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.

El software fue encontrado por la Procuraduría General de Justicia y el FBI en oficinas en Ciudad de México. Como parte del protocolo para la eliminación del FALLCHILL, los servidores que pudieron haber sido vulnerados fueron aislados, a fin de evitar que otros equipos sean contaminados.

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.

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