INSTITUTO TECNOLOGICO DE TIJUANA

DEPARTAMENTO DE SISTEMAS Y COMPUTACIÓN

INGENIERÍA INFORMÁTICA

SEMESTRE: FEB - JUN 22/22

TALLER DE LEGISLACION INFORMATICA

DANIELA ADRIANA SANCHEZ VIZCARRA

UNIDAD A EVALUAR: VI

TEMA:

DELITOS INFORMATICOS

INTEGRANTES DEL EQUIPO	**MATRÍCULA**
TEÍSTA GARCÍA CARLO FERNANDO	20212558
TRIANA CORVERA JESÚS ANTONIO	C20212681

TIJUANA B.C. 31 DE MAYO DEL 2022

INVESTIGACIÓN DE UN CASO DE DELITO INFORMÁTICO

CASO FALLCHILL

Es un malware que fue detectado en varios equipos de una empresa de telecomunicaciones en la Ciudad de México. Entre sus capacidades están las siguientes:

- Extraer información de los discos duros de las computadoras donde se alojaba.
- Iniciar y terminar procesos.
- Intervenir cualquier archivo para modificarlo, ejecutarlo, moverlo o incluso eliminar elementos del sistema.
- Por último, es capaz de borrarse a sí mismo, y así evitar dejar rastros de su presencia, lo que dificulta su detección en las redes vulnerables.

Usualmente FALLCHILL llega a los equipos encubiertos por otros malwares, de manera que es descargado sin que el usuario lo note. Una vez en la máquina, establece comunicación con un servidor de control y utiliza un protocolo de cifrado personalizado, como si se tratase de paquetes TLS/SSL.

FALLCHILL podría estarse usando desde hace algún tiempo para obtener información sobre finanzas, telecomunicaciones, y otros rubros específicos en Estados Unidos.

En noviembre pasado el departamento de Homeland Security en Estados Unidos, junto con el FBI, emitió alertas por la posibilidad de que FALLCHILL estuviera operando desde 2016 en computadoras infectadas en nuestro vecino del norte, permitiendo a hackers monitorear y controlar los equipos. En aquella ocasión se identificaron direcciones IP posiblemente asociadas con el virus, las cuales provenían principalmente de India, Irán y Pakistán.

De acuerdo información de inteligencia estadounidense, FALLCHILL es desplegado por la fuerza militar informática de Corea del Norte, conocida como Hidden Cobra, o Lazarus Group; quienes podrían estar detrás también del hackeo masivo a Sony del 2014 y hasta del ransomware Wannacry.

PGR y FBI descubren malware norcoreano en equipos de empresa en México

La Procuraduría General de la República (PGR) en colaboración con el FBI identificaron y erradicaron un software malicioso de origen norcoreano conocido como Fallchill dentro de la infraestructura del ciberespacio mexicano, de acuerdo con un comunicado de las autoridades mexicanas.

A través de la Agencia de Investigación Criminal, la PGR descubrió que el malware se encontraba alojado en la red de una empresa privada de telecomunicaciones radicada en la Ciudad de México.

De acuerdo con la agencia de seguridad mexicana, para la erradicación de Fallchill, una de las acciones que se llevaron a cabo fue aislar los servidores vulnerables de la red, con lo que se evitó que el software malicioso se propagara hacia otros nodos de Internet.

El Departamento de Seguridad de Estados Unidos (DHS) en conjunto con el Buró Federal de Investigaciones (FBI) publicó una alerta técnica en la que describe cómo identificar direcciones IP asociadas con una herramienta de control remota (RAT) utilizadas por el gobierno de Corea del Norte en la red estadounidense.

De acuerdo con la alerta publicada por el Equipo de Respuesta a Emergencias Informáticas (CERT) de Estados Unidos, el software es capaz de obtener la siguiente información de los sistemas infectados:

- Información de la versión del sistema operativo (SO),
- Información del procesador,
- Nombre del sistema,
- Información de la dirección IP local,
- ID única generada,
- Dirección de Control de Acceso a Medios (MAC).

Con la obtención de esta información, los habilitadores del malware son capaces de llevar a cabo las siguientes acciones en los equipos infectados por Fallchill:

- Obtener información sobre todos los discos instalados, incluido el tipo de disco y la cantidad de espacio libre en el disco;
- Crear, iniciar y terminar un nuevo proceso y su hilo principal;
- Buscar, leer, escribir, mover y ejecutar archivos;
- Obtener y modificar las marcas de tiempo del archivo o directorio;
- Cambiar el directorio actual para un proceso o archivo;
- Eliminar malware y artefactos asociados con el malware del sistema infectado.

El gobierno de Estados Unidos conoce como Hidden Cobra a las actividades cibernéticas maliciosas realizadas por el gobierno de Corea del Norte. “El FBI tiene gran confianza en que los actores de Hidden Cobra están usando las direcciones IP (...) para mantener una presencia en las redes de las víctimas y para una mayor explotación de la red”, refiere la alerta del (CERT) de Estados Unidos.

Aunque en el caso de México, Fallchill fue descubierto en una empresa del sector de telecomunicaciones, de acuerdo con la alerta técnica del CERT estadounidense, Hidden Cobra ha utilizado el malware Fallchill desde el 2016 para vulnerar las redes de industrias como la aeroespacial, de telecomunicaciones y financiera en territorio estadounidense.

La PGR refirió en su comunicado que en el último cuatrimestre del 2017, “la Agencia de Investigación Criminal (AIC) identificó y mitigó más de 289 casos de incidentes de seguridad informática que afectan tanto al sector público como privado”.

Referencias bibliográficas:

- https://www.xataka.com.mx/otros-1/lo-que-tienes-que-saber-del-virus-norcoreano-que-llego-a-mexico-y-fue-eliminado-por-la-pgr-y-el-fbi
- https://akubica.com/detectan-en-mexico-virus-norcoreano-llamado-fallchill/
- https://blog.orcagrc.com/casos-de-delitos-informaticos-en-mexico
- https://www.eleconomista.com.mx/tecnologia/PGR-y-FBI-descubren-malware-norcoreano-en-equipos-de-empresa-en-Mexico-20180109-0084.html