VAULT 7

Vault 7 es una serie de documentos que WikiLeaks comenzó a publicar el 7 de marzo de 2017, detallando las actividades y capacidades de la Agencia Central de Inteligencia (CIA) de los Estados Unidos para realizar vigilancia electrónica y guerra cibernética. Los archivos, que datan de 2013 a 2016, incluyen detalles sobre las capacidades de software de la agencia, como la capacidad de comprometer automóviles, televisores inteligentes, navegadores web incluidos Google Chrome, Microsoft Edge, Mozilla Firefox y Opera, los sistemas operativos de la mayoría de los teléfonos inteligentes incluidos iOS de Apple y Android de Google, y sistemas operativos de computadoras incluidos Microsoft Windows, macOS y Linux. Una auditoría interna de la CIA identificó 91 herramientas de malware de más de 500 herramientas en uso en 2016 que fueron comprometidas por la publicación. Las herramientas fueron desarrolladas por la Rama de Apoyo a las Operaciones de la CIA.

La publicación de Vault 7 llevó a la CIA a redefinir a WikiLeaks como un “servicio de inteligencia hostil no estatal”. En julio de 2022, el ex ingeniero de software de la CIA, Joshua Schulte, fue declarado culpable de filtrar los documentos a WikiLeaks, y en febrero de 2024 fue sentenciado a 40 años de prisión por cargos de espionaje y a 80 meses (6,6 años) de prisión por cargos de pornografía infantil.

El Presupuesto del Programa de Inteligencia Nacional (NIP) asigna a la CIA una cifra estimada de entre 14.000 y 20.000 millones de dólares anuales (dentro del presupuesto global de inteligencia de EEUU, que supera los 60.000 a 90.000 millones). El Presupuesto Oficial proviene directamente de los ingresos del Estado federal estadounidense y de la emisión de deuda pública. Es decir, en última instancia, la totalidad del presupuesto estatal recae sobre los ciudadanos, ya sea de forma directa, diferida o indirecta. El Estado no posee recursos propios ajenos a la economía de la sociedad que administra.

¿El CNI hace algo aparte de tocarse los cojones por turnos en los pisos de arriba de ciudadanos víctimas a los que vigilan, acosan, torturan electrónicamente? Joder la tecnología que usan es toda de la C.I.A., deben ser la mofa de la inteligencia mundial.

Fuego angelical (Angelfire)

```
WINDOWS
```

Es un implante compuesto por cinco componentes: Solartime, Wolfcreek , Keystone (anteriormente MagicWand), BadMFS y el sistema de archivos transitorios de Windows. Se trata de un marco persistente capaz de cargar y ejecutar implantes personalizados en ordenadores objetivo con sistema operativo Microsoft Windows (XP o Win7).

Solartime modifica el sector de arranque de la partición de forma que, cuando Windows carga los controladores de dispositivos al iniciar el sistema, también carga y ejecuta el implante Wolfcreek , que, una vez ejecutado, puede cargar y ejecutar otros implantes Angelfire . Según la documentación, la carga de implantes adicionales provoca fugas de memoria que podrían detectarse en los equipos infectados.

Keystone forma parte del implante Wolfcreek y es responsable de iniciar aplicaciones maliciosas para el usuario. Los implantes instalados nunca acceden al sistema de archivos, por lo que existen muy

pocas pruebas forenses de que el proceso se haya ejecutado alguna vez. Siempre se disfraza como “C:\Windows\system32\svchost.exe” y, por lo tanto, puede detectarse en el administrador de tareas de Windows si el sistema operativo está instalado en otra partición o en una ruta diferente.

BadMFS es una biblioteca que implementa un sistema de archivos oculto que se crea al final de la partición activa (o en un archivo en disco en versiones posteriores). Se utiliza para almacenar todos los controladores e implantes que Wolfcreek iniciará. Todos los archivos están cifrados y ofuscados para evitar el escaneo de cadenas o encabezados PE. Algunas versiones de BadMFS pueden detectarse porque la referencia al sistema de archivos oculto se almacena en un archivo llamado “zf”.

El sistema de archivos transitorios de Windows es el nuevo método para instalar AngelFire . En lugar de almacenar componentes independientes en el disco, el sistema permite al usuario crear archivos transitorios para acciones específicas, como la instalación, la adición y eliminación de archivos de AngelFire , etc. Estos archivos transitorios se añaden a la aplicación 'UserInstallApp'.

Flor de cerezo

proporciona un método para monitorizar la actividad en internet y explotar vulnerabilidades de software en objetivos de interés. En concreto, CherryBlossom se centra en comprometer dispositivos de red inalámbrica, como routers y puntos de acceso (AP), para lograr estos objetivos. Estos dispositivos Wi-Fi se utilizan habitualmente como parte de la infraestructura de internet en hogares, espacios públicos (bares, hoteles o aeropuertos), pequeñas y medianas empresas, así como en oficinas corporativas. Por lo tanto, estos dispositivos son el objetivo ideal para ataques de intermediario (Man-In-The-Middle), ya que pueden monitorizar, controlar y manipular fácilmente el tráfico de internet de los usuarios conectados. Al alterar el flujo de datos entre el usuario y los servicios de internet, el dispositivo infectado puede inyectar contenido malicioso para explotar vulnerabilidades en las aplicaciones o el sistema operativo del ordenador del usuario objetivo.

El dispositivo inalámbrico se ve comprometido al implantarle un firmware CherryBlossom personalizado ; algunos dispositivos permiten actualizar su firmware a través de una conexión inalámbrica, por lo que no es necesario el acceso físico al dispositivo para una infección exitosa. Una vez instalado el nuevo firmware en el dispositivo, el router o punto de acceso se convierte en una llamada FlyTrap . Una FlyTrap envía una señal a través de Internet a un servidor de comando y control denominado CherryTree . La información transmitida contiene información de estado y seguridad del dispositivo que CherryTree registra en una base de datos. En respuesta a esta información, CherryTree envía una Misión con tareas definidas por el operador. Un operador puede usar CherryWeb , una interfaz de usuario basada en navegador, para ver el estado de la FlyTrap y la información de seguridad, planificar las tareas de la Misión , ver los datos relacionados con la Misión y realizar tareas de administración del sistema.

Las misiones pueden incluir tareas en Objetivos para monitorear, acciones/exploits para realizar en un Objetivo , e instrucciones sobre cuándo y cómo enviar la siguiente baliza. Las tareas para un Flytrap incluyen (entre otras) el escaneo de direcciones de correo electrónico, nombres de usuario de chat, direcciones MAC y números VoIP en el tráfico de red que pasa para activar acciones adicionales, la copia de todo el tráfico de red de un Objetivo, la redirección del navegador de un Objetivo (por ejemplo, a Windex para explotación del navegador) o el proxy de las conexiones de red de un Objetivo . FlyTrap también puede configurar túneles VPN a un servidor VPN propiedad de CherryBlossom para dar a un operador acceso a clientes en la WLAN/LAN de Flytrap para una explotación adicional. Cuando Flytrap detecta un Objetivo , enviará una Alerta a CherryTree y comenzará cualquier acción/exploit contra el Objetivo. CherryTree registra las Alertas en una base de

datos y, potencialmente, distribuye la información de la Alerta a las partes interesadas (a través de Catapult).

Arquímedes

Herramienta utilizada por la CIA para atacar ordenadores dentro de una red de área local (LAN), generalmente empleada en oficinas. Permite redirigir el tráfico del ordenador objetivo dentro de la LAN a través de un ordenador infectado con este malware y controlado por la CIA. Esta técnica es utilizada por la CIA para redirigir el navegador web del ordenador objetivo a un servidor de explotación, simulando una sesión de navegación normal.

El documento ilustra un tipo de ataque dentro de un “entorno protegido”, ya que la herramienta se implementa en una red local existente, abusando de las máquinas existentes para tomar el control de las computadoras objetivo y permitir una mayor explotación y abuso.

Colmena

creado por su “Embedded Development Branch” (EDB).

HIVE es un malware de infraestructura de back-end con una interfaz HTTPS pública que utilizan los implantes de la CIA para transferir información exfiltrada de las máquinas objetivo a la CIA y recibir comandos de sus operadores para ejecutar tareas específicas en dichas máquinas. HIVE se utiliza en múltiples implantes de malware y operaciones de la CIA. La interfaz HTTPS pública utiliza dominios de cobertura de apariencia inofensiva para ocultar su presencia.

Las empresas antivirus y los expertos forenses han detectado que algunos programas maliciosos posiblemente patrocinados por un Estado utilizaban este tipo de infraestructura de back-end tras analizar el comportamiento de comunicación de estos implantes específicos, pero no han podido atribuir el back-end (y, por lo tanto, el implante en sí) a operaciones dirigidas por la CIA. En una reciente publicación del blog de Symantec , que logró atribuir las actividades de “Longhorn” a la CIA basándose en Vault 7 , se describe dicha infraestructura de back-end:

Para los servidores de comando y control (C&C), Longhorn suele configurar una combinación específica de dominio y dirección IP para cada objetivo. Los dominios parecen estar registrados por los atacantes; sin embargo, estos utilizan servicios de privacidad para ocultar su verdadera identidad. Las direcciones IP suelen pertenecer a empresas legítimas que ofrecen servicios de servidor virtual privado (VPS) o alojamiento web. El malware se comunica con los servidores C&C a través de HTTPS, utilizando un protocolo criptográfico subyacente personalizado para proteger las comunicaciones y evitar su identificación.

Los documentos de esta publicación podrían permitir a los investigadores de software malicioso y a los expertos forenses analizar este tipo de comunicación entre los programas maliciosos y los servidores back-end utilizados en actividades ilegales anteriores.

Referencia

- https://en.wikipedia.org/wiki/Vault_7

From:
https://wiki.cibertortura.eu/ -

Permanent link:
https://wiki.cibertortura.eu/doku.php?id=vault7:start

Last update: **2026/08/21 20:13**