Diseño de indicadores de compromiso para la detección temprana de incidentes de seguridad en la red del Ministerio de Relaciones Exteriores

María Milena Sánchez Barragán

Trabajo de grado para optar al título profesional:

Maestría en Ciberseguridad y Ciberdefensa

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

2018

MINISTERIO DE DEFENSA NACIONAL

COMANDO GENERAL FUERZAS MILITARES

ESCUELA SUPERIOR DE GUERRA

DISEÑO DE INDICADORES DE COMPROMISO PARA LA DETECCIÓN TEMPRANA DE INCIDENTES DE SEGURIDAD EN LA RED DEL MINISTERIO DE RELACIONES EXTERIORES

ALUMNO: MARÍA MILENA SÁNCHEZ BARRAGÁN

DIRECTOR: MSC. IVÁN CAMILO CASTELLANOS ROMERO

MAESTRÍA EN CIBERSEGURIDAD Y CIBERDEFENSA

TRABAJO DE GRADO PARA OPTAR EL TÍTULO DE MAGISTER EN CIBERSEGURIDAD Y CIBERDEFENSA

BOGOTÁ - COLOMBIA
2018

Nota de aceptación

Presidente del Jurado

Jurado

Jurado

Jurado

Bogotá, septiembre del 2018

Agradecimientos

Agradezco primeramente a Dios nuestro señor, por permitirme esta oportunidad educativa y haberme dado las capacidades para desarrollar este trabajo de grado.

A mi hija María Alejandra, esposo Giovanni, madre Adela y suegra Margarita quienes me han colaborado, apoyado y amado siempre.

Al ingeniero y director Iván que con su experiencia y conocimiento guio y dirigió este proyecto de grado.

Gracias a todos y cada uno.

Resumen

En el primer capítulo se desarrolla un marco teórico que aborda conceptos relevantes en este trabajo de grado. En los capítulos dos y tres se contextualiza los antecedentes internacionales y nacionales, resaltando los riesgos e impactos que un malware puede provocar si una Entidad no está preparada o no tiene bien definido un esquema de ciberdefensa.

Se analiza la situación actual del Ministerio de Relaciones Exteriores con el objetivo de demostrar la necesidad de diseñar una estrategia que permita la identificación temprana de incidentes de seguridad, así como fortalecer las instancias en el entorno digital (CONPES CONPES 3854 de 11 de abril de 2016, estrategia E4.1.). Por otra parte, el mecanismo o flujo de datos empleado para el diseño de los indicadores de compromiso puede ser implementado en cualquier entidad privada o pública, la cual parte de una metodología deductiva que proviene de lo general a lo específico

Por último, se ejemplariza un caso de estudio de un ciberataque a una Entidad con el propósito de proyectar la necesidad de emplear un esquema de ciberdefensa, en este caso con foco al diseño de indicadores de compromiso como control preventivo para mitigar impactos a nivel de disponibilidad de servicio.

Palabras clave:

Indicadores de Compromiso, Evento de seguridad de la información, Incidente de seguridad de la información, Protección de datos, Activo, Malware, Ciberseguridad, Ciberdefensa.

CONTENIDO

INTRODUCCIÓN

La terminología para comprender la importancia de la ciberseguridad y su contexto en la sociedad actual es un primer paso para estudiar a fondo las implicaciones de las redes de información a nivel mundial y su incidencia en el quehacer diario de las empresas. De igual forma en el siguiente trabajo de grado se abordan otros conceptos directamente relacionados a ciberseguridad y se ejemplifican los malware más concurrentes en la red del Ministerio de Relaciones Exteriores y de emplear medidas para evitar ciberataques, dado que estos son cada vez más numerosos y peligrosos en el ciberespacio, es así como se observa la necesidad de utilizar nuevas herramientas y técnicas para contrarrestar los ataques.

Así mismo, es importante conocer las contramedidas recomendadas por la UIT-T X.1205 de la Unión Internacional de Telecomunicaciones (2008), donde se habla de diversas tecnologías de Ciberseguridad disponibles para contrarrestar las amenazas. Dentro de estas recomendaciones se aborda también el estudio del comportamiento de las amenazas, como los cambios que estas realizan cuando ingresan a un sistema de información, esta técnica es llamada indicadores de compromiso - IoC. Los IoC comprenden el concepto de inteligencia de amenazas, que no solo se basa en obtener un hash o una dirección IP, sino tener pleno conocimiento de los activos de la red, así como de los servicios que presta, un entendimiento global del sistema.

Adicionalmente, para garantizar un nivel de seguridad adecuado es necesario actuar antes de que se produzca un incidente o, por lo menos, detectarlo en un primer momento para reducir su impacto y alcance. Por esta razón las empresas y diferentes entidades han optado por impulsar la entrada en servicio de Sistemas de Alerta Temprana para la detección rápida de incidentes y anomalías dentro de las redes de información.

Para finalizar el presente trabajo de grado se investigó la técnica de los indicadores de compromiso para contrarrestar los malware más constantes en los activos del Ministerio de Relaciones Exteriores y así poder implementar medidas para combatir los ataques informáticos de la organización en el menor tiempo posible.

TÍTULO

Apoyando el CONPES 3854 de 11 de abril de 2016, en la estrategia E4.1. Fortalecer las instancias y entidades responsables de la defensa nacional en el entorno digital (DE1), en un plan de fortalecimiento que permita generar una autonomía cibernética conducente a identificar, detectar y atender posibles amenazas en contra del Estado y su infraestructura critica; por lo anterior este trabajo se fundamenta y se titula: "Diseño de Indicadores de Compromiso para la Detección Temprana de Incidentes de Seguridad en la Red del Ministerio de Relaciones Exteriores".

FORMULACIÓN DEL PROBLEMA

Actualmente el Ministerio de Relaciones Exteriores ha sido víctima de varios incidentes de seguridad como malware y ciberataques a uno de los sistemas de información. Dentro de los reportes de la herramienta de Mesa de Ayuda – Aranda, los TK. 108501, TK 110026, TK 111494 y TK 112471 registraron que los usuarios de Cancillería Interna como Externa fueron afectados por un malware que cifró la información de sus equipos, obstruyendo la posibilidad de visualizar la información y de igual forma solicitaba un pago para la entrega de una clave que permitiría descifrar la información. Los incidentes mencionados se originan por un malware que se encuentra dentro de la familia TeslaCrypt y es conocido como Ransomware, para estos casos se realizó las

consultas e investigaciones con los proveedores informando que no era posible recuperar la información de los equipos.

El incidente fue escalado al proveedor y con el personal de seguridad se realizaron actividades de contención y prevenciones futuras, con el fin de prevenir un impacto mayor a futuro. Además, no se sabe si estos incidentes se repitan y comprometan la red de la organización.

Los principales malware para correo en Cancillería son:

Tabla 1
Principales Malware Cancillería

Malware	Cantidad
EXE	1407
MALICIOUS PAYLOAD	425
WIN32/TISIFI.B	367
ACE	327
JAR	315
097M/MACROBE.C	305
JS/JASOBFUS.A!ML	273
JS/NEMUCOD.TSM	185
097M/DONOFF.EC	173
JS/NMUCOD.TSF	167

Nota: tabla recuperada de la consola de administración del antivirus System Center (2016) del Ministerio de Relaciones Exteriores.

Los principales malware detectados en la consola de antivirus en los equipos de Cancillería son:

Tabla 2
Principales malware detectados en la consola de antivirus

Nombre de la amenaza	Categoría de amenaza	Cantidad
TrojanClicker:JS/Plucoki.A	Notificador sigiloso	1317
PUA:Win32/FileTypeAssistant	Software no deseado	1317
Joke:Win32/Molesto	Programa de broma	1317
BrowserModifier:Win32/	Modificador de explorador	1317
PUA:Win32/uTorrent	Software no deseado	1317
BrowserModifier:Win32/Foxiebro	Modificador de explorador	1317
PUA:Win32/DSNet	Software no deseado	1317
PUA:Win32/MegaDownloader	Software no deseado	1317

Program:Win2/Vigram.A	Software no deseado	1317
Worm:Win32/gamarue.F	Gusano	1317

Nota: tabla recuperada de la consola de administración del antivirus System Center (2016) del Ministerio de Relaciones Exteriores.

Por lo anterior, es necesario diseñar una estrategia que alerte cuando se presente un comportamiento anómalo en uno de los equipos de la entidad y de igual forma permita integrarse con una herramienta para que notifique a tiempo el ataque cibernético, con el objetivo de mitigar el impacto y ejecutar acciones correctivas a tiempo para minimizar el riesgo de la seguridad de la información institucional.

Pregunta de investigación: ¿Existe en el Ministerio de Relaciones Exteriores un diseño de indicadores de compromiso para la detección temprana de incidentes de seguridad de la información?

JUSTIFICACIÓN

Durante el 2016, el Ministerio ha sido víctima más de tres (3) veces de malware llamada Ransomware, el cual cifra la información del equipo y luego pide rescate por ellos, este tipo de malware ha alertado a los usuarios pues el Ministerio no cuenta con un respaldo de datos a los equipos de los usuarios e información tan importantes como la de la Ministra, asesores de la Ministra y directores podría perderse, lo que se busca con el diseño de los indicadores de compromiso es detectar más rápidamente estos incidentes. Esto no significa que un usuario infectado con este tipo de malware no podrá recuperar la información, sino evitaría que otros sean infectados.

Por lo anterior se hace necesario que el Ministerio diseñe una estrategia que permita la detección temprana de incidentes de seguridad ocasionados por malware, debido a que actualmente los eventos se atienden por notificación de los usuarios una vez el hecho se haya presentado, y en

muchos casos es imposible volver a un estado inicial la información, las mejores prácticas de la industria tecnológica y estrategias de ciberseguridad informan que las entidades deben implementar tecnologías para la prevención y rápida detección de incidentes, estas prácticas ayudaran a mitigar el riesgo y el impacto organizacional.

Con el diseño de los indicadores de compromiso, el Ministerio podrá emprender actividades de diagnóstico y contención temprana a incidentes de seguridad, evitando un riesgo de pérdida o fuga de información a la ciudadanía, pues un ciberataque podría acarrear daños a los datos y afectar la protección de la información.

OBJETIVO GENERAL

Diseñar indicadores de compromiso para la detección temprana de incidentes de seguridad en la red del Ministerio de Relaciones Exteriores.

OBJETIVOS ESPECÍFICOS

- Determinar las variables de los malware más recurrentes del Ministerio de Relaciones Exteriores, para el establecimiento de los indicadores de compromiso.
- Investigar los malware más característicos de la Entidad con el propósito de registrar los comportamientos anómalos que pudiese presentar la red del Ministerio.
- Establecer indicadores de compromiso - IOCs para el Ministerio que puedan detectar amenazas de una manera temprana.

ALCANCE

En este trabajo de grado se desarrolla un estudio para el diseño de indicadores de compromiso que más afectan al Ministerio de Relaciones Exteriores, contemplando las diferentes fuentes de información con las que cuenta la Entidad.

1. METODOLOGÍA

El presente trabajo de grado se desarrolla bajo la metodología deductiva que desciende de lo general a lo particular, contempla un contexto internacional destacando los principales incidentes de seguridad que se han presentado en entidades de estado como privadas, como referente de estos eventos se podrá visualizar cuales fueron las medidas preventivas y correctivas implementadas.

Se aborda conceptos en temas de incidentes de seguridad, indicadores de compromiso y herramientas tecnológicas para mitigar los impactos tecnológicos que enfrente el día a día las organizaciones.

Se realiza una propuesta de indicadores de compromiso para el Ministerio de Relaciones Exteriores, con el ánimo de fortalecer la defensa del entorno digital de la entidad. Los indicadores de compromiso seleccionados se desarrollan con la respectiva investigación y análisis suministrada por CVE - Common Vulnerabilities and Exposures, que incluye proveedores, proyectos e investigaciones en el campo de las vulnerabilidades técnicas nacionales e industriales.

2. MARCO TEÓRICO

Este capítulo contextualiza los conceptos y documentos más notables de fuentes web bibliográficas, como insumo para el diseño de los indicadores de compromiso más significativos para la red del Ministerio de Relaciones Exteriores.

2.1. Categorías de estudio de campo

Al iniciar la revisión del tema de investigación es importante identificar las categorías y áreas comprendidas en el tópico central para hacer claridad en el lenguaje básico común que se va a utilizar. En este caso, el estado del arte se enfoca en la revisión del conjunto de núcleos temáticos, con el fin de formalizar y definir el objeto de investigación, así como las áreas temáticas correspondientes. Es importante tener en cuenta que se trata de temas como Indicadores de Compromiso, Incidentes de Seguridad de la Información, y por supuesto, aquellos que se relacionan con Ciberseguridad y Ciberdefensa.

2.2. Ciberseguridad y Ciberdefensa

De acuerdo con Zubieta (2015) no existe una definición consensuada de Ciberseguridad, razón por la cual muchos se refieren a ella como sinónimo de seguridad informática, seguridad de la información o seguridad en cómputo; sin embargo, esta idea no es del todo correcta dado que el concepto de Ciberseguridad se encuentra más asociado al termino de Ciberespacio. El Diccionario de la Real Academia Española (RAE) en su 22ª edición define Ciberespacio, única acepción, como el "ámbito artificial creado por medios informáticos". Así pues, la RAE se refiere a un entorno no físico creado por un equipo informático con el objetivo de interoperar en una Red, entendiendo que el mayor ámbito del ciberespacio es Internet (RAE, 2017). Con esta aclaración es posible la comprensión del término desde diferentes ámbitos, uno de ellos es el aportado por ISACA

(Mendoza, 2017) que describe el término como la protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados, teniendo en cuenta que la información protegida es netamente digital. En consecuencia, para ISACA el término se halla comprendido dentro de la Seguridad de la Información y, por ende: Ciberespacio, Ciberseguridad y Seguridad de la información, son términos que no pueden entenderse como equivalentes.

En el año 2008 la Unión Internacional de Telecomunicaciones (ITU) en su texto sobre Recomendaciones sobre Ciberseguridad en el Ciberespacio define el término de una forma más global que ISACA aportando otros elementos de análisis. ITU R 1205 (2008) dice que es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el Ciberentorno. También advierte que los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el Ciberentorno, y enfatiza en que la Ciberseguridad es la encargada de garantizar que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el Ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes: disponibilidad; integridad, que puede incluir la autenticidad y el no repudio; y confidencialidad.

Por su parte, la norma ISO/IEC 27032 del 2012 también aporta referentes respecto al término, poniéndolo en relación con otros dominios de la seguridad (ver figura 1) y proporciona

un marco para el intercambio de información, el manejo de incidentes y la coordinación para hacer más seguros los procesos y ayudar a prepararse, detectar, monitorizar y responder a los ataques que pueden ser de ingeniería social, hackers, malware, spyware hasta otros tipos de software no deseados.

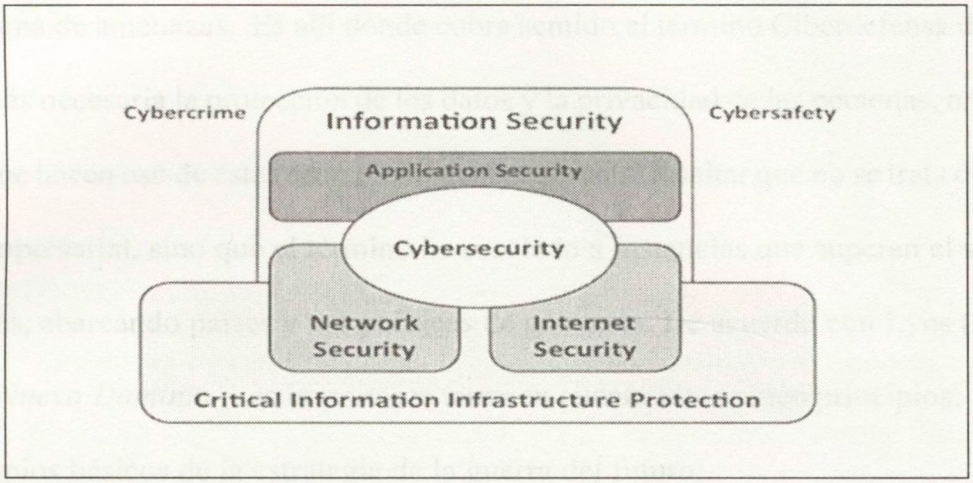


Figura 1. Relación entre Ciberseguridad y otros dominios de seguridad.
Organización Internacional de Normalización. (2012) Norma ISO/IEC 27032. Recuperado de: https://www.iso.org/standard/44375.html.

Sin importar los límites de cada acepción es importante resaltar que el objetivo principal de la Ciberseguridad es proteger la información, independientemente de que ésta pertenezca a una organización o si se trata de información personal, ya que nadie está exento de padecer algún riesgo de seguridad.

Casi en este mismo ámbito tiene lugar el término Ciberdefensa, pues con el advenimiento de la Computación en la Nube o Informática en la Nube, el fenómeno del Ciberespacio se ha convertido en un nuevo paradigma tecnológico de gran impacto social. Se trata de un '*Nuevo Dominio*' en donde un gran conjunto de servidores de información se encuentra desplegados a lo largo de todo el mundo almacenando y descargando millones de aplicaciones y datos puestos a disposición de organizaciones, empresas y usuarios. La Nube, que a su vez ha sido posible gracias a tecnologías de virtualización, tecnologías de banda ancha y de gran velocidad de transferencia

de datos, a su vez se nutre gracias a la proliferación de dispositivos de todo tipo con acceso a Internet, desde PC de escritorio hasta netbooks, teléfonos inteligentes, tabletas electrónicas como iPad o libros electrónicos como los lectores de libros electrónicos (ebook), etc., trayendo infinidad de ventajas de todo tipo a organizaciones, empresas y usuarios, pero a su vez, presentando un nuevo panorama de amenazas. Es allí donde cobra sentido el término Ciberdefensa dado que cada vez se hará más necesaria la protección de los datos y la privacidad de las personas, organizaciones y empresas que hacen uso de este recurso. Sin embargo, cabe resaltar que no se trata de un ejercicio personal o empresarial, sino que el término ha escalado a instancias que superan el simple uso de las tecnologías, abarcando países y sus políticas de gobierno. De acuerdo con Lyns (2010) para la defensa del *'Nuevo Dominio'* es importante tener en cuenta estos cinco principios:

Principios básicos de la estrategia de la guerra del futuro:

- El ciberespacio debe ser reconocido como un territorio de dominio igual que la tierra, mar y aire en lo relativo a la guerra.
- Cualquier posición defensiva debe ir «más allá» del mero mantenimiento del ciberespacio «limpio de enemigos» para incluir operaciones sofisticadas y precisas que permitan una reacción inmediata.
- La defensa del ciberespacio (ciberespacial) debe ir más allá del mundo de las redes militares –dominios.mil y.gov. del Departamento de Defensa, para llegar hasta las redes comerciales (dominios. com .net,.info,.edu, etc.) y que deben estar subordinados al concepto de Seguridad Nacional.
- La estrategia de la Defensa Ciberespacial debe realizarse con los aliados internacionales para una política efectiva de «alerta compartida» ante las amenazas mediante establecimiento de Ciberdefensa con países aliados.

• El Departamento de Defensa debe contribuir al mantener e incrementar el dominio tecnológico de Estados Unidos y mejorar el proceso de adquisiciones y mantenerse al día con la agilidad que evoluciona la industria de las Tecnologías de la Información. (p. 97)

Como es comprensible, estos principios posicionan el término Ciberdefensa como una categoría de análisis que desborda el mero hecho de la protección de la información digital, sino que concierne a toda una estrategia político-militar que debe ser asumida por cada una de las naciones y por ende se encuentra subordinada al concepto de Seguridad Nacional.

2.3. Ciberataques

Uno de los ejes de esta investigación es la detección temprana de incidentes de seguridad en la red, por tanto, es fundamental comprender a qué hace referencia este ítem. Así pues, a continuación, se indagará respecto a los incidentes de seguridad en la red, específicamente sobre el tema de los Ciberataques.

Desde un punto de vista corriente, un Ciberataque puede ser entendido como cualquier tipo de maniobra ofensiva hecha por individuos u organizaciones que atacan a sistemas de información como lo son infraestructuras, redes computacionales, bases de datos que están albergadas en servidores remotos, por medio de actos maliciosos usualmente originados de fuentes anónimas que también roban, alteran o destruyen un blanco específico mediante hackeo de un sistema vulnerable. Sin embargo, una de las definiciones más completas la ofrece el Manual Tallinn sobre el Derecho Internacional en Ciberguerra (2013), dicho manual lo describe como aquella operación cibernética, ofensiva o defensiva, de la que se espera que pueda causar pérdidas de vidas humanas, lesiones a las personas o daños o destrucción de bienes.

Esta interpretación es muy importante dado que implícitamente incorpora un nuevo concepto en el campo de la investigación; estamos hablando de la Ciberguerra. Así como las

Tecnologías de la Información, las computadoras e Internet han transformado la economía, la cultura y los modos de vida, también se da un fenómeno que cambia las formas de combate, pues se puede decir que, a la pólvora, el avión y demás armas convencionales de guerra, se suma la posibilidad de generar ataques digitales. La amenaza es compleja y potencialmente muy peligrosa dado que pueden generarse tanto perdidas de bienes materiales o inmateriales, como trascender al plano físico humano y causar lesiones que atentan contra la vida de las personas.

Según Soesanto (2016), investigador del Consejo Europeo para las Relaciones Exteriores (ECFR) y experto en Ciberseguridad, sólo han ocurrido dos ciberataques que han superado ese límite físico:

> El primero fue el uso del gusano informático Stuxnet en agosto de 2007 para infectar la planta de enriquecimiento de uranio de Natanz en Irán (atribuido a EE UU e Israel), y el segundo es un ciberataque mucho menos conocido contra una planta siderúrgica alemana (sin nombre) en 2015 que nadie se ha atribuido públicamente, y que causó daños considerables y sin especificar.

Soesanto (2016) también describe otros ataques como el virus Shamoon contra la petrolera saudí Aramco en el 2012 (atribuido a Irán), que borró parcialmente o destruyó por completo los discos duros de 35.000 ordenadores de la compañía.

El incidente llevó a que el secretario de Defensa de EE UU declarara en aquella época que Shamoon es uno de los primeros (programas de malware) que puede inutilizar y destruir ordenadores hasta el punto de tener que reemplazarlos.

Cuando los ciberataques alcanzan tales niveles, el tema se torna aún más complejo, pues el límite entre el término en cuestión y temas como actos de guerra, actividades criminales, ciberdelincuentes y ciberterrorismo, se vuelven cada vez más imprecisos. En consecuencia,

trasladar los conflictos bélicos del campo de batalla al Ciberespacio constituye un nuevo plano de operaciones que cambia las armas convencionales por '*Ciberarmas*' tales como: virus informáticos, programas especiales que penetran en la seguridad de los equipos, y sistemas informáticos. Allí los implicados ya no son las fuerzas armadas sino especialistas informáticos en telecomunicaciones, y los objetivos militares pasan a ser los sistemas financieros, bancarios y militares, así como las instituciones públicas, las grandes corporaciones y los sistemas de telecomunicaciones.

Al retornar al tema de esta investigación sobre el Diseño de Indicadores de Compromiso para la Detección Temprana de Incidentes de Seguridad en la Red del Ministerio de Relaciones Exteriores, es pertinente aclarar que una de las motivaciones para la formulación de este proyecto han sido los diferentes incidentes de seguridad a los que ha sido víctima la Red del Ministerio de Relaciones Exteriores de Colombia. Los ciberataques han sido identificados como un tipo de malware llamado Ransomware. Al respecto, Del Rivero (2015) escribe lo siguiente:

> Los ataques Ramsomware (ransom significa rescate y ware en referencia a la palabra software), son un tipo de programa informático malintencionado que restringe el acceso a determinadas partes del sistema infectado, encriptando la información para utilizarla como rehén de cobro a cambio de quitar esa restricción. (p. 138)

Se dice que, a partir del 2012, el uso de estafas Ransomware han crecido internacionalmente, por tanto, todas las estrategias que se diseñen o implementen para ponerle freno a este fenómeno que le ha tomado ventaja a las instituciones, corporaciones y gobiernos resultaría no sólo pertinente, sino que sumamente necesario.

2.4. Indicadores de Compromiso (IoC)

A continuación, se intentará definir y contextualizar el tópico de Indicadores de Compromiso IoC, que al igual que los otros ya abordados, constituye una pieza clave dentro de la investigación.

Como ya se ha mencionado, el uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el Ciberespacio, en donde se pueden presentar conflictos y agresiones que atentan contra la Seguridad Nacional, la economía, y en general, el normal funcionamiento de la sociedad. En este contexto, las Ciberamenazas son cada vez más elaboradas, más desarrolladas y orientadas a objetivos muy concretos. Razón por la cual es necesario contar con herramientas y protocolos que permitan detectar y responder frente a este tipo de amenazas.

Cuando se presentan estas situaciones, se puede decir que estamos frente a un Incidente de Seguridad, es decir, "un evento adverso que compromete o intenta comprometer la confidencialidad, integridad o disponibilidad de la información" Acosta (2015).

De acuerdo con este concepto, la clave para determinar si un comportamiento anormal se trata de un Incidente de Seguridad está en el análisis preliminar del estado del sistema en dicho momento, por consiguiente se procede a la revisión de múltiples variables tales como: el aumento del tráfico de red, alto consumo de CPU o de memoria RAM, lentitud en la respuesta de procesos, ejecución de binarios extraños, cambios en los ficheros de configuración, tratando de rastrear posibles modificaciones en los sistemas que puedan atribuirse a códigos dañinos (virus, troyanos, etc.). Al comprobarse que el sistema se encuentra frente a una APT (Amenaza Avanzada Persistente) es decir, un tipo de ataque sofisticado, que se ejecuta durante un largo periodo de

tiempo y está dirigido específicamente a una Organización, se puede proceder de forma paralela a perfilar una respuesta acorde con la tipología del evento (ver figura 2).

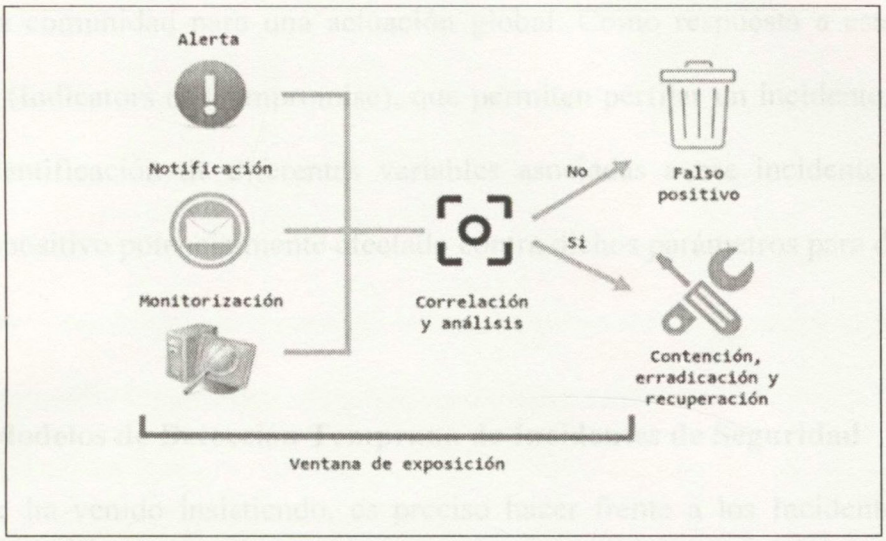


Figura 2: Ventana de exposición" en la respuesta a incidentes.
Acosta, D (2015). El papel de los indicadores de compromiso (indicators of compromise – ioc) en la respuesta a incidentes de seguridad y la investigación forense. Recuperado de: http://blog.isecauditors.com/2015/09/papel-de-los-ioc-en-respuesta-incidentes-seguridad-investigacion-forense.html

Pese a que cada código dañino o APT utiliza un código a medida, para que las herramientas de detección no sean capaces de identificarlo ni detenerlo, este siempre realiza cambios en el sistema orientados a aumentar sus privilegios en el mismo, y es en ese momento cuando se pueden interpretar esas modificaciones que realiza en el sistema como indicadores de que el sistema ha sido comprometido.

Eso "es lo que se conoce como Indicador de Compromiso (Indicator of Compromise – IoC) por lo tanto, los indicadores de compromiso sirven para identificar si un sistema ha sido comprometido (a modo de herramienta forense), o si se está intentando comprometerlo". (Méndez, 2015, p. 7).

La minimización de la ventana de exposición entre el tiempo de detección de un incidente y su respuesta es un factor clave en el proceso de respuesta a incidentes. Debido a la gran cantidad de información que se requiere para esta detección y la generación se conclusiones o inferencias

que den paso a acciones de contención, corrección y recuperación, es necesario un procedimiento automatizado que facilite la identificación de incidentes ya analizados y permita compartir dichos hallazgos con la comunidad para una actuación global. Como respuesta a esta necesidad han surgido los IoC (Indicators of Compromise), que permiten perfilar un incidente, crear una línea base para la identificación de diferentes variables asociadas a ese incidente en particular y comparar un dispositivo potencialmente afectado contra dichos parámetros para dar una respuesta rápida y efectiva.

2.5. Modelos de Detección Temprana de Incidentes de Seguridad

Como se ha venido insistiendo, es preciso hacer frente a los Incidentes de Seguridad mediante el diseño de estrategias oportunas de Ciberseguridad las cuales servirán para aumentar la eficiencia y rentabilidad de las empresas, lo que redundará en el aumento de su productividad y beneficiará a sus empleados, clientes, socios, y, en general, a los grupos de interés.

Para garantizar un nivel de seguridad adecuado es necesario actuar antes de que se produzca un incidente o, por lo menos, detectarlo en un primer momento para reducir su impacto y alcance. Por esta razón las empresas y diferentes entidades han optado por impulsar la entrada en servicio de Sistemas de Alerta Temprana para la detección rápida de incidentes y anomalías dentro de las redes de la Administración.

Muchos de estos sistemas se basan en el análisis y correlación de registros generados por las herramientas de seguridad instaladas en las redes para detectar de manera proactiva cualquier anomalía y ataque.

También se emplean sistemas similares que permitan monitorizar en tiempo real el tráfico entrante y saliente de las salidas de Internet de los diferentes organismos, recolectando información de seguridad relevante y proporcionando información de los ataques recibidos, ofreciendo una

visión en tiempo real del estado de la seguridad de las redes monitorizadas, relacionando la información proporcionada por los diferentes sensores y disponiendo de estadísticas que permitan monitorizar la eficacia de las medidas de seguridad.

Respecto a estos Sistemas de Alerta Temprana, Candau (2011) escribe lo siguiente:

> Los Sistemas de Alerta Temprana permiten disponer de información técnica que conlleva a la implantación de medidas de seguridad adicionales que impidan que ataques similares se vuelvan a reproducir. Así como la detección de patrones de ataque comunes a diversas organizaciones que permitan aplicar de forma eficaz medidas de contención y eliminación de los mismos. (p. 341)

La constitución de esta línea de acción ha sido el salvavidas de un sin número de organizaciones y empresas que han tomado la seguridad como un proceso o perspectiva de protección de sistemas, redes, aplicaciones y servicios de red.

A continuación, se reseñarán algunas tecnologías y recomendaciones de Ciberseguridad que pueden servir como guía o modelo para contrarrestar las amenazas en la Red, estas funcionan bajo el principio Detección Temprana de Incidentes de Seguridad.

- **La Recomendación UIT-T X.1205:** La Recomendación UIT-T X.1205 fue aprobada el 18 de abril de 2008 por la Comisión de Estudio 17 (2005-2008) del UIT-T por el procedimiento de la Resolución 1 de la AMNT. Esta expone diversas tecnologías de Ciberseguridad disponibles para contrarrestar las amenazas, como pueden ser los encaminadores, los cortafuegos, la protección antivirus, los sistemas de detección de intrusión, los sistemas de protección contra intrusión, la computación segura y la auditoría y supervisión. También expone los principios de protección de la red, como la defensa en profundidad y la gestión de acceso aplicadas a la Ciberseguridad. Así mismo, aborda

estrategias y técnicas de gestión de riesgos, incluida la importancia de la formación y la educación a la hora de proteger la red. Se presentan ejemplos de cómo se protegen diversas redes con las tecnologías presentadas. El análisis de amenazas incluye la descripción del tipo de posibles ataques, los agresores potenciales y sus métodos y las consecuencias del éxito de un ataque. La [UIT-T X.805] permite la detección dinámica y la mitigación de las vulnerabilidades de seguridad para las amenazas conocidas. La arquitectura de seguridad divide lógicamente un conjunto complejo de características de seguridad de la red de extremo a extremo en diversos componentes arquitecturales, lo que permite la adopción de un método sistemático para la seguridad de extremo a extremo que puede utilizarse para planificar nuevas soluciones de seguridad y para evaluar la seguridad de las redes existentes.

- **Hacking Ético:** *Ethical Hacking* es una metodología utilizada para simular un ataque malicioso sin causar daño, este consiste en pruebas de intrusión, también conocidas como "Análisis de Penetración" realizadas para conocer el nivel de seguridad que tiene una organización. Actualmente el Hacking Ético es una práctica habitual que permite evaluar las vulnerabilidades de los Sistemas y Redes en términos de confidencialidad e integridad. Comprueban la seguridad de las Red y verifican empíricamente la resistencia de las aplicaciones y servicios. El analista procura realmente comprometer las maquinas o redes objetivo atacando al hardware o al software con metodologías diseñadas de acuerdo con la legislación personal de datos y seguridad de la información. Una vez los Hackers expertos (profesionales en seguridad informática) han reconocido las vulnerabilidades del sistema, se pueden implementar las mejoras en su configuración, acceso e incluso rediseño de este para reparar dichas fallas. De acuerdo con Curso de Ciberseguridad y Hacking Ético

(Gutiérrez, 2013) se debe seguir un protocolo que inicia con una simulación de intrusión en donde se aplica un test de penetración (penTest) dirigido a la detección temprana de fallas de seguridad. Luego continua con un "Ataque Puro" en donde se realiza el acceso a la red y los sistemas, y finalmente se realiza un "borrado de huellas" para evitar que, tras un análisis forense, se descubra información comprometedora del atacante. Para el Hacking Ético se utilizan diferentes herramientas de footprinting y scanning entre otras.

- **OSSIM (Open Source Security Information Management):** Tal como afirma Ichasco (2015), OSSIM es una plataforma de seguridad que permite tratar la información generada, almacenarla y priorizarla mediante técnicas de correlación brindando una visión completa de la red desde una perspectiva de confidencialidad, integridad y disponibilidad. Funciona con una colección de herramientas bajo la licencia GPL, diseñadas para ayudar a los administradores de red en la seguridad de las computadoras, detección de intrusos y prevención. El objetivo del proyecto es ofrecer una herramienta que ayude a la administración de eventos de seguridad mediante un motor de correlación y una colección detallada de herramientas open source y elementos de software tales como: Arpwatch; utilizado para detección de anomalías en direcciones MAC., P0f; utilizado para la identificación pasiva de OS., Pads; utilizado para detectar anomalías en servicios, Openvas; utilizado para la evaluación y correlación cruzada (Sistema de detección de intrusos vs Escaner de Vulnerabilidad), Snort; utilizado como sistema de detección de intrusos (IDS) como también para la correlación cruzada con Nessus, Spade; es un motor de detección de anomalías en paquetes. Utilizado para obtener conocimiento de ataques sin firma, Tcptrack; utilizado para conocer la información de las sesiones, lo cual puede conceder información útil relativa a los ataques, Ntop; el mismo construye una impresionante base

de datos con la información de la red, para la detección de anomalías en el comportamiento, Nagios; utilizado para monitorear la disponibilidad de los hosts y servicios, nfSen; visor de flujos de red para la detección de anomalías de red, Osiris; es un sistema de detección de intrusos basado en host (HIDS), Snare; colecciona los logs de sistemas Windows, OSSEC; es un sistema de detección de intrusos basado en hosts, OSSIM; también incluye herramientas desarrolladas específicamente para él siendo el más importante un motor de correlación con soporte de directivas lógicas e integridad de logs con plugins.

Como ya se ha manifestado, estos tres modelos que se reseñaron; la Recomendación UIT-T X.1205, Hacking Ético y OSSIM, no son las únicas metodologías, herramientas o recomendaciones que existen para contrarrestar las amenazas en la Red, sino que se presentan con el fin de profundizar en la forma en cómo se han implementado las estrategias de Ciberseguridad que atienden al principio de prevención y sistemas de Detección Temprana de Incidentes de Seguridad.

En este mismo ámbito también se inscriben otros modelos de implementación, los cuales se expondrán a continuación, pero contrario a los anteriores, éstos aplican el concepto IoC (Indicator of Compromise). Su estudio es fundamental dado que los IoC son parte central de la propuesta de investigación que da lugar a este estado del arte, la cual es a saber, el Diseño de indicadores de compromiso para la detección temprana de incidentes de seguridad en la Red del Ministerio de Relaciones Exteriores de Colombia.

Recordemos que los IoCs funcionan bajo un protocolo como el siguiente:

Tras una evidencia inicial de un equipo/s comprometidos se investiga vía análisis forense cual es el IoC de la intrusión y se crea. Una vez creados se despliega en nuestros sistemas o redes objetivo para buscar la existencia de este IoC en otros sitios. Si se identifican nuevos sistemas

sospechosos se recolectarán estas nuevas evidencias que tras analizarlas ayudarán a identificar más en profundidad la intrusión, descartar falsos positivos, etc., que nos ayudarán a refinar y crear nuevos IoCs de forma que volvemos a iniciar el círculo hasta que creamos haber recopilado toda la información necesaria (Moreno 2013).

De acuerdo con Acosta (2015) desde la perspectiva de la industria han surgido diferentes modelos de implementación del concepto de IoC. A pesar de que no existe un modelo estándar, a continuación, se presentan algunos de los modelos más empleados. Vale la pena aclarar que estos se eligen dependiendo de las necesidades de la organización.

- **OASIS Cyber Threat Intelligence (CTI):** esta iniciativa está respaldada por algunos de los principales fabricantes de soluciones de seguridad y está orientada hacia la definición y estandarización de un conjunto de representaciones de información y protocolos para gestionar la necesidad de analizar, modelar y compartir datos de inteligencia contra amenazas informáticas. Está compuesto por tres subcomités: STIX (Structured Threat Information), TAXII (Trusted Automated Exchange of Indicator Information) y CybOX (Cyber Observable Expression).
- **IODEF (Incident Object Description Exchange Format):** en diciembre de 2007 se publicó la RFC 5070, que contiene la descripción básica del esquema XML para el registro de variables técnicas relacionadas con incidentes conocidos para ser empleados principalmente por centros de respuesta a incidentes (CSIRT), orientado hacia la automatización en el procesamiento de datos de incidentes y la gestión de un formato común para construir herramientas interoperables para la gestión de incidentes.
- **The OpenIoC (Open Indicators of Compromise):** OpenIoC es un esquema extensible de XML publicado bajo los términos de la licencia Apache 2, que permite describir las

características técnicas que identifican una amenaza conocida, la metodología de un atacante u otra evidencia de compromiso para la detección rápida de brechas de seguridad en un sistema. Esta iniciativa surgió como parte de las estrategias de gestión de incidentes de MANDIANT quienes son reconocidos por sus análisis de casos de Ciberespionaje a nivel mundial. Actualmente se encuentra en su versión 1.0 y la versión 1.1 se encuentra en formato DRAFT.

A manera de conclusión podemos agregar que los IoCs representan una manera eficiente y rápida para identificar amenazas avanzadas que, en algunos casos, pasarían inadvertidas por otros sistemas.

3. CONTEXTO INTERNACIONAL

Esta tercera fase del trabajo de grado consiste en presentar un muestreo representativo de incidentes de seguridad en el ámbito Internacional con el fin de caracterizar este tipo de situaciones. De igual forma se expondrán algunos modelos de detección temprana de incidentes de seguridad que se han desarrollado, asociados o no al concepto IoC (Indicators of Compromise).

3.1 Incidentes de Seguridad a nivel Internacional

Al realizar un análisis documental son innumerables los casos de incidentes de seguridad reportados a nivel Internacional, los ataques malware, ransomware y phishing son los ataques más utilizados por los cibercriminales para engañar a los usuarios.

Según Néstor Ganuza Artiles en su cuarto capítulo de Situación de la ciberseguridad en el ámbito internacional y en la OTAN, uno de los casos de Estonia en el año 2007 se presentó varios hechos importantes a nivel cibernético como el comienzo de ciberataques a sistemas de información a las infraestructuras públicas y privadas del país, y los medios de comunicación locales, nacionales e internacionales se hacían eco de la situación con puntos de vista diferentes. Los tipos de ataque que enfrento Estonia fueron: ataques de denegación de servicio (DoS), ataques de desfiguración de sitios web (web site defacement), ataques a servidores de sistemas de nombres de dominio, correo basura (spam).

Otro hecho relevante es el caso de Georgia en el año 2008, los ciberataques se presentaron en tres fases, la primera pre-conflicto armado con ataques de pequeña enmendadura que contabilizaban la denegación de servicios (DoS), la segunda fase fue ataques a sitios web con preferencia a sitios gubernamentales y agencias de noticias, la tercera y última ataques de menor escala finalizando el 27 de agosto de 2008.

Según Valle, M (2015), periodista especializada en tecnología y Ciberseguridad, algunos de los mayores ciberataques de la historia son los siguientes:

- **Ciberataque a Saudi Aramco (2012):** 35.000 ordenadores fueron borrados parcialmente o incluso destruidos, la capacidad de la compañía para suministrar el 10% del petróleo de todo el mundo, estaba en peligro. Durante meses, una de las mayores empresas del mundo estuvo desconectada de la red, por precaución y tuvieron que volver al papel y al fax para llevar a cabo las gestiones de la empresa.
- **Ataque a Sony Pictures (2014):** este ataque produjo daños por valor de 100 millones de dólares, y se comprometieron 100 Tb de datos.
- **Celebgate (2014):** caso en el que de las imágenes íntimas de famosas fueron filtradas por hackers usando una sofisticada pieza de junto con un programa de violación de contraseñas de código abierto.
- **Hacking Team (2015):** Hacking Team es una controvertida firma de software italiana popular por suministrar de forma legal herramientas de espionaje e intrusión remota como spyware y malware. Entre sus clientes figuran agencias de inteligencia y gobiernos. La compañía sufrió un ataque donde se han filtrado a la red 500 Gb de datos confidenciales.
- **El filtrado de datos a Ashley Madison (2015):** sufrió una filtración de datos de 40 millones de usuarios de una red de citas extramatrimoniales.
- **Ataque al gobierno de Estados Unidos (2015):** la Oficina de Administración de Personal de Estados Unidos recibió un ciberataque que dejó al descubierto datos confidenciales de 21,5 millones de personas: los números de la seguridad social, contraseñas, usuarios y huellas dactilares.
- **Coche Chrysler (2015):** tomaron el control de la electrónica de un vehículo Chrysler en movimiento y llevaron a cabo todo tipo de acciones que en principio sólo puede realizar el

sistema de conducción. Como consecuencia, Chrysler retiró casi un millón y medio de coches que podían ser vulnerables a estos ataques.

Estos casos que acabamos de referir llaman la atención por ser atípicos debido a su impacto por la afectación a gran estala de la que fueron capaces. En este mismo aspecto es importante mencionar el incidente reportado el 12 de mayo de 2017 que alcanzó 45.000 ataques en 74 países (Tecnósfera, 2017).

Se trató de un ciberataque mundial con el virus conocido como ransomware, el cual afectó, entre otros, a los equipos de la sede de Telefónica en Madrid, al sistema de salud británico y al Ministerio del Interior Ruso.

Según lo documentado por Olveira (2017), el ransomware causa un secuestro exprés de datos y pide un rescate para liberar el sistema, y puede infectar al resto de ordenadores vulnerables de la red. WanaCrypt0r cifra archivos del disco duro con extensiones como .doc .dot .tiff .java .psd .docx .xls .pps .txt o .mpeg, entre otros, y aumenta la cuantía del rescate a medida que pasa el tiempo.

> Después de cifrar los ficheros del disco duro, WanaCrypt0r cambia el nombre de los nombres de las extensiones de los archivos afectados por .WNCRY. Después, el virus hace saltar a la pantalla el siguiente mensaje: "Ooops, tus archivos importantes están encriptados" y solicita el rescate de 300 dólares (274 euros, aproximadamente) en bitcoins (un tipo de moneda digital) para liberarlos. El mensaje incluye instrucciones sobre cómo realizar el pago y un cronómetro. (El País, 2017)

De acuerdo con el diario El Tiempo (Tecnósfera, 2017), uno de los casos más nombrados fue el de la empresa española Telefónica. El Centro Criptólogico Nacional (CCN) (2015) de España alertó de "un ataque masivo de 'ransomware' que afecta a sistemas Windows, bloqueando el acceso a los archivos (tanto en sus discos duros como en las unidades de red a las que estén

conectadas)". El centro explicó que basta la infección de un solo equipo para comprometer a toda la red corporativa.

Otro blanco de los ataques fue el Servicio Nacional de Sanidad (NHS) del Reino Unido. Al menos 40 hospitales y entidades británicos se vieron afectados, lo que obligó a desviar ambulancias y a suspender citas programadas.

Colombia también fue víctima de este ataque global informático. Según reportes de la compañía Etek International (citada en Tecnósfera, 2017) se confirmaron tres casos, incluida una entidad pública. Sin embargo, no se trata de un hecho sin precedentes, pues de acuerdo con investigaciones realizadas por el periódico El Tiempo la infección de 'malware' en el país se ha incrementado en el último año en un 114 por ciento.

> La particularidad de este fenómeno es que no necesariamente es un cibercriminal o una persona con conocimiento en sistemas, también se puede considerar como un servicio. A los colombianos los están atacando a través de las plataformas de Gobierno. Por ejemplo, se han detectado correos falsos con invitaciones de la Dian, boletines ficticios de la Policía o citaciones a juzgados. (Tecnósfera, 2017)

Pese a que Colombia ha logrado significativos avances en su seguridad cibernética, las organizaciones colombianas aún están en batalla contra las amenazas. La clave parece centrarse en generar consciencia en estas áreas, alentando a las organizaciones colombianas a que cuenten con tecnología, inteligencia y experiencia para combatir efectivamente un ataque cibernético o prevenir amenazas cibernéticas.

De acuerdo con las consideraciones presentadas anteriormente, el panorama actual de la Ciberseguridad resulta desalentador, entre otras cosas porque este tema no se trata como una prioridad.

El ACR de 2017 (INFOSERTEC, 2017) informa que sólo el 56% de las alertas de seguridad son investigadas y menos de la mitad de las alertas legítimas reparadas. Los defensores, confiados en sus herramientas, luchan contra la complejidad y los desafíos de mano de obra, dejando vacíos de tiempo y espacio para que los atacantes utilicen la ventaja.

Es por ello por lo que iniciaremos reseñando las recomendaciones que da Cisco (2017) para prevenir, detectar y mitigar las amenazas, con el propósito de minimizar los riesgos:

- Hacer de la seguridad una prioridad empresarial: el liderazgo ejecutivo debe ser dueño y concientizar al resto con respecto a la importancia de la seguridad y financiarla como una prioridad.
- Medir la disciplina operacional: revisar las prácticas de seguridad y controlar puntos de acceso a sistemas de red, aplicaciones, funciones y datos.
- Comprobar la eficacia de la seguridad: establecer métricas claras. Utilícelos para validar y mejorar las prácticas de seguridad
- Adoptar un enfoque de defensa integral: hacer de la integración y la automatización una prioridad en la lista de criterios de evaluación para aumentar la visibilidad, agilizar la interoperabilidad y reducir el tiempo de detección y detención de ataques. Los equipos de seguridad pueden enfocarse en investigar y resolver amenazas verdaderas.

Como resultado de este proceso de investigación se formulan además dos horizontes de acción en los que se debe profundizar para mejorar el panorama de Ciberseguridad en el contexto nacional, teniendo en cuenta que la falta de prevención y de sensibilización frente al tema son factores principales de la problemática.

El primero que tomar en cuenta inmediatamente es la "Sensibilización a todos los niveles" es decir, que, en las instituciones y empresas, todos; directivos, empleados, profesionales y

ciudadanos, reciban formación en Ciberseguridad, de tal forma que se tome conciencia respecto a la problemática que se presenta, y se instruyan en protocolos a seguir para no exponerse a incidentes de seguridad o para saber cómo manejarlos.

Un segundo horizonte de acción estaría encaminado hacia el "Incremento de la capacidad de vigilancia", esto es, desplegar sistemas que potencien las capacidades de detección e investigación de incidentes en redes y sistemas, facilitando su contención y eliminación. Así como la implementación de sistemas de gestión centralizada de eventos de seguridad y complementar con herramientas capaces de detectar anomalías de manera temprana.

Este horizonte constituye un lugar valioso de trabajo ya que los Sistemas de Alerta Temprana son la base de interés de esta investigación, que como ya se ha mencionado, tiene como objetivo el Diseño de Indicadores de Compromiso para la detección temprana de incidentes de seguridad en la red del Ministerio de Relaciones Exteriores de Colombia.

4. CONTEXTO NACIONAL

En este apartado se enunciarán eventos importantes en Colombia que han sido importantes para el comienzo de la Ciberseguridad y Ciberdefensa. A partir de la Ley 527 de 1999 se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones, con esta ley se empieza la revolución informática y el impacto en las comunicaciones nacionales. Mas adelante, en el 2009 se reglamenta la Ley 1273 de delitos informáticos.

En el 2011 se da inicio al COPES 3701 el cual define los lineamientos de política para la Ciberseguridad y Ciberdefensa, cual fue liderado por el Ministerio de Defensa Nacional y como líder en su momento. Este documento busco advertir y vigilar el aumento de los ataques cibernéticos que trascienden a nivel internacional, el modelo de coordinación política para la Ciberseguridad y Ciberdefensa en Colombia se estableció con una comisión intersectorial (ver figura 3).

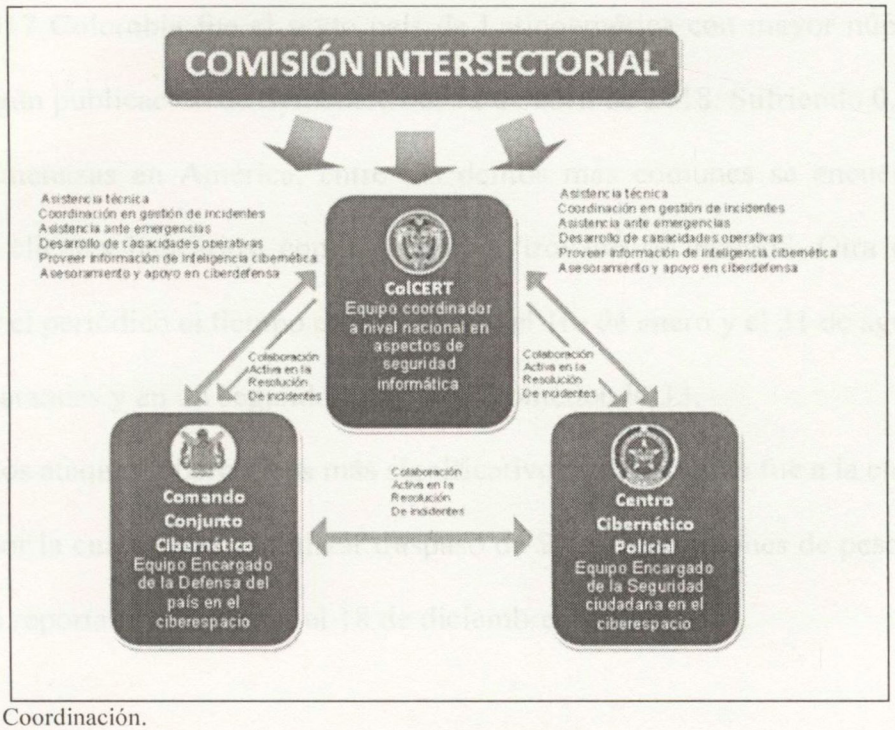


Figura 3: Modelo de Coordinación.
Documentos CONPES 3701 (2011). Recuperado de: https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

Con el CONPES 3701 se crea el ColCERT como organismo coordinador a nivel Colombia para atender temas de Ciberseguridad y Ciberdefensa.

En el 2013 mediante el Decreto 1377 se reglamenta la Ley 1581 de 2012 por la cual se dictan disposiciones generales para la protección de datos personales en Colombia. Otro avanece nacional se enmarca con el convenio de Budapest, el cual busca aplicar y priorizar una política para proteger a la sociedad de los ciberdelincuentes, adoptando una legislación y cooperación internacional. También se tiene cooperación con INTERPOL para contrarrestar los delitos cibernéticos.

Un informe publicado por Symantec, del 2013, informa que el coste de los delitos cibernéticos en Colombia ha alcanzado los US$464 millones. Otro informe relocalizado por la firma KPMG en el mismo año comunica que los crímenes económicos han supuesto en el último año una afectación económica cercana al 1% del PIB, esta encuesta buscaba medir el impacto de los cibercrímenes en las empresas con mayor impacto nacional.

En el 2017 Colombia fue el sexto país de Latinoamérica con mayor número de ataques cibernéticos, según publicación de Symantec del 12 de abril de 2018. Sufriendo 0,36% reportadas por todas las amenazas en América, entre los delitos más comunes se encuentra el robo de información de clientes bancarios, conocido como "troyano financiero". Otra cifra reveladora comunicada por el periódico el tiempo dice que entre el 1ro de enero y el 31 de agosto del 2017 se registraron 117 ataques y en un segundo se estarían cometiendo 33.

Uno de los ataques cibernéticos más significativos en Colombia fue a la entidad financiera Bancolombia, por la cual lograron realizar traspaso de $160.000 millones de pesos a 360 cuentas bancarias, así lo reporta el espectador el 18 de diciembre de 2014.

En materia de Ciberseguridad son muchos los desafíos que se plantean al momento de hacer frente a los Incidentes que se presentan, sobre todo por la incesante evolución del Cibercrimen, y sus versátiles modos de ataque.

Algunas de los obstáculos que actúan en contra de las empresas, instituciones o usuarios para avanzar en sus estrategias de seguridad son las limitaciones presupuestarias, la mala compatibilidad de los sistemas y falta de talento capacitado. Esta situación se agudiza en el ámbito de las empresas (grandes, medianas y pequeñas), pues el tema de seguridad informática no se trata como una prioridad, lo que se traduce en sistemas obsoletos, protocolos anticuados y falta de capacitación en los empleados para enfrentar las amenazas.

De acuerdo con una investigación de la Revista Semana (2016) en lo corrido del 2015 el país sufrió pérdidas por alrededor de un billón de pesos debido a ataques cibernéticos de diversa índole, robo de información y fraudes informáticos. Respecto a esto, Cisco (2015) resalta que el robo de información es un tema complejo dado que a medida que las organizaciones generan más información y mucho más valiosa, los piratas informáticos también diversifican su abanico de delitos. Esto implica un reto enorme tanto para las autoridades como para las propias empresas, que siguen sin dimensionar el dinero que pueden perder.

El 'Informe Anual de Seguridad', presentado por la firma estadounidense Cisco (2016), revela que los directores de las empresas han descuidado los procesos y herramientas para combatir los ataques informáticos, al punto de que varios de estos sistemas ya están "obsoletos". El envejecimiento de la tecnología y las fallas en los procesos a nivel corporativo, son solo algunos de los factores que explican por qué solo el 45% de las empresas confían ciegamente en sus protocolos de seguridad. La investigación de Cisco también sostiene que uno de los aspectos más

preocupantes es que el 31% de los dispositivos analizados en las empresas ya no reciben soporte o mantenimiento por parte del vendedor.

Ante la evolución y la complejidad de los delitos cibernéticos, la realidad es que los esfuerzos que ha estimado Colombia no han sido suficientes para combatir el problema. La Revista Semana (2016) conoció el borrador del CONPES 2016 en donde se reconoce la poca infraestructura y capacidad que ha tenido Colombia para enfrentar la delincuencia del mundo digital. El informe observa que las capacidades de las entidades responsables de Ciberseguridad y Ciberdefensa son limitadas, por lo que el país sufre mayores índices de probabilidad en la materialización de los riesgos digitales a los que se encuentra expuesto. En esa misma línea, el Comando Conjunto Cibernético (CCOC) también se muestra ineficiente, al poner a consideración que sus Unidades Cibernéticas de las Fuerzas y los organismos de inteligencia del Estado no cuentan con los recursos humanos, técnicos y financieros suficientes para asegurar la defensa nacional en el entorno digital. Algo que también alerta es el valor que representa para el país estar a merced de los delitos informáticos. En el borrador del CONPES, las estimaciones sobre el costo que dicha problemática le ha representado al país oscilan en el 0,14 % del PIB. Lo que pone en evidencia que las empresas aún no dimensionan el costo que puede tener un ciberataque para su negocio, ello considerando que el acceso a datos privados y la indisponibilidad de un sitio, pueden significar el fin de una marca, una organización o institución.

Hemos llegado a la cuarta fase de este recorrido por el campo de la Ciberseguridad y Ciberdefensa. Una vez rectificados los conceptos claves en este campo y realizadas las indagaciones sobre los casos más destacados en el ámbito de Ciberataques y Detección Temprana de Incidentes de Seguridad, sólo nos resta contextualizar un poco el panorama actual de la Ciberseguridad, y brindar algunas perspectivas y recomendaciones que pueden aplicarse teniendo

en cuenta el estado de la Ciberseguridad en nuestro país a partir de estrategias de control a nivel preventivo como son los indicadores de compromiso.

5. SITUACIÓN ACTUAL EN EL MINISTERIO DE RELACIONES EXTERIORES

En este punto de la investigación vale la pena describir algunos eventos de seguridad que se han presentado en la red del Ministerio de Relaciones Exteriores y que se expondrán a continuación como parte de los Incidentes de Seguridad en el Contexto Nacional.

Actualmente el Ministerio de Relaciones Exteriores ha sido víctima de varios incidentes de seguridad como malware y ciberataques a uno de los sistemas de información. Dentro de los reportes de la herramienta de Mesa de Ayuda – Aranda, el día 27 de noviembre de 2015 una usuaria de un consulado fue afectada por un malware conocido como Locker Ransomware, este mismo evento se repercute el 02 de marzo de 2016 en la ciudad de Bogotá. El 14 de junio de 2016 reporta otro usuario que no puede acceder a información de su equipo y que visualiza una pantalla donde solicitan pago por rescatar la información. Se realizó las investigaciones pertinentes con los proveedores concluyendo que la información no era posible recuperarla porque estaba cifrada y la única persona que sabía la clave era el ciberdelincuente. No obstante, el día 09 de noviembre de 2015, varios usuarios informaron "El portal del Sistema Maestro está mostrando en algunos iconos la palabra hacking". Los especialistas analizaron e informaron que el Sistema Maestro recibió un ataque informático donde fue necesario eliminar todo el contenido del sitio atacado y restaurarlo al último backup más confiable.

Estos incidentes ponen en evidencia la inminente necesidad de diseñar una herramienta que permita detectar a tiempo ataques cibernéticos para prevenir un mayor impacto y tomar acciones correctivas que minimicen el riesgo reputacional de la organización, así como mitigar el riesgo de pérdida de información institucional.

Inicialmente para el desarrollo de este trabajo de grado se realizó un levantamiento de información para poder determinar apropiadamente las variables que influyen en el comportamiento de la Entidad, de esta forma tener claridad en el diseño de los indicadores de compromiso para el Ministerio de Relaciones Exteriores.

El principal criterio pare el diseño de los indicadores de compromiso es analizar el comportamiento de los malware, identificar cual o cuales son las variables de comportamiento que afecta el sistema, como servicios o llaves de registro comprometidos. Es por eso, por lo que es recomendable tener una copia exacta del sistema sin ningún tipo de compromiso, también llamado equipos de prueba o desarrollo con el cual se pueda comparar e identificar qué fue lo que afecto el malware.

En la actualidad hay aplicaciones desarrollas para la definición de estos indicadores como son MANDIANT y OPENIOC. MANDIANT se basa en el diseño de un frameword que documenta las características técnicas de una amenaza ya conocida, así determina la metodología que utiliza el atacante para afectar a un sistema o una aplicación. En el caso de OPENIOC busca fallos de seguridad que se estable en un framework de código abierto, basado en agrupar ficheros, registros, servicios y procesos que son las principales variables que un atacante compromete a través de estos malware.

En el caso de AlienVault ha diseñado un archivo OpenIOC donde establece indicadores para detectar las actividades de malware llamada "Red October" que es utilizada para verificar la actividad relacionada con ciber espionaje en los sistemas (Blasco, 2013).

Para entender el negocio al cual se va a estudiar en este trabajo de grado, que procesos soporta, cual es el flujo de información, cuál es su finalidad, requerimientos regulatorios y que tecnologías soporta.

El Ministerio de Relaciones Exteriores posee catorce procesos de gestión, tres procesos estratégicos donde se encuentra la gestión de información y tecnología sobre el cual se centra este trabajo de grado, tres procesos misionales donde se involucra el proceso de servicio al ciudadano como uno de los principales del Ministerio ya que debe atender las necesidades del colombiano en el exterior.

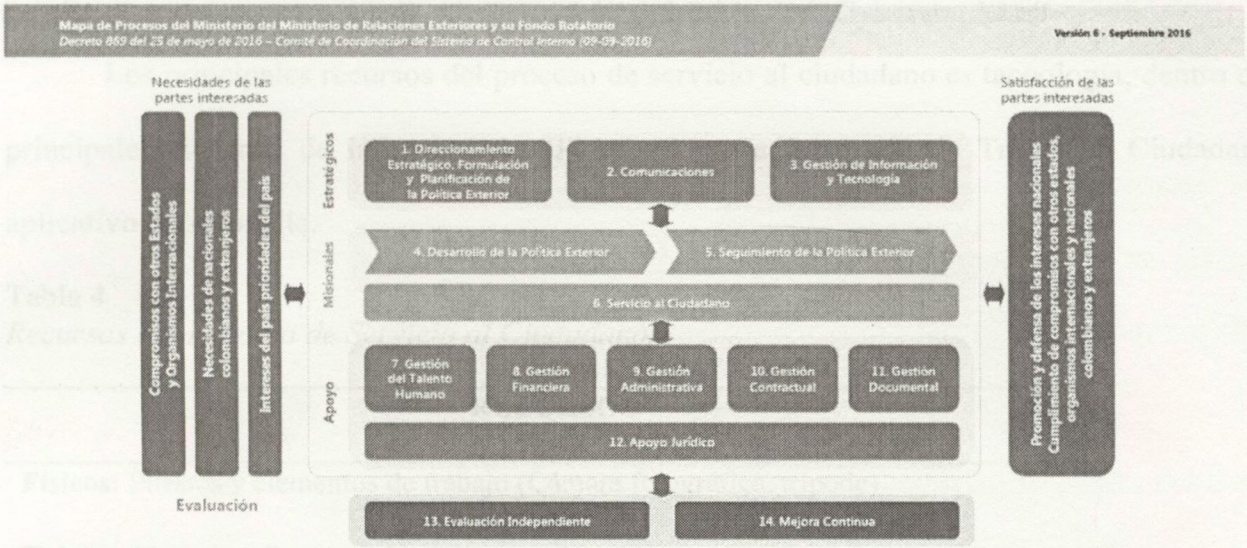


Figura 4: Mapa de procesos Ministerio de Relaciones Exteriores.
Ministerio de Relaciones Exteriores y su Fondo Rotatorio. (2016) Mapa de procesos. Sistema de Gestión de Calidad. Recuperado de: https://sigc.cancilleria.gov.co/portal/index.php?idcategoria=8.

Las principales actividades que el proceso del servicio al ciudadano es atender los siguientes tramites: pasaporte, apostilla y/o legalización, estos servicios son soportados por el proceso de gestión de información y tecnología.

Tabla 3
Proceso- Servicio al Ciudadano

Proveedor-Proceso		**Entrada-Insumo**	**Actividades claves del proceso.**	**Responsable**	**Salida-Producto y/o Servicio**	**Cliente- Proceso**	
Externo	**Interno**					**Interno**	**Externo**
			Hacer				
		Documentos necesarios	Adelantar los trámites (Pasaporte, Apostilla y/o	Dirección de Asuntos Migratorios, Consulares y	Pasaporte.		
					Libreta de Tripulante terrestre.		

Usuario.	para la elaboración del trámite.	Legalización) solicitados por los usuarios y de competencia del Ministerio de Relaciones Exteriores.	Servicio al Ciudadano. (Grupo Interno de Trabajo Apostilla y Legalización).	Apostilla. Legalización.	Usuario.

Tabla 3: Tabla del Ministerio de Relaciones Exteriores.
Ministerio de Relaciones Exteriores (2017). Caracterización de Proceso. República de Colombia. Recuperado de: https://sigc.cancilleria.gov.co/archivos/SC-PR-08/SC-PR-08%20Serrvicio_al%20Ciudadaadno_V8.pdf.

Los principales recursos del proceso de servicio al ciudadano es tecnología, dentro de los principales sistemas de información: SITAC (Sistema Integrado de Traites al Ciudadano) y aplicativo de Apostilla.

Tabla 4
Recursos del Proceso de Servicio al Ciudadano.

RECURSOS
Físicos: Puestos y elementos de trabajo (Cámara fotográfica, trípode)
Talento Humano: Personal de planta, provisionales y contratistas internos y externos
Tecnológicos: Equipo de cómputo, escáner, datafono, impresora, huellero y Pad de firmas y aplicativos (Aplicativo de Apostilla, Sistema Integral de Trámites al Ciudadano –SITAC, Sistema de Correspondencia Oficial –SICOF, Plataforma de llamadas Aspect 7.1 y Plataforma SharePoint de Atención a Peticiones, Quejas, Reclamos, Solicitud de Información, Sugerencias o Felicitaciones). **Financieros:** Presupuesto.

Tabla 4. Nota: Tabla del Ministerio de Relaciones Exteriores.
Ministerio de Relaciones Exteriores (2017) Sistema de Gestión de Calidad. República de Colombia. Recuperado de: https://sigc.cancilleria.gov.co/archivos/SC-PR-08/SC-PR-08%20Serrvicio_al%20Ciudadaadno_V8.pdf.

Los requerimientos regulatorios de cumplimiento aplicables a esta investigación son:

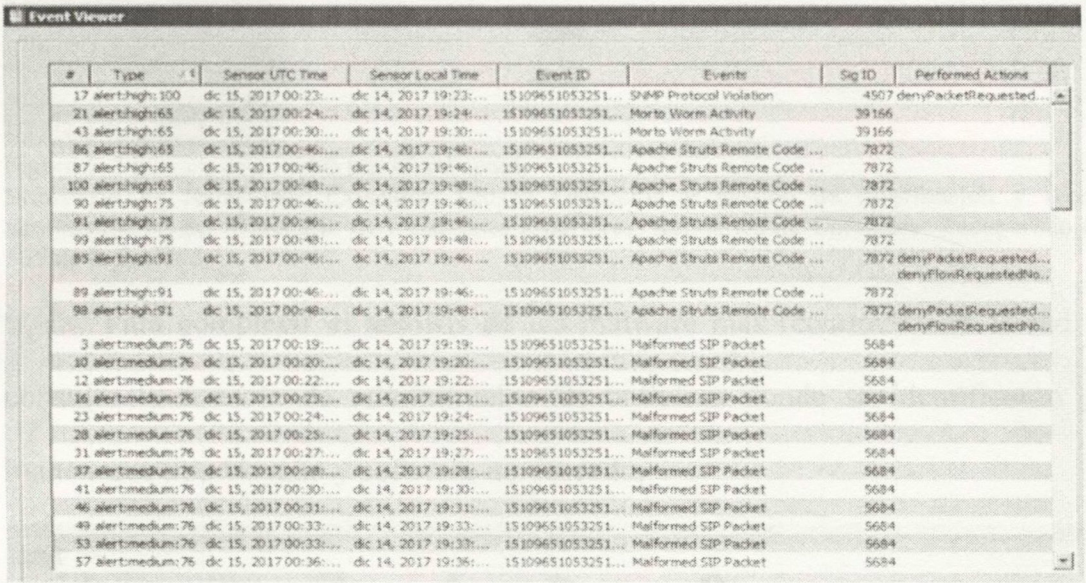
- Ley 1437 de 2011, por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo en sus artículos 53 a 64.
- Ley 527 de 1999 (Acceso y Uso de Mensajes de datos), Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de

las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

- Ley 1266 de 2008 - Dicta disposiciones generales del hábeas data y regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países.
- Ley 1273 de 2009 - Modifica el Código Penal y crea un nuevo bien jurídico tutelado que se denomina "protección de la información y de los datos".
- Ley 1581 de 2012, dicta disposiciones para la protección de datos personales, la cual tiene por objeto "desarrollar el derecho constitucional que tiene todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos (...)".
- Ley 1712 de 2014 - Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- Decreto 1413 de 2017. Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 1078 de 2015, para reglamentarse parcialmente el capítulo IV del título III de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015 estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
- Decreto 1377 de 2013 - Por el cual se reglamenta parcialmente la Ley 1581 de 2012 que constituye el marco general de la protección de los datos personales en Colombia.
- Decreto 1078 de 2015 por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Titulo 9 -Capitulo 1 Estrategia de Gobierno en Línea.

5.1 Alertas de vulnerabildiades en la Entidad

Los evetnos mas resaltantes en la red de la entidad son a nivel de ingenieria social (suplantacion de correos electronicos, ataques internos). Adicionalmente se analizaron los eventos mas criticos y continuos de las herramientas de seguridad del Ministerio encontrando, en el IPS: SNMP Protocol Violation, Morto Worm y Apache Struts.


Event Viewer

#	Type	Sensor UTC Time	Sensor Local Time	Event ID	Events	Sig ID	Performed Actions
17	alert:high:100	dic 15, 2017 00:23:...	dic 14, 2017 19:23:...	1510965105325 1...	SNMP Protocol Violation	4507	denyPacketRequested...
21	alert:high:65	dic 15, 2017 00:24:...	dic 14, 2017 19:24:...	1510965105325 1...	Morto Worm Activity	39166	
43	alert:high:65	dic 15, 2017 00:30:...	dic 14, 2017 19:30:...	1510965105325 1...	Morto Worm Activity	39166	
86	alert:high:65	dic 15, 2017 00:46:...	dic 14, 2017 19:46:...	1510965105325 1...	Apache Struts Remote Code ...	7872	
87	alert:high:65	dic 15, 2017 00:46:...	dic 14, 2017 19:46:...	1510965105325 1...	Apache Struts Remote Code ...	7872	
100	alert:high:63	dic 15, 2017 00:48:...	dic 14, 2017 19:48:...	1510965105325 1...	Apache Struts Remote Code ...	7872	
90	alert:high:75	dic 15, 2017 00:46:...	dic 14, 2017 19:46:...	1510965105325 1...	Apache Struts Remote Code ...	7872	
91	alert:high:75	dic 15, 2017 00:46:...	dic 14, 2017 19:46:...	1510965105325 1...	Apache Struts Remote Code ...	7872	
99	alert:high:75	dic 15, 2017 00:48:...	dic 14, 2017 19:48:...	1510965105325 1...	Apache Struts Remote Code ...	7872	
85	alert:high:91	dic 15, 2017 00:46:...	dic 14, 2017 19:46:...	1510965105325 1...	Apache Struts Remote Code ...	7872	denyPacketRequested... denyFlowRequestedNo...
89	alert:high:91	dic 15, 2017 00:46:...	dic 14, 2017 19:46:...	1510965105325 1...	Apache Struts Remote Code ...	7872	
98	alert:high:91	dic 15, 2017 00:48:...	dic 14, 2017 19:48:...	1510965105325 1...	Apache Struts Remote Code ...	7872	denyPacketRequested... denyFlowRequestedNo...
3	alert:medium:76	dic 15, 2017 00:19:...	dic 14, 2017 19:19:...	1510965105325 1...	Malformed SIP Packet	5684	
10	alert:medium:76	dic 15, 2017 00:20:...	dic 14, 2017 19:20:...	1510965105325 1...	Malformed SIP Packet	5684	
12	alert:medium:76	dic 15, 2017 00:22:...	dic 14, 2017 19:22:...	1510965105325 1...	Malformed SIP Packet	5684	
16	alert:medium:76	dic 15, 2017 00:23:...	dic 14, 2017 19:23:...	1510965105325 1...	Malformed SIP Packet	5684	
23	alert:medium:76	dic 15, 2017 00:24:...	dic 14, 2017 19:24:...	1510965105325 1...	Malformed SIP Packet	5684	
28	alert:medium:76	dic 15, 2017 00:25:...	dic 14, 2017 19:25:...	1510965105325 1...	Malformed SIP Packet	5684	
31	alert:medium:76	dic 15, 2017 00:27:...	dic 14, 2017 19:27:...	1510965105325 1...	Malformed SIP Packet	5684	
37	alert:medium:76	dic 15, 2017 00:28:...	dic 14, 2017 19:28:...	1510965105325 1...	Malformed SIP Packet	5684	
41	alert:medium:76	dic 15, 2017 00:30:...	dic 14, 2017 19:30:...	1510965105325 1...	Malformed SIP Packet	5684	
46	alert:medium:76	dic 15, 2017 00:31:...	dic 14, 2017 19:31:...	1510965105325 1...	Malformed SIP Packet	5684	
49	alert:medium:76	dic 15, 2017 00:33:...	dic 14, 2017 19:33:...	1510965105325 1...	Malformed SIP Packet	5684	
53	alert:medium:76	dic 15, 2017 00:33:...	dic 14, 2017 19:33:...	1510965105325 1...	Malformed SIP Packet	5684	
57	alert:medium:76	dic 15, 2017 00:36:...	dic 14, 2017 19:36:...	1510965105325 1...	Malformed SIP Packet	5684	

Figura 5: Evento IPS
Ministerio de Relaciones Exteriores (2017). Dirección de gestión de información y tecnología. Plataforma del IPS del Ministerio de relaciones Exteriores. República de Colombia. Recuerado: Servidor IPS

No obstante, se consideraron los eventos de la herramienta de seguridad antispam de Office 365 adquirida por el Minsiterio, encontrando gran cantidad de malware Nemucod, Schopets.K y Jasobfus.

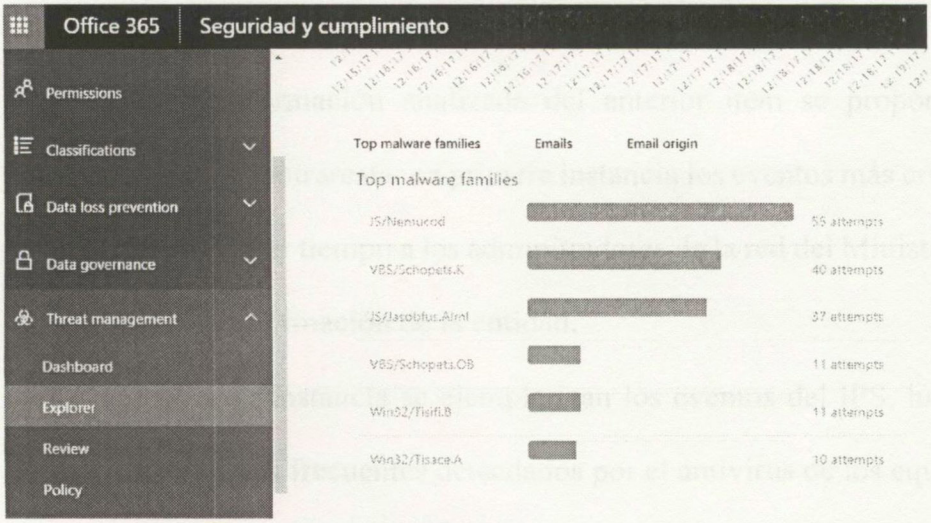


Figura 6: Malware detectados por el antispam

Ministerio de Relaciones Exteriores (2018) Detección y gestión de información y tecnología. Consola de administración del Ministerio de Relaciones Exteriores. República de Colombia. Recuperado de: servicio de office 365 de la Entidad.

Para completar el analisis de los malware mas recurrentes en la red del Ministerio se consulto la consola de adminitracion de antivirus donde se identificaron gran cantidad de manenazas tipo troyano y software no deseado.

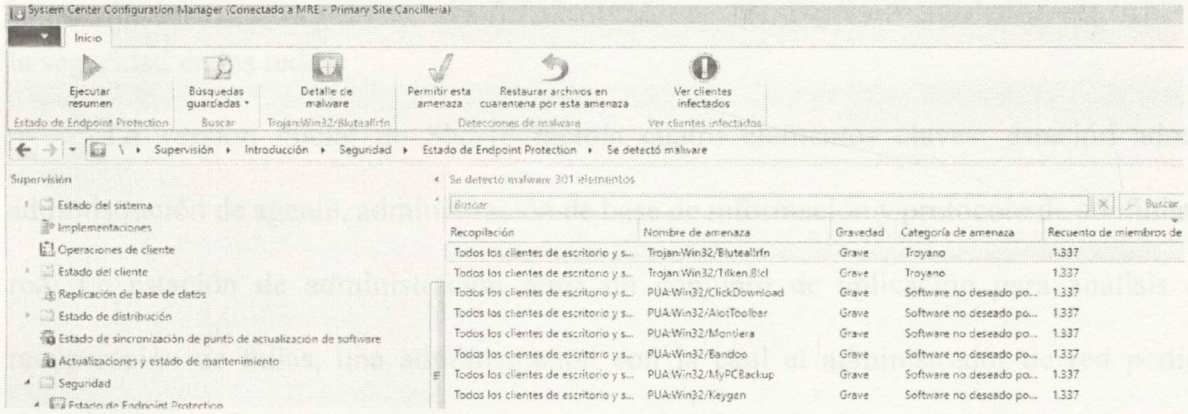


Figura 7: Malware detectados por el Antivirus

Ministerio de Relaciones Exteriores (2018) Dirección de gestión de información y tecnología. Consola de administración del Ministerio de relaciones Exteriores. República de Colombia.. Recuperado de: Servidor de antivirus de la Entidad.

A partir de toda esta informacion se investigo el comportamiento de los eventos mas criticos con el proposito de dar una propuesta de investigacion, contemplando las herramientas tecnologicas que tiene el Ministerio como es el correlacionador de eventos para construir los indicadores de compromiso.

6. DISEÑO DE INDICADORES DE COMPROMISO

Con la información analizada del anterior ítem se propone construir indicadores de compromiso para contrarestar en primera instancia los eventos más criticos de la red del Ministerio y asi alertar en menor tiempo a los adminitradores de la red del Ministerio de malwares que pueden comprometer la información de la entidad.

En primera instancia se ejemplarizan los eventos del IPS, luego los del AntiSpam y por ultimo los virus mas frecuentes detecdados por el antivirus de los equipos.

6.1. SNMP Protocol Violation

El protocolo de administración de red simple – SNMP, fue presentado en 1988 como una solución para administrar múltiples redes y facilitar el enrutamiento entre servidores, estaciones de trabajo y otros recursos de red. Consigo ha venido nuevas versiones como SNMPv1, SNMPv2 y SNMPv3, cada uno de ellos con mejoras en cuanto a normas de internet y sobre todo salvaguardar la seguridad en las redes.

La versión inicial de SNMP incluía cuatro elementos claves: estación administrada, administración de agente, administración de base de información y protocolo de administración de red. La estación de administración tenía un conjunto de aplicación para análisis de datos, recuperación de fallas, una administración con la cual el administrador de red podía realizar monitoreo y así poder controlar la red evitando posibles fallas o errores en el trasporte de la información. La administración de base de información mantenía un resumen de la información de cada uno de los elementos de red. La arquitectura de este protocolo de red SNMP normalmente se ejecuta sobre datagramas de usuario (UDP).

Algunos estándares que especifican el protocolo SNMP en los que se puede encontrar, son: RFC1155, identifica la gestión de internet basa en TCP/IP; RFC1156, administración de base de

información para redes basadas en internet TCP/IP; RFC1157, protocolo de administración simple SNMP; RFC1215, definición de trampas usada para el SNMP; RFC1270, servicios de comunicación SNMP; RFC1352 protocolo de seguridad SNMP y RFC2570, introducción a SNMPv3.

Contextualizando el RFC1352 protocolo de seguridad, este define tres servicios de seguridad, los cuales son: integridad de daos, autenticación de origen de datos y la confidencialidad de los datos. Este protocolo permite proporcionar un mecanismo de comunicación confiable, asociando protocolo de privacidad que proporciona un mecanismo de comunicación protegida.

No obstante, este protocolo no es inmune a ataques cibernético, por todo lo contrario es uno de los más deseados por los atacantes al estar presente en todo el camino de los datos, por eso las multiles vulnerabildiades que se pueden relacionar con este protocolo, entre las cuales se encuentran CVE-2002-0012 y CVE-2002-0013 con SNMP Protocol Violation, esta vulnerabilidad puede provocar denegación de servicio u obtener privilegios en el manejo de capturas SNMPv1. Para vulnerar este protocolo un atacante no requiere conocer las direcciones IPs internas de una entidad.

Como se menciona en el anterior párrafo una denegación de servicio en una entidad, puede acarrea pérdidas financieras, así como pequeños tiempos de indisponibilidad de servicios en una entidad perjudica a usuarios que puedan estar conectados, así mismo puede traer consigo perdida de imagen y confianza en los usuarios, por eso este tipo de indicador de compromiso es vital diseñarlo y adaptarlo a la red de la entidad. Uno de los comportamientos de este indicador es cuando se detecta un error en la descodificación del protocolo SNMP. El comportamiento más usual de este ataque es el aumento de escaneo (solicitudes) en los puertos UDP 161 y 162 y 1993.

A continuación de ilustra la ficha técnica del indicador de compromiso para la violación de protocolo SNMP.

Tabla 5
Ficha técnica Protocol Violation.

Descubierto	12 de febrero de 2002
CVE	CVE-2002-0012, CVE-2002-0013
CVE-2002-0012	Puntuación CVSS: 10.0 Confidencialidad: completo Integridad: Completo Disponibilidad: Completo Acceso ganado: Administración Tipo de vulnerabilidad: Negación de privilegios de ganancia de servicio CWE ID: 264
CVE-2002-0013	Puntuación CVSS: 10.0 Confidencialidad: completo Integridad: Completo Disponibilidad: Completo Acceso ganado: Administración Tipo de vulnerabilidad: Negación de privilegios de ganancia de servicio CWE ID: 264
Comportamiento	Las vulnerabilidades se deben a la forma en que SNMPv1 maneja los mensajes de trampa (CAN-2002-0012) enviados desde los agentes a los administradores, y solicitan mensajes (CAN-2002-0013) enviados desde los administradores a los agentes. Aumento en el escaneo de puertos UDP 161 y 162, y 1993.

Elaboración propia a partir de tablas basada en los detalles aportados por la CVE 0012 y 0013 del 2002. Fuente: https://www.cvedetails.com.

6.2. Morto Worm

Para empezar un Worm es un gusano informático que ejecuta un software mal intencionado con el propósito de propagarse en las redes informáticas. De acuerdo con los ingenieros B. Rajesh, Y.R. Janardhan Reddy y B. Dillip Kumar Reddy el primer gusano en la historia fue desarrollado por Bob Thomas en el año de 1971 con el objetivo de ayudar a los controladores de tránsito aéreo, este gusano fue llamado "creeper", este gusano no era capaz de reproducirse por sí mismo.

El gusano llamado Morris en el año 1988 fue capaz de propagarse e infectar a los usuarios de internet, con un gran número de equipos infectados en cuestión de pocas horas. Esta infección trajo consigo cambios significativos, debido a que "creeper" era capaz de ejecutar exploits

(programa o código que se aprovecha de un agujero) realizar desbordamiento de bufer (se produce cuando los datos escritos en un búfer debido a la insuficiencia de espacio corrompen los valores de direcciones adyacentes al búfer asignado), rutinas de depuración en correos, rastrear contraseñas y atacar a otros equipos informáticos. Otras de las grande grandes infecciones reconocidas en la historia fue el gusano "Code Red", este podía propagarse a través de la corriente de internet, además podía escanear y mejor su rendimiento de difusión.

Un gusano contiene las siguientes fases: escanear a la víctima, explotar a la víctima, ejecutarse, clonarse sobre la víctima y técnicas de ocultamiento.

Se clasifican en cinco tipos de gusanos informáticos, la primera clasificación son los gusanos sigilosos que trascienden de forma rápida, en segunda clasificación los polimorfos es un software que se basa en firmas y pueden cambiar durante la propagación, en tercera clasificación los gusanos archivo son versiones de virus modificados que se ocultan, tercera clasificación los gusanos multivector, el cual usa diferentes métodos de propagación para poder atacar y la quinta clasificación se encuentra los gusanos de correo electrónico que son enviados como lo dice su nombre mediante archivos adjuntos y se ejecutan automáticamente cuando se abre los archivos.

El gusano Motor Worm ejecuta un software que explota una vulnerabilidad de Windows llamada CVE-2012-0002, realizando denegación de servicio. Es tan infeccioso que puede obtener hasta 37 conexiones usando el protocolo de escritorio remoto con un nombre de usuario administrador en tan solo 4 minutos. Este tipo de ataque es perjudicial para la entidad, porque compromete la confidencialidad y disponibilidad por completo. Si llegase a presentarse en uno de los servidores solo permitiría apagar el equipo y volver a crear un nuevo servidor a partir de los backup, tomaría más tiempo que un RTO (tiempo de recuperación objetivo) o plan de contingencia, y se estaría realizando una acción posterior al ataque, al diseñar un indicador de

compromiso de este tipo gusano permitiría alertar a los administradores para aislar y controlar adecuadamente un incidente de esta categoría.

Se propone que el indicador de compromiso para Morto Word se realiza a partir de la identificación de algún cambio en los archivos del sistema o registros que se ilustra a continuación de la tabla 6.

Tabla 6.
Ficha técnica Morto Worm

Descubierto	22 de septiembre de 2011
CVE	CVE-2012-0002
CVE-2012-0002	Puntuación CVSS: 9.3 Confidencialidad: completo Integridad: Completo Disponibilidad: Completo Acceso ganado: Ninguno Tipo de vulnerabilidad: Ejecutar código CWE ID: 94
Comportamiento	El malware suele copiarse en las siguientes rutas: % Windir% \ Offline Web Pages \ cache.txt % Windir% \ Offline Web Pages \ [CURRENT DATE] % System% \ Sens32.dll % System% \ sens.dll El gusano crea los siguientes registros: HKEY_LOCAL_MACHINE \ SYSTEM \ WPA \ sr HKEY_LOCAL_MACHINE \ SYSTEM \ WPA \ sn HKEY_LOCAL_MACHINE \ SYSTEM \ WPA \ rmd HKEY_LOCAL_MACHINE \ SYSTEM \ WPA \ md HKEY_LOCAL_MACHINE \ SYSTEM \ WPA \ it HKEY_LOCAL_MACHINE \ SYSTEM \ WPA \ ie HKEY_LOCAL_MACHINE \ SYSTEM \ WPA \ id HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services \

Elaboración propia a partir de tabla que expone algunas de las especificaciones de la CVE del 2012. Fuente: https://www.cvedetails.com.

6.3.Apache Struts

Apache Struts es un framework de programacion utilizado por los programadores de apliaciones. Un framework es un conjunto de herramientas, normas y biblitecas que ayudan a desarrollar aplicaciones. Algunos de los inconvenientes con este tipo de framework es la dificultar

de compender el modelo, el numero excesivo de archivos que se requieren para producir y la reiteracion de las tareas que se realizan. Los ataques de Apache Struts esta catalogado como unos de los top 10 d el 2017, fuente de OWASP Top-10 2017.

Algunos productos Cisco (equipos de comunicaciones como router, swicth, firewall) que intervienen en la red del ministerio, incorporan una versión del paquete Apache Struts 2 que se ve afectada por las vulnerabilidades CVE-2017-9793; CVE-2017-9804; CVE-2017-9805. Estas vulnerabildiades son princiapalmente afectadas en las disponibildiad del servicio, por lo que se plantea diseñar un indicador de compromiso que alerte a los adminitradores de redes mediante un correo, que cuando se descubra una explotación de los Snort SID 44315 y 44327 a 44330, se alerte y se analice el incidente de forma preventiva y no reactiva. A continuacion se ilustra la ficha técnica del indicador de compromiso para el ataque de Apache Struts.

Tabla 7
Ficha técnica Apache Strauts.

Descubierto	5 de septiembre de 2017
CVE	CVE-2017-9793; CVE-2017-9804; CVE-2017-9805
CVE-2017-9793	Puntuación CVSS: 5.0 Confidencialidad: ninguno Integridad: ninguno Disponibilidad: parcial Acceso ganado: Ninguno CWE ID: 20
CVE-2017-9804	Puntuación CVSS: 5.0 Confidencialidad: ninguno Integridad: ninguno Disponibilidad: parcial Acceso ganado: Ninguno CWE ID: 399
CVE-2017-9805	Puntuación CVSS: 6.8 Confidencialidad: parcial Integridad: parcial Disponibilidad: parcial Acceso ganado: Ninguno Tipo de vulnerabilidad: Ejecutar código CWE ID: 502

Comportamiento	Mediante una regla de Snort se puede detectar explotación de las vulnerabilidades, Snort SID 44315 y 44327 a 44330.

Elaboración propia a partir de información brindada por la CVE 9793, 9804 y 9805 del año 2017. Fuente: https://www.cvedetails.com.

Los siguientes eventos hacen referencia a las consultas del antispam:

6.4. JS/Nemucod

El malware Nemucod es un troyano reconocido como JavaScript (se ejecuta en el lado del cliente), su principal medio es a través del correo electrónico y potencialmente peligrosos. Después de realizar la instalación, descarga un archivo el cual se comunica a una página de WordPress (Sistema de gestión de contenidos, originalmente como una plataforma de blog) que descarga archivos temporales con la extensión .exe como Rundll32.exe o WShellu.

La primera protección contra este malware fue el 1ro de diciembre de 2015 por Symantec. A partir del 2016 los ciberdelincuentes lo hacen parte del virus Ransomware que cifra la información de los computadores con el método RSA-2014 con el fin de que las victimas paguen para poder volver a consultar la información.

Las recomendaciones que informa Symantec son:

- Tener un firewall para las conexiones entrantes a los servicios, en el cual solo se permita los estrictamente necesarios.
- Gestionar adecuadamente la complejidad de las contraseñas, para mitigar el daño cunado una computadora ya está comprometida.
- Aumentar el nivel de privilegio de acceso a la computadora, es decir que si se ejecuta una aplicación visualice una ventana para otorga o denegar la ejecución de un programa.
- Inactivar la reproducción automática para evitar el inicio de archivos ejecutables.

- Inactivar el uso de archivos compartidos, de requerir este servicio usar contraseña para limitar el acceso.
- Configurar en el servidor de correo, el bloqueo y eliminación de correos con documentos adjuntos que contenga extensiones como: .vbs, .bat, .exe, .pif y .scr.

Este malware permite a los atacantes remotos ejecutar un código a través de un documento manipulado, la vulnerabilidad es reconocida como CVE-2017-0199 o también como Microsoft Office DLL Loading. El vector de acceso de este malware es a través de la red, no requiere autenticación para ejecutarse, el impacto que puede ocasionar a un usuario es el compromiso de la integridad del sistema, la confidencialidad y disponibilidad.

El diseño del indicador de compromiso para el malware JS/Nemucod, comprende la detección de archivos como TrojanDownloader contenidos a través de adjuntos como foto.zip o Gilberto_Bond.zip que intentan tener conexión remota a través del puerto 80 a las URLs que se mencionan en la ficha técnica de la taba 7

Tabla 8
Ficha técnica JS/Nemucod.

Descubierto	1 de diciembre de 2015
CVE	CVE-2017-0199
CVE-2017-0199	Puntuación CVSS: 9.3 Confidencialidad: Completo Integridad: Completo Disponibilidad: Completo Acceso ganado: ninguno Tipo de vulnerabilidad: Ejecutar código.
Comportamiento	Variantes de Nemucod: - Invoice_ref- <random numbers> .zip (por ejemplo Invoice_ref-06977496.zip) - detectado como TrojanDownloader: JS / Nemucod - foto.zip - detectado como TrojanDownloader: JS / Nemucod.AT - Gilberto_Bond.zip - detectado como TrojanDownloader: JS / Nemucod.AR - 8221261_notice_to_appear_000986189.zip - detectado como TrojanDownloader: JS / Nemucod.P Además, la amenaza se conecta a un host remoto, como: - sahasafe.com utilizando el puerto 80

- ohelloweuqq.com
- thisisitsqq.com
- hpalsowantsff.com

Las URL a las que se conecta:

- hpalsowantsff.com
- ohelloweuqq.com
- thisisitsqq.com
- • zahasafe.com/systs

Descarga archivos, como:

- 69.exe (detectado como Ransom: Win32 / Tescrypt)
- 87.exe (detectado como Ransom: Win32 / Tescrypt)

Elaboración propia a partir de información brindad por la CVE 0199 del 2017 Fuente: https://www.cvedetails.com, y así mismo, Cisco (2017) Multiple Vulnerabilities in Apache Struts 2 Affecting Cisco Products: September 2017. Fuente: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170907-struts2.

6.5. VBS/Schopets.K

El malware VBS se encuentra dentro de la familia de virus interpretados, que se compone de un código fuente, el cual es ejecutado por una aplicación o un servicio en particular. Este tipo de malware son más fáciles de manipular porque permite realizar modificaciones de escritura. Los dos tipos de virus interpretados con los virus macro o virus Scripting.

Los virus macro proviene de correos con archivos adjuntos que se procesan como un archivo de texto u hojas de cálculo que contienen un lenguaje de programación para ejecutarse y así mismo poder ser propagado. Los virus Scripting son parecidos a los macros, su diferencia se presenta en que los macros están escritos en procesadores de texto, mientras los Scripting están escritos en un lenguaje que comprende un servicio ejecutado por el sistema operativo. En el caso de los VBScript pueden ser ejecutados por la característica de Windows Scripting Host.

También los VBSScript son conocidos como código malicioso, que tienen como intención trasmitir de un sistema remoto a un sistema local y luego ejecutarse en el local ejecutando instrucciones explicitas.

Las vulnerabilidades identificadas para este virus se encuentran CVE-2016-3202, esta vulnerabilidad podría dañar la memoria del equipo, de tal forma que el ciberdelincuente podría

ejecutar código arbitrario en el contexto del usuario, decir obtener los mismos derechos del usuario que emplea la computadora. Así como puede instalar programas, ver, cambiar o eliminar datos y nuevos derechos de usuario. Por lo anterior este tipo de vulnerabilidad se puede volver tan crítica como cualquier otra, es importante resaltar que el acceso no autorizado a una Entidad del estado puede ser tan perjudicial hasta llegar el extremo de eliminar datos sensibles de la Entidad.

El diseño de indicador de compromiso para este tipo de virus es trascendental porque mitigaría la posibilidad de ser comprometido a riesgos de perdida de información. La siguiente ficha técnica propone un IoC que al momento de descargar un archivo tipo VBScript y que intente conectarse a una URLs como babyemozioni o tertrodefordown o baptistown-nj, notifique al administrador del sistema para que desconecte el equipo evitando la ejecución de código. La ficha técnica del indicador de compromiso para VBS/Schopets. K se ilustra a continuación.

Tabla 9
Ficha técnica VBS/Schopets. K

Descubierto	21 de octubre de 2003
CVE	CVE-2016-3202; CVE-2017-0149
CVE-2016-3202	Puntuación CVSS: 7.6 Confidencialidad: completo Integridad: completo Disponibilidad: completo Acceso ganado: ninguno Tipo de vulnerabilidad: Denegación de servicio CWE ID: 20.
CVE-2017-0149	Puntuación CVSS: 7.6 Confidencialidad: completo Integridad: completo Disponibilidad: completo Acceso ganado: ninguno Tipo de vulnerabilidad: Denegación de servicio CWE ID: 119.
Comportamiento	Descarga un VBScript ejecutando malware Ransom:Win32/Locky el cual es almacenado en % APPDATA% \\ *Local* \\ *Temp* \ *<randomName> .exe y se* conecta a las URLs: - *hXXp: // babyemozioni [dot] it / KJSkjdhf* - *hXXp: // tertrodefordown [dot] info / af / YTkjdJH7w1* - *hXXp: // baptistown-nj [dot] com / KJSkjdhf* Esta descripción se basa en el análisis de la siguiente muestra:

SHA1: 5f3903d6296744dcc19e2590dec1eb3fd6598c7f.

Elaboración propia a partir de tabla de la información brindada por el CVE 3202 del año 2016 y 0149 del 2017. Fuente: https://www.cvedetails.com. Así mismo, retoma datos de Microsoft (2017) Trojan Downloader. Fuente: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=TrojanDownloader:VBS/Schopets.

6.6. JS/Jasobfus.A!ml

Es un malware tipo troyano que a través de archivos scripts descarga malware remoto al equipo de la víctima, los archivos que descarga en el equipo de la víctima pueden ser encriptados y luego pedir rescate por ellos.

Este tipo de malware tiene asociado la vulnerabilidad CVE-2010-3129, la cual realiza una búsqueda de conexión no confiable hacia un servicio que generalmente es uTorrent 2.0.3, permitiendo al ciberdelincuente ejecutar código arbitrario y realizar ataques de secuestro DLL a través de un troyano plugin_dll.dll, userenv.dll, shfolder.dll, dnsapi.dll, dwmapi .dll, iphlpapi.dll, dhcpcsvc.dll, dhcpcsvc6.dll o rpcrtremote.dll ubicado en la carpeta torrent o btsearch.

Algunos consejos para evitar este malware se encuentran no ingresar a páginas de mala reputación o también llamadas listas negras y evitar hacer clic en los adjuntos de los correos electrónicos por el cual es el método que más utilizan los ciberdelincuentes.

El impacto que puede generar este malware es tan significativo porque compromete la confidencialidad, integridad y disponibilidad del sistema, el indicador de compromiso para este tipo de ataque es a partir de la detección en la modificación no autorizada de una de las DLL de un servidor.

Es un malware tipo troyano que a través de archivos scripts descarga malware remoto al equipo de la víctima, los archivos que descarga en el equipo de la víctima pueden ser encriptados y luego pedir rescate por ellos.

Tabla 10
Ficha técnica JS/ Jasobfus. A!ml

Descubierto	26 de agosto de 2010

CVE	CVE-2010-3129
CVE-2010-3129	Puntuación CVSS: 9.3 Confidencialidad: Completo Integridad: Completo Disponibilidad: Completo Acceso ganado: ninguno Tipo de vulnerabilidad: Ejecutar código CWE ID: No está definido.
Comportamiento	Ejecuta código arbitrario y realizar ataques de secuestro DLL a través de un troyano, como: plugin_dll.dll, userenv.dll, shfolder.dll, dnsapi.dll, dwmapi .dll, iphlpapi.dll, dhcpcsvc.dll, dhcpcsvc6.dll o rpcrtremote.dll que se encuentra en la carpeta con archivos como .torrent o .btsearch.

Elaboración propia a partir de información brindada por el CVE 3129 del 2010. Fuente: https://www.cvedetails.com.

6.7.VBS/Schopets.OB

El malware VBS/Schopets.OB se encuentra dentro de la misma familia del malware VBS/Schopets.K que contiene un scrip malicioso que se puede ejecutarse por algún servicio del sistema, en algunos casos hacerse pasar por otro tipo de documento, la técnica de ingeniería social sigue siendo uno de los puntos débiles para los cibernautas, usa códigos arbitrarios que se pueden aprovechar de comandos ejecutados en PowerShell. Además, este malware descarga e instala otros virus informáticos poniendo al equipo lento.

El impacto que puede ocasionar este malware es completo, puede comprometer la confidencialidad, integridad y disponibilidad de la información, convirtiéndose en un ente importante a controlar para los sistemas y todos los servicios de la Entidad.

El indicador de compromiso se comprende una vez se detecte el almacenamiento de un archivo temporal con nombre vmGeOn.exe

Tabla 11
Ficha técnica VBS/Schopets. OB.

Descubierto	21 de septiembre de 2017
CVE	CVE-2010-3129
CVE-2010-3129	Puntuación CVSS: 9.3 Confidencialidad: Completo Integridad: Completo

	Disponibilidad: Completo Acceso ganado: ninguno Tipo de vulnerabilidad: Ejecutar código CWE ID: No está definido.
Comportamiento	Guarda los archivos que descarga en: % User Temp% \ vmGeOn.exe -> detectado como Ransom_LOCKY.TH918.

Elaboración propia a partir de información basada en las tablas que recoge información brindada por el CVE 3129 del año 2010. Fuente: https://www.cvedetails.com. Así mismo, contiene datos aportados por Ramirez (2017) *VBS_LOCKY*. Fuente: https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/VBS_LOCKY.TH918.

Los siguientes malware corresponden a la consulta del antivirus del Ministerio:

6.8. PUA:Win32/Softonic

¿Qué es PUA? Es un software potencialmente no deseado, que en la mayoría de las veces viene incluido en software free, que así mismo se financia de ventanas emergentes, navegadores o páginas de inicio predeterminadas por el software y no por el usuario.

Para antiguar en el malware PUA:Win32/Softonic, se iniciará con describir que es software fundado en Barcelona en el año1997 por el grupo Intercom, con el ánimo de apoyar a las personas a encontrar información y a disfrutar de software para mejorar sus vidas. Desafortunadamente este software ha sido utilizado para infectar a los ordenadores, siendo un puente entre el usuario y la descarga no deseada o maliciosa.

Symantec en su publicación del 29 de junio de 2015, informa que es una aplicación potencialmente no deseada que puede descargar software adicional en el computador. Así mismo Symantec crea nuevas definiciones en sus antivirus para detectar este tipo de archivos no deseados el 26 de junio de 2015.

PUA.softonic descarga e instala VLC Media Player (reproductor de multimedia libre) permitiendo descargar e instalar aplicaciones peligrosas y no deseadas. En la mayoría de las ocasiones informa al usuario si permite instalarla, una vez esta sea permitida modifica la configuración del navegador que el usuario esté utilizando.

Además la aplicación Softonic afecta el rendimiento del equipo al permitir instalar software no deseado, adicionar barras de herramientas en los buscadores de internet, este rendimiento repercute en el buen servicio que un usuario puede brindar a un ciudadano a la hora de realizar o solicitar una Apostilla, pasaporte o visa, por eso se plantea el siguiente indicador de compromiso el cual se alertara una vez detecte un archivo con nombre SoftonicDownloader o identifique una conexión con los dominios: daemon-tools.sd.softonic.com, utorrent.sd.softonic.com, v2br.sftcdn.net, v1jp.softonic.jp o www.softonic.jp a continuación se detalla la ficha técnica de este malware.

Tabla 12
Ficha ténica PUA: Win32/Softonic.

Descubierto	22 de junio de 2016
CVE	CVE-2009-3857
CVE-2009-3857	Puntuación CVSS: 4.3 Confidencialidad: ninguno Integridad: ninguno Disponibilidad: parcial Acceso ganado: ninguno Tipo de vulnerabilidad: denegación de servicio CWE ID: 119.
Comportamiento	Sitios web de las descargas: - download2094.mediafire.com - download1652.mediafire.com - download1334.mediafire.com - download1388.mediafire.com - download1446.mediafire.com Nombres de archivo: - SoftonicDownloader_para_ares.exe - SoftonicDownloader_para_atube-catcher.exe - SoftonicDownloader_for_vlc-media-player.exe - SoftonicDownloader_para_winrar.exe - SoftonicDownloader_para_photoscape.exe - SoftonicDownloader_for_utorrent.exe - SoftonicDownloader_para_utorrent.exe - SoftonicDownloader_for_winrar.exe - SoftonicDownloader_para_vlc-media-player.exe La aplicación se comunica con los dominios: - daemon-tools.sd.softonic.com - utorrent.sd.softonic.com - v2br.sftcdn.net

- v1jp.softonic.jp
- www.softonic.jp

Esta descripción fue publicada usando análisis automatizado.

Elaboración propia a partir información brindada por el CVE 3857 del año 2009. Fuente: https://www.cvedetails.com. Del mismo modo, está basada en datos aportados por Microsoft (2015). *PUA: Win32/Softonic.* Fuente: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=PUA:Win32/Softonic.

6.9. PUA: Win32 / CandyOp

Este tipo de malware es muy particular porque inicialmente es molesto para los usuarios, es de aquellos que de repente abre páginas web no deseadas o molestas o carga una página inicial sin solicitarse. Este tipo de malware puede presentarse en navegadores como Google Chrome, Mozilla, internet explore, safari sin haberse realizado la descarga, viene inmerso, por eso es importante revisar donde se debe realizar descargas con confianza.

La aplicación CandyOp afecta el rendimiento del equipo, el cual agrega archivos que se ejecutan al arranque del equipo, inyecta procesos al sistema, cambia la configuración del navegador, agrega un proxy local, modifica la configuración DNS, detiene las actualizaciones de Windows.

De acuerdo con la publicación de Microsoft del 11 de marzo de 2015, este malware puede afectar el comportamiento del equipo porque:

- Adiciona archivos que se ejecutan al inicio sin autorización
- Puede modificar los archivos de arranque del sistema
- Agrega otros procesos en el sistema
- Deshabilita el control de acceso al usuario.
- Instala programas que se inician automáticamente
- Registra un proveedor de servicios en capas (LSP) que intercepta el tráfico en la red para inyectar anuncios publicitarios en el navegador.

El diseño del indicador de compromiso para este malware se comprende cuando realiza una conexión a sitios como: download.freemake.net, www.magicaljellybean.com, www.cdisplayex.com, cdn.loadto.net, github-cloud.s3.amazonaws.com o cuando detecta un archivo con nombre uTorrent.exe, FreemakeVideoConverterSetup.exe, FreemakeVideoDownloaderSetup.exe, youtube_downloader_hd_setup.exe, CDex-1.79-win32.exe, BitTorrent.exe, KeyFinderInstaller.exe, FYDLoad_inflvto_13.exe, o FreemakeAudioConverterSetup.ex, a continuación se ilustra la ficha técnica

Tabla 13
Ficha técnica PUA: Win32/CandyOp.

Descubierto	17 de julio de 2017
CVE	CVE-2017-1000036
CVE-2017-1000036	Puntuación CVSS: 4.3 Confidencialidad: ninguno Integridad: parcial Disponibilidad: ninguno Acceso ganado: ninguno Tipo de vulnerabilidad: ejecutar código CWE ID: 79.
Comportamiento	Sitios web de descarga: - download.freemake.net - www.magicaljellybean.com - www.cdisplayex.com - cdn.loadto.net - github-cloud.s3.amazonaws.com Nombres de archivo: - uTorrent.exe - FreemakeVideoConverterSetup.exe - FreemakeVideoDownloaderSetup.exe - youtube_downloader_hd_setup.exe - CDex-1.79-win32.exe - BitTorrent.exe - KeyFinderInstaller.exe - FYDLoad_inflvto_13.exe - FreemakeAudioConverterSetup.exe

Elaboración propia que contiene alguna información brindada por el CVE 1000036 del año 2017. Fuente: https://www.cvedetails.com. Asimismo, está basada en información expuesta por Microsoft (2015) PUA:Win32/CandyOpen. Fuente: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?name=PUA%3aWin32%2fCandyOpen.

6.10. PUA: Win32 / InstallCore

El malware PUA: Win32 / InstallCore generalmente son paquetes de aplicaciones como barras de herramientas, adware (software publicitario) u optimizadores de sistemas. También InstallCore es conocido como un software basado en HTML que ayuda a que las aplicaciones se instalen correctamente, que se compone de un motor de instalación analítica y monitoreo. Este tipo de malware es tan sutil que aprende del comportamiento del usuario perfilando publicidad relevante para él.

La publicación realizada por Microsoft del 11 de marzo de 2015 informa que este malware es capaz de añadir archivos al inicio del arranque del sistema operativo del computador, modifica asociaciones de archivos, agrega otros procesos al sistema, instala otros navegadores y modifica la configuración de estos, modifica el acceso directo de un navegador, instala extensiones de otros navegadores y desactiva el UAC – Control de acceso de usuario.

Algunos síntomas atribuibles a este malware es la instalación no autorizada de archivos y carpetas, permitiendo realizar cambios en el registro para ejecutarse al inico del sistema.

El indicador de compromiso para este malware parte con el descubrimiento de conexiones hacia las paginas www.newclearchuckle.com, www.signssharepackage.com, www.bulkcentralgift.com, www.sendchucklebulk.com, www.vaultsfactorycentral.com o con la instalación de programas como: FlashPlayerPro.exe, FlvPlayerSetup.exe, HDSetup.exe, FYD_Setup.exe, installer.exe, JavaPlugin.exe, MediaDownloaderSetup.exe, setup.exe o FlashPlayerPro (1).exe. con la identificación de alguno de ellos inmediatamente debe notificar al administrador del sistema para que indague y reaccione a ejecutar medidas preventivas.

Tabla 14
Ficha técnica PUA: Win 32/IntallCore

Descubierto	25 de julio de 2012
CVE	CVE-2013-2423
CVE-2012-0002	Puntuación CVSS: 4.3 Confidencialidad: ninguno Integridad: parcial Disponibilidad: ninguno Acceso ganado: ninguno Tipo de vulnerabilidad: Omitir restricción CWE ID: no está definida.
Comportamiento	Sitios de descarga: - www.newclearchuckle.com - www.signssharepackage.com - www.bulkcentralgift.com - www.sendchucklebulk.com - www.vaultsfactorycentral.com Nombres de archivo: - FlashPlayerPro.exe - FlvPlayerSetup.exe - HDSetup.exe - FYD_Setup.exe - installer.exe - JavaPlugin.exe - MediaDownloaderSetup.exe - setup.exe - FlashPlayerPro (1).exe Se comunica con los dominios: - rp.bororeb.com - os.bororeb.com - sui-generator.sensic.net - info.bororeb.com - img.bororeb.com

Elaboración propia que contiene algunas especificaciones aportadas por el CVE 002 del año 2002. Fuente: https://www.cvedetails.com.

6.11. PUA: Win32 / AskToolbar

AskToolbar es una barra de herramienta que se instala en el navegador de internet. En la publicación de Microsoft del 13 de agosto de 2015 comunica que esta aplicación afecta la calidad del uso, porque instala aplicaciones adicionales, modifica la página de inicio del navegador y cambia el proveedor del navegador. También es conocida como adware (software publicitario).

El comportamiento de esta amenaza es que descarga software de terceros como: gsf-cf.softonic.com, storage.inbox.com, zebulon.fr y down.filepuma.com. con nombre MapsSetup.exe, EmailNotifierSetup.exe, TVSetup.exe, MusicSetup.exe, PublicTransportSetup.exe, SocialNetworksSetup.exe, EmailNotifierSetup (1).exe, MapsSetup (1).exe y CustomizableSetup.exe. con cualquier comportamiento de estos debe notificar al administrador del sistema para que tome acciones y así prevenir posibles infecciones mayores que puedan acarrear una indisponibilidad del servicio. A continuación, se detalla el indicador de compromiso para este malware.

Tabla 15
Ficha técnica PUA: Win32/ AskToolbar.

Descubierto	22 de septiembre de 2011
CVE	CVE-2007-5107; CVE-2007-5108
CVE-2007-5107	Puntuación CVSS: 9.3 Confidencialidad: completo Integridad: completo Disponibilidad: completo Acceso ganado: administración Tipo de vulnerabilidad. Desbordamiento de código CWE ID: 119
CVE-2007-5108	Puntuación CVSS: 10.0 Confidencialidad: completo Integridad: completo Disponibilidad: completo Acceso ganado: ninguno CWE ID: no está definida

Comportamiento	Sitios web de descarga: - ak.pipoffers.apnpartners.com - www.avery.com Nombres de archivo: - OffercastInstaller_AVR_U-0087-01-P_.exe - WeatherBugSetup.exe - SFInstaller_SFFZ_filezilla_8992693_.exe - YTDSetup.exe - OffercastInstaller_AVR_U-0090-01-P_.exe - Setup-SopCast-3.5.0-2012-3-22.exe - CuteWriter.exe - OffercastInstaller_AVR_U-0087-01-P_ (1).exe - OffercastInstaller_AVR_U-0112-01-P_.exe Se comunica con los siguientes dominios: - pipoffers.apnpartners.com - offers.offercast.com - 7500.biz - downloads.earthnetworks.com - files.goodgamestudios.com.

Elaboración propia que recoge información de las CVE 5107 y 5108 del año 2007. Fuente: https://www.cvedetails.com. Del mismo modo, recopila información aportada por Microsoft (2015). PUA: Win32/Asktoolbar. Fuente: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?name=PUA%3aWin32%2fAskToolbar.

6.12. PUA: Win32 / Conduit

Win32/Conduit comúnmente viene incorporado en descargas libres "free" que un usuario requiere como drive, tarjetas de memoria o aplicaciones que usuario necesita y lo hace de forma ilegal.

El 29 de junio de 2016 Microsoft informa que este malware afecta el rendimiento del sistema al permitir añadir archivos al inicio del sistema, inyectar un controlador, adicionar otros procesos al sistema, instalar otros navegadores y también permite modificar la configuración del navegador.

Esta aplicación tiene comportamientos sospechosos cuando se identifica descargas desde sitios como: s.bdirectdownload-about.com, d.computerbild.de, d110.cdn.m6web.fr, cdn.bitmedianetwork.com y ec.ccm2.net, también se distngue porque se instalan aplicaciones de archivo bsplayer266.1075.exe, FLV_Runner.exe, InstallConverter_brch.exe, WiseConvert.exe,

WiseConvert_1.5.exe, InstallConverter_brff.exe, Pconverter.exe, RadioG.exe o FileConverter_1.1.exe. al momento de tener alguno de estos comportamientos debe notificar al administrador del sistema para que este malware no vaya a implicar un desbordamiento de bufer. Como se relaciona en la tabla 17 este malware no afecta la integridad, disponibilidad o confidencialidad de la información, pero puede reducir el rendimiento en el servicio.

Tabla 16
Ficha técnica PUA: Win32/ Conduit.

Descubierto	13 de abril de 2011
CVE	CVE-2011-0663
CVE-2011-0663	Puntuación CVSS: 9.3 Confidencialidad: completo Integridad: completo Disponibilidad: completo Acceso ganado: ninguno Tipo de vulnerabilidad: desbordamiento de código CWE ID:189.
Comportamiento	Sitios de descarga: - s.bdirectdownload-about.com - d.computerbild.de - d110.cdn.m6web.fr - cdn.bitmedianetwork.com - ec.ccm2.net Nombre de archivo: - bsplayer266.1075.exe - FLV_Runner.exe - InstallConverter_brch.exe - WiseConvert.exe - WiseConvert_1.5.exe - InstallConverter_brff.exe - Pconverter.exe - RadioG.exe - FileConverter_1.1.exe Se comunica con los siguientes dominios: - sp-download.spccint.com - orbtr-installer.databssint.com - spms-download.spccint.com - c-sp-storage.spccint.com - spms-storage.spccint.com Registro asociadas asociados con Win32/Conduit.SearchProtect.H.

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run""= "%AppData%\.exe" HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run""= "%AppData%\.exe" HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Associations "LowRiskFileTypes"="random"

Elaboración propia basada en información brindada por el CVE 0663 del año 2011. Fuente: https://www.cvedetails.com. Del mismo modo, contiene datos aportados por Microsoft (2015) PUA: Win32/Conduit. Fuente: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=PUA:Win32/Conduit. Finalmente, expone alguna información brindada por Eliminar Pc virus (2017) Fuente: http://www.eliminarelpcvirus.com/guia-para-desinstalar-el-malware-win32conduit-searchprotect-h/.

6.13. Ransomware

En principio un Ransomware es un malware que obstaculiza el acceso a la información almacenada en uno de los recursos del computador a los usuarios que quieren consultarla o modificarla, este bloqueo se genera mediante un bloqueo de encriptación, el cual no es posible desbloquearlo hasta que se pague al ciberdelincuente. Este es una nueva metodología que utilizan los ciberdelincuentes para obtener ganancia y aprovecharse de la necesidad de los usuarios en recuperar y acceder a la información que contenía en el computador.

La razón por la cual este tipo de malware ha obtenido gran auge es porque utiliza gran cantidad de métodos de encriptación y por lo cual la solución no es genérica. El Ransomware se clasifica en dos tipos principales: Locker Ransomware y Crypto Ransomware.

Retomando el Crypto Ransomware, según Mateiu, Monica. (2018). Se origina desde el siglo XX donde un troyano llamado "SIDA" cifraba archivos de la víctima. Después de este virus los criptógrafos Adam L Young y Moti M Yung remediaron esta deficiencia a través de algoritmos conocidos como clave pública.

El Locker Ransomware se reconoce porque bloquea la interfaz de la computadora con el usuario, donde visualiza una imagen solicitando el pago para el rescate para que el usuario pueda acceder nuevamente a la computadora. En algunos casos se disfrazan de autoridades policiales reclamando el pago de multas a los usuarios.

De acuerdo con Gazet, A. (2010) surgió Ransomware como Krotten, Archiveus,y GPCoder en el 2005, con múltiples variantes. Esta técnica combinada con la ingeniería social facilita el mercado a los ciberdelincuentes.

El Ransomware no criptográfico es una técnica de JavaScript que puede tomar control de un navegador con la potestad de pedir rescate y revertirse una vez se haya hecho el pago. En la actualidad esta estrategia ha surgido con el tipo de ataque de extorsión por denegación de servicio, es decir buscan a una víctima preferiblemente una entidad prestigiosa que carezca de una vulnerabilidad de denegación de servicio, la atacan, generando indisponibilidad de los servicios a la ciudadanía y haciendo imposible a los administradores de red poderla poner otra vez en funcionamiento, como algunas entidades la indisponibilidad del servicio puede acarrear sanciones financieras al estado, prefieren pagar al ciberdelincuente para que detenga el ataque de denegación de servicio y así poder poner nuevamente la disponibilidad de los servicios.

Habitualmente los Ransomware llega a través de los correos electrónicos de las víctimas que al momento de descargar archivos adjuntos ejecuta un script o un algoritmo de cifrado.

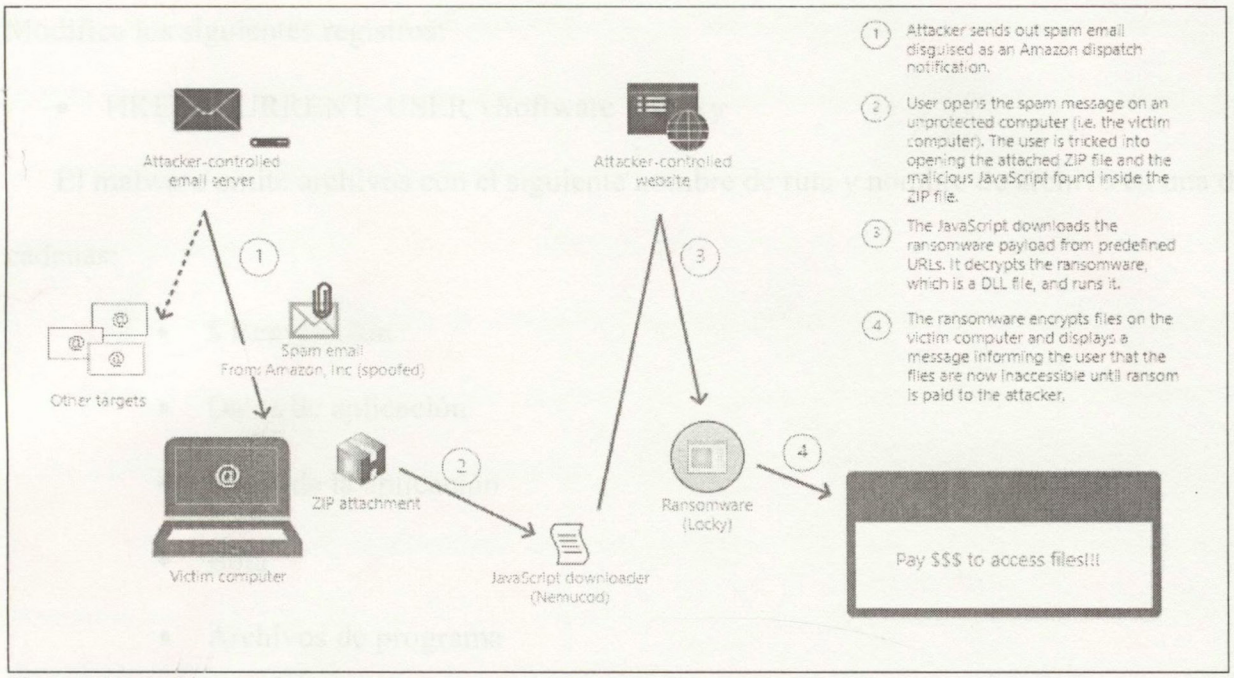


Figura 8. Modo de operar de ransomware.
Microsoft Technet (2016) Don't let this Black Friday/Cyber Monday spam deliver Locky ransomware to you. Fuente: https://cloudblogs.microsoft.com/microsoftsecure/2016/11/23/dont-let-this-black-friday-cyber-monday-spam-deliver-locky-ransomware-to-you/?source=mmpc.

Cuando se ejecuta el JavaScript se conecta a las siguientes URLs:

- hxxp: // livingnetwork .co.za / hfvg623? zvMNzYWImo = zvMNzYWImo
- hxxp: // ayurvedic .by / hfvg623? zvMNzYWImo = zvMNzYWImo
- hxxp: // marcelrahner .com / hfvg623? zvMNzYWImo = zvMNzYWImo
- hxxp: // copeigoan .net / hfvg623? zvMNzYWImo = zvMNzYWImo
- hxxp: // sheerfoldy .com / hfvg623? zvMNzYWImo = zvMNzYWImo

Esta amenaza puede crear archivos en el equipo que incluyen:

- _Locky_recover_instructions.txt
- _Locky_recover_instructions.bmp
- % temp% \ svchost.exe - locky ransomware
- [ID] [identificador] .locky (archivos cifrados)

Modifica los siguientes registros:

- HKEY_CURRENT_USER \ Software \ Locky

El malware omite archivos con el siguiente nombre de ruta y nombre de archivo en una de sus cadenas:

- $ Recycle.Bin
- Datos de aplicación
- Datos de la aplicación
- Bota
- Archivos de programa
- Archivos de programa (x86)
- Información del Volumen del Sistema
- temperatura
- thumbs.db
- tmp
- Windows
- winnt

Análisis de Donna Sibangan y Marianne Mallen (2016).

De acuerdo al análisis de Donna Sibangan se propone el diseño del indicador de compromiso para Ransomware, que al momento de identificar alguna conexión con las URLs o modificación en los archivos del sistema como se menciona anteriormente se dispare una alarma o una notificación a los administradores de los servidores, informándoles que se identifica un comportamiento anormal en un determinado equipo, de esta forma el administrador puede actuar tempranamente para que así mismo pueda ejecutar actividades preventivas y mitigar un posible

impacto de este tipo de ataque. Es de reconocer que este virus es de gran impacto para la Entidad, debido a que la presencia de este ocasiona pérdidas de información que puede ser sensible para la organización y así aumenta el nivel de riesgo por indisponibilidad del servicio o robo de la información de la Entidad.

Sin embargo, este diseño de indicador de compromiso debe ser continuamente analizado y actualizado, como se investigó, las técnicas de criptografía que utilizan continuamente los ciberdelincuentes son cada vez más amplias y variantes.

Para finalizar se desarrollará un caso de estudio de una entidad con indicadores de compromiso.

- **Caso de estudio**

Base del diseño de indicadores, es entender los medios y recursos que utilizan los atacantes. De la misma manera orientan a los administradores de la red hacia donde enfocar sus controles y a quien o a que hacer seguimiento. A continuación, se describe las etapas que se deben tener presente en un incidente de seguridad atendido con IoC.

Etapa uno: Condiciones de seguridad para la prevención y protección contra daños físicos a la red y sus componentes. Protección misma de la información como la Data, los registros, los archivos. Contra perdida, sustracción, alteración, incendios, sobre carga, no disponible. Todo lo que normalmente denominamos hardware debe ser supervisado y controlado físicamente, su acceso, su conexión, sus condiciones de funcionamiento.

Etapa dos: Protección y dispositivos de seguridad en la red y sus componentes. Los dispositivos, el hardware deben ser asegurados físicamente mediante dispositivos y mediante software.

Etapa tres: Condiciones especiales de seguridad para hardware y software crítico. Ejemplo inventado, en una red existen 3 servidores, uno de archivos, otro de aplicaciones y un tercero que se encarga de la impresión, además existen otros 500 dispositivos entre servidores, computadores, portátiles, tabletas, etc. Se deberán contemplar condiciones especiales de seguimiento a los malware de los servidores; en nuestro caso de indicadores de compromiso para la detección temprana de incidentes de seguridad en la Red del Ministerio de Relaciones Exteriores.

Etapa cuatro: Seguridad e Higiene. Eso dice la Norma Industrial, sin perder el contexto anterior, se debe mantener la salud, la limpieza de los datos, datos innecesarios, malware instalados, etc. Estas tareas de higiene y salud industrial igual deben entenderse como limpiar datos de basura y/o limpiar la información, priorizando aquellos dispositivos, activos de información o estructuras de datos que son críticos, están más expuestos o afectan más la prestación del servicio. De ahí la importancia de mantener la relación entre Mapa de Riesgos institucional y un diseño efectivo de indicadores para la seguridad de la red.

Etapa cinco: Protección de los usuarios y de acuerdo con su perfil. Los administradores de los servidores del ejemplo serán supervisados a través de los indicadores del malware dado que, por ser administradores, son los usuarios que se podrían ver más atacados.

Etapa seis: Señalización y avisos de seguridad. Idealmente, un sistema de indicadores tempranos de malware en la red estar en capacidad de enviar un mensaje, cada vez que sus indicadores de compromiso, previamente diseñados y programados se disparan por una alarma de peligro en la red.

Etapa siete: Kit, conjunto de herramientas de seguridad digital personal. Equivalente a un botiquín de primeros auxilios. Una opción especial de seguridad para los usuarios es dotar la red

de información y herramientas importantes, tipo indicadores de compromiso que alerten y permitan actuar frente a las acciones de los atacantes vía malware.

CONCLUSIONES

La investigación de un incidente de seguridad es de vital importancia, a partir de este se pueden orientar todos los esfuerzos de los administradores y así poder atender adecuadamente un incidente de seguridad en tiempos más cortos y con la seguridad que no va a repercutir en otros equipos de red o aun peor que estos incidentes se vuelvan recurrentes.

El principal objetivo de los indicadores de compromiso es identificar qué dispositivos y servicios se vieron afectados o comprometidos, así sea el mínimo cambio que se haya producido sobre un elemento de red, a partir de este se puede empezar a realizar un análisis exhaustivo para obtener cual o cuales fueron los cambios que se realizaron o fueron comprometidos al servicio.

El correcto análisis de los malwares, sus consecuencias como comportamiento, permite un apropiado diseño de indicadores de compromiso para la red de una entidad, a partir de estos se pueden prevenir futuros incidentes de seguridad de la información, como indisponibilidad del servicio, confidencialidad e integridad de la información y no repudio

Los ejemplos mencionados deben tomarse en cuenta para entidades públicas y privadas, las cuales deben invertir más en la protección de sus datos y en la capacitación de sus empleados para prevenir consecuencias desastrosas en el manejo de la información. La primera acción preventiva que se debe ejecutar es la "Sensibilización a todos los niveles" es decir, tanto las instituciones y empresas, todos en general reciban formación en Ciberseguridad, de tal forma que se tome conciencia respecto a la problemática que se presenta, y se instruya protocolos a seguir para no exponerse a incidentes de seguridad o para saber cómo manejarlos.

Los IoC son un buen complemento en los sistemas de información porque ayuda a contrarrestar los ciberataques y a vigilar de manera permanente y estricta los cambios que pueda presentarse en un activo. Sin embargo, puede presentarse muchos falsos positivos y ser algo tedioso la revisión continua de estos eventos, una de las recomendaciones para la aplicación de los IoC es tener un especialista dedicado a esta herramienta y que conozca e investigue el comportamiento de los malware y tenga pleno conocimiento de los sistemas de información e infraestructura tecnológica de la organización.

Para que las entidades nacionales de la defensa nacional puedan fortalecer y generar una autonomía cibernética conducente a identificar, detectar y atender posibles amenazas en contra de su infraestructura tecnológica, se recomienda implementar indicadores de compromiso.

Referencias Bibliográficas

Acosta, D. (2015) *El papel de los indicadores de compromiso (indicators of compromise – ioc) en la respuesta a incidentes de seguridad y la investigación forense*. Recuperado de: http://blog.isecauditors.com/2015/09/papel-de-los-ioc-en-respuesta-incidentes-seguridad-investigacion-forense.html

Blasco, J (2013) *AlienvaultLabs*. Recuperado de: https://github.com/jaimeblasco/AlienvaultLabs/blob/master/malware_analysis/RedOctober/48290d24-834c-4097-abc5-4f22d3bd8f3c.ioc.

Candau, J. (2011). *Estrategias nacionales de Ciberseguridad: Ciberterrorismo*. Ministerio de Defensa: Instituto Español de Estudios Estratégico. Recuperado de: https://es.scribd.com/document/338680779/Dialnet-LineasDeAccionDeLaEstrategiaNacionalDeCibersegurid-3837589-pdf.

Centro Criptológico Nacional (2015) *Ciberamenazas2014-Tendencias-2015*. Recuperado de: https://www.ccn-cert.cni.es/publico/dmpublidocuments/IE-Ciberamenazas2014-Tendencias-2015.pdf.

CISCO (2016) Informe anual de seguridad. Recuperado de: http://www.cisco.com/c/dam/m/es_es/internet-of-everything-ioe/iac/assets/pdfs/security/cisco_2016_asr_011116_es-es.pdf.

CISCO (2017) Multiple Vulnerabilities in Apache Struts 2 Affecting Cisco Products: September 2017. Recuperado de: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170907-struts2.

Common Vulnerabilities and Exposures (CVE) (1999-2018). *CVE Details. The ultimate security data source*. Recuperado de: https://www.cvedetails.com/index.php.

Conexión Inversa. (2013). Indicadores de compromiso ante una intrusión (IoCs), Redline, Mandiant y APT1. Recuperado de: http://conexioninversa.blogspot.com.co/2013/03/indicadores-de-compromiso-ante-una.html

Decreto N° 1377. Secretaría Jurídica Distrital de la Alcaldía Mayor de Bogotá, Colombia. 27 de junio de 2013. Recuperado de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646.

Decreto N° 1078. Secretaría Jurídica Distrital de la Alcaldía Mayor de Bogotá, Colombia. 26 de mayo de 2015. Recuperado de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=62513.

Del Moral, L (2014). *Curso de Ciberseguridad y Hacking Ético*. Recuperado de: https://books.google.com.co/books?id=sua0BAAAQBAJ&pg=PA16&dq=CIBERATAQUES&hl=en&sa=X&ved=0ahUKEwiWweXD_q7UAhUCRiYKHR24DgMQ6AEIKTAA#v=onepage&q=CIBERATAQUES&f=false.

Del Rivero, M (2015). Smart Cities, una visión para el ciudadano, LID Barcelona. Recuperado de: https://books.google.com.co/books?id=h-33DQAAQBAJ&pg=PT87&dq=CIBERATAQUES+RANSOMWARE&hl=en&sa=X&ved=0ahUKEwiB1ayEgK_UAhUBdSYKHUgjAZcQ6AEIjAA#v=onepage&q=CIBERATAQUES%20RANSOMWARE&f=false

El Espectador (2014). El robo del siglo que no alcanzó a ser. Recuperado de: https://www.elespectador.com/noticias/judicial/el-robo-del-siglo-no-alcanzo-ser-articulo-533907

Real Academia Española (2017) Diccionario virtual de la RAE. Recuperado de: http://dle.rae.es/?id=98Wdd57.

Ganuza, N. La situación de la ciberseguridad en el ámbito Internacional y en la OTAN. Recuperado de: Dialnet-SituacionDeLaCiberseguridadEnElAmbitoInternacional-3837337.pdf

Guía para desinstalar el malware win 32/ conduit.SearchProtect. H (2017) Recuperado de: http://www.eliminarelpcvirus.com/guia-para-desinstalar-el-malware-win32conduit-searchprotect-h/.

Gutiérrez, L (2014) Curso de Ciberseguridad y Hacking Ético 2013. Ed: Punto Rojo Libros. Recuperado de: https://books.google.com.co/books?id=sua0BAAAQBAJ&pg=PA67&lpg=PA67&dq=hacking+etico+%2B+borrado+de+huellas+%2B+ataque+puro&source=bl&ots=XDdtX8MVGI&sig=_VYL9LjASyctyHa8aE3hZOUf3M0&hl=es&sa=X&ved=0ahUKEwjowo2O7IHbAhXix1kKHRDbBo8Q6AEIXTAJ#v=onepage&q=hacking%20etico%20%2B%20borrado%20de%20huellas%20%2B%20ataque%20puro&f=false

Ichasco (2015) Ossim: Instalación y configuración. Recuperado de: https://blog.ichasco.com/ossim/.

INFOSERTEC (2017) Reporte Anual de Ciberseguridad de Cisco 2017. Recuperado de: https://infosertec.com.ar/2017/02/02/seguridad-reporte-anual-de-ciberseguridad-cisco-2017/

International Organization for Standarization (2012) ISO/IEC 27032:2012. Information technology -- Security techniques -- Guidelines for cybersecurity. Recuperado de: https://www.iso.org/standard/44375.html.

Ley N°527. Secretaría Jurídica Distrital de la Alcaldía Mayor de Bogotá, Colombia. 18 de agosto de 1999. Recuperado de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276.

Ley N° 1266. Corte Constitucional de Colombia. 31 de diciembre de 2008. Recuperado de: https://www.uiaf.gov.co//recursos_user///2014/OAJ/Ley%20Estatutaria%201266%20de%202008%20Habeas%20Data.pdf.

Ley N° 1273. Secretaría Jurídica Distrital de la Alcaldía Mayor de Bogotá, Colombia. 05 de enero de 2009. Recuperado de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492.

Ley N° 1581. Secretaría Jurídica Distrital de la Alcaldía Mayor de Bogotá, Colombia. 17 de octubre de 2012. Recuperado de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981.

Ley N° 1712. Secretaría Jurídica Distrital de la Alcaldía Mayor de Bogotá, Colombia. 06 de marzo de 2014. Recuperado de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882.

Libreta de apuntes. (2017). Reporte anual de Ciberseguridad CISCO 2017. San José CA. Recuperado de: http://libretadeapuntes.com/2017/01/reporte-anual-de-ciberseguridad-cisco-2017/

Lyns, W. (2010) *Foreign Affairs*, vol. 89, nº 5, septiembre/octubre de 2010, pp. 97.

Mendoza, M.A (16 de junio del 2015) ¿Ciberseguridad o seguridad de la información? Aclarando la diferencia. We live Security. Buenos Aires, Argentina. Recuperado de: https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia/.

Méndez, A. (2015). *Guía de seguridad (CCN-STIC-423) indicadores de compromiso (IoC).* España: Centro Criptológico Nacional. Recuperado de: https://www.ccn-

cert.cni.es/en/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1090-ccn-stic-423-indicadores-de-compromiso.html.

Microsoft (2016) Don't let this Black Friday/Cyber Monday spam deliver Locky ransomware to you Recuperado de: https://cloudblogs.microsoft.com/microsoftsecure/2016/11/23/dont-let-this-black-friday-cyber-monday-spam-deliver-locky-ransomware-to-you/?source=mmpc.

Microsoft (2015) PUA:Win32/Softonic. Recuperado de: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=PUA:Win32/Softonic.

Microsoft (2015) PUA:Win32/CandyOpen. Recuperado de: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?name=PUA%3aWin32%2fCandyOpen.

Microsoft (2015) PUA:Win32/InstallCore. Recuperado de: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?name=PUA%3aWin32%2fInstallCore.

Microsoft (2016) PUA:Win32/AskToolbar. Recuperado de: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?name=PUA%3aWin32%2fAskToolbar.

Microsoft (2016) PUA:Win32/Conduit. Recuperado de: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=PUA:Win32/Conduit.

Microsoft (2017). TrojanDownloader:VBS/Schopets. Recuperado de: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=TrojanDownloader:VBS/Schopets.

Ministerio de Defensa (2010). *Ciberseguridad, retos y amenazas a la Seguridad Nacional en el Ciberespacio*. Cuadernos DE Estrategia Instituto Español de Estudios Estratégicos Instituto Universitario «General Gutiérrez Mellado». Recuperado de: http://www.seaceptanideas.com/biblio/Cuaderno_IEEE_149_Ciberseguridad.pdf.

Ministerio de Relaciones Exteriores (2016) Mapa de Procesos del Ministerio de Relaciones Exteriores y su fondo rotatorio. Recuperado de: https://sigc.cancilleria.gov.co/portal/index.php?idcategoria=8

Ministerio de Relaciones Exteriores (2017) Caracterización del proceso. Recuperado de: https://sigc.cancilleria.gov.co/archivos/SC-PR-08/SC-PR-08%20Serrvicio_al%20Ciudadaadno_V8.pdf

Ministerio de Relaciones Exteriores (2017) Dirección de gestión de información y tecnología. Plataforma del IPS de la Cancillería.

Ministerio de Relaciones Exteriores (2016) Consola de administración del antivirus System Center de la Cancillería.

Ministerio de Relaciones Exteriores (2018) Consola de administración del antispam de la Cancillería.

Moreno, M (2013) Recolección distribuida de los IoCs. Valencia, España. Recuperado de: https://www.securityartwork.es/2013/11/19/recoleccion-distribuida-de-iocs/.

Oliveira, J. (15 de mayo de 2017). El Ataque de 'Ransomware' se extiende a Escala Global. *El País*. Recuperado de: http://tecnologia.elpais.com/tecnologia/2017/05/12/actualidad/1494586960_025438.html

Ramírez, O (2017) *VBS_LOCKY.TH918.* Recuperado de: https://www.trendmicro.com/vinfo/us/threatencyclopedia/malware/VBS_LOCKY.TH918 .

Revista Semana (03 de abril del 2016). Colombia perdió un billón de pesos por ataques cibernéticos. Recuperado de: http://www.semana.com/tecnologia/articulo/colombia-perdio-un-billon-de-pesos-por-ataques-ciberneticos/463949.

Romano, O y Barros, R (2016). Reporte Anual de Seguridad de Cisco- Desafíos que enfrentan las empresas por los rápidos avances de los atacantes. Recuperado de: http://la5pata.com/2016/01/20/reporte-anual-de-seguridad-de-cisco-desafios-que-enfrentan-las-empresas-por-los-rapidos-avances-de-los-atacantes/.

Schmitt, M (2013). *Tallinn Manual on the international law applicable for cyber warfare*. Recuperado de: https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf.

Soesanto, S. (1 de octubre de 2016). No todos los ataques son ciberataques. El País. Recuperado de: http://tecnologia.elpais.com/tecnologia/2016/09/28/actualidad/1475059265_198963.html.

Tecnósfera. (13 de mayo de 2017). Colombia también es víctima del Ataque Global Informático. *El Tiempo*. Recuperado de: http://www.eltiempo.com/tecnosfera/novedades-tecnologia/ataque-cibernetico-afecta-redes-de-74-paises-87390.

Unión Internacional de Telecomunicaciónes. (2008). UIT-T X.1205: Aspectos generales de la ciberseguridad. Recuperado de:

https://www.itu.int/rec/T-REC-X.1205-200804-I/es.

Valle, M (2015). Los 8 mayores ciberataques de los últimos años. Globb Security. Madrid, España. Recuperado de: http://globbsecurity.com/mayoriberataques-ultimos-anos-35861/

Zubieta, J. (2015) *Ciberdiccionario: Conceptos de Ciberseguridad en lenguaje entendible*. Recuperado de: https://books.google.com.co/books?id=nckJBwAAQBAJ&printsec=frontcover&dq=ciberseguridad&hl=en&sa=X&ved=0ahUKEwiq44r7_K7UAhURySYKHZDwCMoQ6AEIJTAA#v=onepage&q=ciberseguridad&f=false.

SIGLAS

APT	Amenaza persistente avanzada
CVE	Common Vulnerabilities and Exposures
HIDS	Sistema de detección de intrusos basado en host
IDS	Sistema de detección de intrusos
IoC	Indicadores de Compromiso
IPS	Sistema de prevención de intrusos
MAC	Media Access Control
PUA	Aplicación común y potencialmente no deseada
SNMP	Protocolo Simple de Administración de Red
TIC	Tecnologías de la información y las telecomunicaciones
UAC	Control de acceso de usuario
UIT	Unión Internacional de Telecomunicaciones