FUNDACION UNIVERSITARIA LOS LIBERTADORES

El papel de la CIA (Ciberinteligencia de Amenazas) dentro de las ciberamenazas que afectan las PYME´s.

Cesar Mauricio Salamanca

Giovanny Andrés Aguilar Restrepo

Juan David Cornejo Pinzón

Proyecto de Investigación presentado como requisito para optar el título de Especialista de Seguridad de la Información

Facultad de Ingeniería y Ciencias Básicas

20 de noviembre de 2021

EL PAPEL DE LA INTELIGENCIA DE AMENAZAS DENTRO DE LAS CIBERAMENAZAS QUE AFECTAN A LAS PYME

PROBLEMÁTICA

Actualmente las organizaciones se encuentran en un constante cambio tecnológico que se vio incrementado con los acontecimientos vistos por la pandemia, lo cual ha hecho que se implementen programas de conectividad para trabajo remoto sin tener en cuenta muchas veces las brechas de seguridad que se pueden abrir. Debido a esta necesidad de hiper conectividad las organizaciones han tenido que buscar formas de protegerse de nuevos tipos de ataques los cuales se han incrementado al tener nuevos vectores que antes no se habían contemplado.

Es por esto que se hace importante identificar, analizar y crear maneras de protegerse de las ciber amenazas de última generación, las cuales ante más temprano sea su detección permitirá una mejor respuesta ante cualquier incidente.

De acuerdo a la información suministrada por la compañía [1]Acronis se registraron más de 400.000 nuevas muestras de malware por día durante el 2020.

Algunas otras cifras compartidas por el fabricante Kaspersky en su [2]boletín de seguridad del año 2020 indica incrementos en los ataques web de tipo malware para los usuarios de equipo final, URL maliciosas, ataque de cifradores y cripto monederos.

[1] Acronis, (2020), 2021 en revisión: las últimas amenazas cibernéticas que surgieron y cómo mantenerse protegido, Fuente: https://www.acronis.com/es-es/articles/latest-cyber-threats-2020/

[2] Kaspersky, (2020), Boletín de seguridad Kaspersky 2020. Estadísticas, Fuente: https://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2020_sp.pdf

INTRODUCCION

Cuando una organización conoce las amenazas y los riesgos estos pueden ser gestionados oportunamente, pero en la actualidad las compañías desafortunadamente siguen actuando de manera reactiva y su actuación ante un incidente es descoordinada, en parte porque no conocen la problemática o no han definido de manera adecuada los roles a seguir en la cadena de responsabilidad organizacional establecida.

El fraude BEC, los ataques de ransomware, las oleadas de malware, las ciberextorsiones entre otras amenazas vienen afectando la cadena productiva de las empresas, y por ello es importante conocer las tipologías y modalidades que utiliza el cibercrimen en Colombia.

Es claro que para enfrentar una amenaza es importante conocer cómo actúa y que puntos débiles internos de la organización aprovecha. Identificar las vulnerabilidades oportunamente permite entonces corregir los fallos en la seguridad e infraestructura e implementar planes de mejoramiento que abarquen desde los recursos tecnológicos, humanos y del proceso mismo afectado en el incidente presentado.

Teniendo en cuenta lo anterior se hace necesario tener una metodología clara y precisa que posibilite abarcar todos los temas de ciberseguridad a los que puede enfrentar una PYME y que le permita actuar de forma práctica y oportuna, para lograr esto pretendemos mostrar como el uso de la inteligencia de amenazas puede cubrir estas necesidades.

OBJETIVO GENERAL

Explicar y Analizar de manera metodológica la Inteligencia de amenazas y sus beneficios en las organizaciones.

OBJETIVOS ESPECIFICOS

- Identificar las amenazas de forma temprana, descubrir tácticas, técnicas y procedimientos para posibles ataques (TTP) por medio de la inteligencia de amenazas.

- Dar a conocer los diferentes recursos como son tipos de formatos, fuentes de consulta para la metodología Inteligencia de Amenazas

- Identificar y analizar el top 3 de ciberamenazas de mayor impacto que se han identificado por la industria de seguridad.

1. ACERCA DE LA INTELIGENCIA DE AMENAZAS

1.1 ¿Qué es Inteligencia de Amenazas?

El término inteligencia de amenazas, también conocido como Threat Intel, CiberInteligencia de amenazas o CIT; es la recopilación, filtración y análisis de la información sobre las amenazas o incidentes que pueden afectar una organización. Por medio de la recopilación de información de fuentes externas (públicas y privadas) e internas (logs, alertas de SIEM, etc.), se puede lograr tener una mejor perspectiva de las amenazas a las que se enfrenta una organización y que con esta información permita tener una toma de decisiones más efectiva.

La información que se obtiene puede ser de fuentes abiertas y publicas que no se encuentran estructuradas, esta puede ser de blogs, redes sociales, foros o publicaciones.

Además, también se obtiene información de fuentes cerradas y de forma estructurada que se pueden obtener de fabricantes que comparten Indicadores de compromiso (IoC), xml, STIX, OpenIoC.

1.2 La Importancia de la Inteligencia de Amenazas

Desde hace años, las organizaciones están expuestas a una gran variedad de amenazas, recibiendo en ocasiones numerosos intentos de ataque. Por otro lado, las motivaciones de los atacantes se van ampliando y las técnicas que emplean evolucionan de manera muy rápida, superando las defensas de seguridad tradicionales y los enfoques operativos, ya que aún existe un gran número de empresas que siguen medidas reactivas en lugar de proactivas.

La Inteligencia de amenazas permite a las organizaciones estar al día de los ataques que están ocurriendo en diferentes contextos, aumentando el conocimiento sobre la situación y permitiendo una detección más rápida en caso de un incidente.

1.3 Tipos De Inteligencia De Amenazas

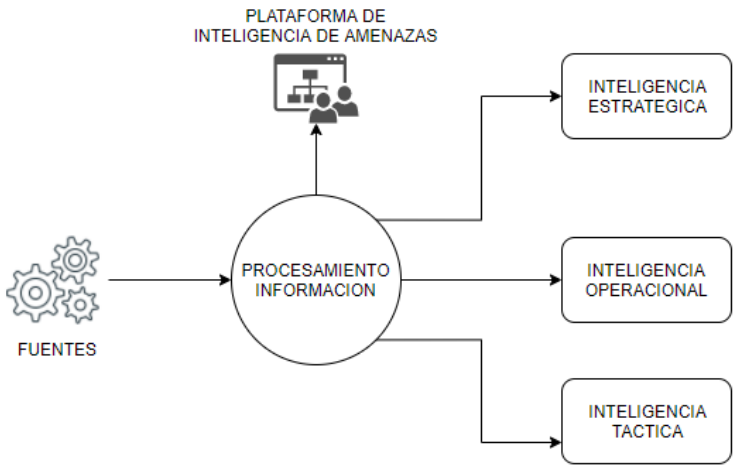


Gráfico 1. Principales vectores de engaño BEC

1.3.1 Inteligencia de Amenazas Estratégica

Se centra en un análisis de alto nivel para personal no técnico, busca comprender y considerar las tendencias de las amenazas. Ayuda a definir la postura de ciberseguridad de una organización y con esto permite tener una visión más clara a la hora la toma de decisiones empresariales. Este tipo de información suele ser útil para altos ejecutivos y directivos de una organización, así como el director de TI y el CISO.

1.3.2 Inteligencia de Amenazas Operacional

Analiza en detalle las tácticas, técnicas y procedimientos (TTP) utilizadas por los atacantes: su motivación, quien, como y cuando ejecuto el ataque, su línea de tiempo, etc. Este tipo de información es útil con mayor frecuencia para los forenses de seguridad informática y el personal de respuesta a incidentes.

1.3.3 Inteligencia de Amenazas Táctica

Este tipo de inteligencia de amenazas se centra en la información que se obtiene de la automatización de herramientas especializadas las cuales correlacionan los eventos que se desarrollan por medio de comportamientos, estos comportamientos se generan en los artefactos que hacen parte de un sistema de información, brinda información sobre indicadores de compromiso, IP de comando y control, ataques persistentes, etc.

1.4 Fases de la Inteligencia de Amenazas

- **Planificación y dirección (Direction):** Establecer las metas para la estrategia de Inteligencia de amenazas de la organización. Por ejemplo, qué activos de información, sistemas o procesos de negocio hay que proteger. Impacto, prioridades, etc.
- **Recolección (Collection):** Recolección de amenazas usando fuentes externas e internas.
- **Procesamiento (Processing):** Transformación de la información recogida en información que pueda ser usada dentro de la organización.
- **Análisis (Analysis):** Revisión de la información obtenida de la fase de procesamiento con el fin de generar valor a esta información y convertirla en inteligencia para la toma de decisiones.
- **Difusión (Dissemination):** Es la forma y el medio como se comparte el análisis de la información obtenida con las personas al interior de la organización para las cuales esta información les genera valor.
- **Retroalimentación (Feedback):** Es imprescindible un feedback constante para ser capaces de adaptar el proceso de Inteligencia de amenazas a los requisitos de los distintos grupos a los que afecta.

Gráfico 2. Principales vectores de engaño BEC

2. RECURSOS PARA INTELIGENCIA DE AMENAZAS

Actualmente existen muchos medios por los cuales se puede automatizar la inteligencia de amenazas, esto ayuda a que el tiempo que se emplea en hacer inteligencia de amenazas sea más eficiente al no tener que disponer de una gran cantidad de tiempo para la recolección y procesamiento de la información, información que es útil en la fase de análisis.

A continuación, se expondrán algunas de las herramientas usadas en la industria de la ciberinteligencia que permite llevar a cabo esta actividad de forma automatizada.

2.1 Fuentes de Consulta

Las plataformas de inteligencia de amenazas realizan una recopilación de datos de manera automática, estos datos provienen de diversas fuentes y con diferentes formatos. Para realizar inteligencia de Amenazas, la recopilación de la información de varias fuentes es un factor fundamental. Existen variedad de fuentes y tipos de formatos los cuales son admitidos y que se encuentran estandarizados para que se puedan compartir de manera más eficaz con la comunidad.

Las categorías para realizar inteligencia de amenazas más conocidas son:

- Fuentes de Código Abierto: Este tipo de información está disponible abiertamente. Se basa en encontrar información a través de los medios de comunicación, foros de ciberseguridad, comunidades, redes sociales, blogs, etc. La información obtenida se puede extraer para obtener inteligencia y se puede realizar análisis de monitoreo de marca y permite identificar problemas de o ataques denominados ocupación de dominios.

- **Consultas Deep Web y Dark Web:** Esta fuente de información no se encuentra disponible en los buscadores que comúnmente utilizamos, por esto en esta categoría el proveedor de servicios para la inteligencia de amenazas cuenta con el conocimiento para poder acceder y para analizar lo que sucede en foros, blog, chats, grupos de piratas informáticos que se encuentra en la Deep web y la Dark web.

  En estas plataformas de intercambio de archivos, brindan la información y permiten identificar nuevos vectores de amenazas, activos robados, nuevas herramientas y técnicas utilizadas por los atacantes.

- Inteligencia de Amenazas Internas: Cuando se tiene un proveedor de servicios para la Inteligencia de amenazas de manera gestionada, la organización se beneficia de la información que se suministran a otros clientes. Cuanta más información pueda obtener el proveedor de otros clientes, los algoritmos internos de su plataforma y su equipo de trabajo aprenderán más acerca del panorama de amenazas, permitiendo

esto que llegue más información a la organización, que sea más actualizada y mucho más útil.

- Compartir Indicadores de Compromiso (IoC): Esta información se obtiene y se utiliza para descubrir actividades en nuestro sistema y archivos que indiquen acerca de alguna actividad maliciosa. Los IOC se obtiene de manera abierta, y permite prevenir futuros ataques puesto que es más fácil identificar problemas como, por ejemplo: comportamiento inusual en el tráfico de la red, modificación de privilegios de usuario, modificación de archivos del sistema, direcciones IP sospechosas, intentos de inicio de sesión, entre otras.

2.2 Plataformas de Inteligencia de Amenazas

Actualmente existen diferentes plataformas y herramientas que permiten realizar la fase de recolección y procesamiento de la inteligencia de amenazas.

La automatización mediante el uso de plataformas de inteligencia de amenazas (de sus siglas en inglés Threat Intelligent Platform –TIP) consolida, correlaciona y clasifica la información de forma estructurada con el fin de entregar a los equipos de seguridad información fácilmente consumible.

En el siguiente cuadro logramos identificar diferentes plataformas, las cuales se pueden encontrar bajo diferentes modelos de licenciamiento, este listado se logró obtener luego de realizar una consulta en varias fuentes de internet.

Es importante resaltar que la evaluación del uso de una plataforma de inteligencia de amenazas debe ir acorde con el modelo de maduración de cada entorno empresarial, con el fin de no llegar a incurrir en gastos innecesarios.

NOMBRE	FABRICANTE	DESCRIPCION	FASE CTI	ENLACE
Alienvault Open Threat Exchange (OTX)	AT&T	Proporciona acceso a una comunidad de seguridad donde puede contribuir, discutir, investigar, validar y compartir datos de amenazas.	Fase Recolección Fase Difusión	https://otx.alienvault.com/
Mandiant Advantage	Fireeye (Mandiant)	Plataforma SaaS (Software como servicio) que permite a las organizaciones acceder a información actualizada y relevante sobre las ciberamenazas. Tienen una red de colaboradores a nivel mundial que alimentan las bases de conocimiento de la plataforma.	Fase Recolección Fase Procesamiento Fase Análisis	https://www.mandiant.com/advantage/threat-intelligence

Recorded Future	Recorded Future	Es un producto SaaS que unifica automáticamente la inteligencia de amenazas de fuentes abiertas / cerradas y técnicas en una sola solución. Su tecnología utiliza el procesamiento del lenguaje natural (NLP) y el aprendizaje automático para entregar esa inteligencia de amenazas en tiempo real.	Fase Recolección Fase Procesamiento Fase Análisis	https://www.recordedfuture.com/solutions/threat-intelligence/
Splunk	Splunk	La plataforma de inteligencia de amenazas de Splunk se centra en la inteligencia procesable desarrollada a través del aprendizaje automático. A través de su inteligencia, puede desarrollar líneas de base para sus datos y detectar desviaciones de comportamientos pasados o determinar anormalidades. Splunk también proporciona análisis predictivo a través de una mayor visibilidad de las transacciones comerciales, la entrada de IoT y las operaciones de seguridad.	Fase Recolección Fase Procesamiento Fase Análisis	https://www.splunk.com/
Exabeam	Exabeam	Su servicio de inteligencia sobre amenazas Exabeam puede recopilar pruebas como direcciones IP sospechosas, direcciones IP en la lista negra, URLs de phishing conocidas, etc. Con esta información, Exabeam permite a los analistas aprovechar la inteligencia en sus productos. Por lo tanto, pueden automatizar las guías de investigación y activar las alertas sin el ruido habitual de las soluciones SIEM.	Fase Recolección Fase Procesamiento Fase Análisis	https://www.exabeam.com/product/threat-intelligence/
MISP	Open Source	La plataforma de intercambio de información de malware (MISP) es una solución de software de código abierto para recopilar, almacenar, distribuir y compartir indicadores de seguridad cibernética y análisis de malware.	Fase Recolección Fase Difusión	https://www.misp-project.org/

OpenCTI	Open Source	Es una plataforma que permite a las organizaciones gestionar sus conocimientos y observables sobre ciberamenazas. Ha sido creada para estructurar, almacenar, organizar y visualizar información técnica y no técnica sobre ciberamenazas.	Fase Recolección Fase Procesamiento Fase Análisis	https://github.com/OpenCTI-Platform/opencti
AIEngine (Artificial Intelligent Engine)	Open Source	AIEngine es un motor de sistema de detección de intrusión de red interactivo/programable Python/Ruby/Java/Lua y Go de última generación con capacidades de aprendizaje sin intervención humana, clasificación de dominios DNS, detección de Spam, colector de red, análisis forense de red y muchos otros.	Fase Recolección Fase Análisis	https://bitbucket.org/camp0/aiengine/src/master/
Malstrom	Open Source	Es un repositorio de seguimiento de amenazas y artefactos forenses, almacena las reglas y notas YARA para la investigación.	Fase Recoleccion	https://github.com/opensourcesec/malstrom
Mantis	Open Source	Plataforma que está conformada por varias aplicaciones Django que, combinadas, soportan la gestión de la inteligencia sobre ciberamenazas expresada en estándares como STIX, CybOX, OpenIOC, IODEF (RFC 5070), etc.	Fase Procesamiento	https://django-mantis.readthedocs.io/en/latest/index.html
Megatron	Open Source	Es una herramienta implementada por CERT-Suecia (Computer Emergency Respond Team) que recoge y analiza los archivos de registro con máquinas maliciosas, por ejemplo, de Shadowserver. Aparte de la gestión de correo abusivo, Megatron puede utilizarse para recoger estadísticas, convertir archivos de registro y hacer análisis de archivos de registro durante la gestión de incidentes.	Fase Recolección Fase Análisis	https://github.com/cert-se/megatron-java

2.3 Formatos para Inteligencia de Amenazas

Existen diferentes tipos de formatos empleados y estandarizados para compartir Inteligencia de Amenazas en su gran mayoría se basan en Indicadores de Compromisos.

A continuación, indicaremos los tipos de formatos más utilizados.

- **STIX (Structured Threat Information Expression):** Permite compartir Inteligencia de Amenazas de forma Coherente lo que facilita a las comunidades de seguridad comprende que ataque tiene mayor probabilidad de anticipar y responder de manera más rápida y efectiva

- **TAXII (Trusted Automated Exchange of Intelligence Information:** Es un protocolo utilizado para intercambiar información de Inteligencia de amenazas por medio de la capa de aplicación sobre HTTPS siempre y cuando las organizaciones definan una API que se alinee con otros modelos comunes.

- **CybOX (Cyber Observable Expressión):** Implementa y proporciona una estructura para informar sobre eventos de seguridad, la información que se comparte por medio de formato JSON, indica la actividad de un puerto, la información de una IP, malware, detección de intrusiones, claves de registro, respuesta y manejo de incidentes, entre otras.

- **Otras Formatos disponibles:**

    - IODEF (Incident Description Exchange Format)
    - OpenIOC (Open Indicators of Compromise)
    - CIF (Collective Intelligence Framework)
    - OTX (Open Threat Exchange)

3 PRINCIPALES TIPOS CIBER AMENAZAS

La (CIA) ciberinteligencia de Amenazas permite identificar de manera clara y estructurada muchos de los tipos de nuevos ciberataques que surgen en los últimos años, gracias a la profundización de estudios sobre los distintos comportamientos, fuentes o vectores de ataques y modos de infección ejecutados por los malware, adicional permite obtener información de primera mano, que posibilita generar medidas preventivas y reactivas para los administradores de activos críticos, CISO, ingenieros de ciberseguridad que tengan bajo su responsabilidad y que necesiten aplicar nuevos controles dentro de sus organizaciones pequeñas o medianas. Según el top 3 de ciberamenazas se puede describir los siguientes tipos que más generan impacto dentro del nicho empresarial de la pyme y pequeña empresa:

3.1 Ataque BEC

En Colombia las pymes y las pequeñas organizaciones reciben alrededor del 90% de los ciberataques, éstas se deben a la ingeniería social.

Los cibercriminales utilizan diversos métodos para obtener información confidencial de las entidades, de sus directivos y los empleados, entonces una vez obtenida dicha información, procederán a suplantar las identidades, a falsificar los correos electrónicos y realizar transacciones bancarias de dinero hacia cuentas manejadas por éstos ciberdelincuentes, además con la información robada se podrían hacer salidas de insumos, remesas y mercancías engañando a clientes y terceros.

El blanco fundamental buscado por los ataques BEC, están dirigidos a la cadena de suministros. Las comunicaciones con terceros e inversionistas, requieren de contar con contextos seguros, que garanticen la integridad de la información utilizada en los distintos canales digitales o virtuales.

Los atacantes elaboran escenarios falsos pero convincentes, para engañar a empleados clave manipulando así a los ejecutivos, con el fin lograr su aval en acciones no autorizadas que permiten acrecentar el fraude o suplantación de sus clientes y proveedores mediante el robo directo de información confidencial, tomando como base la técnica de ingeniería social.

Los principales vectores de ataque más utilizados por los ciberdelincuentes son:

Gráfico 3. Principales vectores de engaño BEC

En Colombia, se pudo determinar que la cifra promedio de pérdidas por ciberataques, puede variar entre 300 millones y 5.000 millones de pesos, según el tamaño pyme impactada.

- **Estafa CEO (suplantación de gerente):**

Ésta inicia a través de un correo electrónico malicioso empleado por la técnica llamada (Phishing), los autores de éste, toman control de la cuenta de correo electrónico del director o gerente de la organización y de esta manera emiten comunicados y notificaciones falsas a los empleados encargados de ejecutar los pagos y transferencias.

Gráfico 4. Estafa de CEO – Suplantación de Gerente

- **Suplantación de clientes:**

Los atacantes engañan a clientes para hacer que éstos realicen pagos de sus facturas de servicios pendientes, logrando que el dinero arribe a las cuentas bancarias que ellos manejan.

Para poder extraer las ganancias, los criminales apertura cuentas bancarias con información y documentación robada de las pymes afectadas mediante la técnica llamada ingeniería social. Luego, diversifican el dinero, utilizando las mal llamadas mulas bancarias.

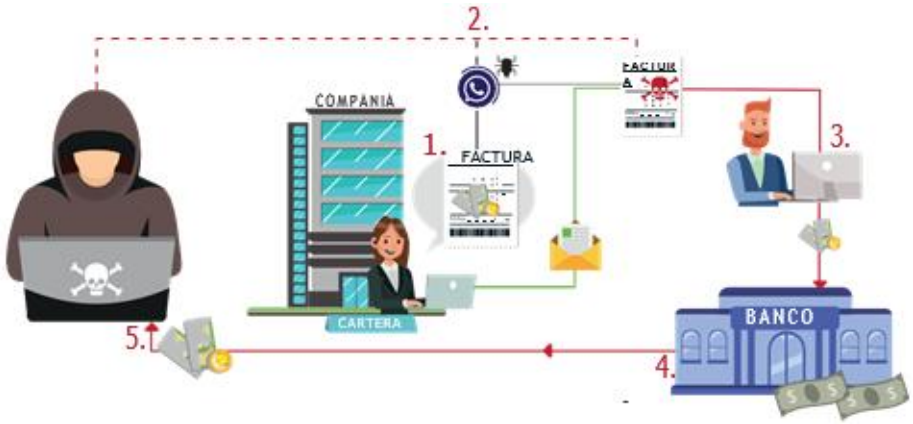


Gráfico 5. Suplantación de Clientes

3.2 Ransomware

Este tipo de ataque su nombre deriva de la combinación de las palabras Ransom o rescate en inglés y ware referente a Software, en ese orden de ideas quedaría como Ransomware: Software de Rescate. Esta técnica ha tenido un incremento en los últimos dos años en Colombia y está relacionada al alto uso de las Criptomonedas como medio para monetizar las ganancias obtenidas por los secuestros y extorsiones del Cibercrimen a nivel mundial.

Colombia estuvo bajo ataque de Ransomware alrededor de un 30% sobre el marco latinoamericano en el último año, seguido de Perú con un 16%, México con un 14%, Brasil con el 11% y A por último argentina con el 9%.

Las PYMES fueron el blanco predilecto por los ciber atacantes, pues ellos conocen muy bien que las inversiones en materia de seguridad de la información suelen ser pobres para este tipo de organizaciones pequeñas.

Esta modalidad de ataque hace que aquellas empresas encargadas en materia de seguridad de la información, y que brindan servicios de antimalware se incrementen en la oferta misma, además las hacen que las organizaciones gubernamentales redoblen sus esfuerzos de la lucha contra el cibercrimen, tales como EUROPOL e INTERPOL.

Sin embargo y a pesar de los tantos esfuerzos aplicados por algunas organizaciones encargadas de la búsqueda de las llaves de cifrado de la información secuestrada, tales como www.nomoreransom.org, no es posible recuperar la información cifrada, dado que muchos algoritmos de cifrado que son utilizados en las últimas versiones y derivados de los malware, aún no se tienen dispuestas en la Internet ni tampoco en la Dark Net de manera abierta; únicamente bajo modalidad de pago en moneda bitcoin.

Principales Vectores de ataque:

Gráfico 6. Principales vectores de ataque del ransomware

Los vectores más utilizados por los ciberdelincuentes, tienen que ver por lo general con el envío masivo de correos electrónicos, los cuales utilizan asuntos y mensajes llamativos que logran alcanzar un porcentaje tan elevado en el que permiten que las víctimas ejecuten clic sobre estos enlaces inmersos en estos correos electrónicos.

El correo electrónico es el principal medio de propagación del Ransomware de tipo Lockscreen, el cual se caracteriza por no permitir el acceso y el uso del equipo mediante una pantalla de bloqueo disparada desde el arranque del sistema operativo, dado que una vez se produzca el engañado sobre la víctima, esta es dirigida a un servidor para que se produzca la descarga del malware.

El proceso inicia una vez ejecutado el archivo infectado, la instrucción dada por el malware, cifra la información objetivo, evitando así la acción de por parte de diferentes sistemas de seguridad de seguridad tales como: antivirus, Sandbox o firewall, para solicitar una cuantía de dinero a cambio de quizás restablecerla.

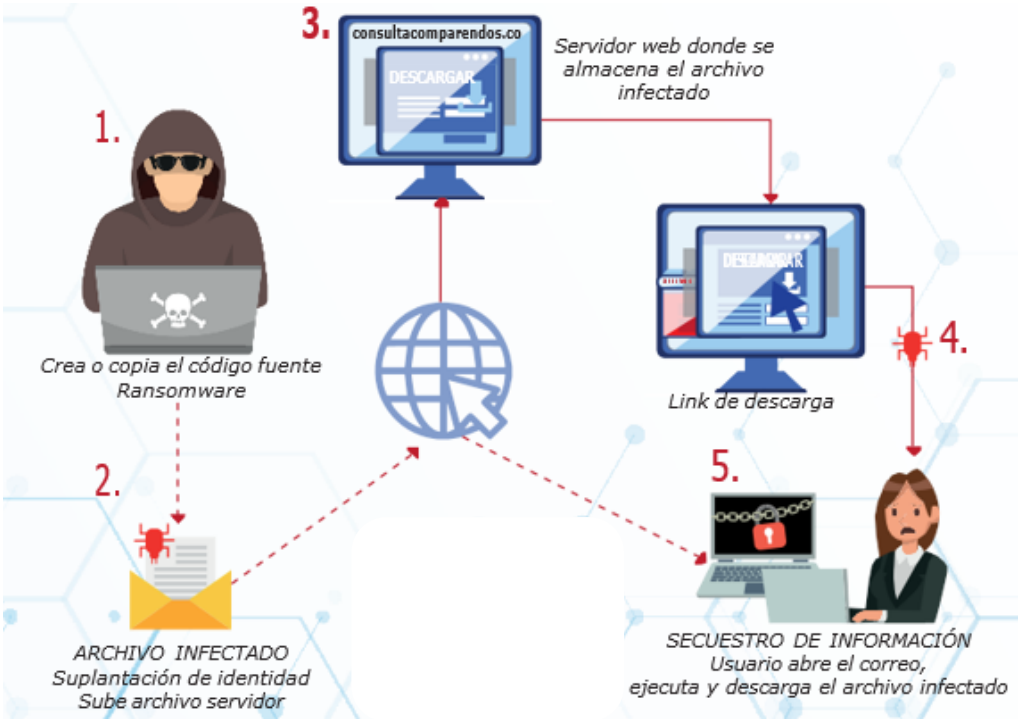


Gráfico 7. Proceso de infección de un ransomware de tipo LockScreen

En la mayoría de los casos, el evento de seguridad se da al acceder archivos adjuntos en correos electrónicos o redireccionamientos a través de enlaces, es como se consigue la infección del sistema a explotar.

En Colombia han sido detectados cinco tipos de clases de ransomware, como los más comunes:

1. Ransomware de cifrado: cifra archivos personales y documentos, hojas de cálculo, imágenes y videos.
2. Lock Screen Ransomware WinLocker: Bloquea la pantalla del equipo de cómputo y posterior a ello solicita el pago del rescate de la información.
3. Master Boot Record (MBR) Ransomwarealware: consiste en bloquear esta parte del disco duro del computador que permite iniciar el sistema operativo.
4. Ransomware de cifrado de servidores web: Su principal objetivo de ataque son los servidores web y el cifrar todos los archivos personales.
5. Ransomware de dispositivos de telefonía celular: Los dispositivos móviles, que en su mayoría su sistema operativo sea Android, pueden llegar a infectarse mediante descargas no oficiales de programas previamente manipulados por los atacantes.

Del total análisis de muestras analizadas en los sitios web de antivirus más comunes, tales como Kaspersky, ESET, Mc Afee, Norton Labs, entre otros, se logran identificar variaciones de Wannacry, Crysis, Darma, y Ryuk, los cuales han ven ido siendo los responsables de la obstaculización, interrupción, modificación y finalmente la encriptación de los datos en su gran mayoría aquellas pymes o pequeñas empresas comprometidas por este tipo de ataque.

Existen algunos enlaces que redireccionan a sitios web maliciosos, donde el delincuente logra que la víctima descargue el malware que compromete los datos e información relevante de la entidad.

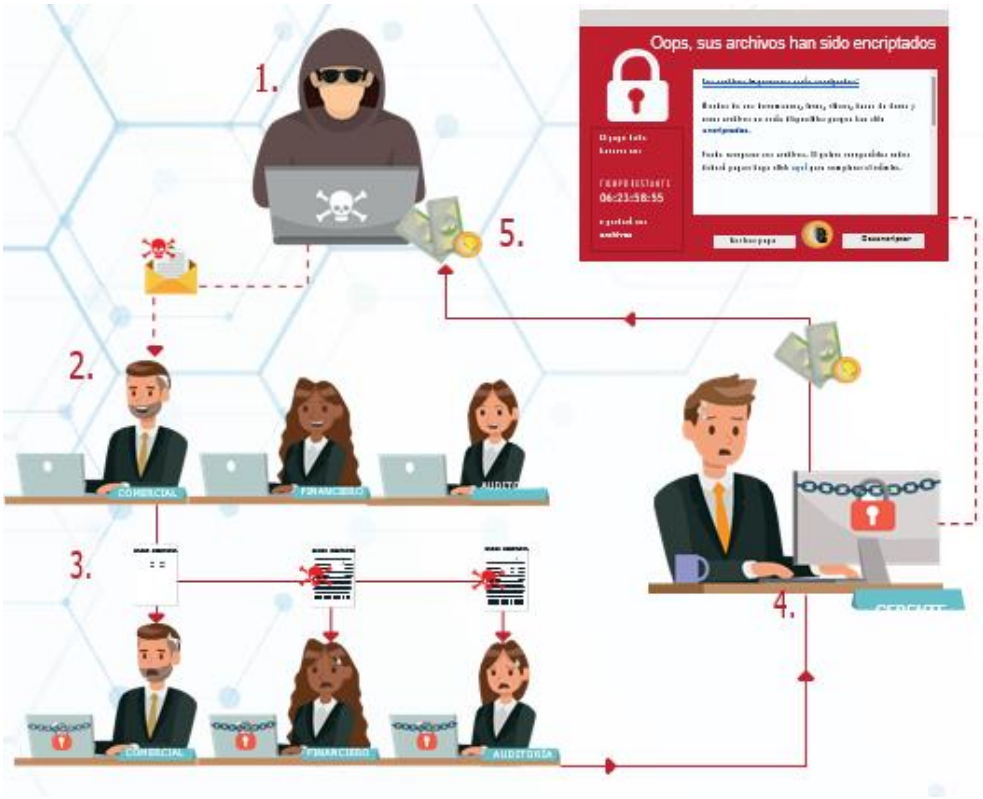


Gráfico 8. Mensaje de cifrado de la información y cobro por rescate

Las cifras de cobro de rescate pueden llegar a estar entre 0.5 y 5 BITCOINS, que viene siendo el monto más común que perciben los delincuentes, teniendo en cuenta que esto depende de la cotización de la criptomoneda.

La dificultad en la trazabilidad de las transacciones en materia de las criptomonedas, se ha convertido en un promotor para las redes de cibercriminales, en donde el modelo de ecuación criminal, entiende perfectamente que siempre las ganancias logradas, serán mayores a los pronósticos o proyecciones financieras realizadas, aparte la alta disminución de ser ubicados, arrestados y posteriormente condenados.

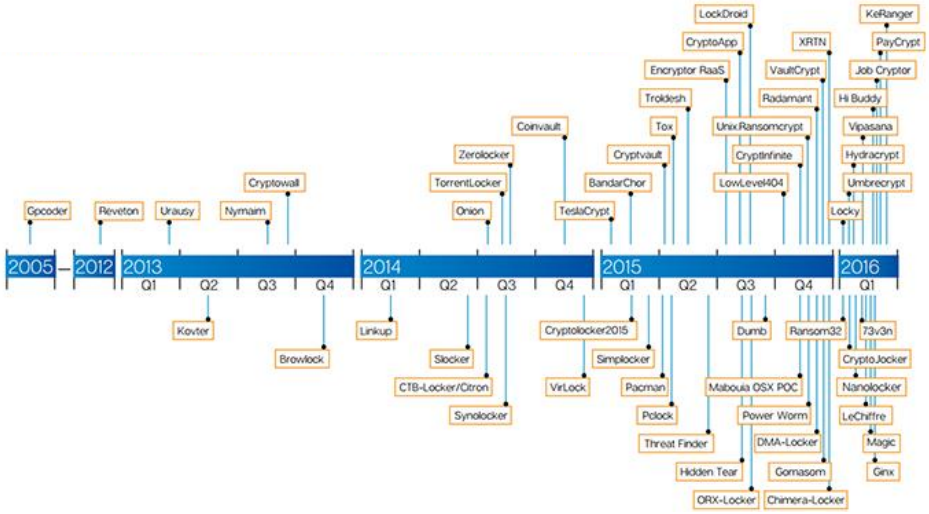


Grafico 9. Ransomware descubierto en los últimos años

Este tipo de malware no discrimina el tamaño de la empresa, ni la infraestructura, en su lugar, el principal alcance consiste en lograr sobrepasar los controles de seguridad, convirtiéndose en su mayoría inmune a cualquier sistema de prevención y detección tal y como un IDS o IPS común, debido a sus técnicas de ofuscamiento en la estructura del código o algoritmo de ejecución.

Por ejemplo, el ransomware: SAMSAM, para los últimos años, cobró relevancia en Colombia, ya que permite al atacante el robo de contraseñas de acceso remoto a los dispositivos, a través del acceso a credenciales RDP (Remote Desktop Protocol) y de este modo secuestrar de manera literal la información de las empresas comprometidas.

Estos tipos de ataques estuvieron dirigidos a individuos o entidades con efectos negativos altamente severos por la complejidad del mismo ataque. SamSam elevó el monto de los rescates y solicitud de recompensa, al ubicarse entre 32 y hasta más de 160 millones de pesos por ataque.

Otro tipo de ransomware llamado GandCrab, ha sido mucho más común que SamSam, y este exigió rescates a partir de los 3 millones de pesos colombianos. Todos ellos en moneda Bitcoin.

Para los casos que fueron atendidos por los fabricantes de antivirus, se ha logrado evidenciar un relevante aumento en este tipo de ciberataques, debido a que los ciberdelincuentes usan diversos métodos criptográficos para poder implementar nuevos mecanismos que imposibilitan su detección.

3.3 Ataque DDoS o Denegación de Servicio Distribuido:

Dentro del ciberespacio, lo que corresponde a las páginas y las aplicaciones o servicios Web, también son un blanco apetecido por los ciberdelincuentes ya que éstos vienen a ser los activos esenciales para el negocio de muchas empresas en Colombia, pues desde allí es que se atienden a los terceros o proveedores y a sus clientes o éstos canales transaccionales se convierten en las principales plataformas de información de todos sus productos y servicios en línea, incurriendo en el modelo de e-Commerce o comercio electrónico.

Un ataque de denegación de servicios distribuido, conocido mejor como un DDoS, es capaz de inhabilitar el uso de un sistema principal de información, también puede afectar una aplicación o un servidor puntual, y con el fin de bloquear la salida del servicio para el que está destinado. Según la inteligencia de amenazas, estos ataques pueden tener su origen en fallas de configuración, sistemas des actualizados o empleados inconformes.

En los últimos años los ciberatacantes han mejorado y evolucionado sus técnicas hasta el punto de utilizar sofisticadas redes maliciosas o BOTNETS en las que consiguen elevar de manera considerable la cantidad de peticiones al servicio online que se desean atacar.

La consecuencia final de la ejecución de este tipo de ataque, es lograr la caída total o parcial e interrupción de los sistemas o servicios Web, generando graves daños reputacionales y operativos sobre las entidades impactadas, ya que sus servicios quedarían inutilizables por un determinado tiempo y que éste depende de la correcta implementación de los procesos de continuidad del negocio, planes de continuidad y contingencia, recuperación de desastres y sistemas de hyperconvergencia o centros alternos de procesamiento. Estos últimos se pueden evidenciar más en las empresas grandes ya sean públicas o privadas, lastimosamente en las pymes, pequeñas y algunas medianas empresas no cuentan con un sistema de continuidad del negocio pleno, lo cual facilita que los tiempos fuera de línea de sus servicios afectados por DDoS, sean mucho más altos, perjudicando la estabilidad y confianza de sus clientes.

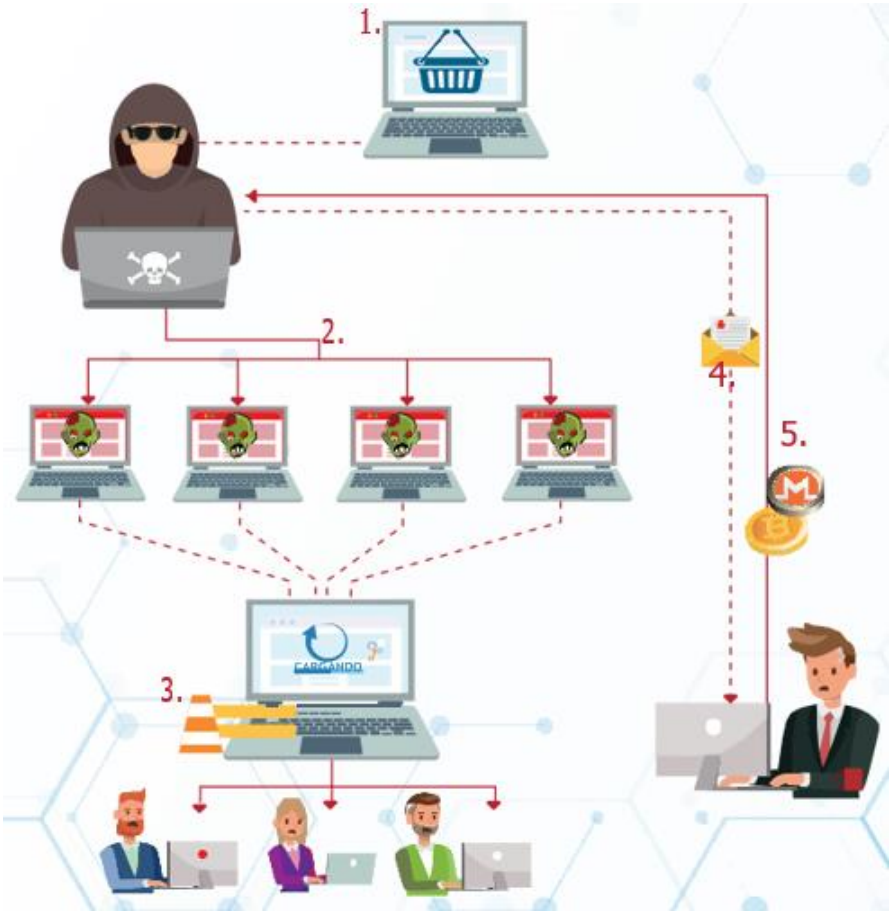


Gráfico 10. Ataque por pasos de denegación de servicio

Factores más comunes de ataques DDoS en Colombia:

- ✓ Reconocimiento y escaneo de los servicios de la compañía a afectar.
- ✓ Utilización de redes Botnet para lanzar ataques dirigidos a los servicios online.
- ✓ Interrupción de los servicios para los usuarios y terceros (clientes).
- ✓ Exigencia mediante correo electrónico o chat de ciber extorsión.
- ✓ Solicitud y demanda de pagos en criptomonedas, principalmente Bitcoins

Debido al gran impacto generado en las entidades, el cibercriminal aprovecha la cercanía de fechas especiales en las que la empresa presente mayor transaccionalidad y aumento de procesos de operación, en estas épocas el Cibercrimen ha sido clave para impactar el negocio de las empresas objetivo de su ataque y se aprovechan de la situación, ejerciendo presión y extorsionando o aplicando el concepto de ciberchantaje a las pymes o pequeñas empresas. Estos mensajes se envían a través de correos electrónicos o chats dirigidos a los responsables de TI o directivos de compañías, para que éstos en su afán, transfieran

pagos a cuentas y billeteras electrónicas en Bitcoins. Según la Policía Nacional en su Centro Cibernético de ciberseguridad y delitos informáticos, el acceder a los requerimientos de los cibercriminales sólo contribuye a que estas redes oscuras dispongan de más recursos para sofisticar sus ataques a otras compañías de igual o mayor nivel.

Gráfico 11. Ejemplo de correo emitido posterior a un ataque DDoS.

3.4 Malware o Software Malicioso

Los ciberdelincuentes utilizan el malware con múltiples propósitos, tales como extraer información personal o credenciales, sustraer dinero o evitar que los propietarios accedan a sus equipos o dispositivos.

El malware hace referencia a todo programa diseñado en afectar un sistema operativo en especial, impactando de manera negativa ya sea en rendimiento o uso de recursos sobre los dispositivos o equipos de cómputo comprometidos.

Se considera dañino si lo miramos desde el punto de vista que ingresa a un dispositivo sin autorización, el cual ejecuta procesos y subprocesos en segundo plano, inadvertidos por el propietario del sistema vulnerado, y qué además que hace el uso indebido de la información confidencial, o del sistema, sustrayendo datos relevantes, multimedia.

El malware es capaz de comprometer dispositivos tales como celulares, tabletas electrónicas, y electrodomésticos que dispongan de tecnología de conexión y administración online.

Según el departamento de ciberseguridad y de delitos informáticos de la Policía Nacional de Colombia, se registraron para el último año, un 57% de los ciber delitos reportados en nuestro país, corresponden a robos por medios informáticos y uso de malware para este fin.

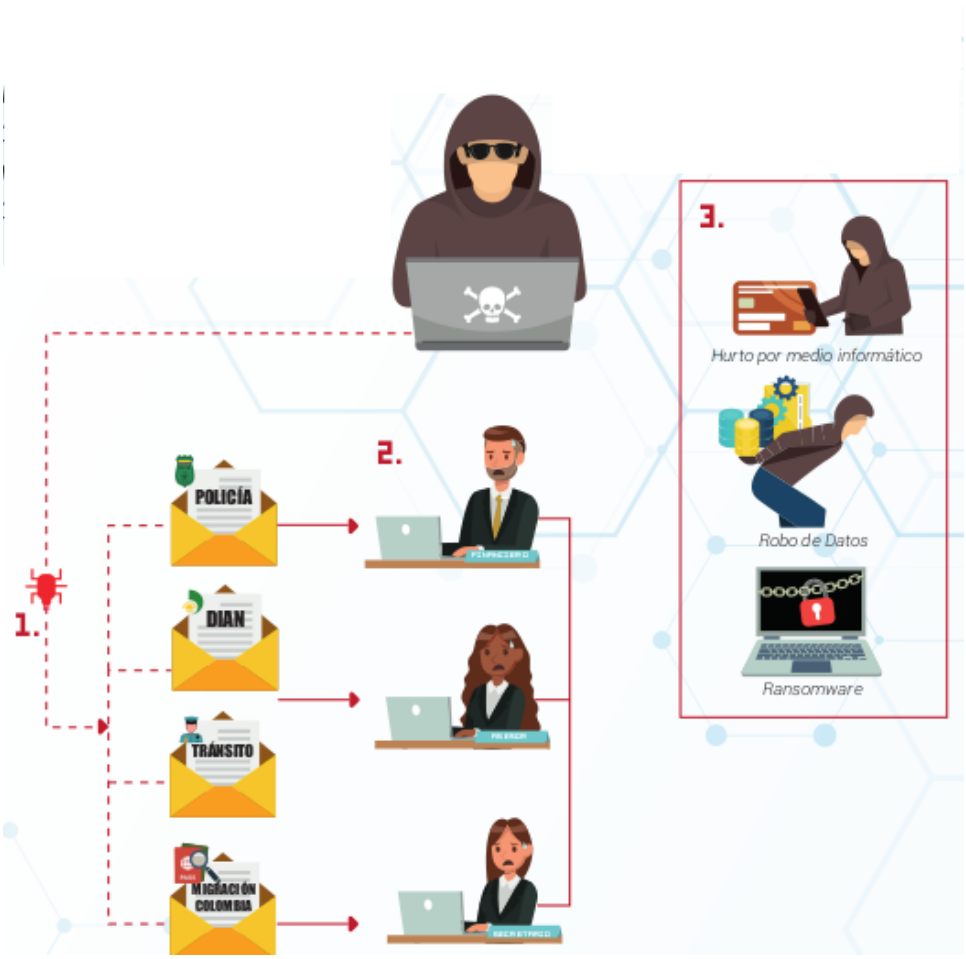
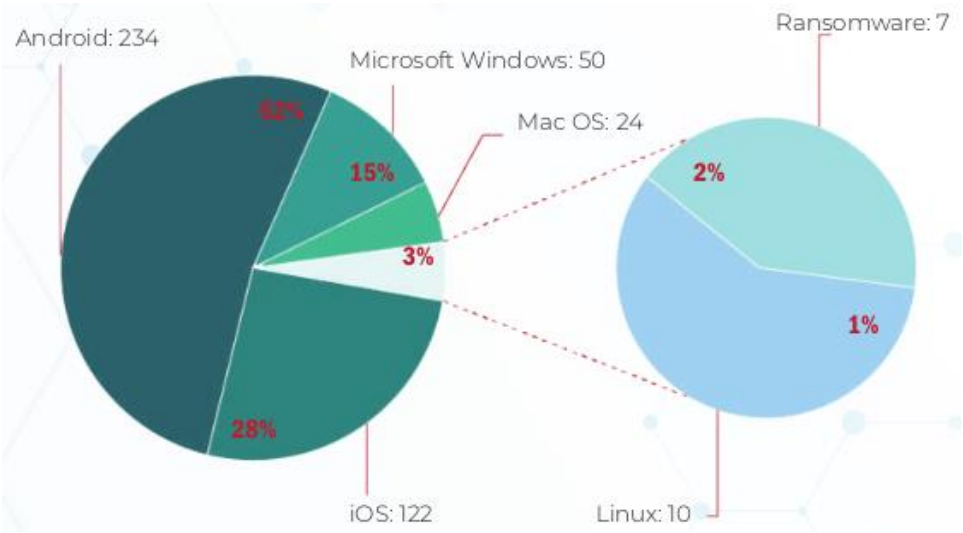


Gráfico 12. Principales medios de mensajes utilizados por los malware

La infección de Malware sigue en aumento, registrando múltiples casos de empresas que reportaron este tipo de infección relacionada con malware en su infraestructura de tecnología. Donde siguen siendo las PYMES las más afectadas por este tipo de ataques.

Gráfico 13. Métodos de dispersión de malware

Desde el 2019, el Centro Cibernético Policial ha analizado 447 muestras nuevas de Malware, con una tasa de 30% de éxito en el compromiso de sistemas de empresas en Colombia.



De las cepas de virus analizadas, se encontró que para un 8% se han recibido a través del servicio de CAI VIRTUAL y el 92% restante corresponden a solicitudes formales tramitadas por diferentes medios de recepción judiciales.

Gráfico 14. Análisis de muestras estadísticas generales de sistemas operativos afectados

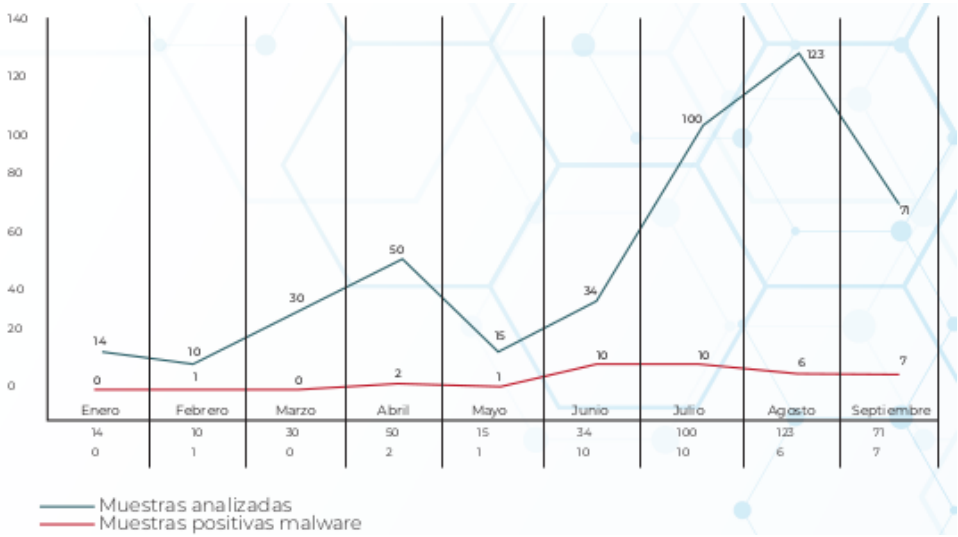


Gráfico 15. Análisis de muestras 2019

Principales vectores de ataques del Malware:

El principal vector de ataque es el correo electrónico, el cual se ha convertido en el medio más usado por los atacantes para realizar campañas masivas de distribución de Malware a través de la suplantación de entidades oficiales tales como la fiscalía general de la Nación, la Dirección de Impuestos y Aduanas Nacionales DIAN o el centro de tránsito y movilidad.

4 CONCLUSIONES

La implementación de la metodología Inteligencia de Amenazas se enfocó en gran manera sobre las pequeñas y medianas empresa, permitiendo agregar valor en arras de mejorar el proceso y brindar una información a aquellas organizaciones que no cuenta con personal para la seguridad de la información.

La implementación de la inteligencia de amenazas al interior de una organización permite tener una visión global y adecuada de las ciberamenazas, esto ya que al consultar diferentes fuentes de información logra dar a los equipos de seguridad métodos de identificación temprana a ciberamenazas que podrían materializarse en su organización si no se detectan eficazmente.

Inicialmente se enfocó en logra hacer entender a las organizaciones el por qué y el para qué, de las Inteligencia de amenazas, sus fases, los tipos de inteligencia, luego se dio a conocer las herramientas y recursos para poder interactuar con la metodología, para finalmente dar a conocer de acuerdo a la misma, cuáles son algunos de los mayores riesgos o amenazas que se encuentran actualmente vulnerando a las organizaciones.

El estudio de las tendencias de las ciberamenazas nos brinda la información necesaria sobre cuáles son los cambios que se han venido presentando y cómo van variando, las ciberamenazas han tenido un súbito incremento por causa de la pandemia, la industria de la seguridad, por medio de evaluaciones constantes han logrado identificar cada año los mayores retos a los cuales se debe enfrentar los equipos de seguridad y suelen dar sus predicciones acordes con el comportamiento de las ciberamenazas.

La creación de conciencia y cultura en ciberseguridad sobre las pymes o pequeñas empresas ayudará a ubicarlas de manera proactiva y a los encargados responsables por vigilar los activos críticos de información, en un contexto de ciberamenazas más real, lo cual ayudará a preparase, conociendo los principales vectores de ataque y los distintos modos de operación, lo cual se traducirá en ahorro de costos de recuperación y reducción de impacto y probabilidad sobre los riesgos de seguridad de la información que registren la organización.

Para finalizar cabe resaltar algunos de los beneficios de implementar adecuadamente un programa de inteligencia de amenazas (CTI):

- Proporciona una mayor comprensión de las ciberamenazas.
- Prevenir la perdida de datos identificando las causas de la fuga de datos.
- Orienta la respuesta de incidentes.
- Identificar amenazas avanzadas a partir del análisis de amenazas.
- Compartir información de amenazas.
- Descubrir tácticas, técnicas y procedimientos para posibles ataques (TTP´s).
- Detectar brechas en una etapa temprana o inicial
- Identificar indicadores de compromiso (IoC).
- Utiliza los indicadores para construir una defensa perimetral más proactiva

5 FUENTES DE REFERENCIAS

1.Sir Alistair MacFarlane, (2013), Information, Knowledge & Intelligence, fuente https://philosophynow.org/issues/98/Information_Knowledge_and_Intelligence.

2. Lance James, (2017), Fail vs Finished: The Difference Between Information and Intelligence, from https://misti.com/infosec-insider/fail-vs-finished-the-difference-between-information-and-intelligence.

3. RFSID, (2017), Threat Intelligence, Information, and Data: What Is the Difference?, fuente https://www.recordedfuture.com/threat-intelligence-data/.

4. BEN S, (2016), Information vs. Intelligence, fuente http://www.intelligence101.com/information-vs-intelligence/.

5. Jack Medland-Slatter, (2017), What is the difference between data and information in business?, from https://www.perceptive.co.nz/blog/what-is-the-difference-between-data-and-information-in-business.

6.(2017), The Benefits of Intelligence-led Security Testing, fuente https://www.secalliance.com/blog/benefits-intelligence-led-security-testing/.

7.(2015), Intelligence-Led Penetration Testing Services, fuente https://www.baesystems.com/en/cybersecurity/download-csai/resource/uploadFile/1434557450333.

8. Shannon Williams, (2015), Intelligence-led testing imperative for security, fuente https://securitybrief.co.nz/story/intelligence-led-testing-imperative-security/.

9. Red Teaming & Intelligence-Led Penetration Testing, fuente https://www.digitalmarketplace.service.gov.uk/g-cloud/services/618463585381615.

10. Robert M Lee, (2014), Cyber Threat Intelligence, from https://www.tripwire.com/state-of-security/security-data-protection/cyber-threat-intelligence/.

11. RSA, (2016), Four Characteristics of Top-Notch Threat Intelligence, fuente https://www.rsa.com/en-us/blog/2016-12/four-characteristics-of-top-notch-threat-intelligence.

12. Four Features to Look for in a Threat Intelligence Service, fuente https://searchsecurity.techtarget.com/ThreatIntelligence/Four-Features-to-Look-for-in-a-Threat-Intelligence-Service.

13. (2015), Threat Intelligence Platforms, fuente https://cdn2.hubspot.net/hubfs/454298/ebook/Threat-Intel-Platform-ebook-ThreatConnect.pdf.

14. Norah Abraham, Why You Need Cyber Threat Intelligence, fuente https://datafloq.com/read/why-you-need-cyber-threat-intelligence/3590.

15. RFSID, (2016), 6 Surprising Benefits of Threat Intelligence From the Web, fuente https://www.recordedfuture.com/threat-intelligence-benefits/.

16. Yinon Hacmon, (2018), 6 Benefits "Threat Intelligence" can provide, fuente https://www.cybersett.com/single-post/2018/01/14/6-Benefits-Threat-Intelligence-can-provide.

17. Jon Friedman and Mark Bouchard, (2015), Definitive Guide to Cyber Threat Intelligence, fuente https://cryptome.org/2015/09/cti-guide.pdf.

18. Integrate Threat Intelligence Into Your Security Operations, fuente https://www.infotech.com/research/ss/integrate-threat-intelligence-into-your-security

19. Centro Cibernético Policial, Fuente https://caivirtual.policia.gov.co/

20. The No More Ransom Project, Fuente https://www.nomoreransom.org/es/index.html

21. La importancia de la fase de Dirección y Planificación en Inteligencia, Fuente https://cdn.shopify.com/s/files/1/2642/0470/files/ciclo_inteligencia_e9ecdf5a-332b-422a-bba8-175a0d5e8cec.png?v=1554275982