International Multidisciplinary Engineering Congress
Booklets

RENIECYT
Registro Nacional de Instituciones y Empresas Científicas y Tecnológicas
1702902 CONACYT

RENIECYT - LATINDEX - Research Gate - DULCINEA - CLASE - Sudoc - HISPANA - SHERPA UNIVERSIA - Google Scholar DOI - REDIB - Mendeley - DIALNET - ROAD - ORCID

Title: Un caso de estudio relacionado con la importancia de educar sobre la seguridad informática a nivel personal y empresarial

Authors: URUETA-HINOJOSA, Daniel Edahi, ALANÍS-CANTÚ, Reynaldo, TORRES-DEL-CARMEN, Felipe de Jesús y MOTA-CRUZ, Juan Esteban

Editorial label ECORFAN: 607-8695
BCONIMI Control Number: 2020-39
BCONIMI Classification (2020): 120320-0039

Pages: 18
RNA: 03-2010-032610115700-14

ECORFAN-México, S.C.
143 – 50 Itzopan Street
La Florida, Ecatepec Municipality
Mexico State, 55120 Zipcode
Phone: +52 1 55 6159 2296
Skype: ecorfan-mexico.s.c.
E-mail: contacto@ecorfan.org
Facebook: ECORFAN-México S. C.
Twitter: @EcorfanC

www.ecorfan.org

Holdings
Mexico Colombia Guatemala
Bolivia Cameroon Democratic
Spain El Salvador Republic
Ecuador Taiwan of Congo
Peru Paraguay Nicaragua

Contenido

- Introducción
- Objetivo
- Antecedentes
- Desarrollo
- Resultados
- Conclusiones
- Recomendaciones

Introducción

- En la década de los años 90 cuando aparecen los primeros virus y las personas empiezan a tener conciencia sobre los peligros que conlleva usar una computadora
- Actualmente, con la masificación de los medios electrónicos de comunicación la seguridad informática está más vigente que nunca antes
- El nivel de cultura en la materia de los usuarios, empresas e instituciones está lejos de ser el ideal

Objetivo

- Identificar el nivel de cultura sobre seguridad informática a nivel personal y empresarial usando técnicas de ingeniería social

Seguridad informática

- La **seguridad informática** es un conjunto de herramientas y estrategias cuyo objetivo es garantizar la integridad, disponibilidad y confidencialidad de la información en un sistema
- Su importancia radica en el hecho de que la mayoría de las acciones de nuestro día a día dependen de ella

Ingeniería social

- La **ingeniería social** es la manipulación psicológica de personas para que realicen cierta acción o den información sensible. Algunos casos son:
  - Llamadas de extorsión
  - Robos bancarios en cajeros automáticos
  - Robo de identidad con llamadas telefónicas

Ingeniería social (II)

Los tipos de ingenierīa social son:

- *Basadas en personas*
  - Impersonar (Imitar)
  - Observación
  - Estudio de conductas
- *Basadas en computadoras*
  - Engaños virales
  - Phishing (Suplantación de identidad)
  - Software malicioso

Phishing

- El origen de su nombre puede ser del dicho:
  "Si le das un pescado a un hombre, él comerá por un día pero enséñale a pescar y tendrá para comer toda su vida"

Phishing == Fishing == Pescar

- Intenta obtener información sensible como: usuarios, contraseñas, tarjetas de crédito, entre otras. Es por eso que se le denominan: ataques de robo de identidad

Bad USB (Rubber Ducky)

- Es una herramienta de inyección de pulsos de teclado disfrazada de una unidad USB.
- Las computadoras lo reconocen como un teclado regular y aceptan automáticamente acciones pre-programadas.

Figura. Ejemplo de una Bad USB

Desarrollo

El desarrollo consistió en dos partes:

- Creación un punto de acceso falso el cual proporciona acceso a Internet por medio de un modem 4g donde se usaron técnicas de phishing
- Desarrollo de una BadUSB de bajo costo usando un Arduino, así como un programa malicioso a ejecutarse

Resultados (I)

- Cuando el usuario se intenta conectar al punto de acceso falso, se muestra una página en la cual el usuario ingresa sus credenciales

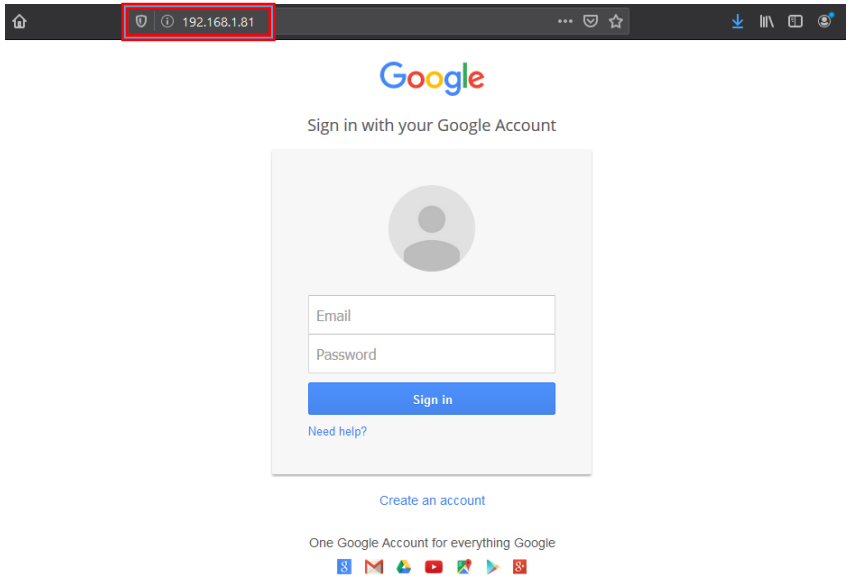

Figura. Sitio web falso mostrado al usuario

Resultados (I)

- Una vez que se ingresan, son capturadas por el sistema y se hacen visibles al atacante

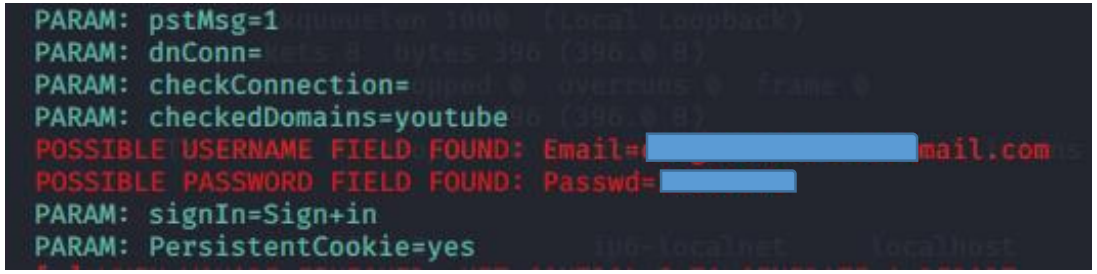

Figura. Ejemplo de la captura de un usuario y contraseña por el sistema

Resultados (I)

- Estableciendo el dispositivo durante dos horas se obtuvieron los resultados siguientes:

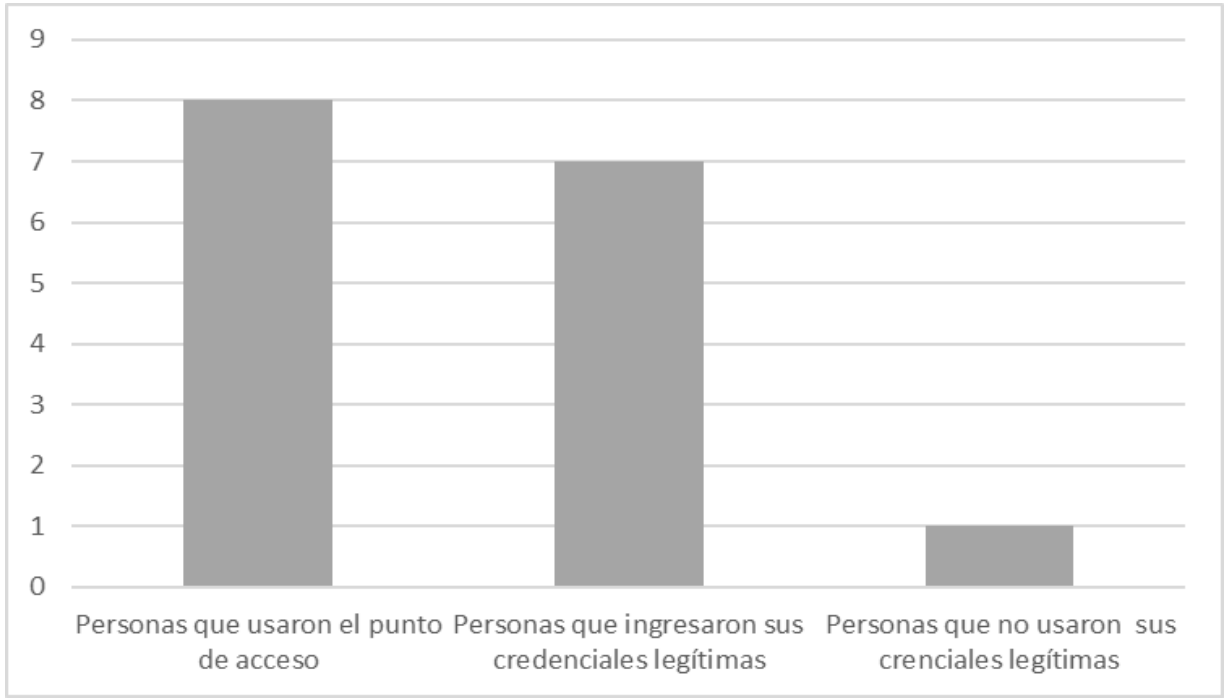

Figura. Resultados obtenidos usando el punto de acceso falso

Resultados (II)

- La vista al conectarse la bad USB a una computadora se muestra como sigue:

Figura. Ejemplo de la vista de la Bad USB conectada a una computadora

Resultados (II)

- Una vez se conecta, se ejecuta una primera secuencia de comandos que sirven para descargar un archivo malicioso

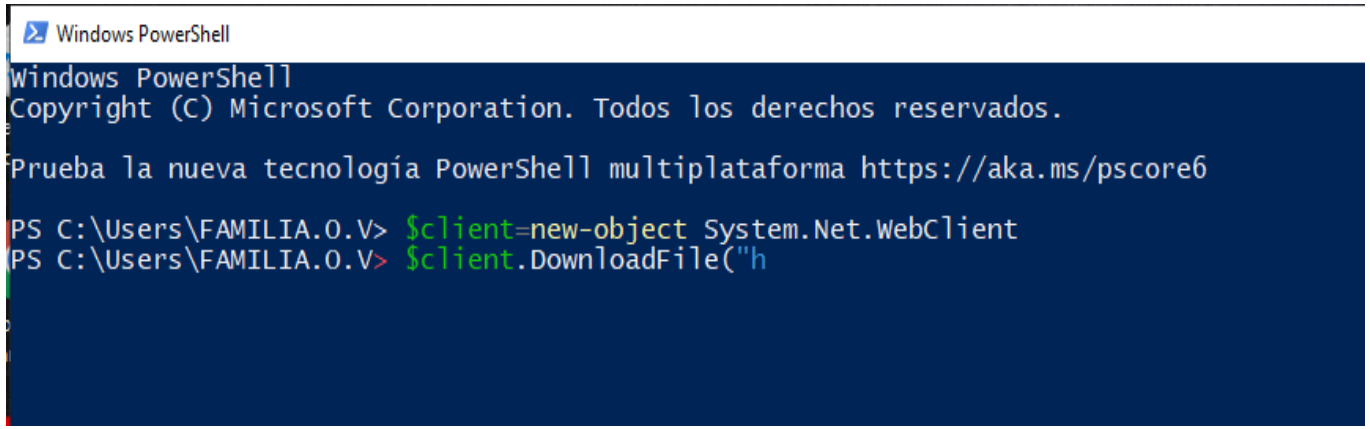

Figura. Primera secuencia de comandos ejecutados por la Bad USB

Resultados (II)

- Una segunda secuencia de comandos se encarga de ejecutar el archivo malicioso

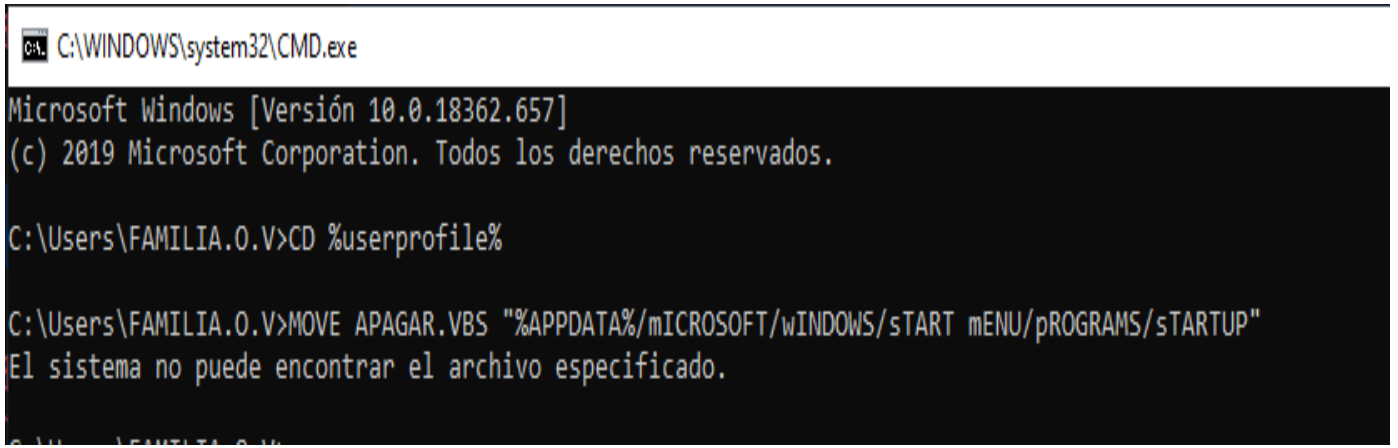

Figura. Segunda secuencia de comandos ejecutados por la Bad USB

Resultados (II)

- Para este caso, al conectar la Bad USB se instalaba un programa que evitaba iniciar la computadora
- El dispositivo se dejó a la deriva y solamente se esperó, en una hora, dos usuarios conectaron el dispositivo a su computadora, infectándose
- Las computadoras de los implicados, fueron desinfectadas

Conclusiones

Los resultados indican que es necesaria una mayor educación en seguridad informática para todos los usuarios

Si bien el punto de acceso falso está orientado más hacia un objetivo en específico, en el caso de la Bad USB al poder ejecutar cualquier tipo de archivo se tiene un peligro mayor

La Bad USB puede permitir que usuarios inserten el dispositivo en las computadoras de sus trabajos, generando pérdidas económicas cuantiosas

Recomendaciones

Se propone crear campañas que permitan concientizar a personas, instituciones y empresas a los peligros que están expuestos

ECORFAN®