ATAQUE DE FICKLE STEALER EN MICROSOFT WINDOWS

Entrega

La entrega de Fickle Stealer se realiza a través de cuatro métodos diferentes: cuentagotas VBA, descargador VBA, descargador de enlaces y descargador de ejecutables. Estos métodos se utilizan para descargar un script de PowerShell que se encarga de realizar el trabajo preparatorio antes de ejecutar la carga útil Packer and Stealer. El primer método, cuentagotas VBA, utiliza un documento de Word con una macro VBA que carga un archivo XML y ejecuta un script codificado con Windows Script Encoder. El segundo método, descargador VBA, también utiliza un documento de Word, pero en este caso descarga directamente el archivo u.ps1. El tercer método, descargador de enlaces, descarga el archivo bypass.ps1 directamente. Por último, el descargador de ejecutables es un archivo ejecutable de DotNet que se hace pasar por un visor de PDF y descarga la carga útil. Estos métodos de entrega demuestran la complejidad y flexibilidad de Fickle Stealer para elegir su objetivo.

Trabajo preparatorio

Antes de ejecutar la carga útil Packer and Stealer, Fickle Stealer realiza una serie de tareas preparatorias. Estas tareas se llevan a cabo a través de archivos de script como Bypass.ps1/u.ps1, Falso WmiMgmt.msc y HttpListener. El objetivo principal de estos scripts es omitir el Control de cuentas de usuario (UAC) y ejecutar Fickle Stealer. Para lograr esto, se crea una nueva tarea que ejecuta Engine.ps1 después de 15 minutos. Además, se utiliza una técnica llamada Método simulado de directorios confiables, donde se coloca una copia falsa de WmiMgmt.msc en una ruta diferente para engañar al sistema y obtener los derechos de administrador necesarios. También se utiliza un objeto Shockwave Flash del control ActiveX para abrir un navegador web y descargar la carga útil. Estas tareas preparatorias demuestran la complejidad y sofisticación de Fickle Stealer en su objetivo de robar información valiosa.

Proceso de solicitud de evaluación

Durante el proceso de solicitud de evaluación, al convertir una cadena se elimina el espacio final después de "Windows". Esta acción puede parecer insignificante, pero tiene un impacto importante en la ejecución de WmiMgmt.msc. Al ser considerado como ejecutado desde una ruta confiable, este archivo se ejecuta con autenticación elevada, lo que permite al atacante acceder a información confidencial sin ser detectado. Además, es importante destacar que MMC busca en el archivo MSC los idiomas locales, y si no los encuentra, intenta encontrar uno para en-US. Esto significa que cuando Fickle Stealer ejecuta la copia de WmiMgmt.msc, se ejecuta el WmiMgmt.msc falso, con autenticación elevada y sin mostrar ningún mensaje UAC. Es importante tener en cuenta que el nivel de prioridad para los idiomas es crucial en este proceso, como se ilustra en el ejemplo del código de idioma chino (Taiwán), o zh-TW. MMC primero intenta encontrar el archivo en la carpeta zh-TW, luego en la carpeta zh-Hant, luego en la carpeta zh, luego en-US y en, y finalmente en la carpeta principal System32. Esto demuestra la importancia de tener en cuenta todos los detalles en el proceso de solicitud de evaluación para evitar posibles vulnerabilidades.

Ejecución de WmiMgmt.msc falso

Una de las principales preocupaciones en el proceso de solicitud de evaluación es la ejecución de archivos falsos, como en el caso de WmiMgmt.msc. Al ser considerado como ejecutado desde una ruta confiable, este archivo se ejecuta con autenticación elevada, lo que permite al atacante acceder a información confidencial sin ser detectado. Además, al no mostrar ningún mensaje UAC, el usuario no tiene forma de saber que se está ejecutando un archivo falso. Es importante destacar que el nivel de prioridad para los idiomas es crucial en este proceso, como se ilustra en el ejemplo del código de idioma chino (Taiwán), o zh-TW. MMC primero intenta encontrar el archivo en la carpeta zh-TW, luego en la carpeta zh-Hant, luego en la carpeta zh, luego en-US y en, y finalmente en la carpeta principal System32. Esto demuestra la importancia de tener en cuenta todos los detalles en el proceso de solicitud de evaluación para evitar posibles vulnerabilidades.

Funcionamiento de Engine.ps1 e inject.ps1

Engine.ps1 e inject.ps1 son dos componentes clave en el funcionamiento de Fickle Stealer. Engine.ps1 se encarga de enumerar los archivos exe en diferentes ubicaciones, como C:\Users\, D:\, E:\ y F:\. Una vez que encuentra un archivo, ejecuta inject.ps1, que se encarga de inyectar el código de shell. Este código simplemente ejecuta u.ps1 desde Internet, lo que permite al atacante acceder a información confidencial de la víctima. Es importante destacar que las rutas de los archivos inyectados están codificadas en base64 y escritas en C:\Users\Public\prepares.dat para evitar la doble inyección. Esto demuestra la complejidad y sofisticación de Fickle Stealer en su funcionamiento.

Funcionamiento de tgmes.ps1

Otra técnica utilizada por Fickle Stealer para mantenerse oculto y enviar información a los atacantes es tgmes.ps1. Este componente se encarga de enviar mensajes al bot de Telegram del atacante para mostrar su condición actual. Para lograr esto, descarga tgmes.ps1 a la carpeta Temp con un nombre de archivo aleatorio y lo ejecuta con el mensaje como argumento. Luego, tgmes.ps1 se elimina inmediatamente para no dejar rastros. Además de los mensajes, tgmes.ps1 también envía información de la víctima, como el país, la ciudad, la dirección IP, la versión del sistema operativo, el nombre de la computadora y el nombre de usuario, al bot de Telegram. Esta técnica demuestra la complejidad y sofisticación de Fickle Stealer en su funcionamiento.

Protección de Fickle Stealer mediante un empaquetador

Para evitar ser detectado por herramientas de análisis, Fickle Stealer utiliza un empaquetador disfrazado de ejecutable legal. Esto significa que el código malicioso se oculta dentro de un archivo aparentemente legítimo, lo que dificulta su detección. Además, el empaquetador modifica la función __cinit en la rutina de inicialización, lo que puede confundir a los analistas y hacer que pasen por alto el código malicioso. También es importante destacar que el código malicioso se ejecuta antes de la función WinMain, que suele ser el punto de entrada proporcionado por el usuario para una aplicación GUI C/C++. Esto puede pasar desapercibido para aquellos que siguen las reglas de análisis típicas, lo que demuestra la complejidad y sofisticación de Fickle Stealer en su protección.

Flujo de ejecución de Fickle Stealer

El flujo de ejecución de Fickle Stealer comienza con la creación de un mutex para evitar una condición de carrera. Luego, realiza una serie de comprobaciones antianálisis para evitar ser detectado por herramientas de análisis. Si se detecta alguna de estas herramientas, Fickle Stealer sale del proceso sin

mostrar un mensaje falso. Una vez que se analiza el mensaje falso, el ladrón envía los datos robados al atacante y toma capturas de pantalla para obtener más información. Finalmente, se elimina y sale del proceso, dejando al atacante con la información robada. Este flujo de ejecución demuestra la complejidad y sofisticación de Fickle Stealer en su funcionamiento.

Funcionamiento de Fickle Stealer

Fickle Stealer es un malware diseñado para robar información confidencial de las víctimas y enviarla a un servidor remoto. Su funcionamiento se basa en una comunicación constante entre el malware y el servidor, donde se envían y reciben datos. Una vez que Fickle Stealer se infiltra en el sistema de la víctima, comienza a recopilar información como el nombre de usuario, la dirección IP, la resolución de pantalla y la versión del sistema operativo. Esta información se almacena en un formato JSON específico y se comprime antes de ser enviada al servidor. Además, Fickle Stealer también es capaz de robar datos de billeteras criptográficas, complementos, extensiones de archivos y rutas parciales, que se almacenan en una lista de objetivos cifrada mediante un algoritmo RC4. Esta lista se envía al servidor para su posterior descifrado y uso por parte del atacante.

Verificación del entorno

Para asegurarse de que está operando en un entorno real y no en una máquina virtual o un entorno de análisis, Fickle Stealer realiza una serie de verificaciones. Una de ellas es llamar a la función GetModuleHandleW para comprobar si algún programa está cargado en la memoria. Además, también consulta objetos WMI como Win32_PortConnector, CIM_Memory y Win32_SMBIOSMemory para obtener información sobre el hardware y el sistema operativo. Otra forma de verificar el entorno es comparando el ID de hardware con una lista negra de posibles IDs utilizados en entornos de análisis. Por último, Fickle Stealer también llama a la función GetEnvironmentVariableW y compara el resultado con una lista negra de nombres de usuario que podrían indicar un entorno de análisis.

Objetivos de Fickle Stealer

Fickle Stealer tiene como objetivo principal robar información confidencial de las víctimas, como datos de billeteras criptográficas, complementos, extensiones de archivos y rutas parciales. Estos objetivos se almacenan en una lista cifrada y se envían al servidor para su posterior descifrado y uso por parte del atacante. Además, Fickle Stealer también recopila información del sistema y del hardware de la víctima, como el nombre de usuario, la dirección IP y la versión del sistema operativo. Esta información se almacena en un formato JSON específico y se envía al servidor para su posterior análisis y uso por parte del atacante. En versiones más recientes de Fickle Stealer, se han agregado nuevas funcionalidades para robar información de aplicaciones instaladas y procesos en ejecución, lo que amplía aún más sus objetivos y su capacidad de recopilación de datos.

FortiGuard Antivirus

FortiGuard Antivirus es un servicio de seguridad que ofrece protección contra el malware, específicamente el malware descrito en el texto inicial como W32/InfoStealer.599C!tr, VBA/TrojanDownloader.BED9!tr y PowerShell/TrojanDownloader.AE38!tr. Este servicio es parte de FortiGate, FortiMail, FortiClient y FortiEDR, y utiliza un motor de detección y bloqueo de malware llamado FortiGuard Antivirus. Este motor es actualizado constantemente para garantizar una protección efectiva contra las últimas amenazas. Los clientes que cuentan con estos productos y tienen sus protecciones actualizadas están protegidos contra el malware mencionado en el texto inicial.

Servicio FortiGuard CDR

El servicio FortiGuard CDR (desarmado y reconstrucción de contenido) es una herramienta de seguridad incluida en FortiGate, FortiMail, FortiClient y FortiEDR. Este servicio se encarga de desarmar y reconstruir el contenido de archivos sospechosos para detectar y bloquear posibles amenazas. Además, el servicio FortiGuard CDR también está disponible para los clientes de Fortinet, lo que les brinda una capa adicional de protección contra el malware. Al estar incluido en varias soluciones de seguridad de Fortinet, el servicio FortiGuard CDR es una herramienta esencial para garantizar la seguridad de los clientes contra las amenazas cibernéticas.

Funcionamiento del malware

El malware Fickle Stealer es una amenaza sofisticada que se propaga a través de métodos comunes de ingeniería social, como correos electrónicos de phishing y descargas maliciosas. Una vez instalado en el sistema, su principal objetivo es recolectar información sensible, incluyendo credenciales de inicio de sesión, cookies del navegador e información de tarjetas de crédito. Además, se comunica con servidores de comando y control utilizando técnicas de cifrado para proteger la información robada durante la transmisión. Esta comunicación también permite a los atacantes enviar actualizaciones y comandos adicionales al malware, lo que le permite modificar su comportamiento y añadir nuevas funcionalidades maliciosas según sea necesario.

Técnicas de evasión y ofuscación

Para evitar ser detectado, Fickle Stealer utiliza técnicas avanzadas de ofuscación y monitorea la presencia de software antivirus en el sistema infectado. Esto incluye la modificación de claves de registro y la creación de tareas programadas para garantizar su ejecución en cada inicio del sistema. Además, utiliza técnicas de cifrado para proteger la información robada durante la transmisión a los servidores de comando y control. También monitorea la presencia de software antivirus y trata de desactivarlo o evadirlo mediante la modificación de procesos y la eliminación de rastros. Estas técnicas hacen que sea difícil detectar y eliminar el malware, lo que lo hace aún más peligroso.

Impacto y consecuencias

El malware Fickle Stealer ha tenido un impacto significativo tanto en individuos como en organizaciones. Para los usuarios individuales, las consecuencias incluyen el compromiso de sus cuentas en línea, lo que puede llevar a pérdidas financieras directas y comprometer su privacidad y seguridad. En el ámbito corporativo, este malware representa una amenaza considerable para la seguridad de la información. Las empresas pueden sufrir el robo de datos confidenciales, lo que afecta su reputación y puede resultar en sanciones legales y financieras. Además, las brechas de seguridad causadas por este malware pueden interrumpir las operaciones comerciales. Por lo tanto, es importante que tanto los usuarios individuales como las empresas tomen medidas para protegerse contra amenazas como Fickle Stealer, manteniendo su software actualizado, educando a los usuarios sobre las tácticas de ingeniería social y utilizando soluciones de seguridad robustas.

Requerimientos de recursos para recuperación y mitigación

La recuperación y mitigación del daño causado por Fickle Stealer requiere de recursos significativos, tanto en términos de tiempo como de dinero. Además, este malware puede ralentizar el rendimiento de los sistemas infectados, lo que afecta directamente la productividad de los individuos y empleados en una organización. La inestabilidad y los fallos en los sistemas infectados también pueden generar

costos adicionales en términos de intervención técnica y reparación. Por lo tanto, es esencial contar con recursos adecuados para hacer frente a las consecuencias de este tipo de amenazas.

Impacto en la confianza en la seguridad informática

El impacto de Fickle Stealer va más allá del robo de información y se extiende a la confianza en la seguridad informática en general. La proliferación de este tipo de malware destaca la necesidad de una mayor conciencia y educación en ciberseguridad. Los usuarios y organizaciones deben adoptar prácticas de seguridad más estrictas, como la implementación de autenticación multifactor, la realización regular de copias de seguridad y la formación en la identificación de correos electrónicos y enlaces sospechosos. La constante evolución de amenazas como Fickle Stealer subraya la importancia de mantenerse vigilante y proactivo en la protección de la información digital.