EDP UNIVERSITY OF PUERTO RICO

RECINTO DE HATO REY

PROGRAMA DE MAESTRÍA EN SISTEMA DE INFORMACIÓN CON ESPECIALIDAD EN SEGURIDAD DE INFORMACIÓN E INVESTIGACIÓN DE FRAUDE

# ANÁLISIS DE CASO: UNITED STATES OF AMERICA V. STANISLAV VITALIYEVICH LISOV
# ANÁLISIS DEL ATAQUE A BANCOS CON EL MALWARE NEVERQUEST 2013-2015
# CASO 1:17-CR-00048

Julio, 2019

PREPARADO POR:

JANEFIX DIAZ RAMOS

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

ANÁLISIS DE CASO:

UNITED STATES OF AMERICA V. STANISLAV VITALIYEVICH LISOV

# ANÁLISIS DEL ATAQUE A BANCOS CON EL MALWARE NEVERQUEST 2012-15

PREPARADO POR:

JANEFIX DIAZ RAMOS

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

Julio, 2019

Aprobado por:

Dr. Miguel Drouyn Marrero, Director

**TABLA DE CONTENIDO**

## TABLA DE FIGURAS

# SECCION I – INTRODUCCIÓN Y TRANSFONDO

## Introducción

Con el pasar del tiempo y la evolución del ser humano nos hemos vistos forzados a retarnos como seres humanos para lograr el crecimiento en muchas áreas y esto ha traído muchos beneficios en nuestro diario vivir, entre las que se encuentra la comunicación, los telegramas, la radio, el televisor y la creación de las computadoras, con las cuales hemos abierto un nuevo mundo con exposición a nivel mundial**.** Cero-Cool (2017) habla que desde finales del 1960 y comienzos de los 1970, que se vio la primera conexión entre ordenadores de Stanford y UCLA, él envió del primer email por Ray Tomlinson, el nacimiento de Arpanet, conocido hoy como internet, y la aparición del primer virus Creeper creado por Robert Thomas de la compañía BBN, un programa que se movía entre ordenadores conectados a Arpanet y que desplegaba el mensaje "*I'm the creeper: catch me if you can*" se ha visto una evolución y crecimiento en la necesidad de proteger nuestros datos y crear conciencia de la importancia en asegurar información, recursos y activos.

Este crecimiento e interés en cuidar y asegurar los sistemas físicos y en la nube viene en momentos que se ha visto un incremento en fraude y en robo de identidad. En un inicio, aquellos primeros virus eran demostraciones de capacidad tecnológicas, pero hoy se han convertidos en armas delictivas, debido a personas inescrupulosas que, por medios de los malware, gusanos, troyanos y otro tipo de virus, logran acceder a información valiosa de víctimas como el seguro social, fechas de nacimiento, cuenta de banco, login de acceso a

redes sociales, entre otros.

En el reportaje que se difundió el 24 de abril del Vocero, Rivera (2019) nos dice que se arrestó a Omar Ramon Olivera Caldera, de 39 años, oriundo de Venezuela, quien, junto a su cómplice también venezolano, utilizaba información personal y contraseñas de clientes del Banco Popular para hacer las transferencias, de dinero a sus cuentas personales. Luego acudía al cajero automático donde retiraba el dinero efectivo utilizando un código de barra que le provee la institución bancaria ya que la aplicación no requiere el uso de una tarjeta de débito, para obtener el dinero en cantidades de $500, que es lo máximo que le permite retirar el banco diariamente en cuentas regulares, y $1,000 para los clientes con cuentas Premium.

Las agencias federales están constantemente detrás de criminales que son responsables de los ataques que están causando perdida de capital y dañando los diferentes sistemas al lograr burlar la seguridad y los diferentes controles. Las agencias federales cuentan con todo tipo de personal en el área del fraude y que hacen todo lo posible para que estos criminales no se salgan con la suya, pero sobre todo para llevar el mensaje que tarde o temprano toda acción tiene consecuencias y no se quedaran impune sus faltas.

Aunque las agencias brinden los debidos adestramientos es necesario que cada individuo en este campo de la seguridad de la información este bien adiestrado, pero sobre todo que cuente con los conocimientos en lo último sobre ciberseguridad, ya que los delincuentes están constantemente cambiando sus tácticas y atacan desde países remotos como Rusia, China y Asia, mientras la gran mayoría de sus víctimas están en E.U, Europa y Latino América. Para finalizar es importante conocer que es algo a lo que estamos

expuestos y las alternativas para minimizar ser víctimas todas se encuentran al alcance de nuestras manos.

**Descripción del caso**.

**Caso:** Estados Unidos vs. Stanislav Vitaliyevich Lisov

**Número de caso**: 1:17-cr-00048-VEC

**Asunto:** Fraude Bancario utilizando el troyano NeverQuest

**Partes en el caso**

**Acusado:** Stanislav Vitaliyevich Lisov alias “Black”, alias “Blackf” “LISOV”.

**Figura 1.** Foto de Stanislav Vitaliyevich Lisov. (Obtenida de: Crimerussia.com, 2019)

**Investigadores**

Geoffrey S. Berman, Procurador de los E.U para el Distrito Sur de Nueva York**.**

William F. Sweeney Jr., Director Adjunto a cargo de la Oficina de Nueva York FBI

Oficina de Asuntos Internacionales del Departamento de Justicia de los E.U.

Unidad de Fraudes Complejos y Ciberdelincuencia de los Estados Unidos

**Abogados**

Oleg Gubarey, abogado defensor en España

**Figura 2.** Foto de Oleg Gubarev. (Obtenida de: Facebook de Oleg Gubarey, 2019)

Juan Manuel Arroyo, abogado defensor durante la vista de extradición a E.U.

**Figura 3.** Foto de Juan Manuel Arroyo. (Obtenida de: LinkedIn, 2019)

**Fiscales**

Michael D. Neff fiscal a cargo del caso para Distrito Sur de Nueva York

Geoffrey S. Berman fiscal para el Distrito Sur de Nueva York

**Jueces**

Honorable Concepción Espejel jueza, presidenta de la sección segunda de la Sala de lo Penal de la Audiencia Nacional corte de España

Honorable Valerie E. Caproni jueza, del Tribunal de Distrito de los Estados Unidos para el Distrito Sur de Nueva York.

**Trasfondo**

Según "España *extraditará"*, (2019), Stanislav Vitaliyevich Lisov quien trabajaba como especialista en administración de sistemas y desarrollador de sitios web en la ciudad de Taganrog, en el sur de Rusia y fue arrestado el 13 enero de 2017 en el aeropuerto de El Prat por el FBI y la Interpol, mientras Lisov se encontraba de luna de miel en España. En la Audiencia Nacional española se aprobó la extradición de Lisov a Estados Unidos, ya que era investigado desde el 2014 por desarrollar el software malicioso llamado 'NeverQuest', un 'troyano bancario' que permitía robar la información bancaria de las victimas permitiendo así el robo de dinero aproximado de 855,000 de cuentas bancarias entre junio del 2012 y enero del 2015. Según "IBM *Threat" (2019),* NeverQuest era el malware entre 2012- 2015 más activo y peligroso del mundo. También se estima que el troyano podría haber generado pérdidas totales a bancos y demás instituciones por valor de unos cinco millones de dólares (4.660.000 euros).


**Figura 4.** Diagrama de troyanos bancarios mundiales 2017. (Obtenido de: “La policía”,2017)

**Descripción de hechos**

Se desprende de la investigación hecha por el FBI en el caso USA vs Stanislav Vitaliyevich Lisov el Tribunal Federal del Distrito de Manhattan (2019) indica que, desde junio de 2012, hasta enero de 2016, el Sr. Stanislav Vitaliyevich Lisov alias "Black" y "Blackf” fue el creador del programa maligno NeverQuest. Este es un software malicioso o malware, más bien conocido como un troyano bancario. Este puede introducirse en las computadoras de las víctimas a través de sitios web como redes sociales, transferencias de archivos y correos electrónicos suplantando la identidad de la víctima. Una vez instalado en la computadora de la víctima, NeverQuest puede identificar cuándo se hace un inicio de sesión en un sitio web de banca en línea y transfiere las credenciales de inicio de sesión de

la víctima, su nombre de usuario y contraseña, a los servidores de computadoras que son s utilizados para administrar el malware NeverQuest. Lisov y sus socios usaron la información obtenida para robar dinero de las víctimas a través de transferencias bancarias, retiros de cajeros automáticos y compras de bienes costosos a través de internet.

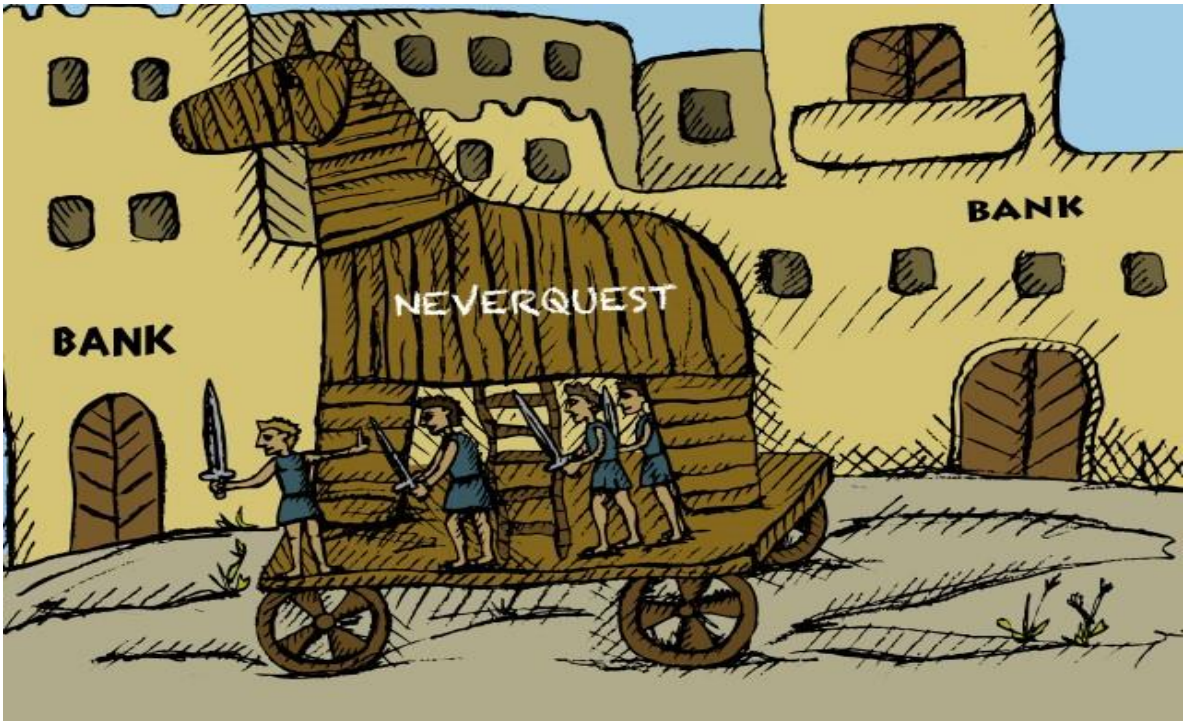



**Figura 5.** Comparación NeverQuest con caballo de Troya. (Obtenido de: *"Neverquest Trojan",2019*)

Lisov fue pieza clave en la creación y administración de una infraestructura ligada directamente a un grupo de computadoras denominadas "Redbots" las cuales estaban infectadas por el troyano "NeverQuest". Lisov contaba con una empresa delictiva, la cual por medio del alquiler y el pago de servidores informáticos los administraba. Esos servidores informáticos contenían listas con millones de credenciales, incluidos nombres de

usuario, contraseñas, preguntas y respuestas de seguridad, para las cuentas de las víctimas en páginas web de diferentes bancos y otros sitios financieros. El 13 de enero de 2017, Lisov fue arrestado en España de conformidad con una orden de arresto provisional. El 19 de enero de 2018, fue extraditado de España a los Estados Unidos. La sentencia de Lisov está programada para el 27 de junio de 2019 a las 11:00 a.m. ante la jueza Valerie E. Caproni.

**Acusaciones, cargos y penalidades**

**Primer cargo**

**Conspiración piratería informática**

**Título 18 del Código de los Estados Unidos, Sección 1030 (a) (2) Fraude y actividad relacionada con computadoras.** En violación de la Constitución y las leyes de los Estados Unidos Estados el acusado Lisov accedió a computadoras sin autorización, y de este modo obtuvo información de Ordenadores, con el fin de comercializar esta y obtener una ganancia financiera, mediante la promoción de estos actos delictivos y criminales.

**Título 18, Unidos Código de los Estados, Sección 1030 (a) (4) Fraude y actividad relacionada con computadoras.** En violación de la Constitución y las leyes de los Estados Unidos Estados el acusado Lisov fue parte y objeto de la conspiración que voluntariamente, a sabiendas, y con la intención de defraudar, logro acceder a ordenadores protegidos sin autorización conducta por la cual hizo progresar su fraude hasta llegar a la suma de $855,000 del fraude.

**Título 18, Estados Unidos Código, Sección 1030 (a) (5) (A) Fraude y actividad relacionada con computadoras.** En violación de la Constitución y las leyes de los Estados Unidos Estados el acusado Lisov fue parte activa de la conspiración al voluntariamente y a sabiendas de lo que haría junto a personas que conocía y desconocía causó la transmisión del programa, información, código y comando, y como resultado de tal conducta, causaría y causó intencionalmente daños sin autorización, a computadoras protegidas.

**Título 18, Estados Código de los Estados, Sección 1030 (a) (6) Fraude y actividad relacionada con computadoras.** En violación de la Constitución y las leyes de los Estados Unidos el acusado Lisov además fue objeto de la conspiración cuando junto a otros conocidos y desconocidos, efectuó transacciones que afectaron el comercio interestatal y extranjero, y computadoras usadas por y para el gobierno de los Estados Unidos, voluntariamente, a sabiendas, y con la intención de defraudar, trafico contraseñas e información similar a través de la cual las computadoras podían ser accedidas sin autorización.

**Segundo cargo**

**Conspiración para cometer fraude electrónico**

**Título 18, Código de los Estados Unidos, Sección 1349 Intento y conspiración.** En violación de la Constitución y las leyes de los Estados Unidos Estados el acusado Lisov voluntariamente, y a sabiendas se combinaron, conspiraron, confederaron, y acordar juntos y entre sí cometer fraude electrónico, ya que el acusado proporcionó una infraestructura en línea crítica que se utilizó para controlar y / o recibir información robada de las

computadoras infectado con el software malicioso el cual fue diseñado para robar información financiera de acceso de las cuentas de las víctimas y Lisov a sabiendas controlaba y recibía la información robada de tales computadoras. Lisov voluntariamente, y a sabiendas**,** con la intención de idear un esquema, para obtener dinero por medio de fraudulentas pretensiones, representaciones el transmitió por medios de comunicación por cable, radio, televisión en la interestatal y comercio exterior, por escritos, signos, señales, imágenes y sonidos con el propósito de ejecutar tal esquema de fraude. En adicción se le acuso de Titulo 18 Confiscación civil Sección 981 (a) (1) (C)**,** Titulo 18 Decomiso penal Sección 982 (a) (2) (B), Título 28 Sección 2461 Modo de recuperación y Sección 853 (p) Confiscaciones penales.

**Penalidades**

Según los documentos de la corte USA v. STANISLAV VITALIYEVICH LISOV el acusado al momento está bajo arresto en espera de ser sentenciado y está expuesto a una condena de un máximo de 25 años con una posible fianza de $5,000,000. La sentencia de Lisov está programada para el 27 de junio de 2019 a las 11:00 a.m. ante el juez Valirie E. Caproni.

**Definición de términos**

**Instant messaging** – La mensajería instantánea es una colección de tecnologías que crea la posibilidad de comunicación basada en texto en tiempo real entre dos o más participantes vía Internet. La mensajería instantánea permite la inmediata transmisión de comunicaciones, incluida la recepción inmediata de acuse de recibo o respuesta. (Mchoes,

Flynn, 2008)

**Internet Service Provider ("ISP") –**Un ISP es un Servicio comercial que proporciona conexiones a internet para sus suscriptores. Los ISP también pueden proporcionar cuentas de correo electrónico de Internet y Otros servicios únicos para cada ISP particular.

**IP address -** La dirección del protocolo o mejor conocida como dirección de IP es una dirección numérica única utilizada por las computadoras en el Internet. Una dirección IP parece una serie de cuatro números, Cada uno en el rango de 0-255, separados por puntos. A cada computadora conectada a Internet se le debe asignar una dirección IP para que el tráfico de Internet sea enviado y dirigido a esa computadora. Puede ser dirigido adecuadamente desde sus fuentes hasta su destino. (Mchoes, Flynn, 2008)

**Server** – Un servidor es una computadora centralizada que proporciona servicios para otras computadoras que se conectan a través de Red o Internet. (Mchoes, Flynn, 2008)

**Proxy -** Un proxy es una computadora que actúa como un "intermediario" para un usuario que realiza conexiones indirectas a otros servicios de red. Una computadora cliente se conecta a un proxy y le indica que se conecte a otra computadora. El destino la computadora percibe una conexión entrante desde el proxy, no la computadora cliente Como muchos servicios de red, los proxys son legítimos, pero a menudo son utilizados por los delincuentes cibernéticos para ocultar sus identidades y ubicaciones. (Mchoes, Flynn, 2008)

**Troyano –** Un troyano es un software malicioso, o malware, que realiza una función

deseable para el usuario antes de ejecutar o instalar, sino que facilita el acceso no autorizado al sistema informático del usuario. (Mchoes, Flynn, 2008)

**Malware** – El malware es un software de computadora diseñado para infiltrarse o dañar una computadora entra al sistema sin consentimiento del administrador. La expresión es un término general utilizado por los profesionales de la computación para describir una Variedad de código de programa hostil o intrusivo. (Mchoes, Flynn, 2008)

**NeverQuest –** es un troyano bancario el cual se propaga a través de las redes sociales, correos electrónicos y transferencias de archivos. Tiene la capacidad de reconocer cientos de bancos online y otros sitios web financieros. Cuando un usuario o victima infectado intenta acceder a uno de los sitios, el troyano reacciona activándose automáticamente y hurtando las credenciales de su víctima puede robar el user y password de la cuenta al igual que preguntas de seguridad y sus respuestas.

**Botnet** – Los botnet son una gran cantidad de bots, llamado red bot o botnet, normalmente son controlados por una computadora llamada servidor de comando y/o control. El dueño del servidor de comando y control puede dirigir la red de bots. El propietario del servidor de comando y control también puede alquilar la botnet o porciones de este a otros individuos. (Mchoes, Flynn, 2008)

**Angler Exploit -** un ransomware que roba todas las contraseñas del equipo para después cifrar los ficheros y el usuario no puede recuperar su sistema.

**Bot** - Un bot es una computadora que ha sido comprometido o infectado por un software malicioso. El bot completa tareas maliciosas y / o ilegales por dirección remota. La mayoría

de los usuarios que tienen una computadora que actúa como un bot no son conscientes de que la computadora ha sido comprometida. (Mchoes, Flynn, 2008)

## SECCIÓN 2 – REVISIÓN DE LITERATURA

### Introducción

Si vemos el contexto histórico del malware, "Virus y antivirus" (s,f), nos habla sobre cómo, Von Neumann en 1949 estableció la idea de programa de almacenado y expuso la Teoría y Organización de Autómatas Complejos, donde hablo por primera vez de la posibilidad de desarrollar pequeños programas replicantes y capaces de tomar el control de otros programas de similar estructura. Luego en los años 70's las computadoras IBM Serie 360 fueron atacadas por un virus llamado Creeper, el que fue creado por Robert Thomas Morris. Este virus emitía un mensaje que decía: "*I'm a creeper… catch me if you can!*".

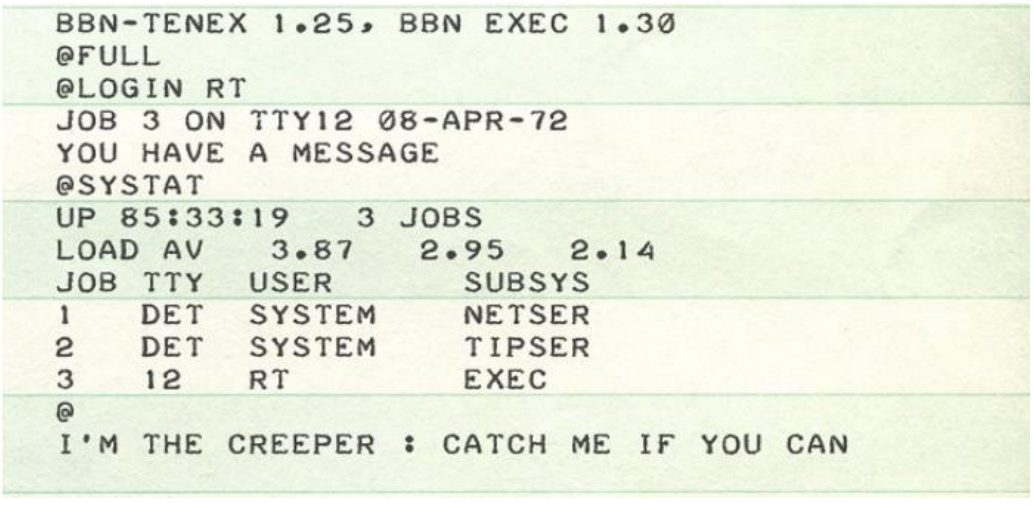



**Figura 6**. Código Creeper. (Obtenido de: Yumal, 2017)

Más adelante en los años 80’s, Dewdwey (1988) habló por primera vez de CoreWar. Cuando Bell Computer, junto a Robert Thomas Morris, Douglas Mcllroy y Victor Vygotsky crean un juego llamado CoreWar, el cual estaba basado en la teoría de Von Neumann y el objetivo de este juego era que los programas de la computadora combatieran entre sí, tratando de ocupar toda la memoria de la máquina y eliminando así a los oponentes. Este es juego es considerado por algunos como el precursor de los virus en informática.

Luego Infante (2004) nos dice que en los 90’s los servicios de banca por internet se volvieron sumamente útiles en los sistemas de internet. El Banca por internet se convirtió en una manera de comunicación entre el banco y el cliente, en donde cualquier persona que tuviera acceso a una computadora e internet podía hacer lo que necesitara con tan solo un click. Era tan solo cuestión de tiempo antes de que los cibercriminales comenzaran a tratar de robarles a los bancos. Sin embargo, como los bancos emplean una seguridad sólida, las ciber delincuentes se dieron percataron que atacar a los bancos en sí serían difíciles. Por lo que comenzaron a robar las credenciales de los clientes que era mucho más fácil porque desde mi punto de vista el cliente no está 24/7 actualizando sus sistemas y así nacieron los primeros troyanos financieros.

Desde ese momento los troyanos financieros han seguido en el fondo su manera básica esconderse en la computadora de la víctima e intentar robar sus credenciales cuando inician

sesión en los servicios bancarios en línea o secuestran sesiones bancarias en línea para realizar transacciones no autorizadas. Las primeras variantes se basaban en tácticas como el registro de pulsaciones de teclas o la redirección de las víctimas a sitios web bancarios falsos. Con el tiempo, las tácticas utilizadas se han vuelto mucho más sofisticadas. Uno de los mayores avances fue el advenimiento de los ataques de hombre en el navegador (MITB), donde el troyano manipula el navegador web de la víctima y cambia lo que se muestra en un sitio web.

Motos (2011) nos dice que uno de los primeros troyanos en ser pioneros en esta técnica fue Zeus, que apareció en 2007. Zeus podría configurarse para atacar virtualmente cualquier sesión de banca en línea mediante la inyección de HTML adicional conocido como "inyecciones web" en las páginas web abiertas en el navegador, permitiendo que el troyano para alterar o reemplazar el contenido y / o mostrar campos adicionales. Esto permitió a los atacantes robar credenciales cuando ingresaron en la página web o crear solicitudes de credenciales adicionales que no fueron solicitadas por el banco, como los códigos PIN.

Una cosa que ha caracterizado a los troyanos financieros es que el sector ha estado en un estado de flujo casi constante, con fugas y acciones de aplicación de la ley que alteran regularmente su dinámica. En 2011, su creador filtró el código fuente de Zeus. De la noche a la mañana, una pieza de software maliciosa que antes estaba bien controlada ahora estaba disponible de forma gratuita para todos. La filtración llevó a la creación de una gran cantidad de clones basados en el código fuente de Zeus, como Citadel y Gameover Zeus.

Poco después, algo similar le sucedió a SpyEye, cuando se rompió el protector de su constructor y se liberó el código fuente.

Las fugas de código fuente no son inusuales en el ciberunderground. En algunos casos, se cree que los autores de malware están detrás de las filtraciones. Si esto ocurre, generalmente parece ser motivado por el temor a una investigación policial. Al liberar el código fuente, los autores pueden "enturbiar las aguas" al poner sus herramientas en manos de múltiples grupos.

A pesar de la percepción pública de que las bandas de troyanos financieros pueden permanecer en el anonimato, las fuerzas policiales han tenido cierto éxito en los últimos años en el desmantelamiento de las operaciones y la detención de jugadores clave. En 2014, los ciber criminales responsables por Gameover Zeus recibieron un golpe por el FBI, por la Agencia Nacional de Crimen del Reino Unido y varias otras fuerzas policiales. Aunque no se realizaron arrestos, la actividad en torno al malware se redujo considerablemente tras las redadas.

Si bien es cierto que los bancos invierten en tecnología y en mantenerse a la vanguardia en cuanto a productos y servicios, también es cierto que dado este auge de servicios en línea que dependen del internet o de alguna aplicación se han visto obligados a invertir mucho más dinero en el área de la seguridad. Por esto siguen tomando medidas de seguridad que y

reducir la desconfianza de los clientes y fomentar su migración de la banca tradicional a la banca electrónica vía Internet.

**Fraudes involucrados**

**Phishing-** técnica utilizada por ciberdelincuentes la cual utilizan para obtener información confidencial como nombres de usuario, contraseñas y detalles de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima. Rivero (2014)

**Troyano-** Según Kapersky.com (2019), Un caballo de Troya o troyano: "es un tipo de malware que a menudo se camufla como software legítimo". Los ciberdelicuentes y/o hackers usan los troyanos para intentar acceder a los sistemas de los usuarios. Normalmente, algún tipo de sistema social engaña a los usuarios para que carguen y ejecuten los troyanos en sus sistemas. Una vez estos están activados, los troyanos pueden permitir a los cibercriminales espiarte, robar los datos confidenciales y obtener acceso por una puerta trasera a tu sistema. Estas acciones pueden incluir las siguientes:

- Eliminación de datos
- Bloqueo de datos
- Modificación de datos
- Copia de datos
- Interrupción del rendimiento de ordenadores o redes de ordenadores

**Troyano Bancario-** Los programas Trojan-Banker, o troyanos bancarios, están diseñados para robar tus datos bancarios de sistemas de banca online, sistemas de pago electrónico y tarjetas de débito o crédito. ("NerverQuest Troyan", s.f)

**NeverQuest -** troyano bancario que se propaga a través de las redes sociales, correos electrónicos y transferencias de archivos. Es un sistema de escritorio compartido, a través del cual los cibercriminales usan el ordenador de la víctima para acceder a su cuenta bancaria por Internet. Este Malware se propaga a través de las redes sociales, correos electrónicos y transferencias de archivos. Posee la capacidad de reconocer cientos de bancos online y otros sitios web financieros. Cuando un usuario infectado intenta acceder a uno de los sitios, el troyano reacciona activándose automáticamente y hurtando las credenciales de su víctima. ("Kapersky.com", 2019)

**Robo de identidad -** El robo de la identidad digital, tanto en Internet como en redes sociales, se produce o bien suplantando la identidad digital de un usuario de Internet y redes sociales, o robando sus claves y contraseñas para acceso a las mismas, con fines generalmente, delictivos, siendo delito en sí mismo el robo o la suplantación de la identidad en Internet. (Vázquez &Apraiz y Asociados, s.f)

**Leyes aplicables**

**Título 18, Código de los Estados Unidos, Conspiración piratería informática Sección 1030 (a) (2), (a) (4), (a) (5) (A), (a) (6)**

(a) Quienquiera que:

2) accede intencionalmente a una computadora sin autorización o excede el acceso autorizado, y de ese modo obtiene:

4) a sabiendas y con la intención de defraudar, accede a una computadora protegida sin autorización, o supera el acceso autorizado, y mediante tal conducta fomenta el fraude intencionado y obtiene algo de valor, a menos que el objeto del fraude y la cosa obtenida consistan únicamente el uso de la computadora y el valor de dicho uso no supera los $ 5,000 en cualquier período de 1 año;

(5) (A) a sabiendas causa la transmisión de un programa, información, código o comando, y como resultado de tal conducta, causa daños intencionalmente sin autorización, a una computadora protegida;

(6) a sabiendas y con la intención de defraudar el tráfico (como se define en la sección 1029) en cualquier contraseña o información similar a través de la cual se pueda acceder a una computadora sin autorización.

**Título 18, Código de los Estados Unidos, Sección 1349 Intento y conspiración.** Cualquier persona que intente o conspire para cometer cualquier delito previsto en este capítulo estará sujeto a las mismas sanciones que las previstas para el delito, la comisión de la que fue objeto del intento o conspiración."

**Title 18 United States Code, Section 982 (a) (2) (B) Decomiso penal.** El tribunal, al imponer una sentencia a una persona condenada por una violación, o una conspiración para violar: sección 471, 472, 473, 474, 476, 477, 478, 479, 480, 481, 485, 486, 488, 481, 501, 510, 542, 545, 555, 842, 844, 1028, 1029, o 1030 de este título, ordenará que la

persona ceda a los Estados Unidos cualquier propiedad que constituya, o se derive de, el producto obtenido directa o indirectamente, como resultado de dicha violación.

**Title 18 United States Code, Section 981 (a) (1) (C) Confiscación civil.** Se confiscará cualquier propiedad real o personal, involucrada en una transacción o intento de transacción en violación de la sección 1956, 1957 o 1960 de este título, o cualquier propiedad rastreable a dicha propiedad.

**Title 28 United States Code, Section 2461 (c) Modo de recuperación.** Si a una persona se le imputa en un caso penal una violación de una Ley del Congreso por la cual se autoriza el decomiso civil o penal de una propiedad, el Gobierno puede incluir un aviso de la confiscación en la acusación o información de conformidad con las Reglas Federales de Procedimiento Penal. Si el acusado es condenado por el delito que dio lugar a la confiscación, el tribunal ordenará la confiscación de la propiedad como parte de la sentencia en el caso penal de conformidad con las Reglas Federales de Procedimiento Penal y la sección 3554 del título 18, Código de los Estados Unidos.

**Title 21 United States Code, Section 853 (p) Confiscaciones penales.** Decomiso de propiedad sustituta en esta sección se aplicará si alguna de la propiedad fuera omitido, no reportado u ocultado por el acusado y esto aplica si:

1. El bien no puede ser localizado en el ejercicio de la diligencia debida;
2. ha sido transferido o vendido a, o depositado con un tercero;
3. ha sido colocado más allá de la jurisdicción de la corte;

4. ha disminuido sustancialmente en valor; o se ha mezclado con otras propiedades que no se pueden dividir sin dificultad.

**Casos relacionados**

**Caso de SpyEye-** Según documentos United States v. Aleksandr Andreevich Panin & Hamza Bendellad (2014) están acusados por su implicación en el desarrollo y la distribución del prolífico malware conocido como SpyEye, que ocasiono cientos de millones de dólares en pérdidas para la industria financiera en todo el mundo.


**Figura 7.** Slogan de SPY EYE. (Obtenido de: Motos, 2011)

Según el fiscal Horn de los EE. UU., los cargos y otra información presentada en el tribunal: hasta que fue desmantelado por el FBI, SpyEye fue el troyano de malware preeminente del 2010-2012, utilizado por un sindicato mundial de ciber delincuentes para infectar a más de 50 millones de computadoras, causando que $ 1 billón en daños financieros a individuos e instituciones financieras de todo el mundo.

SpyEye fue diseñado para automatizar el robo de información confidencial personal y financiera, como credenciales de banca en línea, información de tarjetas de crédito, nombres de usuario, contraseñas, PIN y otra información de identificación personal. El malware facilitó su robo de información personal y confidencial al infectar en secreto las computadoras de las víctimas, lo que permite a los delincuentes cibernéticos controlar de forma remota las computadoras infectadas a través de los servidores de comando y control ("C2"). Una vez que una computadora se infectó y estuvo bajo su control, los delincuentes cibernéticos accedieron de forma remota a las computadoras infectadas, sin autorización, y robaron la información personal y financiera de las víctimas mediante una variedad de técnicas, que incluyen "inyecciones web", "registradores de pulsaciones de teclas" y "capturadores de tarjetas de crédito" ”Los datos personales y financieros robados de las víctimas fueron luego transmitidos a escondidas a los servidores C2, donde solían, entre otras cosas, robar dinero de las cuentas financieras de las víctimas.

Panin y Bendelladj operaban desde Rusia entre 2009 y 2011, Panin conspiró con otros, incluido el coacusado Hamza Bendelladj, para desarrollar, comercializar y vender varias versiones de SpyEye y componentes en Internet. Panin permitió que los ciberdelincuentes personalizaran sus compras para incluir métodos personalizados para obtener información personal y financiera de las víctimas, así como versiones comercializadas que apuntaban a información sobre instituciones financieras específicas, incluidos bancos y compañías de tarjetas de crédito.

Con la asistencia de Bendelladj, a / k / a Bx1, Panin promocionó y promocionó el malware SpyEye en foros en línea, solo para invitados, como Darkode.com y otros foros

exclusivos para delincuentes con base en Rusia. El arresto de Bendelladj en enero de 2013 fue un factor que contribuyó al desmantelamiento de Darkode.com a través de un esfuerzo coordinado de aplicación de la ley en 20 países en julio de 2015.Por su parte, Bendelladj transmitió más de un millón de correos electrónicos no deseados que contenían cepas de SpyEye y malware relacionado a computadoras en los Estados Unidos, produciendo cientos de miles de computadoras infectadas. También desarrolló y vendió "complementos" o complementos maliciosos para botnets, como un "esparcidor", un sistema de transferencia automatizado ("ATS") y "inyecciones web". Estas herramientas maliciosas se diseñaron para automatizar a escondidas el robo de fondos de las cuentas bancarias víctimas y para multiplicar la propagación de malware, incluidos SpyEye y Zeus. El 20 de diciembre de 2011, un gran jurado del Distrito Norte de Georgia presentó una acusación de 23 cargos contra Panin, que aún no se había identificado completamente, y Bendelladj. La acusación formal cobró un cargo de conspiración para cometer fraude bancario y bancario, 10 cargos de fraude bancario, un cargo de conspiración para cometer fraude informático y 11 cargos de fraude informático. Posteriormente se devolvió una acusación de sobra que identificaba a Panin por su verdadero nombre.

Panin fue arrestado por las autoridades estadounidenses el 1 de julio de 2013, cuando voló por el Aeropuerto Internacional Hartsfield-Jackson de Atlanta. El 28 de enero de 2014, Panin se declaró culpable de conspirar para cometer fraude electrónico y bancario. Bendelladj fue detenido en el aeropuerto de Suvarnabhumi en Bangkok, Tailandia, el 5 de enero de 2013, mientras se encontraba en tránsito de Malasia a Argelia. Bendelladj fue

extraditado de Tailandia a los Estados Unidos el 2 de mayo de 2013. El 26 de junio de 2015, Bendelladj se declaró culpable de todos los 23 cargos de la acusación anulada.

Según documentos de la corte indicaban que Panin planeaba lanzar una nueva cepa de SpyEye, llamada "SpyEye 2.0", que, de ser liberada, habría sido una de las redes de bots más prolíficas e indetectables distribuidas hasta la fecha, y la causa sería inconmensurable. Aleksandr Andreevich Panin, a / k / a Gribodemon, 27, de Tver, Rusia, fue sentenciado por la Jueza del Tribunal de Distrito de los Estados Unidos, Amy Totenberg, a nueve años, seis meses de prisión seguidos de tres años de libertad supervisada. Hamza Bendelladj, a / k / a Bx1, 27, de Tizi Ouzou, Argelia, también fue condenada por el Juez Totenberg a 15 años de prisión y tres años de libertad supervisada.

**Caso Troyano Kronos –** "Man Charged for His Role" (2017) nos dice que en el caso United States v. Hutchins (2017), que luego de más de dos años de investigación, un gran jurado federal devolvió una acusación de seis cargos que pesaban en contra de Marcus Hutchins alias "Malwaretech", ya que entre julio de 2014 y julio de 2015 creó y distribuyo el troyano bancario Kronos. Al Sr. Hutchins se le acusó de un cargo de conspiración para cometer fraude y abuso informático, tres cargos de distribución y publicidad de un dispositivo de intercepción de comunicaciones electrónicas, un cargo de tratar de interceptar comunicaciones electrónicas y un intento de acceder a una computadora sin autorización.

La información disponible públicamente en la página del FBI indica que primero se puso a disposición a través de algunas páginas de Internet a principios de 2014 y se

comercializó y distribuyó a través de AlphaBay, un servicio oculto en la red Tor. AlphaBay el “mercado oscuro' en línea más grande”. El sitio ‘Dark Net’ fue una fuente importante de fentanilo y heroína, vinculado a muertes por sobredosis, y utilizado por cientos de miles de personas para comprar y vender bienes y servicios ilegales de forma anónima a través de Internet. El 20 de julio de 2017, el Departamento de Justicia anunció que el mercado de Alphabay se había cerrado a través de un esfuerzo de aplicación de la ley internacional liderado por los Estados Unidos. Consulte www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down

Según la acusación del tribunal de Distrito, el troyano bancario Kronos fue diseñado para recolectar y transferir el nombre de usuario y la contraseña asociados con los sitios web bancarios cuando se ingresan en una computadora infectada a un panel de control alojado en otra computadora inaccesible para la víctima. Según la información disponible al público, desde su creación, Kronos se configuró para filtrar las credenciales de usuario asociadas con los sistemas bancarios ubicados en Canadá, Alemania, Polonia, Francia y el Reino Unido, entre otros países.

**Caso Botnet Kelihos –** De acuerdo al caso United States v. Peter Levashov, (2018). Levashov, de 38 años, fue acusado de conspiración, delitos informáticos y robo de identidad. El botnet Kelihos fue descubierto por primera vez a fines de 2010 y operó hasta que las autoridades estadounidenses lo cerraron casi siete años después. La operación de cese se anunció el 10 de abril de 2017, solo un día después de que el propio Levashov fue capturado mientras estaba de vacaciones con su familia en España. La operación encubierta

marcó la conclusión de una investigación dirigida por el FBI que abarcó más de diez años. En febrero de 2017, España entregó Levashov a las autoridades de los Estados Unidos, mientras rechazaba la solicitud de extradición de Rusia.

Levashov es un operador de botnet veterano que ha estado detrás de al menos otras dos botnets masivas desde finales de los años noventa. En 2009, las autoridades estadounidenses lo acusaron de delitos relacionados con la operación de un precursor de

"Durante más de dos décadas, Peter Levashov operó botnets que le permitieron recopilar información personal de computadoras infectadas, diseminar spam y distribuir el malware utilizado para facilitar múltiples estafas", dijo el Fiscal General Adjunto Benczkowski en el comunicado esta semana.

Según los documentos judiciales y las declaraciones hechas ante el tribunal, una red de bots es una red de computadoras infectadas con software malicioso que permite que un tercero controle toda la red de computadoras sin el conocimiento o consentimiento de los propietarios de las computadoras. Desde fines de la década de 1990 hasta su arresto en abril de 2017, Levashov controló y operó múltiples botnets, incluidos los botnets Storm, Waledac y Kelihos, para recopilar información personal y medios de identificación (incluidas direcciones de correo electrónico, nombres de usuario y nombres de usuario y contraseñas) de computadoras infectadas. Para promover el plan, Levashov difundió el spam y distribuyó otros programas maliciosos, como troyanos bancarios y ransomware, y anunció los servicios de spam y malware de la red de bots Kelihos para que otros los compraran con el fin de enriquecerse. A lo largo de su carrera criminal, Levashov participó y moderó varios foros criminales en línea en los que se intercambiaron y vendieron

identidades y tarjetas de crédito, malware y otras herramientas criminales de ciberdelito. Se estima que hasta el momento de su arresto este malware ocasiono la pérdida de más de 4 billones de dólares.

Levashov se declaró culpable ante el Juez de Distrito Robert N. Chatigny de los Estados Unidos por un cargo de causar daño intencional a una computadora protegida, un cargo de conspiración, un cargo de fraude electrónico y un cargo de robo de identidad con agravantes. El juez Chatigny programó la sentencia para el 6 de septiembre de 2019 y Levashov está detenido en espera de la sentencia.

**Herramientas de investigación**


FTK es una herramienta que ayuda los auditores forenses a realizar búsquedas rápidas en las computadoras y en los celulares. Al utilizar el cien por ciento de los recursos de su hardware, ayuda a nosotros los investigadores a encontrar la información relevante mucho más rápido. El FTK imagen nos ayudara a conseguir cualquier información que este oculta o que haya sido borrada. (Caballero, A. s.f)


El sistema IDEA es una herramienta de análisis de datos que proporciona que ayuda a de manera estructurada realizar auditorías organizadas,

eficientes e integrales, cada aspecto del análisis de datos, desde la importación de datos hasta el informe de resultados. Ayuda analizar la totalidad de datos, garantizando su integridad y proporcionando más de cien tareas automatizadas que facilitan el trabajo para los equipos de trabajo. A atreves de IDEA se automatizará el análisis de datos de sus sistemas financieros, así como del área de recursos humanos, auditoría, contabilidad, entre otras. (*IDEA*, 2019)


- Es una herramienta utilizada por muchas entidades para realizar operaciones forenses gracias a su código abierto. Kali Linux combina las funcionalidades de muchos otros paquetes más pequeños que están más enfocados en su enfoque en una aplicación ordenada con una interfaz de usuario basada en el navegador web. Se usa para investigar imágenes de disco. Cuando hace clic en Autopsy, inicia el servicio y se puede acceder a su interfaz de usuario en el navegador web en http://localhost:9999/autopsy. Nos da al usuario una gama completa de opciones necesarias para crear un nuevo archivo de caso: Nombre del caso, Descripción, Nombre del investigador, Nombre de host, Huso horario del host, etc. Entre sus funcionalidades incluyen: análisis de la línea de tiempo, búsqueda de palabras clave, artefactos web, filtrado hash, talla de datos, multimedia e indicadores de compromiso. Acepta imágenes de disco en formato RAW o E01 y genera informes en HTML, XLS y archivo de cuerpo dependiendo de lo que se requiere para un caso particular. (“Herramientas de análisis forense*”*, (s.f)

## SECCIÓN 3 – SIMULACIÓN DEL CASO

Según Departamento de Justicia Oficina del Fiscal de los Estados Unidos Distrito Sur de Nueva York (2019), el viernes 22 de febrero de este año, Stanislav Vitaliyevich Lisov, de 33 años, conocido bajo los seudónimos “Black” and “Blackf”, compareció ante el Tribunal Federal de Manhattan (EE. UU.) y acepto que es el cerebro detrás del sofisticado troyano bancario NeverQuest. Lisov utilizó el malware para infectar las computadoras de las víctimas, obtener sus credenciales de inicio de sesión para cuentas bancarias en línea y robar dinero de sus cuentas". Por otro lado, el Fiscal Federal Geoffrey S. Berman también dijo: “Este tipo de delito informático se extiende a través de las fronteras, representa una amenaza maliciosa para la privacidad personal y causa un daño financiero generalizado. Por su crimen audaz, este hacker ruso ahora se enfrenta a la justicia en una corte estadounidense ".

### Esquema de fraude

El troyano NeverQuest quien también es conocido como Vawtrak y Snifula es una familia de caballos de Troya que han estado en circulación desde 2012.Las víctimas veían comprometidas sus computadoras de diferentes maneras, por email infectados que contenían documentos en Word con imágenes las cuales tenían oculto en la foto el código de NeverQuest o con archivos .ZIP, los emails regularmente decía que eran de algún paquete el cual no fue entregado o la victima al visitar algunos sitios web los cuales albergaban códigos de redirección de Flash maliciosos los cuales llevaban los

navegadores de las victimas  a páginas de terceros que contenían el kit Angler Exploit que luego dejaría a NeverQuest en sus sistemas. Lisov utilizo NeverQuest al lograr acceso a las computadoras de las víctimas y cuando las personas utilizaban portales bancarios en línea. El malware robaba la información como User, Password, Preguntas de seguridad y las respuestas y cuando ya las tenía desde la misma computadora de la víctima usaba las credenciales robadas y hacia transferencias fraudulentas desde la cuenta de banco.

El sofisticado malware fue capaz de evadir los sistemas de seguridad de autenticación de dos factores (2FA) al inyectar un código adicional en las páginas web. Incluso si se utilizaba un banco en línea que NeverQuest no conocía anteriormente, el malware detectaría el uso de la terminología bancaria (como "IBAN") en las páginas web, descargaría el contenido completo de la página para que se pudieran crear nuevas inyecciones web para robar fondos de otros los clientes bancarios en el futuro. Lisov y sus cómplices utilizaron Neverquest para robar las credenciales de inicio de sesión de los clientes bancarios, aprovecha los mecanismos de inyección para proporcionar a los usuarios formularios falsos en sitios web bancarios legítimos. El troyano bancario puede grabar pulsaciones de teclas, robar contraseñas almacenadas en la PC y tomar capturas de pantalla y videos de la máquina de las víctimas.

El malware de Neverquest puede iniciar sesión en la cuenta bancaria en línea de la víctima y realizar transacciones fraudulentas. Los nombres de usuario y las contraseñas de sitios como Facebook, Twitter y MailChimp fueron recopilados por el malware. Además, LISOV

discutió el tráfico de información de inicio de sesión robada e información de identificación personal de las víctimas.

Según Kapersky.com (2019), otra función del malware es renovar su lista de bancos y crear los códigos que después inyectarían en los nuevos sitios web bancarios, los cuales no estaban en su lista de blancos. Esto se realiza de la siguiente manera:

- Los archivos de configuración contienen una lista de palabras clave que, si se encuentran en una página web en el navegador, entonces el programa malicioso interceptaba el proceso y enviaba todo el contenido de la página web bancaria, así también el URL, a Lisov y sus cómplices.
- Dependiendo de la información recibida, desarrollan un código adicional que inyectarán en ese sitio web.
- Entonces, este nuevo sitio web queda incluido en la lista de sitios web y el nuevo código se añade a la lista de scripts maliciosos en el archivo de configuración.
- Como paso final, el archivo de configuración actualizado se distribuye a todos los equipos infectados.

Esta es la lista de palabras clave utilizadas para desarrollar un código adicional (términos en inglés y en español):

- Available balance
- Account summary
- Checking account
- saldo
- cuenta
- Balance
- Available Balance
- Account Summary
- Checking Account
- Available balance
- Current Balance
- Accounts Balance Footnote
- Saldo
- Cuenta
- Balance
- Business Accounts
- Deposit Accounts
- Account Balances
- Career Builder
- Site Key Challenge Question


**Figura 8.** Esquema NeverQuest

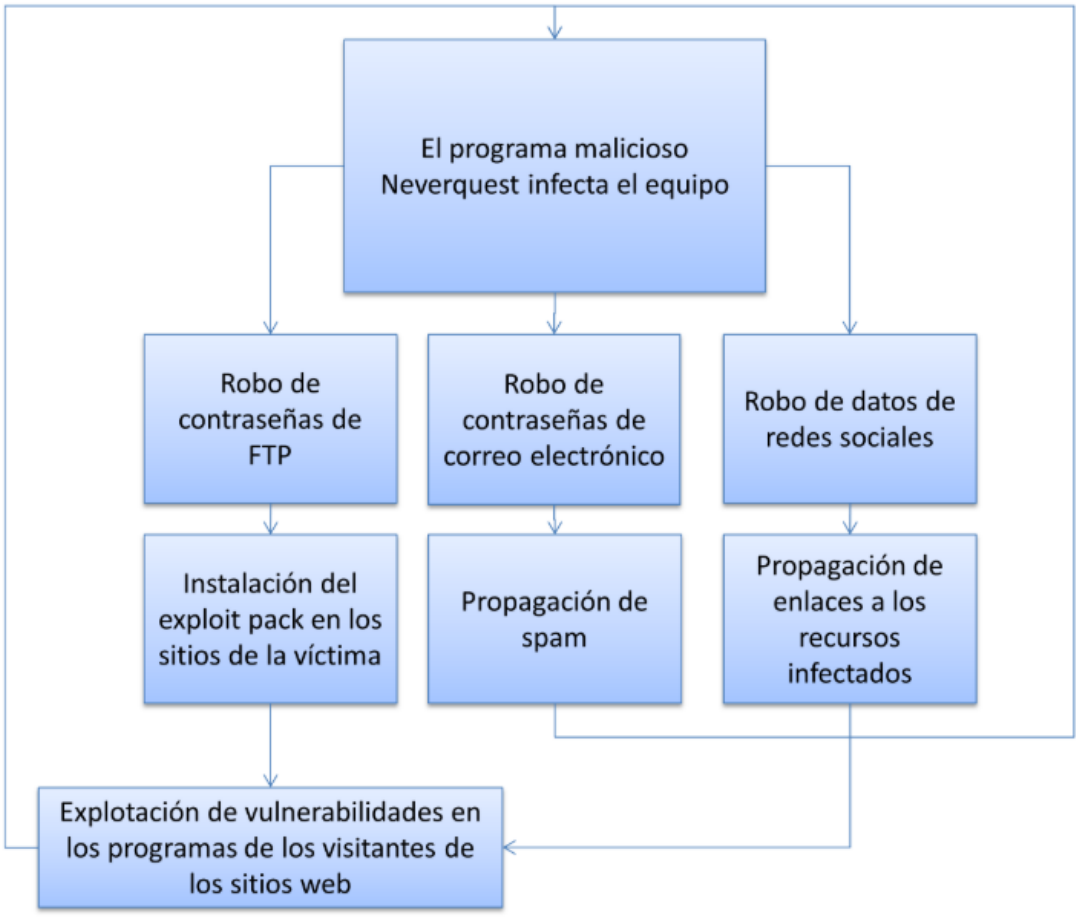



**Figura 9**. Esquema Neverquest explicación manera sencilla.

## SECCIÓN 4 – INFORME DEL CASO

### Resumen Ejecutivo

El Sr. Stanislav Vitaliyevich Lisov es acusado por el Departamento de Justicia de los E.U. y el FBI de fraude Conspiración piratería informática y Conspiración para cometer fraude electrónico. El FBI hace el debido proceso de recopilación de evidencia y mediante la incautación de las computadoras, un USB y un Hard Drive WD Elements SE de 1 TB se recopilo toda la data sensible siguiendo el debido proceso EDRM.

El FBI hizo entrega de un USB y Hard drive con imágenes del disco de la computadora de a la Sra. Janefix Díaz Ramos de JDR Forensic LLC. para analizarlos. Se entregó el USB y el Hard drive con el propósito de obtener evidencia de las imágenes para determinar de qué manera se introdujo en los sistemas y cómo el acusado junto a sus cómplices obtuvo la información de las víctimas.

Como resultado de evaluar lo ocupado, el investigador encontró varias imágenes las cuales correspondían a emails que eran enviados con imágenes y estenografía digital (mensaje oculto en imagen, GIF, ZIP) las cuales contenían el troyano Neverquest, una vez la victima abría el email que contenía la imagen de alguna promoción de venta o servicio, su computadora o servidor se infectaba. En el USB se encontró la imagen que fue posteada en el dark web por el acusado o algún cómplice ofreciendo la venta del troyano para obtener beneficio económico de este. Por otro lado, de igual modo se logró encontrar en el Hard drive externo páginas en Word y Excel con User, password, cálculos de su actividad ilícita sobra las ventas.

## Objetivo

El Departamento de justicia del Distrito Sur de Nueva York y el FBI delegaron la investigación del USB y Hard Drive los cuales contenían información sobre las actividades ilícitas de fraude del Sr. Stanislav Vitaliyevich Lisov y las imágenes recuperadas para su evaluación fueron entregadas a la investigadora Sra. Janefix Díaz Ramos. Imágenes de las computadoras del acusado fueron creadas por el FBI y entregadas en un USB para ser analizadas.

## Alcance del trabajo

El 1 de marzo de 2015, los fiscales del caso Michael D. Neff y Geoffrey S. Berman fiscal para el Distrito Sur de Nueva York le entregaron a la examinadora forense Janefix Díaz lo ocupado del acusado. Luego de seguir el protocolo en la cadena de custodia de evidencia se nos fue entregado un USB de marca PNY de una capacidad de 16GB de almacenaje, el cual fue identificado como Evidencia No.1 con la imagen del Hard Drive externo y Evidencia # 2 el cual contiene información e imágenes que fueron recuperadas por el FBI. El propósito de este trabajo es lograr extraer las capturas fiel y exacto de la evidencia suministrada, así como descubrir si alguna evidencia fue borrada, lograr recuperarla para pasar el debido análisis crítico.

## Datos del caso

- **Número del caso:** 1:17-CR-00048
- **Examinador Forense:** Janefix Díaz Ramos

- **Cliente:** FBI oficina de Nueva York
- **Representante:** William F. Sweeney Jr., Director Adjunto a cargo de la Oficina de Nueva York FBI

**Descripción de los dispositivos utilizados**

A continuación, se detallan los dispositivos utilizados durante el proceso investigativo:

- Una laptop Hewlett Packard (HP), modelo HP 15-BS013DX, Pantalla 15.6" Touchscreen, procesador Intel i3-7100U, 8GB de memoria, 1TB de disco duro y un sistema operativo Windows 10 de 64 bits.

- WD Elements SE Hard Drive external 1 TB

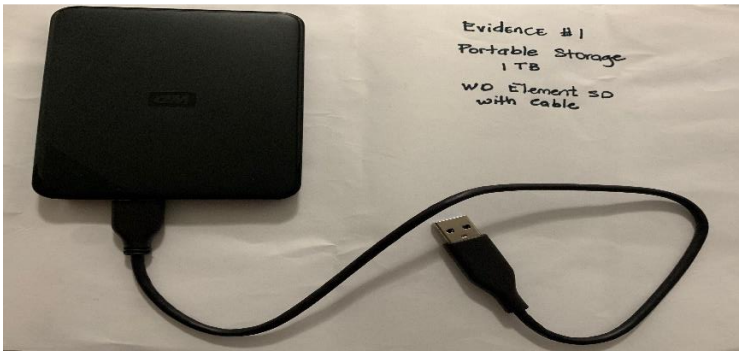



**Figura 10.** Hard drive entregado por fiscales y utilizado para crear las imágenes.

- USB – Marca PNY de 16GB capacidad memoria.

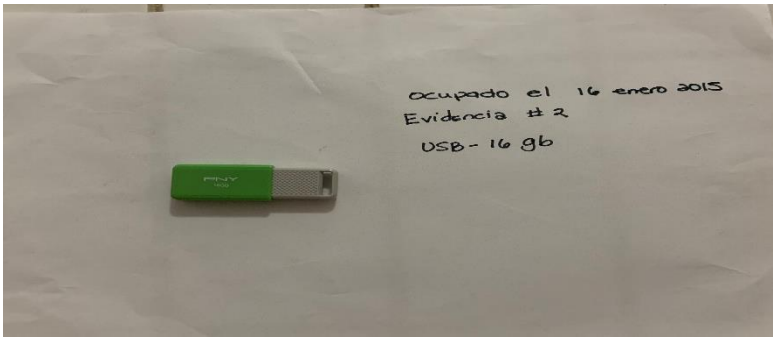



**Figura 11.** USB entregado por los fiscales y utilizado para crear las imágenes.

**Resumen de hallazgos**

El proceso de analizar de manera forense la data digital envuelve el adquirir, lograr preservar y lograr presentar toda la evidencia de manera certera y confiable. Toda esta evidencia por decirlo de algún modo es frágil y los investigadores sin querer modificar o eliminar toda la información que contenga algún dispositivo el cual este siendo evaluado para cualquier investigación por lo cual, si no se procesa de la manera correcta y siguiendo las normas esta puede ser inadmisible de presentarse en un tribunal.

Utilizando el Modelo de Socha (s.f) Referencia de Descubrimiento Electrónico (EDRM) el cual usados en el marco investigativo describe los estándares para la recuperación y el descubrimiento de datos digitales. El EDRM fue desarrollado en 2005 por George Socha Jr. Es modelo de referencia de descubrimiento electrónico consta de nueve pasos para la gestión de la información almacenada electrónicamente (ESI).

- Gestión de la información: implementamos procesos de gestión de datos que alivien los riesgos y los gastos en caso de una solicitud de descubrimiento electrónico.
- Identificación: localizamos las fuentes de información para determinar exactamente qué son los datos y cómo deben gestionarse.
- Preservación: Nos aseguramos de que la información sea relevante para el descubrimiento electrónico y se almacene correctamente.
- Colección: Recopilar información para poder usar las herramientas forenses.
- Procesamiento: Reduzca el volumen del ESI relevante y conviértalo para revisión y análisis.
- Revisión: Determine la relevancia del descubrimiento electrónico de los datos.
- Análisis: Evaluación de la evidencia para el contenido y el contexto del caso.
- Producción: Se produce el informe de la investigación.
- Presentación: Mostramos los resultados de los datos en la declaración al FBI, audiencias y/o juicios y dar paso a validar hechos frente a un jurado de ser necesario.

A continuación, se presentan los hallazgos identificados durante la investigación realizada a los dispositivos entregados por el FBI a el investigador.

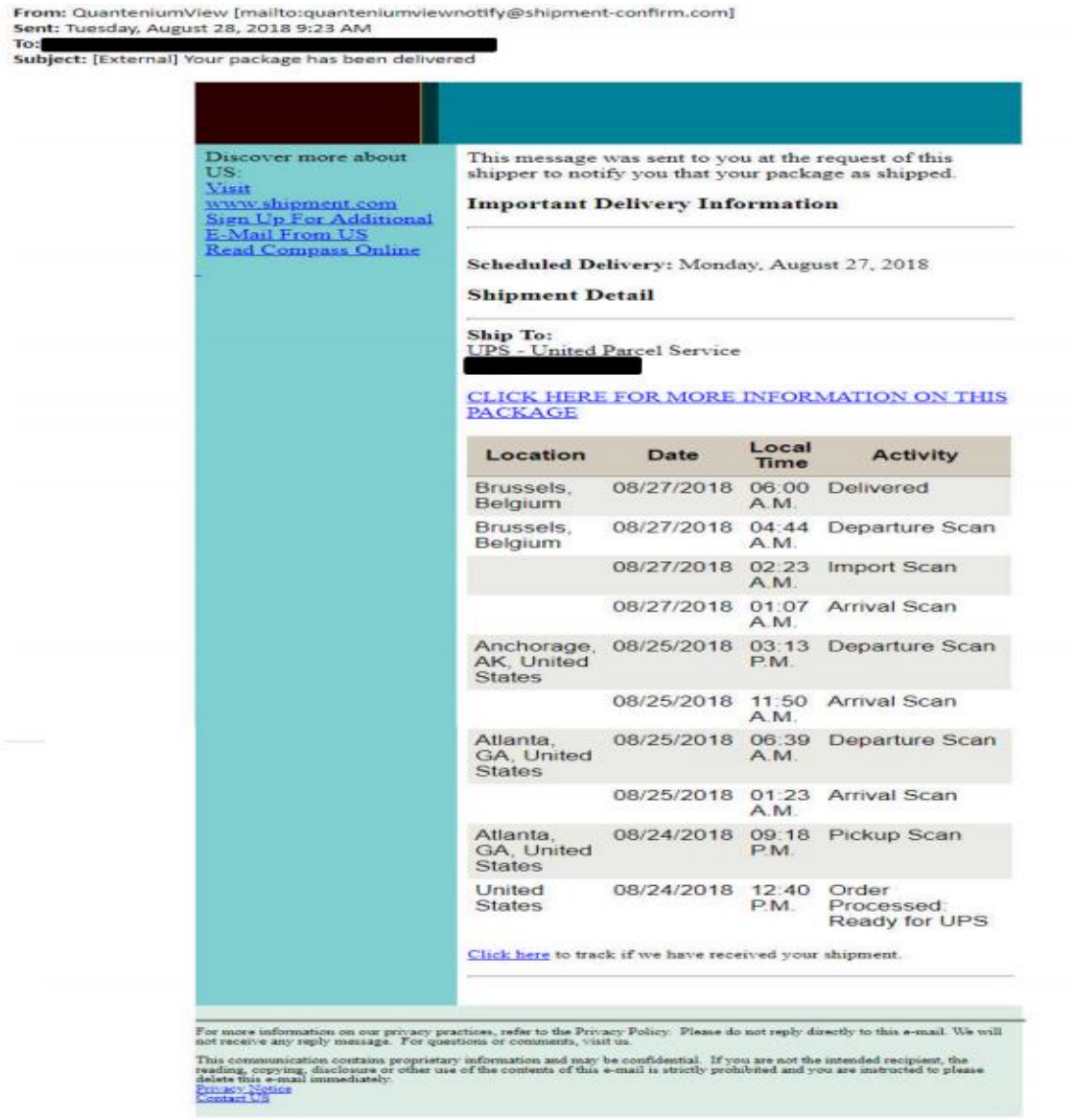



**Figura 13.** Email simulaba tracking de algún paquete de UPS.

- Este tipo de email simulaba ser de UPS el cual tenía la información de tracking de algún paquete, la victima al darle click para ver la información de este ya el sistema se veía comprometido por el malware.

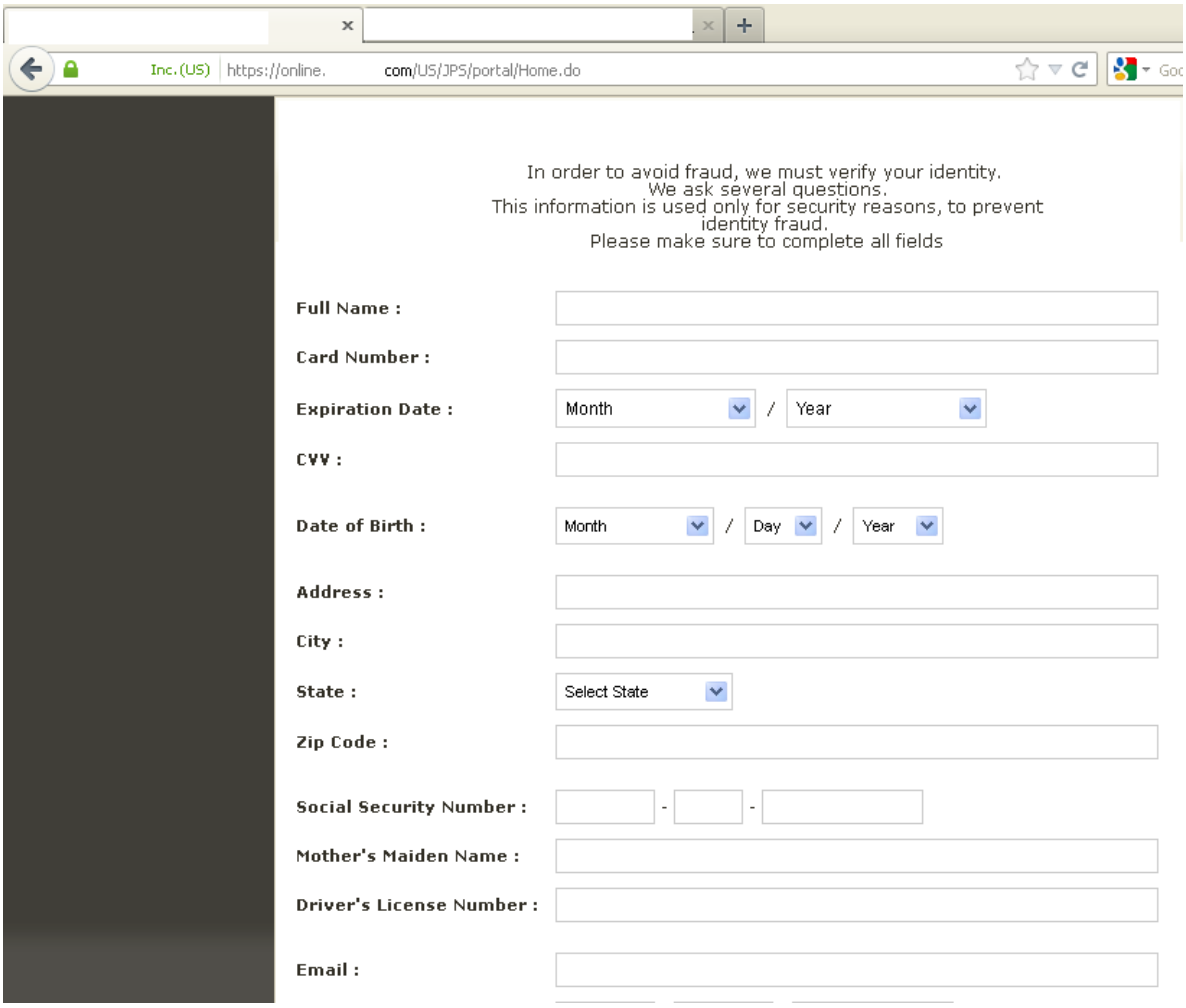



**Figura 14.** Página infectada con el malware que simulaba ser de formulario UPS.

- Al llegar un email que simula ser de UPS las eran redirigidas a este tipo de página la cual decía que para evitar el fraude necesitan verificar la identidad de la víctima y solicitan información confidencial y sensible como Nombre completo, información de tarjeta de crédito, fecha de nacimiento, seguro social y hasta número de licencia de conducir. Las victimas creían que era algo legítimo de UPS, porque irónicamente dicho portal decía que era dicha información era solicitada por razones de seguridad y evitar el fraude.

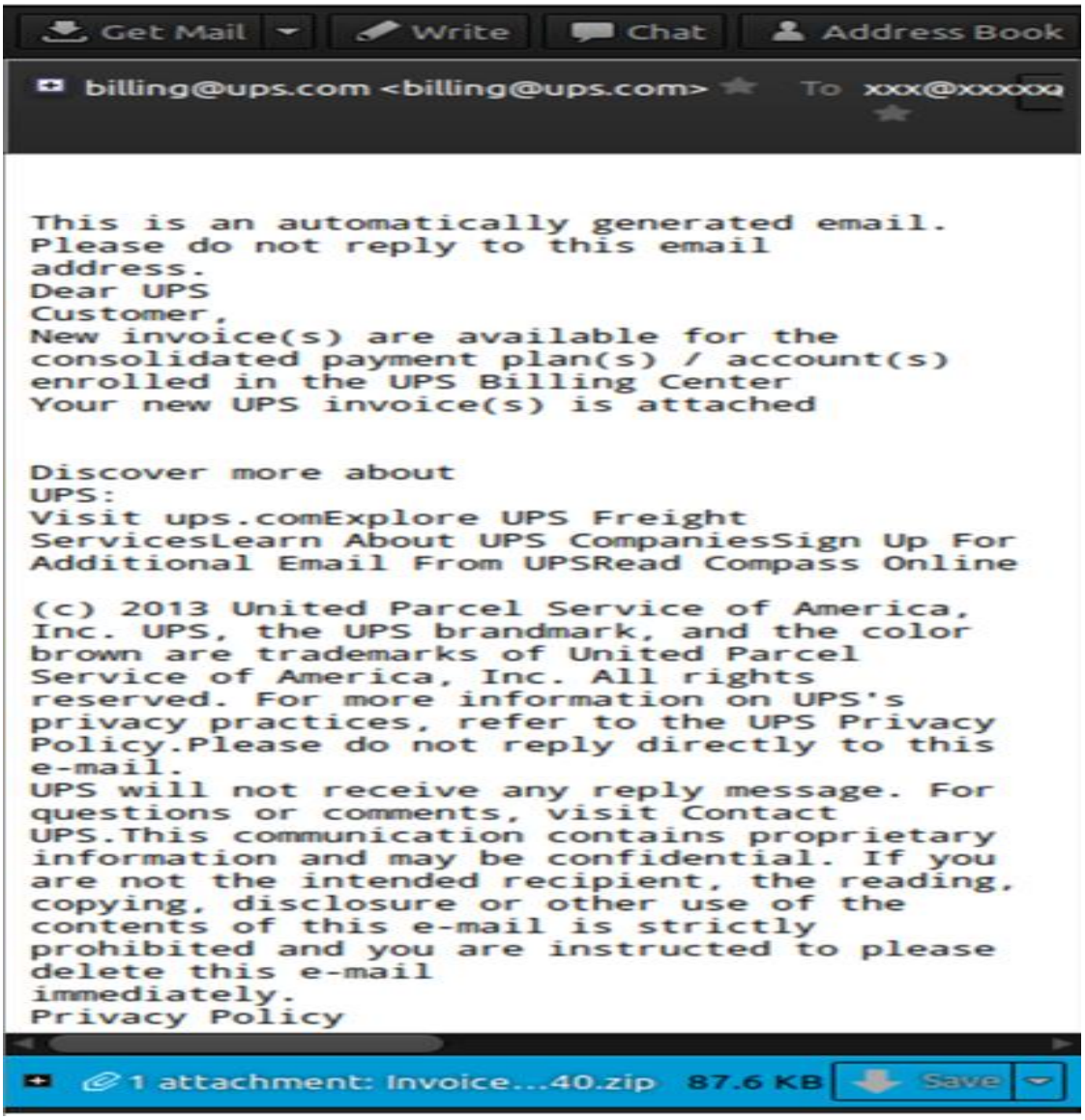



**Figura 15.** Email simulando ser UPS el cual contiene el virus NeverQuest.

- Este tipo de email es una de las maneras por las cuales se propagaba en malware ya que era enviado en cercanas a días festivos ya que era alta la probabilidad que la víctima creyera que era un email legítimo. Al ingresar en el link provisto en el email ya el malware se alojaba en la PC, era cuestión de tiempo que el usuario entrara a una página de banca online y robar su información.

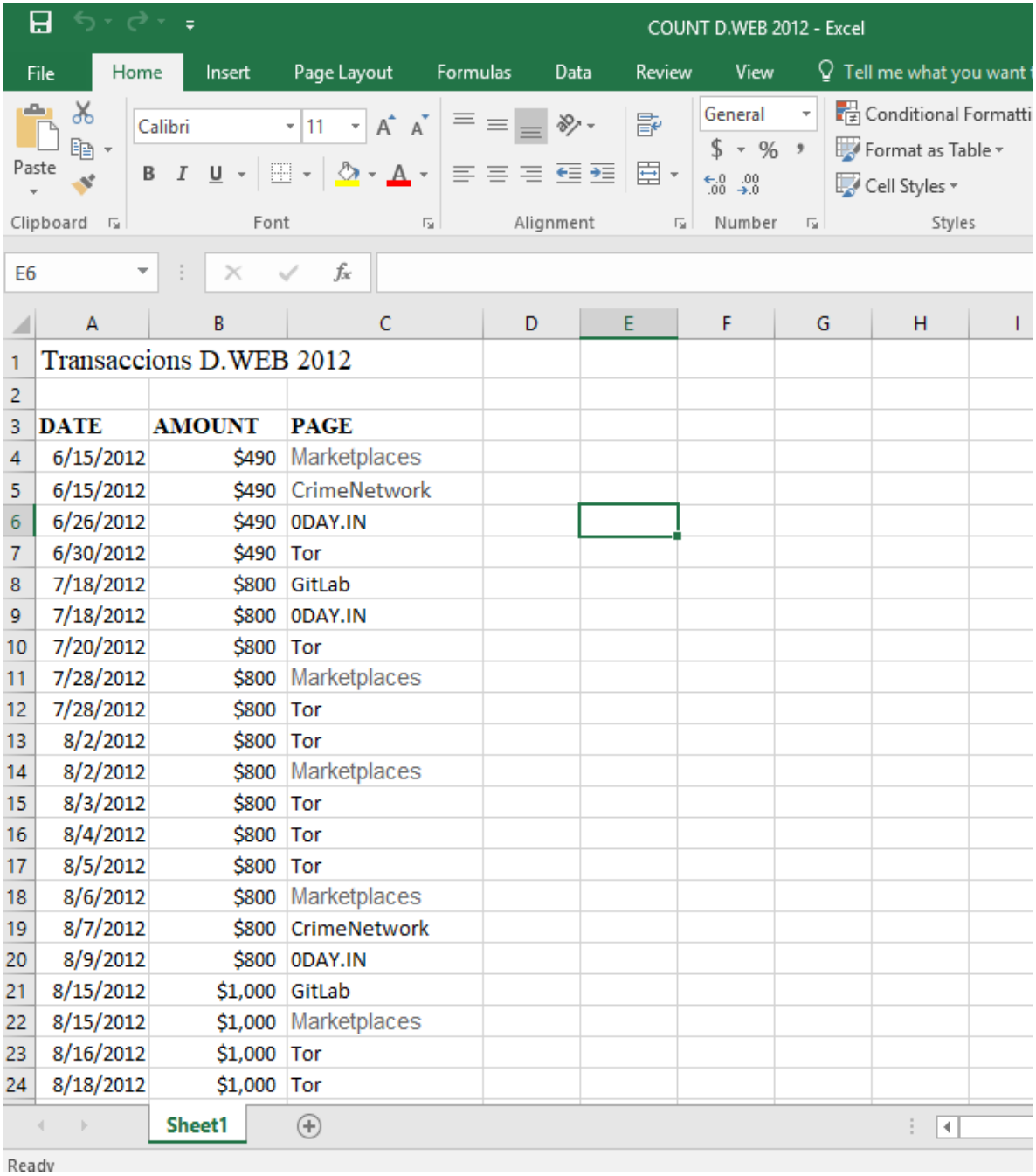



**Figura 16**. Hallazgo de Hoja Excel con cálculos 2012 de ventas de Troyano en Dark web.

- Se logró tener acceso en USB Evidencia # 2 hojas de cálculo de Excel en el cual podemos observar que en efecto se puede decir que desde junio 2012 el acusado Hizo uso del malware para beneficio propio al vender este en el mercado negro.

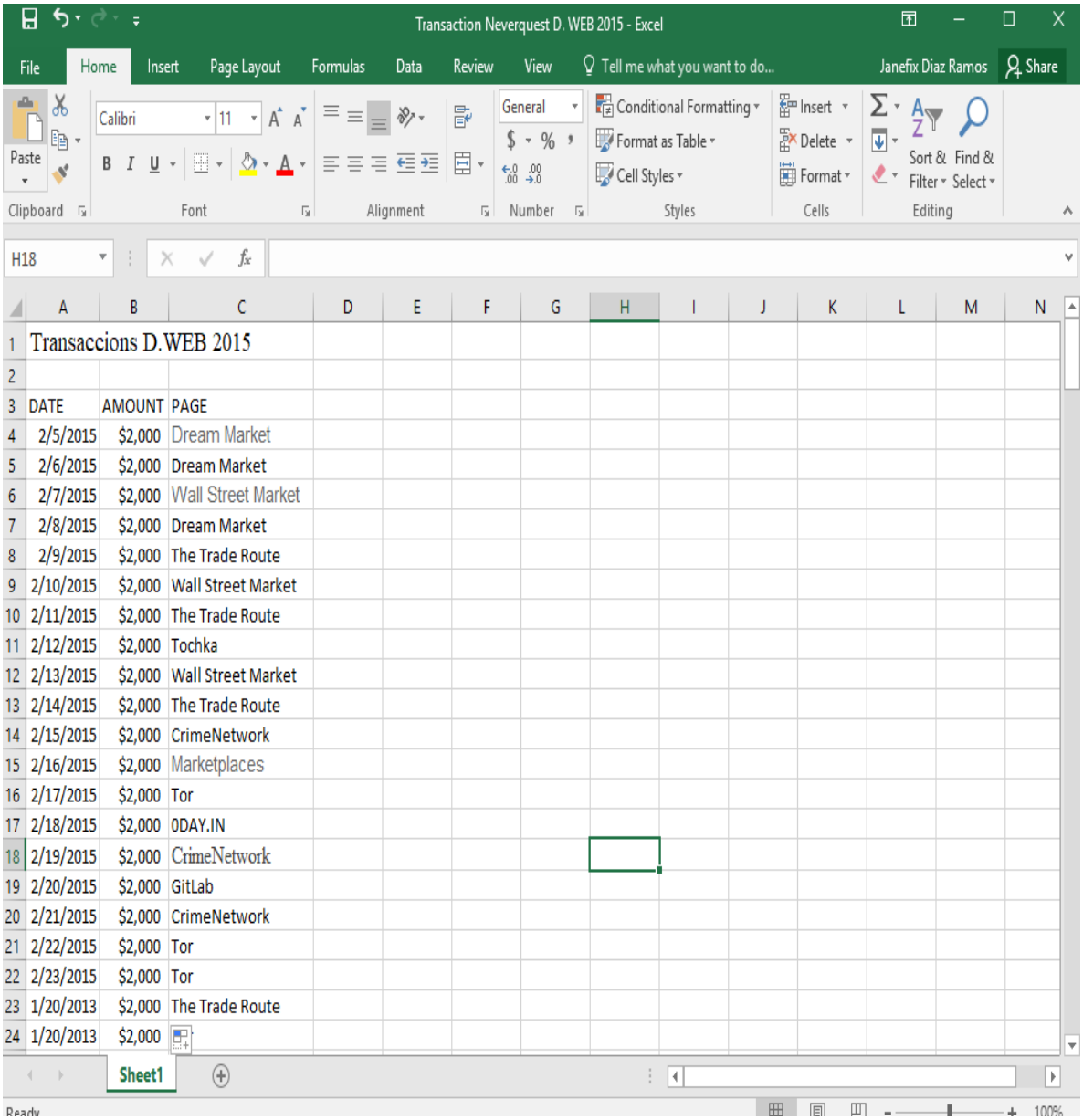
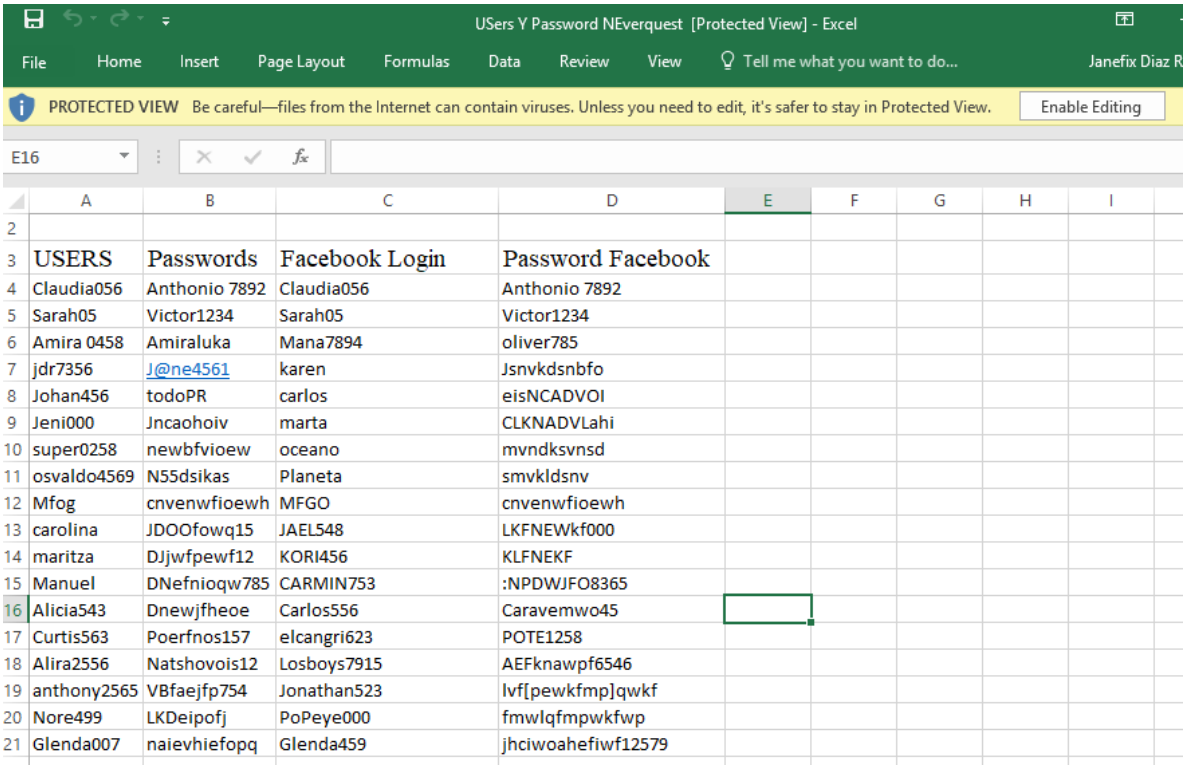



**Figura 17.** Hallazgo de Hoja Excel con cálculos 2015 de ventas de Troyano en Dark web.

- Hoja de Excel encontrada en USB Evidencia #2 de transacciones de venta de NeverQuest hasta el año 2015.




| | A | B | C | D | E | F | G | H | I |
|---|---|---|---|---|---|---|---|---|---|
| 2 | | | | | | | | | |
| 3 | USERS | Passwords | Facebook Login | Password Facebook | | | | | |
| 4 | Claudia056 | Anthonio 7892 | Claudia056 | Anthonio 7892 | | | | | |
| 5 | Sarah05 | Victor1234 | Sarah05 | Victor1234 | | | | | |
| 6 | Amira 0458 | Amiraluka | Mana7894 | oliver785 | | | | | |
| 7 | jdr7356 | J@ne4561 | karen | Jsnvkdsnbfo | | | | | |
| 8 | Johan456 | todoPR | carlos | eisNCADVOI | | | | | |
| 9 | Jeni000 | Jncaohoiv | marta | CLKNADVLahi | | | | | |
| 10 | super0258 | newbfvioew | oceano | mvndksvnsd | | | | | |
| 11 | osvaldo4569 | N55dsikas | Planeta | smvkldsnv | | | | | |
| 12 | Mfog | cnvenwfioewh | MFGO | cnvenwfioewh | | | | | |
| 13 | carolina | JDOOfowq15 | JAEL548 | LKFNEWkf000 | | | | | |
| 14 | maritza | DJjwfpewf12 | KORI456 | KLFNEKF | | | | | |
| 15 | Manuel | DNefnioqw785 | CARMIN753 | :NPDWJFO8365 | | | | | |
| 16 | Alicia543 | Dnewjfheoe | Carlos556 | Caravemwo45 | | | | | |
| 17 | Curtis563 | Poerfnos157 | elcangri623 | POTE1258 | | | | | |
| 18 | Alira2556 | Natshovois12 | Losboys7915 | AEFknawpf6546 | | | | | |
| 19 | anthony2565 | VBfaejfp754 | Jonathan523 | lvf[pewkfmp]qwkf | | | | | |
| 20 | Nore499 | LKDeipofj | PoPeye000 | fmwlqfmpwkfwp | | | | | |
| 21 | Glenda007 | naievhiefopq | Glenda459 | jhciwoahefiwf12579 | | | | | |

**Figura 18.** Hallazgo listo de User y Password de víctimas**.**

- Hoja d Excel con información de miles de usuario, User, Password de cuentas bancarias, logins y password de páginas de redes sociales. Lisov llegó un momento dado que tenía tanta información de victimas que decidió hacer files con información los cuales eran vendidos en el mercado negro.

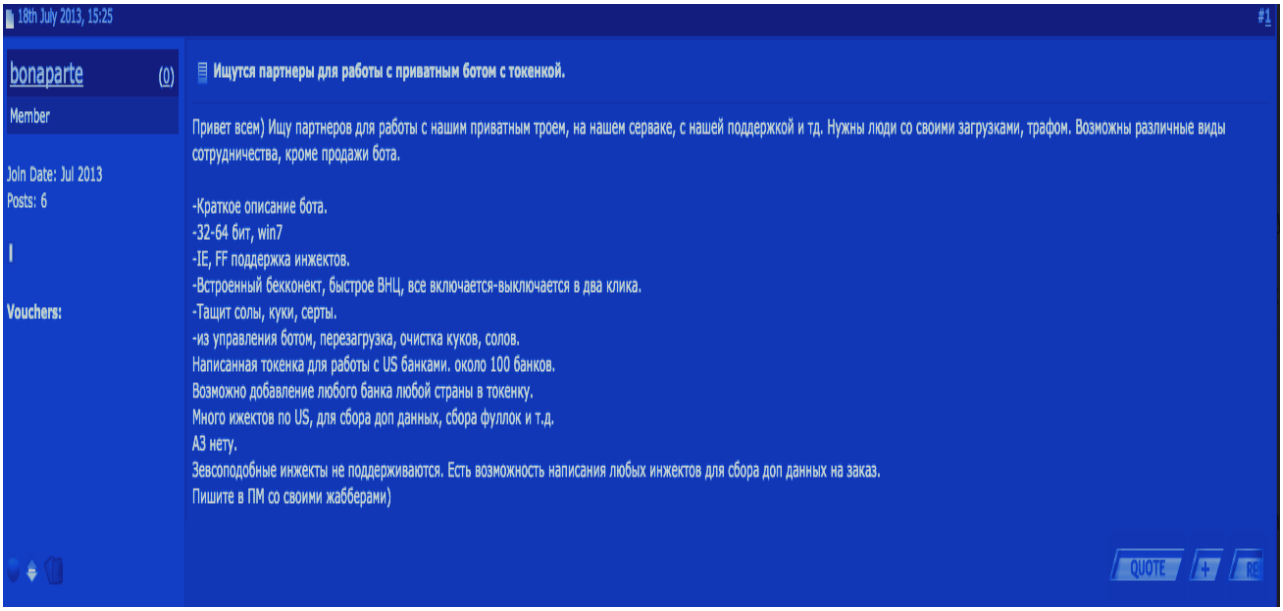



**Figura 19.** Hallazgo de mensaje en el dark web ofreciendo para la venta NeverQuest.

- Se encontró un mensaje en el cual se ofrece para la venta el troyano NeverQuest en la Dark web, Lisov y sus cómplices utilizaban paginas conocidas para este tipo de actividad ilícita como Dream Market, Trade Route, Market Place, Tor y Wall Street Market que precisamente este año el gobierno federal junto a la Interpol pudo dar de baja esta página ilegal.

## Cadena de custodia

JDR Forensic LLC está comprometido con cumplir a cabalidad con todo los reglas, procesos y protocolos para que toda evidencia presentada no se vea comprometida y pueda ser usada en un tribunal. Por medio del proceso de la cadena de custodia comprobaremos la obtención de toda la evidencia, por lo que lo detallaremos a continuación:

**Primer Evento**

- Descripción del evento**:** Recibo de evidencia fue entregado por el fiscal a cargo del caso Michael D. Neff y fue recibida por el agente investigador Janefix Diaz Ramos, examinador de JDR Forensic LLC. La evidencia son un WD Element Hard drive de 1 TB y un USB PNY de 16GB**los** cuales están identificados como Evidencia # 1 y Evidencia # 2.
- Evento verificado por el fiscal Michael D. Neff (en representación del cliente) y Janefix Diaz Ramos (Examinador Forense)
- Fecha de comienzo: 15 marzo de 2017 – 9:00am
- Fecha de culminación: 15 marzo de 2017 – 9:20am
- Lugar de origen: Oficinas Centrales JDR Forensic LLC - 7635 N Blvd Tucson, AZ, United States 85741

**Segundo Evento**

- Descripción del evento: Creación número del caso y asignación de evidencia.
- Evento verificado por: Janefix Diaz Ramos (Examinador Forense)
- Asignar número al caso: 1:17-CR-00048
- Fecha de comienzo: 15 de marzo de 2017 – 9:30am
- Fecha de terminación: 15 de marzo de 2017 – 9:45am
- Lugar de origen: Laboratorio Forense de JDR Forensic, LLC
- Destino: Laboratorio Forense de JDR Forensic, LLC

**Tercer Evento**

- Descripción del evento: Se generó las imágenes del USB y Hard Drive por separado y así evitar la contaminación o perdida de la evidencia en medio de la examinación en *FTK Imager*.
- Evento verificado por: Janefix Diaz Ramos
- Número de caso: 1:17-CR-00048
- Fecha de comienzo: 15 de marzo de 2017 – 10:00am
- Fecha de terminación: 15 de marzo de 2017 – 10:40am
- Lugar de origen: Laboratorio Forense de JDR Forensic, LLC
- Destino: Laboratorio Forense de JDR Forensic, LLC

**Cuarto Evento**

- Descripción del evento: La evidencia se procede a guardarse en bóveda. Un Hard Drive y un USB Evidencia # 1 y 2 del caso 1:17-CR-00048, 4 imágenes en un Hard Drive de 1 TB y 2 en un USB de 16GB marca PNY color verde y gris.
- Evento verificado por: Janefix Diaz Ramos (Examinador Forense) y Carlos Estrada (Supervisor área de la Bóveda)
- Número de caso: 1:17-CR-00048
- Fecha de comienzo: 15 marzo de 2017 – 10:55am
- Fecha de terminación: 15 de marzo de 2017 – 11:30am
- Lugar de origen: Laboratorio Forense de JDR Forensic, LLC

- Destino: Cuarto de evidencia de Laboratorio Forense de JDR Forensic, LLC

**Quinto Evento**

- Descripción del evento: Se busco en la bóveda del cuarto de evidencia de JDR Forensic, LLC las imágenes identificadas Evidencia # 1 y una imagen identificada como *Evidencia # 2* para analizar.
- Evento verificado por: Janefix Diaz Ramos (Examinador Forense) y Carlos Estrada (Supervisor área de la Bóveda)
- Número de caso: 1:17-CR-00048
- Fecha de comienzo: 15 de marzo de 2017 – 12:00pm
- Fecha de terminación: 15 de marzo de 2017 – 12:40pm
- Lugar de origen: Cuarto Laboratorio Forense de JDR Forensic, LLC
- Destino: Laboratorio Forense de JDR Forensic, LLC

**Sexto evento**

- Descripción del evento: Análisis de las imágenes identificadas como *Evidencia # 1* y *Evidencia # 2* utilizando el programa *FTK Imager*.
- Evento verificado por: Janefix Diaz Ramos (Examinador Forense)
- Número de caso: 1:17-CR-00048
- Fecha de comienzo: 16 de marzo de 2017 – 1:20pm
- Fecha de terminación: 16 de marzo de 2017 – 5:30pm
- Lugar de origen: Laboratorio Forense de JDR Forensic, LLC
- Destino: Laboratorio Forense de JDR Forensic, LLC

**Séptimo evento**

- Descripción del evento: Devolución de las imágenes a la bóveda, identificadas como *Evidencia # 1 y Evidencia # 2* cuarto de evidencias de JDR Forensic, LLC.
- Evento verificado por: Janefix Diaz Ramos (Examinadora Forense) Carlos Estrada (Supervisor área de la Bóveda).
- Número del caso: 1:17-CR-00048
- Fecha de comienzo: 18 de marzo de 2017 – 2:00pm
- Fecha de terminación: 18 de marzo de 2017 – 3:10pm
- Lugar de origen: Laboratorio Forense de JDR Forensic, LLC
- Destino: Cuarto de evidencia de JARV, LLC

**Octavo evento**

- Descripción del evento: Se entrega de evidencia original al fiscal a cargo del caso Michael D. Neff.
- Evidencia verificada por: Investigadora Janefix Diaz Ramos y el fiscal a cargo del caso Michael D. Neff
- Numero de evidencia: Evidencia # WD Elements Hard drive 1 TB negro y Evidencia # 2 USB 16GB color verde y gris.
- Fecha de comienzo: 19 de marzo de 2017 - 1:30pm
- Fecha de terminación: 19 de marzo de 2017 - 3:00pm
- Lugar de origen: Laboratorio forense JDR Forensic, LLC.
- Destino: Oficina Central FBI

**Noveno evento**

- Descripción del evento: Se entrega informe de análisis forense al fiscal encargado del caso Michael D Neff.
- Evidencia entregada por: Investigadora Janefix Diaz Ramos al fiscal encargado del caso Michael D Neff.
- Evidencia verificada por: Investigadora Janefix Diaz Ramos y el fiscal Michael D. Neff.
- Fecha de comienzo: 20 marzo de 2017 – 9:00 AM
- Fecha de terminación: 20 marzo de 2017 – 9:20 AM
- Lugar de origen: Laboratorio forense JDR Forensic, LLC
- Destino: Oficina Central FBI

**Procedimiento**

Como perito del caso decidí utilizar la herramienta para análisis forense FTK, y se recuperó imagines del USB y disco externo que se nos fue entregado por el FBI. En estos archivos, que tenía bajo mi custodia, se encontraron correos electrónicos (e-mails), documentos de Word y Excel sobre transacciones en la dark web, de la venta del troyano en el mercado negro desde diferentes páginas y cuentas ingresos que tenía en su computadora.

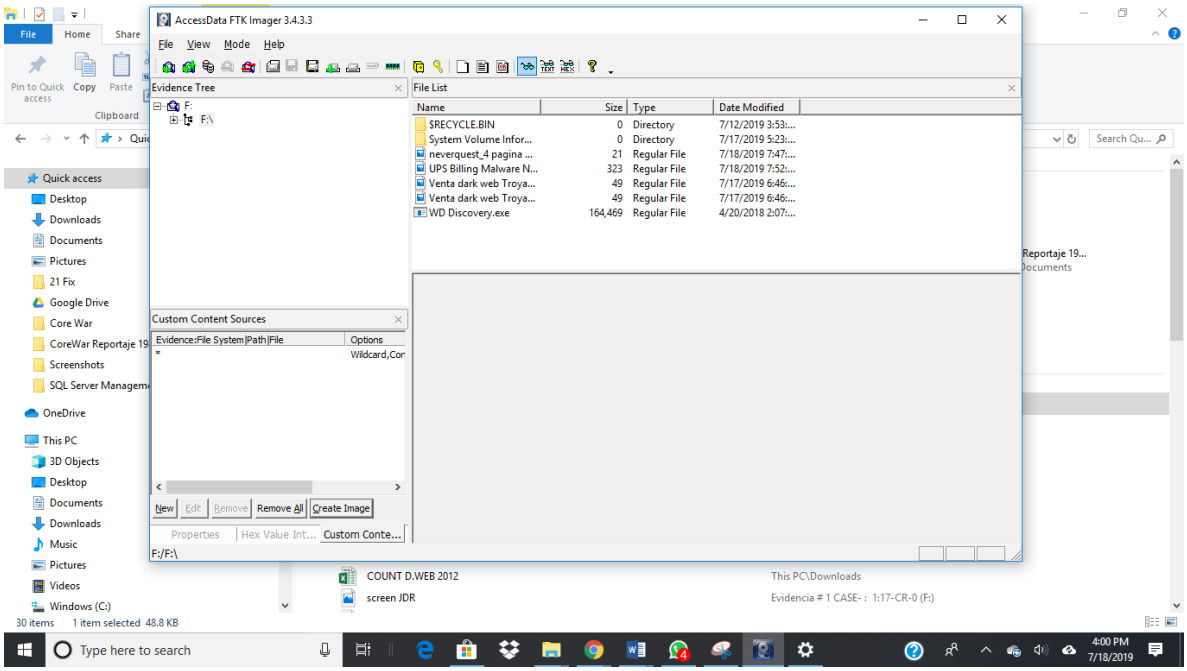



**Figura 20**. Imagen tomada de Evidencia # 1 vemos todos los archivos o documentos que contienen.

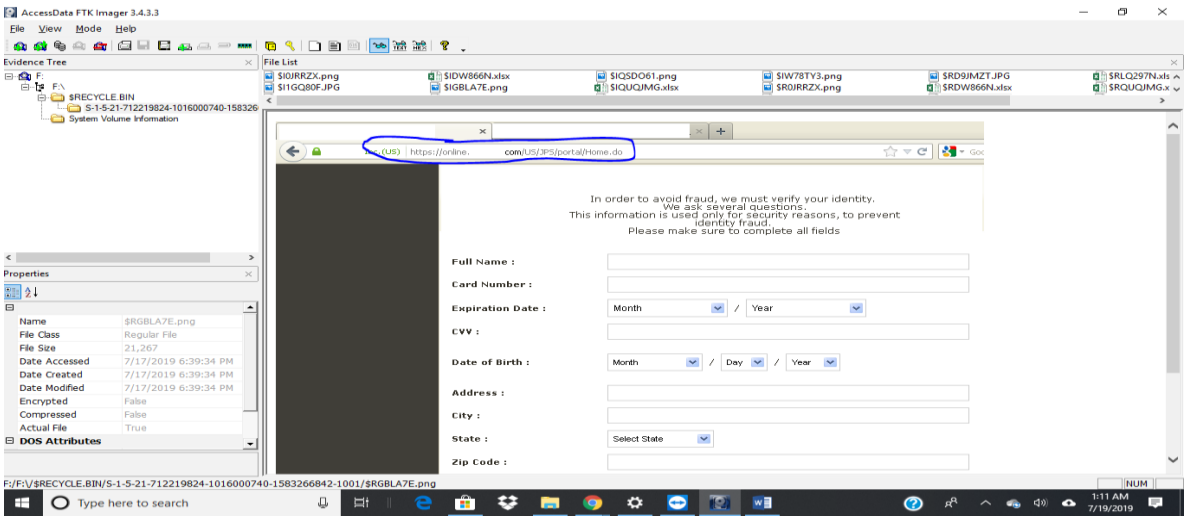



**Figura 21.** Email encontrado en hard drive recuperado de Evidencia # 1.

- En la examinación de identificado como Evidencia # 1 Hard Drive se encontró evidencia enumerada como figura 12. La cual pertenecía a una la simulación de una página de internet creada sin las debidas regulaciones la cual estaba infectada con el troyano y en esta le pedía que la víctima cierta información demográfica y sensible. “In order to avoid fraud, we must verify your identity. We ask several questions. This information is used only for security fraud. Please make sure to complete all fields”. Aunque dicho email indicaba que no era para evitar el fraude por el contrario al llenar ese documento le esta dando toda la información necesaria para ser víctima de alguna actividad ilegal.

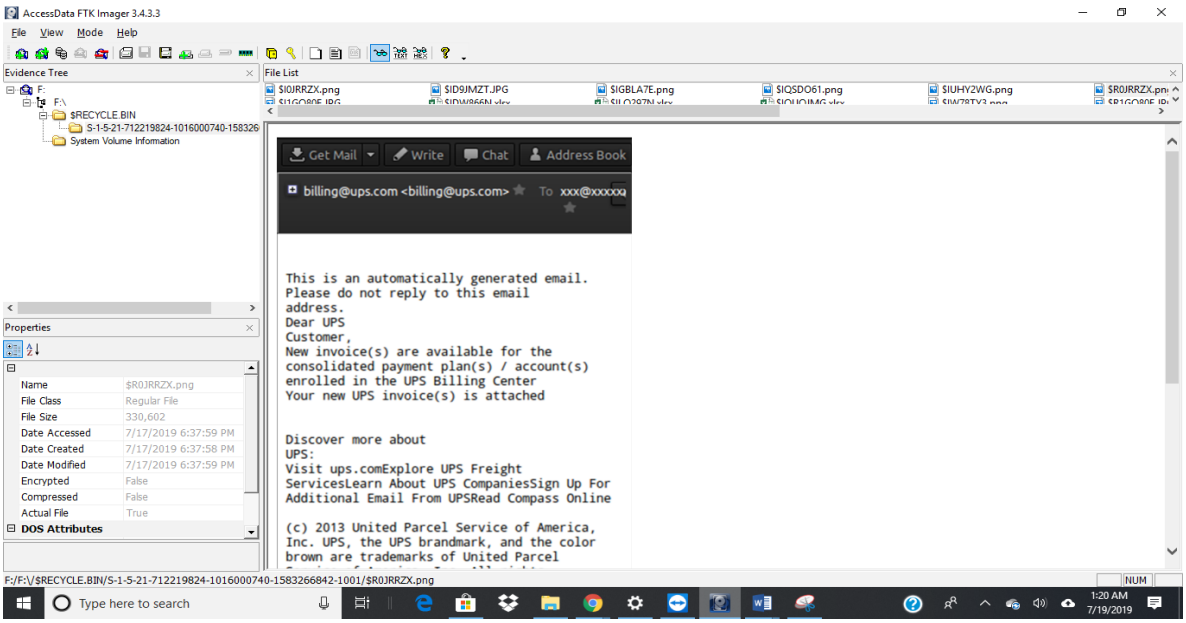



**Figura 22.** Email encontrado en hard drive simulando inscripción UPS recuperado de Evidencia # 1.

- En el hard drive se identificó un email el cual simulaba ser un tipo de inscripción en servicio de UPS, en el cual le pide a la víctima llenar el "formulario" adjunto en un ZIP, el cual contiene el troyano bancario.

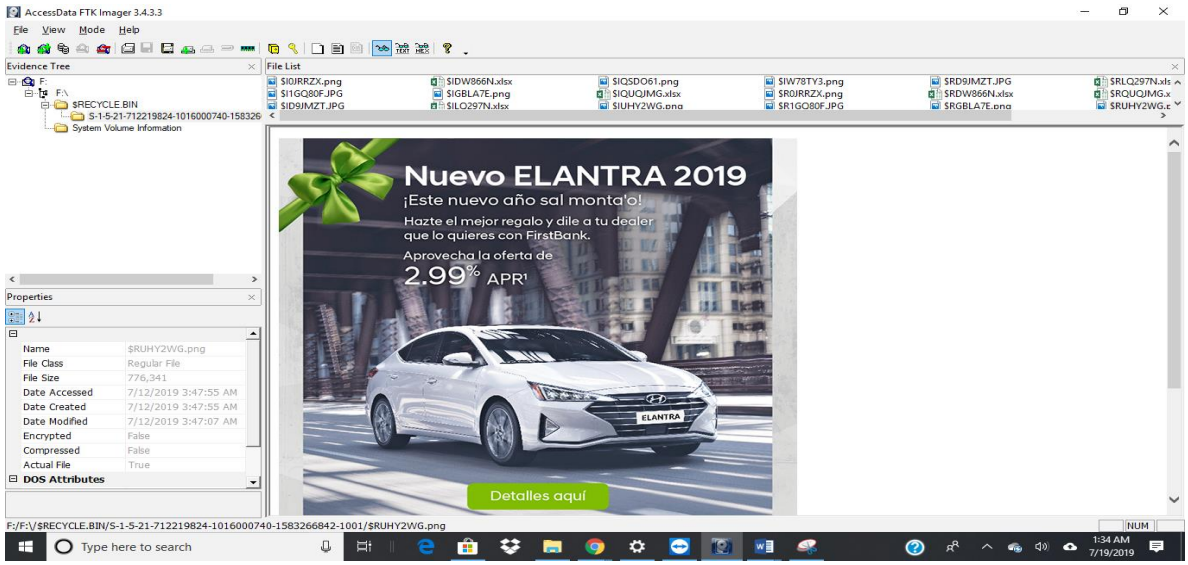



**Figura 23.** Documento en work recuperado del hard drive recuperado de Evidencia # 1.

- En el hard drive se recuperó una imagen de un documento en work el cual era enviado vía email, y la victima al abrirlo descargaba el troyano bancario Neverquest

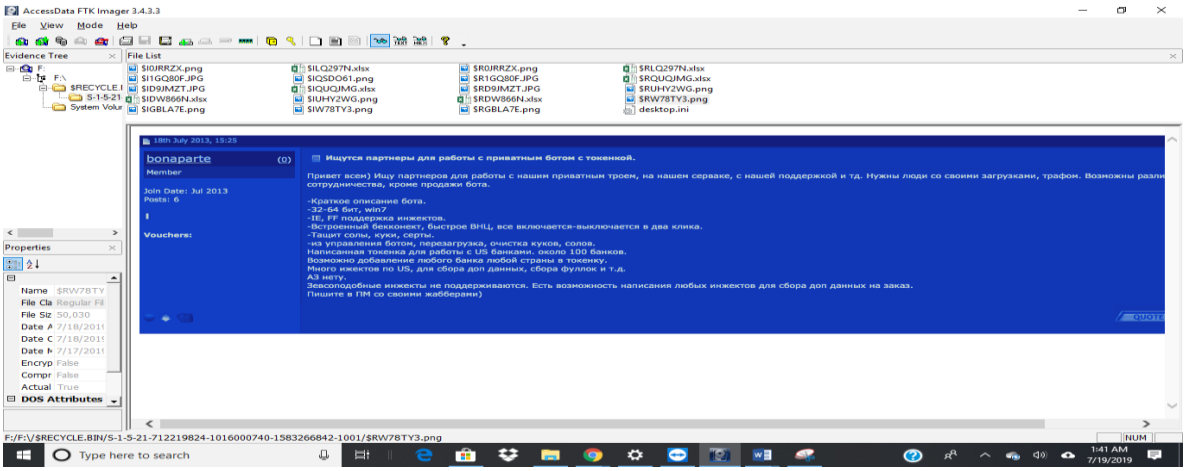



**Figura 24.** Mensaje en Dark Web ofreciendo el malware a la venta en 2015 recuperado de Evidencia # 1.

- Se encontró en el hard drive imagen en idioma ruso, que el acusado ofreció en el dark web la venta del troyano bancario entre los $490 a $2000 dólares.

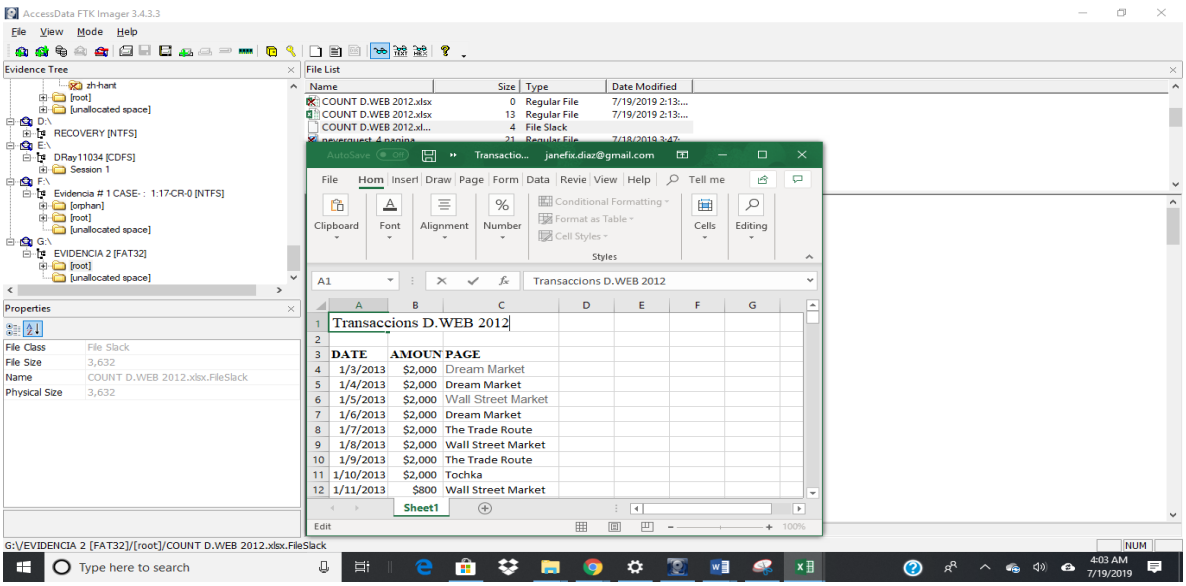



**Figura 25.** Hoja de Excel con día, costo del malware y en que página del dark web fue vendida.

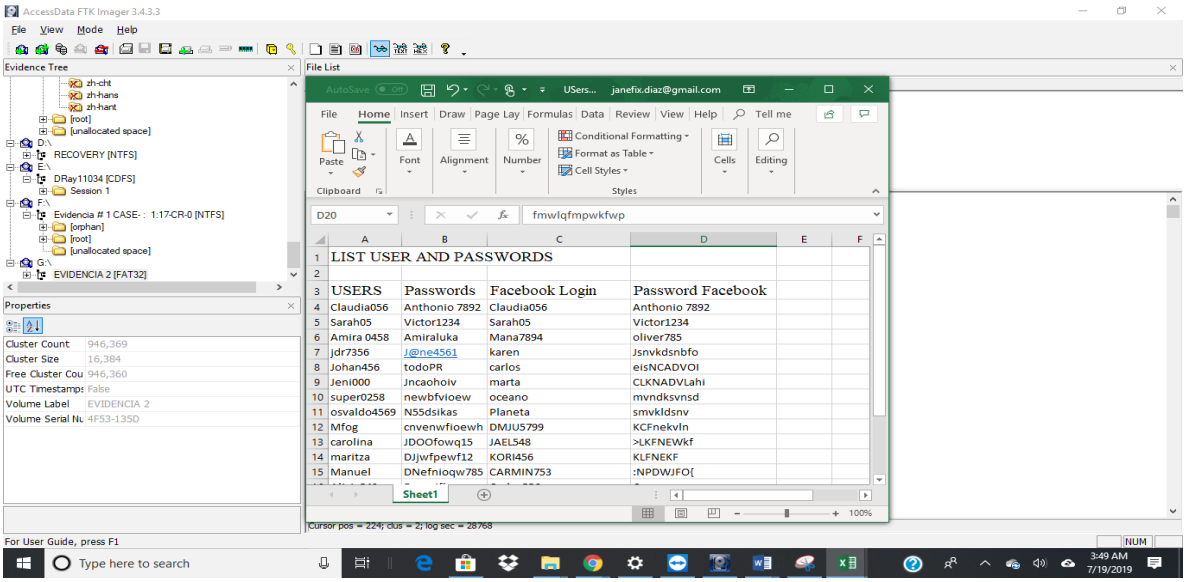



**Figura 26**. Lista de User, Passwords y accesos de Facebook en Excel.

- Se encontró en el USB varias hojas de Excel con User y password que eran obtenidos por medio del esquema de fraude del malware Neverquest lo que demuestra que Lisov no tan solo fue el creador y distribuidor del malware, sino que también utilizo el mismo activamente obteniendo así la información sensitiva la cual uso para lucrarse y vendió la información a terceros.

## SECCIÓN 5 – DISCUSIÓN DEL CASO

Como investigadora del caso 1:17-CR-00048 se entregó la evidencia, la cual fue suministrada por parte fiscal encargado del caso Michael D. Neff y el FBI para su respectivo análisis y reporte, ya que la misma sería presentada en corte a petición del Gobierno de los Estados Unidos. En la investigación se descubrió que el acusado Sr. Stanislav Vitaliyevich Lisov alias “Black” alias “Blackf” desde junio de 2012, hasta aproximadamente enero de 2015, utilizo un software malicioso llamado NeverQuest con la intención de conspirar, defraudar contra los bancos y otras víctimas. Con las pruebas encontradas en el Hard Drive y USB que se nos facilitó, se logra comprobar que el acusado no tan solo creo, distribuyo el malware, sino que también hizo uso de este con una red de botnet adquiriendo así información de las cuentas de bancos, User, Passwords y preguntas de seguridad por medio de ataques cibernéticos. Toda esta información recuperada la cual fue analizada por la investigadora Janefix Diaz Ramos y verificada por el fiscal Michael D. Neff y está lista para ser declarada para que lleve a la convicción del acusado.

## SECCIÓN 6 – AUDITORIA Y PREVENCIÓN

Durante el análisis y evaluación de este caso, se encontraron fallas en la seguridad de información confidencial, accesos y sistemas operativos lo cual provocaba que existiera una vulnerabilidad, la cual fue aprovechada por Lisov y sus conspiradores. Por lo que hablaremos de las vulnerabilidades encontradas en los sistemas. Y de igual modo veremos cómo podemos prevenir o detectar en el futuro otras posibles ataques o vulnerabilidades a las que nos expongamos.

La realidad es que el evitar los riesgos en su totalidad es técnicamente imposible porque depende de muchos factores externos e internos. Sin importar el nivel de exposición en el cual se encuentre una entidad o individuo es responsabilidad de cada uno hacer uso de los recursos con lo que se disponen. La industria bancaria en últimos años a tenido que hacer frente al aumento desmedido de los diferentes tipos de fraude cibernético, que los afecta directamente y ocasiona pérdidas millonarias anualmente. En el caso específico de la utilización de softwares maliciosos, los cuales violentan la seguridad directamente de los diferentes sistemas computarizados y las redes, donde según la evidencia recopilada el Sr. Stanislav Vitaliyevich Lisov logro acceso sin la autorización ni conocimiento del administrador, logrando acezar sistemas bancarios, o alguna red social a los cuales infectó y logro tener control total con su red de botnet los cuales alquilaba y pagaba servidores que controlaban los ordenadores de las víctimas infectados con NeverQuest y tenía acceso de nivel administrativo de esos servidores, causando una perdida estimada de $855,000.

A continuación, están los hallazgos encontrados con recomendaciones para detectar y mitigar a estos:

- Si lo vemos del lado de la institución bancaria podríamos decir que no tenían los controles adecuados en sus firewalls y routers.

  Recomendación: La administración debe establecer una rutina de monitoreo en los accesos, para así poder detectar a tiempo si hay algún ataque de hackers y minimizar su tiempo en el sistema.
- Falta o ninguna protección a documentos sensibles y discos duros de las PC

  Recomendación: Las diferentes instituciones bancarias tienen que tener estipulado un encriptado.

- Usuarios con contraseñas por defecto en routers o múltiples cuentas con el mismo User y Password.

  Recomendación: Cambio automático del user y password con el que viene, ejemplo Admin1234, tienen que tener protocolos de seguridad altos en cada equipo que esté interconectado en la red local, WAN, MAN y el router.

  Usuarios cambiar contraseñas cada 3 meses para minimizar la exposición a pérdidas de información valiosa y de activos que luego ya no puedan ser recuperados en su totalidad.

- Falta de antivirus/ poco o ningún interés en proteger la información

Recomendación: No compartir ningún tipo de acceso, ni de plataformas sociales y mucho menos de los bancos. Por ningún motivo debes compartir el usuario y la clave a otras personas y por motivos de una buena seguridad, estas credenciales se deben cambiar más tardar cada tres meses.

.

- Mal uso del internet y/o emails

  Recomendación:  Ya que el malware NeverQuest afecto el sistema bancario directamente es necesario crear políticas sobre los emails para evitar las filtraciones verificando que la información esté debidamente encriptada. Las diferentes páginas de internet bancario tienen que tener filtros definidos y deben ser actualizados ya que los hackers cambian los cogidos frecuentemente para evitar ser detectados con facilidad.

Prevención

- Mantener siempre actualizado su software de seguridad para protegerse contra cualquier nueva variante de malware.
- Mantener el sistema operativo y otro software actualizado. Las actualizaciones de software con frecuencia incluirán parches para las vulnerabilidades de seguridad recién descubiertas que podrían ser explotadas por los atacantes.

- Es necesario tener cuidado al realizar sesiones bancarias en línea, en particular si se cambia el comportamiento o la apariencia del sitio web de su banco.
- Es necesario borrar cualquier correo electrónico de apariencia sospechosa que reciba, especialmente si contienen enlaces o archivos adjuntos.

Es necesario tener mucho cuidado con cualquier archivo adjunto de correo electrónico de Microsoft Office que le aconseja habilitar las macros para ver su contenido. A menos que esté absolutamente seguro de que se trata de un correo electrónico genuino de una fuente confiable, no habilite las macros y elimine el correo de inmediato. Si sospecha de alguna infección en el sistema o que pudiera estar comprometido, cambie de inmediato las contraseñas de su cuenta bancaria en línea utilizando un sistema no infectado y comuníquese con su banco para alertarles de posibles transacciones fraudulentas.

El Banco Popular recomienda a sus clientes en su sección de *Seguridad - Online* (2019) los siguiente para evitar los casos de fraude:

Banca Online

- Asegúrate de utilizar una contraseña única. No repitas la que utilizas en otros servicios como email, redes sociales, entre otros.
- No utilices datos personales como el número de Seguro Social o de teléfono como contraseña.

- Combina letras mayúsculas y minúsculas con números y símbolos para que tu contraseña sea difícil de adivinar o descifrar.
- Cambiar las contraseñas cada cierto tiempo.

**Seguir este paso minimiza la exposición**

- Verificación de dos pasos para brindarte un nivel de seguridad adicional. Actívalo en Mi Banco Online, en la sección Mi Información.
- Sistema de barra de control de acceso (*firewalls*).
- Al conectarte, tu información se encripta a través del protocolo SSL (Secure Socket Layer) para prevenir el robo o fraude.
- Especialistas en prevención de fraude continuamente revisan las actividades en tus cuentas para alertarte inmediatamente, en caso de notar algo inusual.
- Información de todas las transacciones que realizas, como:
    - Confirmación de pagos y transferencias.
    - Pagos en proceso modificados y los borrados.
    - Transferencias en proceso modificadas.
- Recibe por mensaje de texto o email alertas de:
    - Balances.
    - Compras con tarjeta de débito.

- Compras con tu tarjeta de crédito.
- Retiros en cajeros automáticos.
- Pagos y transferencias.
- Cambios en tu información personal.

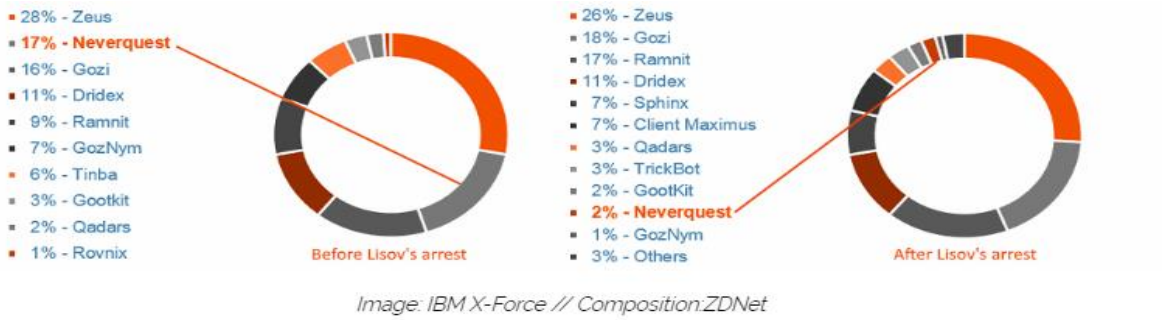



**Figura 27.** Análisis del impacto de Neverquest antes y después del arresto de Lisov. (Obtenido de: Cimpanu, 2019).

## SECCIÓN 7 – CONCLUSIÓN

Al concluir el análisis el caso de Stanislav Vitaliyevich Lisov, podemos observar cómo ha habido un gran aumento de fraude bancario por medio de malware en esta época moderna de fácil acceso a internet y a la tecnología. Y probablemente muchos nos preguntemos ¿Cómo es posible que una era la información muchas personas sean víctimas de este tipo de fraude? Y esto es debido a que nos confiamos y no prestamos atención los detalles que se presentan y por otro lado no tomamos en cuenta que debemos proteger el mundo digital que tenemos en nuestras computadoras, celulares y en la nube. Vivimos en una era tenemos la comodidad y disponibilidad en la palma de nuestra mano y logramos hacer, muchas gestiones con tan solo un click, en casi todas estas interacciones utilizamos nuestra información personal y la comprometemos al exponerlo a otras personas.

En un mundo globalizado donde el Internet ha transformado la manera de hacer negocios, el sistema financiero no podía quedarse atrás. Se incorporaron nuevas tecnologías de información en los servicios bancarios, los cuales a mi entender alteraron las definiciones tradicionales de producto, mercado y cliente, y cambiaron la banca tradicional, la banca global, desarrollándose la banca por Internet, como un medio de comunicación entre los bancos y sus clientes ya sean personas naturales o jurídicas, para realizar transacciones en línea a un menor tiempo y costo para sus usuarios, optimizando mejor sus recursos. Las actividades bancarias del Internet han reducido perceptiblemente las barreras

acelerando la banca Actualmente, los estudios comprueban que el sector que más está usando las tecnologías de la información en el mundo es el sector financiero.

En un comienzo cuando los bancos abrieron sus páginas web, con el fin de atemperarse a los tiempos y las nuevas tecnologías que ya habían sido aceptadas por sus clientes con el e–comerce, y aunque tal vez no estaban convencidos del todo se aventuraron buscando la rentabilidad y el potencial de esta gran ola de interacción entre la tecnología y el área financiera. Es así que las primeras páginas de internet, que, aunque tal vez eran lentas e impedían que el usuario entendiera bien cómo funcionaba les permitía a los bancos repetir los mismos mensajes publicitarios de las sucursales. Posteriormente, la banca lograron hacer grandes inversiones en tecnologías y marketing, que les permiten hoy en día ofrecer una alta gama de servicios online gratuitos, desde consultas de saldos de cuentas de ahorros, transferencias entre cuentas, pago de servicios como luz, agua, teléfono, cable, inversiones en fondos mutuos, pago de impuestos, información de productos y servicios para la banca personal y empresarial, entre otros, a los cuales puede accederse desde la comodidad del hogar, algún coffee shop con acceso a internet o incluso nuestro propio teléfono celular.

Si bien en los inicios de la banca por Internet, los clientes no tenían confianza en este nuevo medio; la facilidad de su uso, la rapidez del servicio online y la reducción de costos que representa al no tener que llegar presencialmente a las oficinas de los bancos tiene sus ventajas hoy en día y dado este auge se ven los bancos más expuestos a los

ciberdelincuentes ocasionado millones de pérdidas que los bancos tienen que cubrir. El que los individuos logren crear conciencia de los miles de amenazas cibernéticas es trabajo de todos no solamente de las instituciones bancarias. La protección contra amenazas como Neverquest exige más que soluciones antivirus estándar y los usuarios necesitan una solución dedicada para proteger sus transacciones. En particular, la solución debe ser capaz de controlar el proceso de ejecución del navegador y evitar cualquier manipulación del mismo por parte de otras aplicaciones.

**SECCIÓN 8 – REFERENCIAS**


*18 U.S. Code § 1349 -Intent conspiration*. (1996). *LII / Legal Information Institute*. Recuperado el 20 de abril de 2019 de: **https://www.law.cornell.edu/uscode/text/18**

Arroyo, J. (s. f). Abogado experto en litigio en Arroyo Castro & Cotarelo. LinkedIn. Recuperado el 20 de abril de 2019 de**: https://es.linkedin.com/in/juan-manuel-arroyo-gonz%C3%A1lez-7ab791136**

*Caballero, A. (s.f). Crear la Imagen Forense desde una Unidad utilizando FTK Imager | Alonso Caballero / ReYDeS*. (2019). *Reydes.com*. Recuperado el 20 de julio de 2019 de: **http://www.reydes.com/d/?q=Crear_la_Imagen_Forense_desde_una_Unidad_utilizando_FTK_Imager**

Cero-Cool. (2017). *El primer virus informático – Creeper | ElSaber21*. *El Saber 21 - Todo lo que tienes que saber hoy en día.* Recuperado el 20 abril de 2019 de: **https://www.elsaber21.com/el-primer-virus-informatico-creeper**

Cimpanu, C. (2019). Russian national, author of Never Quest banking trojan, pleads guilty. ZDnet.com. Recuperado el 15 de julio de 2019 de: **https://www.zdnet.com/article/russian-national-author-of-neverquest-banking-trojan-pleads-guilty/**

*Dewdney, A.K. (1988). Core Wars.Cyberhades.com*. Recuperado el 5 mayo de 2019 de: **https://www.cyberhades.com/2007/12/30/core-wars/**

*District Manhattan Federal Court*. (2019). *Russian Hacker Who Used NeverQuest Malware to Steal Money from Victims' Bank Accounts Pleads Guilty*. *Justice.gov*. Recuperado el 1 abril de 2019 de: **https://www.justice.gov/usao-sdny/pr/russian-hacker-who-used-neverquest-malware-steal-money-victims-bank-accounts-pleads**

*España extraditará al programador ruso Lísov a EE.UU.* (2019). *RT en español*. Recuperado el 18 de Julio de 2019 de**: https://actualidad.rt.com/actualidad/245851-espana-extraditar-programador-lisov**

Goubarev, O. (2019). Facebook. Recuperado el 3 de abril de 2019: **http://oleggubarev.com/es/index.html**

*Herramientas de análisis forense informático con Kali Linux. | Security Hack Labs*. (2019). *Security Hack Labs*. Recuperado el 19 de julio de 2019 de: **https://securityhacklabs.net/articulo/herramientas-de-analisis-forense-informatico-con-kali-linux**

*IBM Threat Intelligence Insights: Botnet Report*. (2019). *Connect.security.ibm.com*. Recuperado el 20 de Julio de 2019 de: **https://connect.security.ibm.com/app/threat-intelligence-insights/report/botnets/neverquest**

*IDEA*. (2019). *IDEA Audit Software | IDEA Data Analysis Software | IDEA*. (2019). *IDEA*. Recuperado el 18 Julio 2019 de: **https://idea.caseware.com/products/idea/**

Infante, B. (2004). *Banca por Internet como una nueva forma de hacer negocios 2004 - GestioPolis*. *Gestiopolis.com*. Recuperado el 20 julio de 2019 de: **https://www.gestiopolis.com/banca-por-internet-como-una-nueva-forma-de-hacer-negocios-2004/**

*La historia de los virus informáticos*. (2017). *OpenMind*. Recuperado el 24 abril de 2019 de: **https://www.bbvaopenmind.com/tecnologia/mundo-digital/la-historia-de-los-virus-informaticos/**

*La policía detiene al creador del 'malware' para bancos 'NeverQuest'*. (2017). *Eldiario.es*. Recuperado el 15 julio de 2019 de: **https://www.eldiario.es/tecnologia/Acusan-software-malicioso-millones-dolares_0_603689978.html**

*Man Charged for His Role in Creating the KRONOS Banking Trojan*. (2017). *Justice.gov*. Recuperado el 5 mayo de 2019 de: **https://www.justice.gov/usao-edwi/pr/man-charged-his-role-creating-kronos-banking-trojan**

Mchoes, F. (2008). Operating System. Recuperado el 5 de mayo de 2019 de: **http://160592857366.free.fr/joe/ebooks/ShareData/Understanding%20Operating%20Systems%206e%20By%20Ann%20McIver%20McHoes%20and%20Ida%20M.%20Flynn.pdf**

Motos, V. (2011). *SpyEye + Zeus: el super troyano bancario*. *Hackplayers.com*. Recuperado de 20 julio de 2019 de: **https://www.hackplayers.com/2011/02/spyeye-zeus-el-super-troyano-bancario.html**

*Latam.kaspersky.com. (2019).Neverquest Trojan: Construido para robar a cientos de bancos*. Recuperado el 15 mayo de 2019 de :**https://latam.kaspersky.com/blog/neverquest-trojan-creado-para-robar-a-cientos-de-bancos/1753/**

*New Fraudulent Email Circulating: UPS - United States*. (2019). *Ups.com*. Recuperado el 15 de julio de 2019 de: **https://www.ups.com/us/en/about/news/fraud-alert.page**

*Ofensiva de los bancos ante la clonación de tarjetas*. (2019). *El Nuevo Dia*. Recuperado el 5 mayo de 2019 de: **https://www.elnuevodia.com/negocios/banca/nota/ofensivadelosbancosantelaclonaciondetarjetas-2493664/**

Rivera, M, (2019). *Venezolano es arrestado por cometer fraude*. *El Vocero de Puerto Rico*. Recuperado 10 Julio 2019 de: **https://www.elvocero.com/ley-y-orden/venezolano-es-arrestado-por-cometer-fraude/article_c8388b68-66dc-11e9-8b9a-4710cb0504ae.html**

Rivero, M. (2014) InfoSpyware, ¿Qué son los malwares? Recuperado el 10 de julio de 2019 de: **https://www.infospyware.com/articulos/que-son-los-malwares/**

*Seguridad - Online*. (2019). *Popular.com*. Recuperado el 15 de julio 2019 de: **https://www.popular.com/seguridad/en-linea/**

*Socha, G. (s. f).* Referencia de Descubrimiento Electrónico EDRM. *Definition from WhatIs.com*. (2019). *SearchCompliance*. Recuperado el 20 de julio de 2019 de: **https://searchcompliance.techtarget.com/definition/EDRM-electronic-discovery-reference-model**

*Software de Análisis Informático: Forensic Tool Kit (FTK)*. (2019). *TechnologyINT*. Recuperado el 2 de Julio de 2019 de: **http://technoint.weebly.com/software-de-anaacutelisis-informaacutetico-forensic-tool-kit-ftk.html**

*Spain to finally extradite 'Russian hacker' Lisov to US*. (2017). *En.crimerussia.com*. Recuperado el 1 mayo de 2019 de: **https://en.crimerussia.com/gromkie-dela/spain-to-finally-extradite-russian-hacker-lisov-to-us/**

Stanislav Lisov Is another Player in The Periphery of The President's World. (2017). Gronda Morin. Recuperado el 20 abril de 2019 de: **https://grondamorin.com/2017/03/21/stanislav-lisov-is-another-player-in-the-periphery-of-the-presidents-world/**

United States v. Peter Levashov, (2018). *Russian National Who Operated Kelihos Botnet Pleads Guilty to Fraud, Conspiracy, Computer Crime and Identity Theft Offenses*. *Justice.gov*.

Recuperado el 6 mayo de 2019 de: **https://www.justice.gov/usao-ct/pr/russian-national-who-operated-kelihos-botnet-pleads-guilty-fraud-conspiracy-computer**

United States v. Aleksandr Andreevich Panin y Hamza Bendellad (2014). *Two Major International Hackers Who Developed the "SpyEye" Malware get over 24 Years Combined in Federal Prison*. (2016). *Justice.gov*. Recuperado el 30 abril de 2019 de: **https://www.justice.gov/usao-ndga/pr/two-major-international-hackers-who-developed-spyeye-malware-get-over-24-years-combined**

*Virus y Antivirus | Información | Historia | Evolución-Información sobre Seguridad-Panda Security*. (s.f). *Pandasecurity.com*. Recuperado el 10 de Julio de 2019 de: **https://www.pandasecurity.com/es/security-info/classic-malware/**

Yumal, FM. (2017). *La historia de Creeper, el primer virus informático jamás programado*. *Xataka.com*. Recuperado el 1 de mayo de 2019 de: **https://www.xataka.com/historia-tecnologica/la-historia-de-creeper-el-primer-virus-informatico-jamas-programado**