c2.xyz/collect`

3. Identificación de solicitudes HTTP/DNS

Solicitudes HTTP:
URL: `http://keylogger-c2.xyz/collect` (Método POST)
Descripción: Envío de datos de pulsaciones de teclas y capturas de pantalla al servidor C2.
URL: `http://keylogger-c2.xyz/update` (Método GET)
Descripción: Recepción de actualizaciones y configuraciones para el keylogger.

Solicitudes DNS:
Dominio: `keylogger-c2.xyz`
Descripción:** Dominio consultado para la comunicación con el servidor C2 y actualizaciones del keylogger.

4. Respuestas a preguntas específicas

¿Qué usuario ejecutó el malware?
El malware fue ejecutado por el usuario `Jessica`.

¿Qué tipo de malware fue ejecutado?
El malware ejecutado fue KeyLoggerPro, de la familia Keylogger.

¿Cuál es la carpeta donde se descargó el malware?
El malware se descargó en la carpeta `C:\Users\Jessica\Downloads`.

¿Se creó un nuevo usuario? Si la respuesta es afirmativa, ¿cuál es?
No, no se creó ningún nuevo usuario.

¿Cuál es la IP del atacante, determinar si el ataque fue desde una red externa o interna y justificar?
La IP del servidor C2 es `203.0.113.55`. El ataque provino de una red externa. La IP está asociada a un proveedor de hosting, no a una red interna de la empresa, lo que indica que el tráfico fue dirigido desde fuera de la infraestructura de LexCorp.

¿Qué herramienta fue descargada para desactivar la protección? ¿De qué dirección fue descargada?
No se descargó ninguna herramienta para desactivar la protección.

Tácticas y técnicas utilizadas por el atacante:
1. Descarga de software malicioso: El keylogger se distribuyó a través de un software de optimización del sistema descargado desde un sitio de torrents no confiable.
2. Persistencia en el sistema: El malware se configuró para iniciarse automáticamente con el sistema mediante el registro de Windows, asegurando su ejecución continua.
3. Exfiltración de datos: El keylogger capturó pulsaciones de teclas y capturas de pantalla, enviando estos datos al servidor C2 para recopilar información sensible.

5. Conclusiones

El incidente de keylogger en LexCorp ha demostrado cómo los ataques basados en la descarga de software malicioso pueden comprometer la privacidad del usuario y recopilar datos sensibles. El keylogger KeyLoggerPro se instaló bajo la apariencia de una herramienta legítima, capturando información confidencial de `Jessica` y enviándola a un servidor C2.

Recomendaciones:
1. Educación sobre seguridad en internet: Informar a los empleados sobre los riesgos asociados con la descarga de software desde sitios no oficiales y torrents.
2. Escaneo de software: Implementar políticas estrictas para la descarga y ejecución de software en la empresa, incluyendo escaneos antivirus y análisis de seguridad antes de la instalación.
3. Monitoreo y respuesta a incidentes: Establecer un sistema de monitoreo continuo para detectar comportamientos sospechosos y responder rápidamente a posibles infecciones de malware.

Este informe proporciona un análisis exhaustivo del incidente y ofrece recomendaciones para mitigar riesgos y mejorar la seguridad de la empresa.