TENDENCIAS CIBERCRIMEN COLOMBIA

DATA

2019 - 2020

TENDENCIAS CIBERCRIMEN COLOMBIA 2019 - 2020

Informe de las tendencias del cibercrimen en Colombia (2019-2020)

Primera edición, Bogotá D. C.
Octubre 29 de 2019
http://www.ccit.org.co
https://www.policia.gov.co/
https://www.policia.gov.co/dijin

EQUIPO DE INVESTIGACIÓN

ADRIANA CEBALLOS LÓPEZ

CR (RA) FREDY BAUTISTA GARCÍA

LORENA MESA GUZMÁN

CARLOS ARGÁEZ QUINTERO

EQUIPO DE POLICÍA NACIONAL

TC ALEX DURÁN SANTOS

MY FÉLIX MIRANDA HERRERA

CT RODRIGO ACEVEDO NIETO

TE. WOLFAN PRADA ROA

IT JEFFER RUIZ LEAL

PT HÉCTOR SANTOS ROCHA

DISEÑO Y DIAGRAMACIÓN

LUNA BAUTISTA VARGAS

ALIADOS ESTRATÉGICOS

CONTENIDO

PRÓLOGO

Alberto Samuel Yohai
Presidente Ejecutivo CCIT

El cibercrimen ha experimentado un crecimiento durante los últimos años casi de forma paralela al uso de las nuevas tecnologías y las pérdidas generadas por los ciberataques sitúan a esta problemática como una de las principales economías ilegales en el País.

El impacto que sufren las empresas colombianas luego de un ciberataque trasciende el coste económico por pérdidas de sus activos financieros y conlleva de manera colateral afectaciones a la productividad, daños reputacionales e incluso implicaciones de carácter legal por fuga de información privilegiada y data sensible.

Conocer los riesgos asociados a la ciberdelincuencia e identificar las buenas prácticas para enfrentarlos fortalece el avance de la cultura de la seguridad de la información además de elevar la confianza digital de las empresas y ciudadanos.

Este propósito demanda el esfuerzo integrado del sector privado, los proveedores de tecnología para la ciberseguridad empresarial y las autoridades responsables de enfrentar las amenazas, por ello durante el 2019 el TicTac de la CCIT viene fortaleciendo la alianza con la Policía Nacional para desarrollar iniciativas conjuntas en la materia.

El estudio Tendencias del Cibercrimen 2019-2020, presentado por el Tanque de Análisis y Creatividad de las TIC - TicTac de la CCIT y su programa SAFE en asocio con la Policía Nacional - Centro Cibernético Policial, presenta las cifras y modalidades de los ciberdelitos en 2019 y las tendencias que enfrentaran las empresas Colombianas y los ciudadanos en 2020, panorama que no es lejano al análisis que agencias de carácter internacional como el EC3 (Centro Europeo Contra la Cibercriminalidad de EUROPOL) han identificado a nivel mundial.

SAFE

PRESENTACIÓN DEL ESTUDIO

El estudio publica los datos estadísticos más relevantes de la cibercriminalidad en Colombia y los métodos y técnicas identificadas en 2019 a partir del análisis de las 15.948 denuncias y reportes realizados por empresas y ciudadanos al Centro Cibernético Policial CECIP.

Mediante la elaboración de un instrumento interno aplicado a estos reportes delictivos fueron identificados los principales vectores de infección utilizados por los ciberdelincuentes así como las técnicas de ofuscación del malware con el cual afectan a las empresas y ciudadanos en el País.

Fueron analizadas 447 muestras en el laboratorio de informática forense del centro cibernético policial en donde se identificaron 33 nuevas clases de programas malignos encontrados en los enlaces, adjuntos y páginas infectadas a las que accedieron las víctimas y que fueron gestionadas desde la plataforma de ciberseguridad de la Policía Nacional a través de su laboratorio de análisis de código malicioso.

Con la finalidad de establecer la relación de las tendencias identificadas en Colombia, en el contexto supranacional, fueron utilizados como fuente los datos publicados en el reciente informe IOCTA 2019 de Europol por sus siglas en Ingles (Internet Organised Crime Threat Assessment) Evaluación de amenazas del Crimen Organizado en Internet y los reportes de empresas líderes en el ámbito de la Ciberseguridad en la Región como Microsoft, CISCO, McAfee, Absolut, Claro y Fortinet todos Aliados de programa SAFE.

En el mismo sentido el informe de Ciber Resiliencia Organizacional publicado en mayo de 2019 por el TicTac de la CCIT y los Estudios sobre Ciberseguridad en el sector financiero de la OEA 2018 y 2019.

ADRIANA CEBALLOS LÓPEZ
Directora desarrollo de programas TicTac

TC ALEX DURÁN SANTOS
Jefe Centro Cibernético Policial DIJIN

INTRODUCCIÓN

El Cibercrimen actúa de una manera coordinada y dispone de recursos económicos ilimitados provenientes de las ganancias derivadas de actividades criminales previas.

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.

Por primera vez se han detallado cada una de las modalidades de mayor afectación e Impacto señalando los actores que intervienen en la cadena criminal e identificando cuáles son los principales métodos de engaño que emplean los criminales a la hora de facilitar y acometer los ataques.

Es claro que para enfrentar una amenaza es importante conocer como 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.

Cuando se conocen las amenazas y los riesgos pueden ser gestionados oportunamente y las compañías desafortunadamente siguen siendo reactivas y su actuación ante un incidente descoordinada, en parte por que no conocen la problemática o no han definido de manera adecuada los roles a seguir en la cadena de responsabilidad organizacional establecida.

CR (RA) FREDY BAUTISTA GARCIA
Asesor Ciberseguridad TicTac CCIT

SAFE

1.

CIBERCRIMEN EN CIFRAS

La dinámica actual del Cibercrimen en Colombia refleja un crecimiento gradual en el número de incidentes cibernéticos reportados a las autoridades del ecosistema de ciberseguridad.

A través de los canales de atención a empresas y ciudadanos dispuestos por la Policía Nacional fueron registrados **28.827** casos durante el 2019.

Del total de los casos registrados, **15.948** fueron denunciados como infracciones a la ley 1273* de 2009 por parte de las víctimas, esta cifra corresponde al **57%** del total de casos informados.

Respecto al 2018 las denuncias disminuyeron un **5.8 %** tras una variación negativa de **983** casos.

Incremento en el número de incidentes respecto al 2018

***Tipifica las conductas de Delitos Informáticos en Colombia.**

2015	*2016*	*2017*	*2018*	*2019*
7.523	**11.225**	**15.840**	**22.524**	**15.948**

Denuncia Física	*Denuncia Virtual*
54,5%	**45,5%**

Cifras denuncias 2015- 2019 / Fuente: SIEDCO Policía, SPOA Fiscalía, ADenunciar.

El 45% del total de denuncias por ciberdelitos en el país se hace a través de la aplicación ADenunciar. Desde *julio de 2017* se han recibido un total **24.711 denuncias** por ciberdelitos en esta plataforma virtual.

Fuente: Policía

12.879 incidentes cibernéticos es decir un **43%** de los casos reportados en 2019, fueron gestionados sin que se llegara a instaurar una denuncia ante la Fiscalía General de la Nacional.

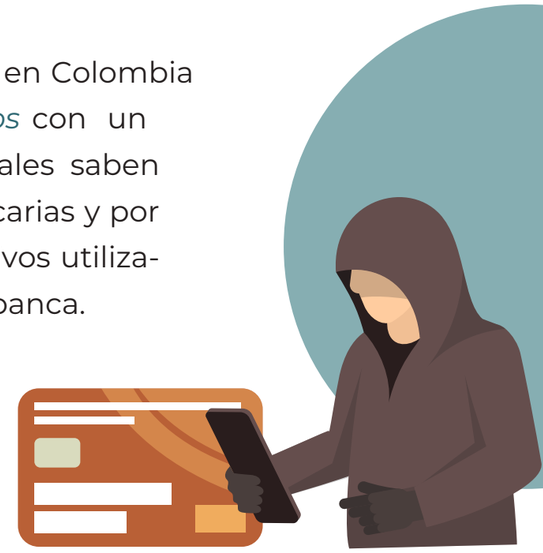
Esta cifra representa un incremento del **54%** respecto del 2018, cuando fueron gestionados **8.363** casos.

Los incidentes más reportados en Colombia siguen siendo los casos de Phishing con un **42%,** *la Suplantación de Identidad* **28%,** *el envío de malware* **14%** *y los fraudes en medios de pago en línea con* **16%**.

DELITOS INFORMÁTICOS QUE MÁS AFECTAN A LOS COLOMBIANOS:

El principal interés de los Cibercriminales en Colombia se basa en la motivación económica y la posterior monetización de las ganancias generadas en cada Ciberataque.

El delito informático más denunciado en Colombia es el *Hurto por medios informáticos* con un total de **31.058** casos, los cibercriminales saben que el dinero está en las cuentas bancarias y por eso buscan comprometer los dispositivos utilizados en la interacción entre usuarios y banca.



Las cifras de denuncias entorno a los fraudes en el sector financiero han disminuido ante la no obligatoriedad de este trámite para reclamaciones ante las entidades bancarias.

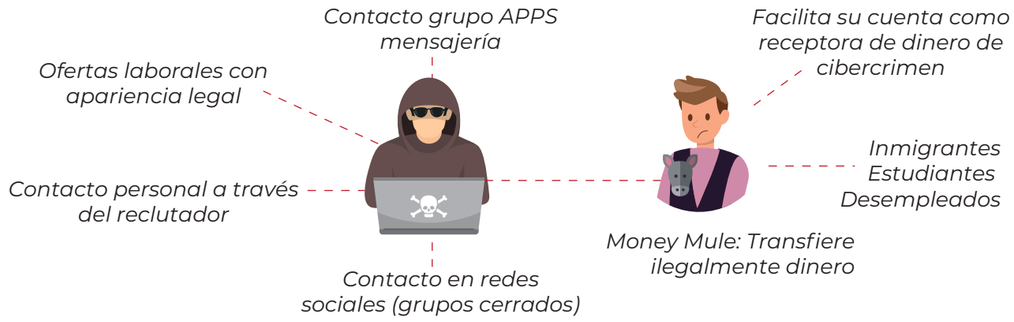
SAFE

En segundo lugar, se encuentra la Violación de datos personales con **8.037** casos.
Este dato revela que la **segunda amenaza** en Colombia para empresas y ciudadanos es el **Robo de Identidad**.

El tercer delito más denunciado es el Acceso abusivo a sistema informático con **7.994** casos, y esto se explica en razón a que, en las fases primarias de los Ciberataques, los cibercriminales buscan comprometer los sistemas informáticos logrando ganar el acceso a los mismos.

En cuarto lugar, con **3.425** casos se encuentra la Transferencia no consentida de activos, conducta criminal que facilita al atacante sustraer el dinero o transferir valiosos activos financieros de las víctimas

Las Money Mules prestan su nombre o su cuenta bancaria para recibir transferencias de dinero producto de la actividad ilícita de los cibercriminales.



Las Money Mules o mulas monetarias se convierten en el eslabón primario de la cadena criminal del Cibercrimen, perciben generalmente un 10% a 15% del total de ganancias.

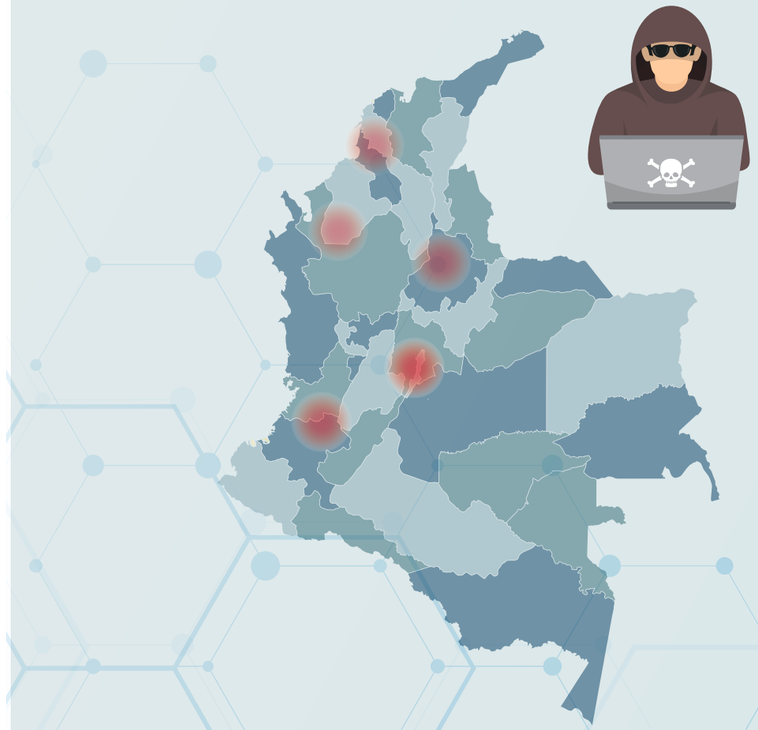
Algunos pueden ser engañados con esquemas de teletrabajo y las redes del Cibercrimen pueden estar en otros continentes.

Finalmente, en quinto lugar se sitúa el delito de Uso de Software Malicioso con **2.387** casos.

DELITOS INFORMÁTICOS POR CIUDADES:

La concentración del fenómeno criminal en 2019 sitúa a Bogotá, Cali, Medellín, Barranquilla y Bucaramanga como las ciudades con mayor afectación por esta problemática con un 55% de los casos registrados.

Si bien la cifra obedece a los centros urbanos con mayor densidad poblacional y penetración de internet en el país, el factor de desarrollo económico influye en los objetivos de los cibercriminales, que enfocan su actuar hacia **PYMES**, entidades financieras y grandes compañías con asiento en estas ciudades.



BOGOTÁ
5.308 casos

CALI
1.190 casos

MEDELLÍN
1.186 casos

BARRANQUILLA
643 casos

BUCARAMANGA
397 casos

SAFE

3.

ATAQUE BEC

Minería de criptomonedas

Cerca del 90% de los ciberataques que sufren las empresas en Colombia se deben a ingeniería social.

A través de distintas técnicas ***los cibercriminales obtienen información confidencial*** *de empresas, directivos y empleados, para luego suplantar identidades, falsificar correos electrónicos y conseguir en la mayoría de los casos desviar dinero hacia cuentas bancarias bajo su control o generar despachos de insumos y mercancías* ***engañando a clientes y proveedores.***

Los Ataques BEC son una de las principales amenazas a la cadena de suministros, componente fundamental en la actividad diaria de una empresa. Las comunicaciones con proveedores externos y socios de confianza requieren de entornos seguros, que garanticen la integridad de correos electrónicos y servicios de mensajería instantánea utilizados.

Los cibercriminales diseñan escenarios simulados para engañar a empleados clave suplantando a ejecutivos, con el fin de que realicen acciones no autorizadas que conllevan a defraudar a las empresas o consiguen suplantar a sus clientes y proveedores mediante el robo de identidad basado en ingeniería social.

Los principales vectores de engaño en 2019 fueron:

80%

Correos Fraudulentos Personalizados (Spear Phishing).

60%

Suplantación de identidad.

53%

Enmascaramiento de correos (Spoofing).

37%

Infección de sitios frecuentemente visitados por empleados (Watering Hole).

2019 *En el último año, los ataques BEC lideran las cifras de denuncias por estafas recibidas por las Autoridades: (Fiscalía y Policía).*

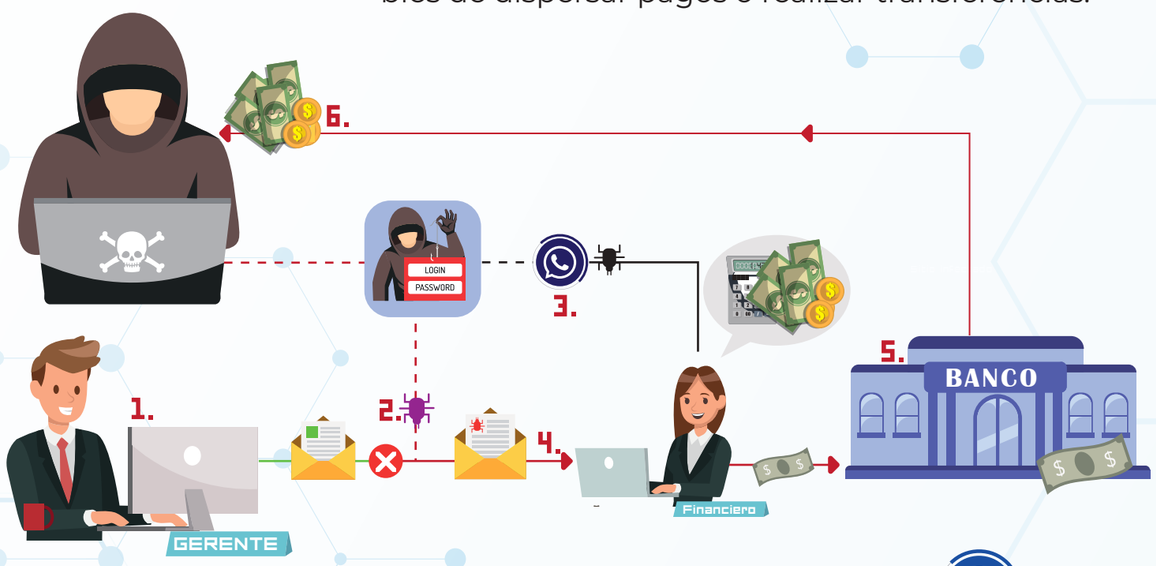
Según el FBI, los ataques BEC durante el 2018 generaron pérdidas en organizaciones globales por valor de 12.000 millones de dólares.

En Colombia, el monto promedio de las cifras de pérdidas por ataque puede oscilar entre 300 millones y 5.000 millones de pesos, según el tamaño de la empresa afectada.

Las modalidades más utilizadas por los cibercriminales:

1. ESTAFA DE CEO (suplantación de gerente)

A través de un correo malicioso (Phishing), los cibercriminales se apoderan de la cuenta de correo del gerente de una compañía y así generan comunicados y correos falsos a los empleados responsables de dispersar pagos o realizar transferencias.



Se presenta cuando se aproximan fechas de pagos de nómina o cuando el gerente se encuentra fuera de la compañía. En ocasiones vincula suplantaciones o instrucciones simuladas a través de servicios de mensajería.

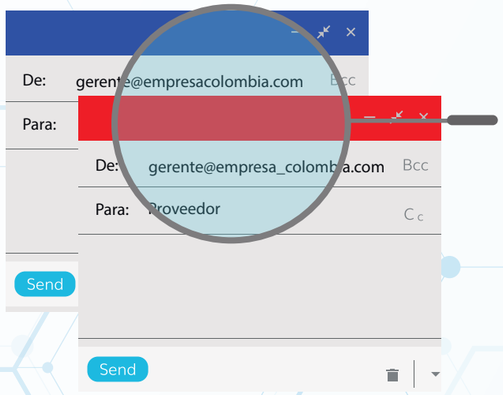
Fake Whatsapp

Los criminales pueden suplantar conversaciones a través de chats falsos.

SAFE

En una variante de esta modalidad, los cibercriminales utilizan técnicas de ingeniería social basados en SOCMINT y OSINT para obtener información de las compañías, sus proveedores y clientes.

Luego de recolectar información disponible en redes sociales y fuentes abiertas, los criminales diseñan escenarios simulados o Pretexting y mediante Spoofing Mail envian correos fraudulentos a proveedores de mercancías o suministros y otros, consiguiendo al final que dichos productos sean despachados a lugares bajo control de estas organizaciones criminales.



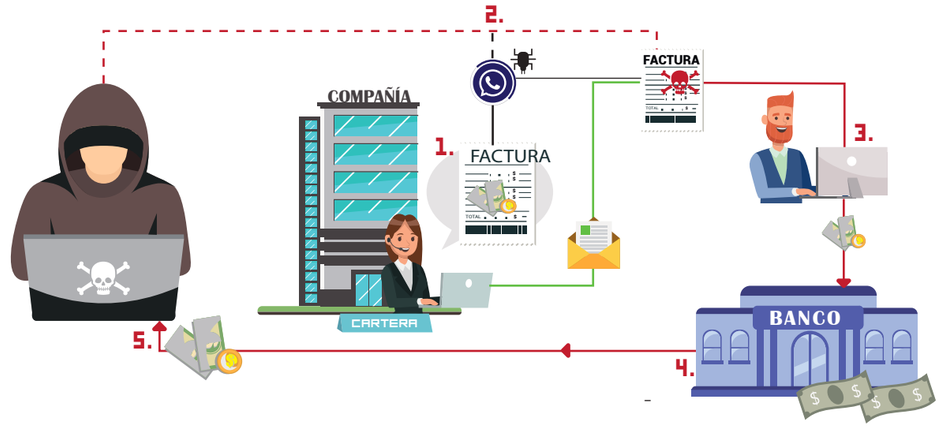
De igual manera, pueden adquirir dominios no asegurados por la compañía víctima.

Spoofing Mail

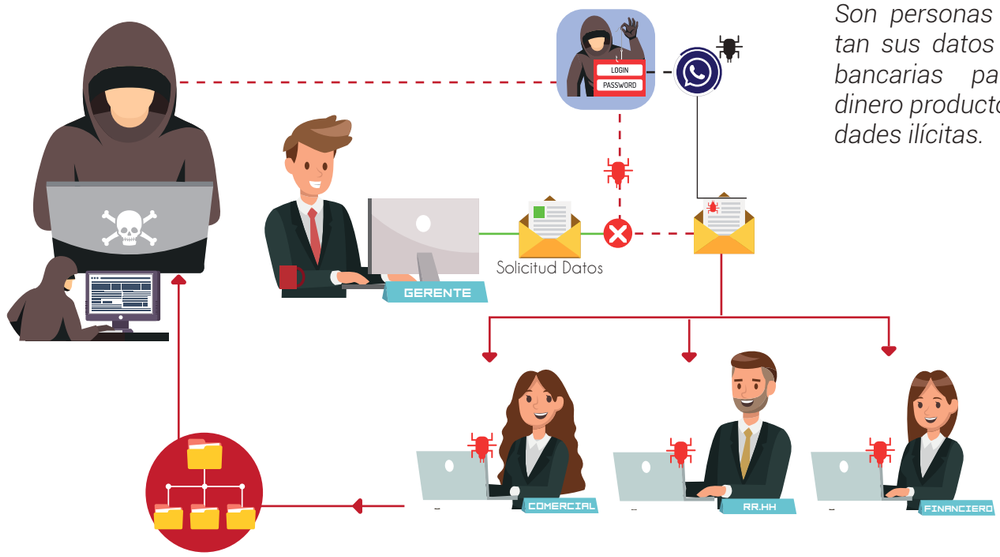
Creación de correos electrónicos suplantando la identidad de una persona o empresa, para hacerse pasar por ella y engañar al destinatario. En ocasiones, los cibercriminales solo cambian un símbolo o letra del correo remitente original.

3. SUPLANTACIÓN DE CLIENTES

En esta modalidad los cibercriminales engañan a clientes para que hagan pagos de sus facturas pendientes y el dinero llegue a cuentas bajo control del atacante.



Para poder retirar el dinero, los criminales abren cuentas bancarias con datos y documentación sustraída de las empresas afectadas mediante ingeniería social. Luego, dispersan el dinero valiéndose de mulas bancarias.



Mone

Son personas que prestan sus datos y cuentas bancarias para recibir dinero producto de actividades ilícitas.

SAFE

4.

RANSOMWARE

Una ciberamenaza subestimada en Colombia

Aunque no se trata de una modalidad reciente, este tipo de ataque que deriva su nombre de la combinación de las palabras Ransom ó rescate en inglés y ware alusivo a Software (Ransomware: Software de Rescate), ha tenido un auge en los últimos dos años en Colombia muy vinculado al creciente uso de las Criptomonedas como medio para monetizar las ganancias del Cibercrimen a nivel mundial.

RANSOMWARE

Colombia recibió el 30% de los ataques de Ransomware en Latinoamérica en el último año, seguido de Perú (16%), México (14%), Brasil (11%) y Argentina (9%).

Las PYMES fueron el blanco preferido por los ciberatacantes, pues conocen que los niveles de seguridad suelen ser más bajos en este tipo de compañías.

83%

De las empresas carecen de protocolos de respuesta a la violación de políticas de seguridad de la información.

711 *Empresas reportaron ataques de Ransomware exitosos contra sus sistemas en 2019.*

Esta problemática mundial ahora ocupa el esfuerzo por igual de compañías de ciberseguridad, servicios antimalware y fuerzas de ley responsables de la lucha contra el cibercrimen global como lo es EUROPOL e INTERPOL.

Pese a todos estos esfuerzos la posibilidad de acceder a la información secuestrada sigue siendo muy baja, en parte porque a diario se detectan nuevas familias de Ransomware y la capacidad de encontrar las claves descifradoras se hace igualmente compleja.

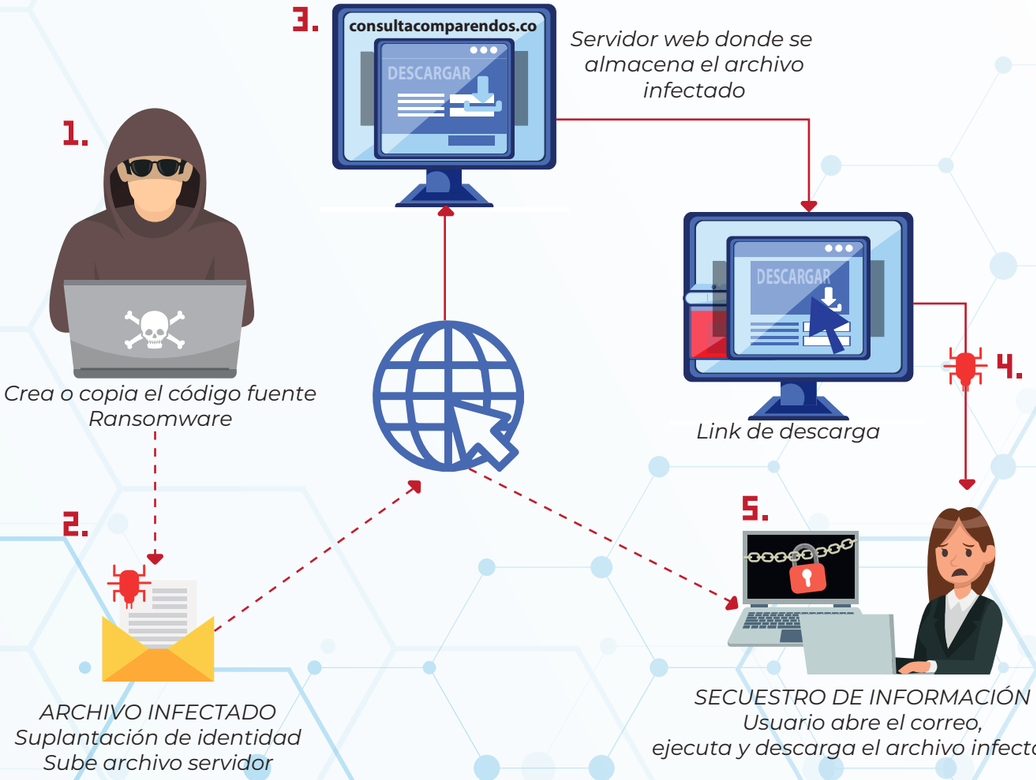
VECTORES MÁS COMUNES EN UN ATAQUE DE RANSOMWARE:

Embargos judiciales | *Reportes a centrales de riesgos.* | *Alarmas de transferencias no consentidas.* | *Foto comparendo* | *Citaciones a diligencias judiciales*

Los vectores utilizados por los cibercriminales apuntan generalmente al envío masivo de correos electrónicos con llamativos y alarmantes asuntos que consiguen en un porcentaje muy alto que las víctimas den clic sobre los enlaces incluídos en los mensajes que notifican.

El principal medio de propagación del Ransomware de tipo Lockscreen (caracterizado por impedir el acceso y el uso del equipo mediante una pantalla de bloqueo), sigue siendo el correo electrónico, puesto que una vez engañado el usuario es dirigido a un servidor para descargar el malware.

Una vez ejecutado el archivo infectado, este cifra la información, evitando cualquier acción por parte de diferentes sistemas de seguridad como antivirus, Sandbox, firewall, para exigir una posterior suma de dinero a cambio de posiblemente restablecerla.



SAFE

En todos los casos, bien sea por archivos adjuntos a correos electrónicos o redireccionamientos a enlaces se consigue la infección del sistema a comprometer.

En Colombia han sido detectado principalmente cinco tipos de clases de Ransomware:

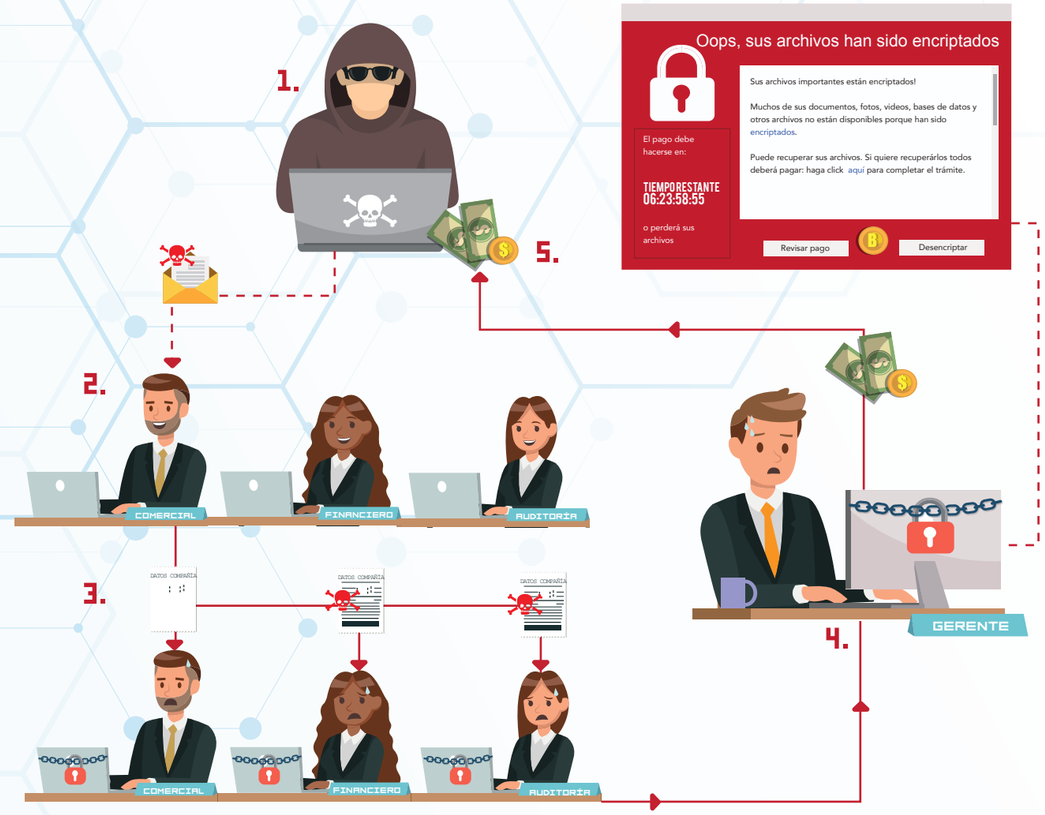
Ransomware de cifrado cifra archivos personales y documentos, hojas de cálculo, imágenes y videos.

Lock Screen Ransomware WinLocker Bloquea la pantalla del PC y solicita el pago.

Master Boot Record (MBR) Ransomwarealware es la parte del disco duro del PC que permite iniciar el sistema operativo.

Ransomware de cifrado de servidores web Su objetivo son los servidores web y cifrar sus archivos.

Ransomware de dispositivos móviles Los dispositivos móviles (principalmente Android) pueden infectarse mediante descargas no oficiales.



Del análisis de muestras remitidas al laboratorio se destacan variaciones de Wannacry, Crysis, Darma, y Ryuk, los cuales han sido responsables de la interrupción, obstaculización, modificación y encriptación del flujo normal de los datos en la mayoría de las entidades afectadas.

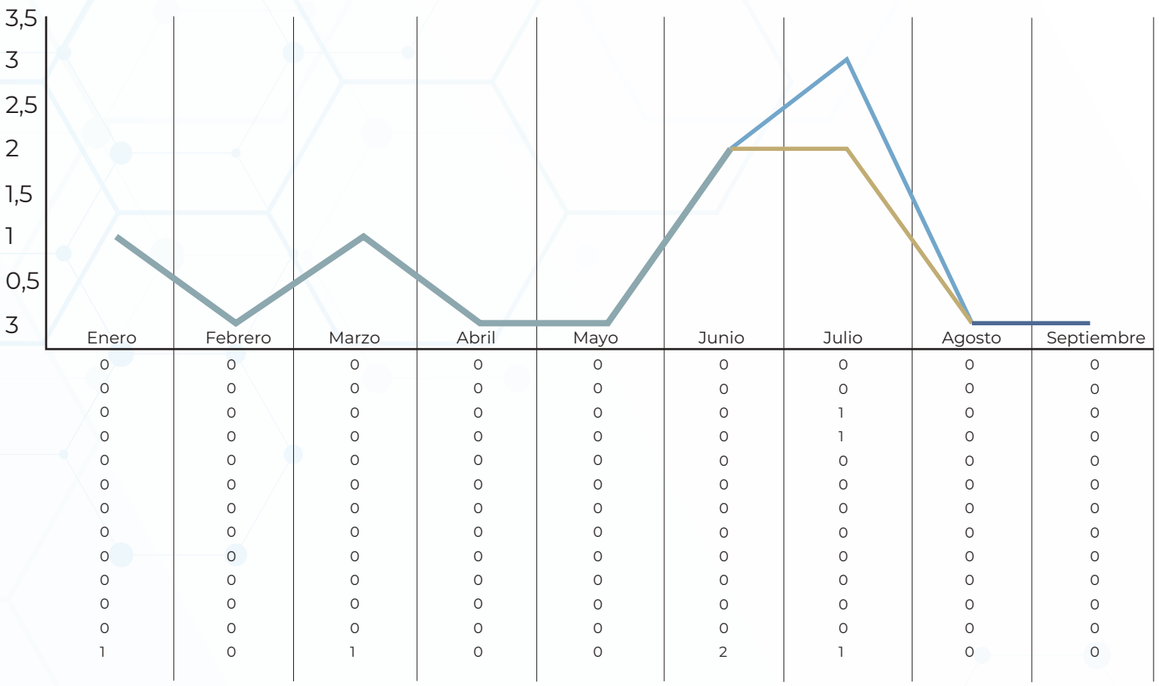
Estos enlaces redireccionan a sitios web maliciosos desde los cuales el cibercriminal consigue que la víctima descargue el malware que compromete los datos de la compañía.

Las cifras de cobro de rescate oscilan entre 0,5 y 5 BITCOINS, y el monto que perciben los atacantes depende de la cotización de la criptomoneda.

La dificultad en la trazabilidad de las transacciones de Criptomonedas, se ha convertido en un aliciente para las redes de cibercriminales que, en el modelo de ecuación criminal, entienden que siempre las ganancias percibidas serán mayores a las probabilidades de ser arrestados o condenados.

Existe ransomware que secuestra la información de teléfonos celulares y en estos casos, el vector de infección es un enlace remitido a través de un mensaje de texto o chat.

Número de muestras de ransomware



- Uliwis
- Satan
- Ryuk
- Darma
- Crysis
- Reveton
- TottentLocker
- CryptoWall
- TeslaCrypt
- Mamba
- Petya
- Grandcrab
- WannaCry

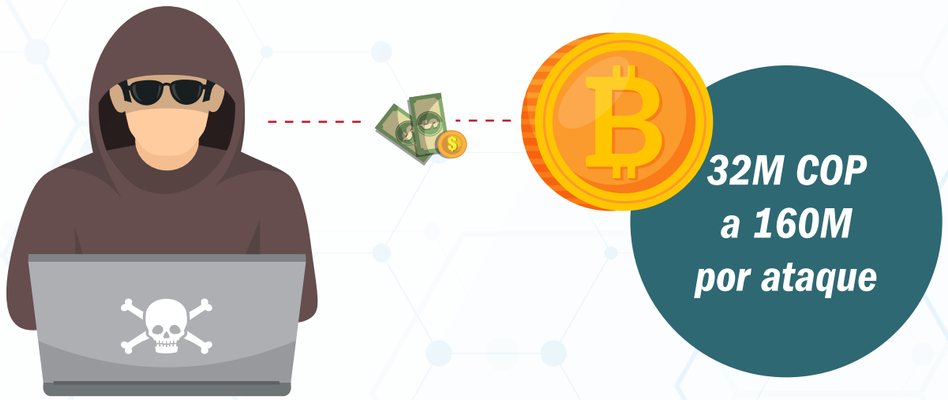
Este tipo de software no discrimina el tamaño de las organizaciones ni la infraestructura, por el contrario, su alcance logra sobrepasar los controles de seguridad, volviéndose generalmente inmune a cualquier sistema de prevención y detección, debido a sus técnicas de ofuscamiento en la estructura del código.

En los últimos meses el RANSOMWARE “SAMSAM” cobró relevancia en Colombia, porque permite al atacante el robo de contraseñas para el acceso remoto a los dispositivos a través del acceso a credenciales RDP (Remote Desktop Protocol) y de ese modo secuestrar la información de las compañias víctimas.

Estos ataques estuvieron dirigidos a entidades o individuos con efectos altamente severos por la complejidad del ataque. SamSam elevó el monto de los rescates al situarlo entre ***32 millones de COP*** hasta más ***160 M*** por ataque.

El Ransomware GandCrab mucho mas común que SAM SAM exigió rescates a partir de ***3 M COP*** . Todos los rescates se piden en Bitcoin.

Para los casos que fueron atendidos por el laboratorio, se ha podido evidenciar un notorio crecimiento en este tipo de ataques, debido a que los ciberdelincuentes utilizan diversos métodos criptográficos para poder incorporar nuevos mecanismos de dificultan la detección.



5.

ATAQUE DDOS

Ataque de denegación de servicio

Los Ataques de Denegación de Servicio son utilizados para inhabilitar un servicio ofrecido por un servidor, haciendo colapsar el sistema aprovechando sus vulnerabilidades.

Las páginas y demás aplicaciones Web, son activos esenciales para el negocio de muchas empresas en Colombia, pues desde allí se atienden a terceros y clientes o se convierten en las principales plataformas informativas de sus productos y servicios online (eCommerce).

Un ataque de denegación de servicios distribuído DDoS, inhabilita el uso de un sistema, una aplicación o un servidor, con el fin de bloquear el servicio para el que está destinado. Estos ataques pueden tener su origen en fallas de configuración o empleados inconformes.

170 *Según cifras del Centro Cibernético Policial, 170 empresas reportaron ataques DDoS que consiguieron interrumpir sus servicios de cara a sus clientes.*

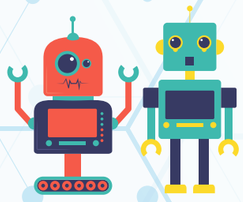
En los últimos años los ciber atacantes han evolucionado sus técnicas hasta el punto de utilizar complejas redes maliciosas o BOTNETS con las que consiguen elevar de manera considerable el número de peticiones al servicio online que se quiere afectar.

Hasta lograr su caída e interrupción ocasionando graves daños reputacionales y operativos a las compañías. Esta variante se conoce como Ataque DDoS

2019

Ataques DDos

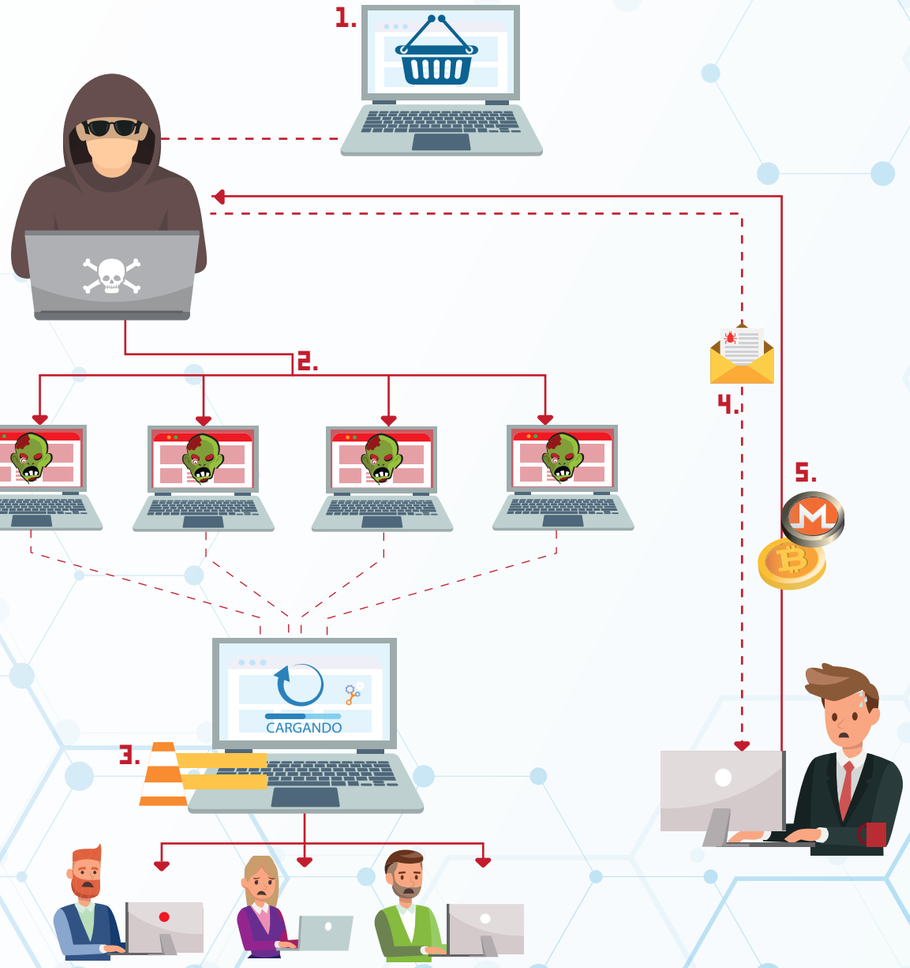
Aumentó la demanda de ataques de larga duración mediante inundación de HTTP.



Botnet *Es una red de equipos informáticos o Bots controlados remotamente y utilizados como plataforma para lanzar Ciberataques.*

Bien sea por competencia desleal, empleados inconformes o ciber-criminales, los Ataques DDoS consiguen saturar los recursos de los sistemas que alojan los servicios que se quieren degradar hasta el punto de dejarlos en estado no funcional.

ATAQUE DE DENEGACIÓN DE SERVICIO



FACTORES MÁS COMUNES DE ATAQUES DDOS EN COLOMBIA:

1. Reconocimiento y escaneo de los servicios de la compañía a afectar.

2. Utilización de redes Botnet para lanzar ataques dirigidos a los servicios online.

3. Interrupción de los servicios para los usuarios y terceros (clientes).

4. Exigencia mediante correo electrónico o chat de ciberextorsión.

5. Solicitud y demanda de pagos en criptomonedas, principalmente Bitcoins.

Dado el impacto generado en las compañías y la necesidad de poder restablecer oportunamente la operación, el Cibercrimen ha incorporado extorsión o Ciberchantaje a la cadena criminal de este ataque.

Según INTERPOL, acceder a las pretenciones de los cibercriminales sólo contribuye a que estas redes dispongan de más recursos para sofisticar sus ataques.

Correo Electrónico

Fecha: Miércoles, 15 Feb 2019 12:42:31 +000
From: DDoS team <ddosteam@safe-mail.net>
btw: Ataque temporalmente detenido.
Si el pago no se recibe en 5 horas, el ataque se reinicia y el precio se doblará.

---------- Original Message ----------

From: DDoS team <ddosteam@safe-mail.net>
Subject: ATAQUE DDOS!
Fecha: Miércoles, 15 Feb 2019 09:32:33
Hola,
Sus cuentas son extremadamente vulnerables a un ataque DDos. Quiero ofrecerle información acerca de cómo configurar su protección y seguridad, para que no sufra de algún ataque de denegación de servicios.
Si quiere arreglarlo, consigne 1.5BTC a - 1E8R3hjksd2UhjkfsZ76SHGUJHWW6 -

En algunos casos, el cibercriminal aprovecha la proximidad de fechas clave para el negocio de la empresa objetivo del ataque y envían correos electrónicos o chats a los responsables de TI o directivos de compañías, para que transfieran pagos a cuentas y billeteras electrónicas y así suspender los ataques.

6.

MALWARE

Unsoftware malicioso

Los cibercriminales utilizan el malware con múltiples finalidades, tales como extraer información personal o contraseñas, robar dinero o evitar que los propietarios accedan a su dispositivo. Puede protegerse contra el malware mediante el uso de software antimalware.

MALWARE

El malware o software malicioso hace referencia a cualquier tipo de software maligno que trata de afectar a un ordenador, a un teléfono celular u otro dispositivo.

Se considera un tipo dañino de software si es destinado a acceder a un dispositivo sin el conocimiento del usuario consiguiendo el control de los datos y/o la información de la víctima o realizando procesos sin la autorización del titular del sistema comprometido.

El malware puede afectar equipos de cómputo, tablets, teléfonos celulares e incluso dispositivos IoT.
La motivación de los atacantes en Colombia, se basa en intereses económicos.

COLOMBIA

612%

Fue el crecimiento de los ataques de Malware en el país a en el último año.

MÉTODOS DE DISPERSIÓN DE MALWARE:

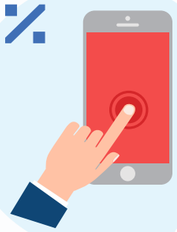
63%

Correos con notificaciones suplantando entidades públicas.

32%

Redireccionamiento hacia sitios web infectados por el atacante.

5%

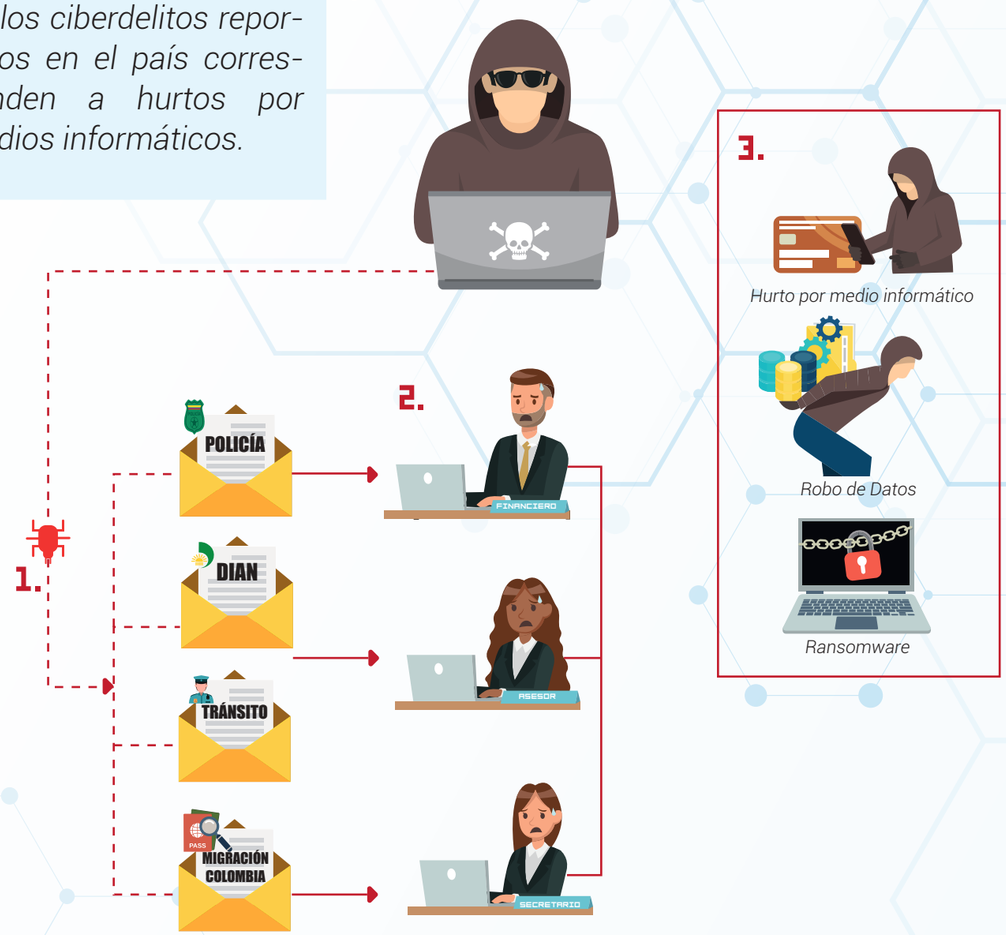


Descarga de aplicaciones maliciosas.

La infección de Malware sigue en crecimiento, pasando de 99 casos de empresas que reportaron infección de malware en su infraestructura en el año 2018 a más de 705 casos registrados durante el año 2019. Siendo las PYMES las más afectadas por estos ataques.

57%

De los ciberdelitos reportados en el país corresponden a hurtos por medios informáticos.



El vector más utilizado para la infección de Malware en las compañías sigue siendo el envío masivo de correos electrónicos con archivos adjuntos que esconden el programa malicioso a instalar por el atacante.

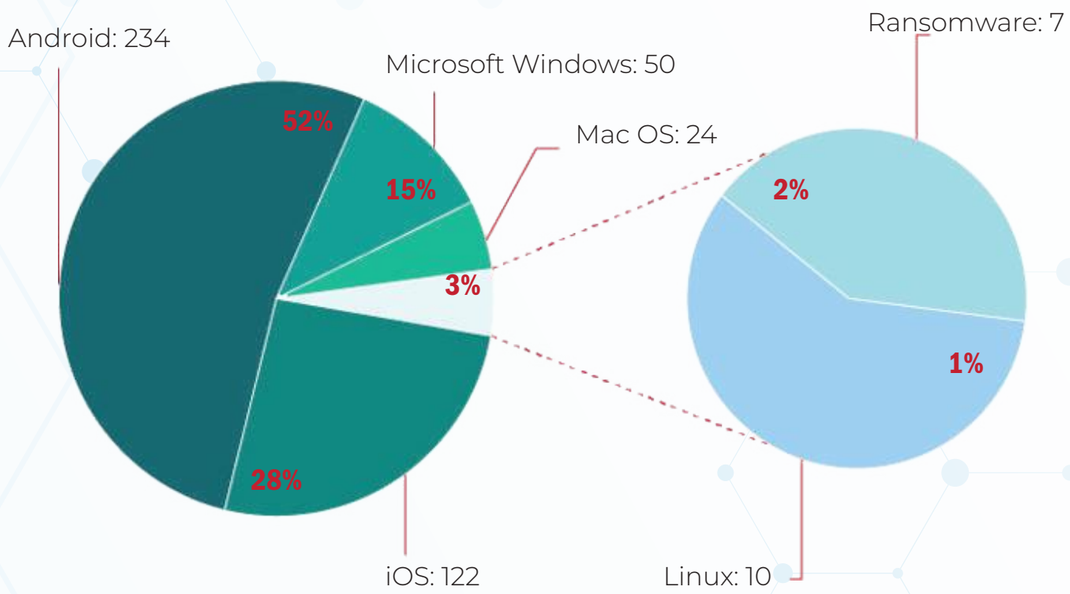
Los asuntos más utilizados como señuelo para conseguir que la víctima abra el correo, siguen siendo las alertas, notificaciones y citaciones judiciales, siendo nuevamente la suplantación de identidades gubernamentales por tercer año consecutivo.

En 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.

INFORME ANÁLISIS DE PROGRAMA MALIGNO EN COLOMBIA 2019:

Para el año 2019, se han logrado analizar un total de **447** muestras, de las cuales 33 han sido identificadas como código malicioso (Malware), correspondientes a: Virus, Troyanos, Backdoors, Rootkit, RAT, Dropper y Ransomware.

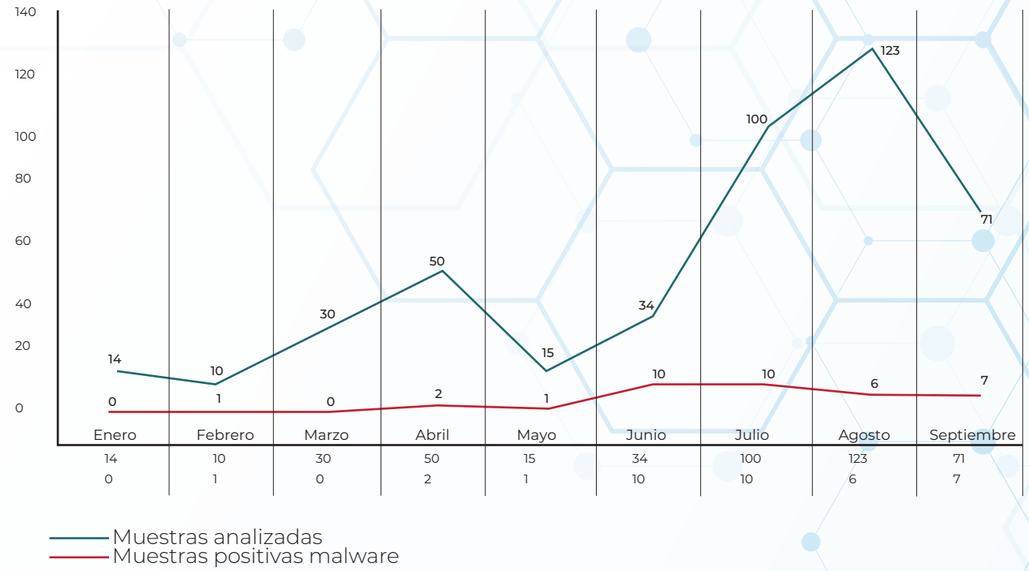
ANÁLISIS DE MUESTRAS ESTADÍSTICAS GENERAL



Muestras analizadas por Sistema Operativo- Fuente Laboratorio Informática Forense

De las cepas analizadas, un **8%** se han recibido a través del servicio de CAI VIRTUAL y el **92%** restante corresponden a solicitudes formales realizadas por diferentes despachos judiciales.

ANÁLISIS DE MUESTRAS 2019

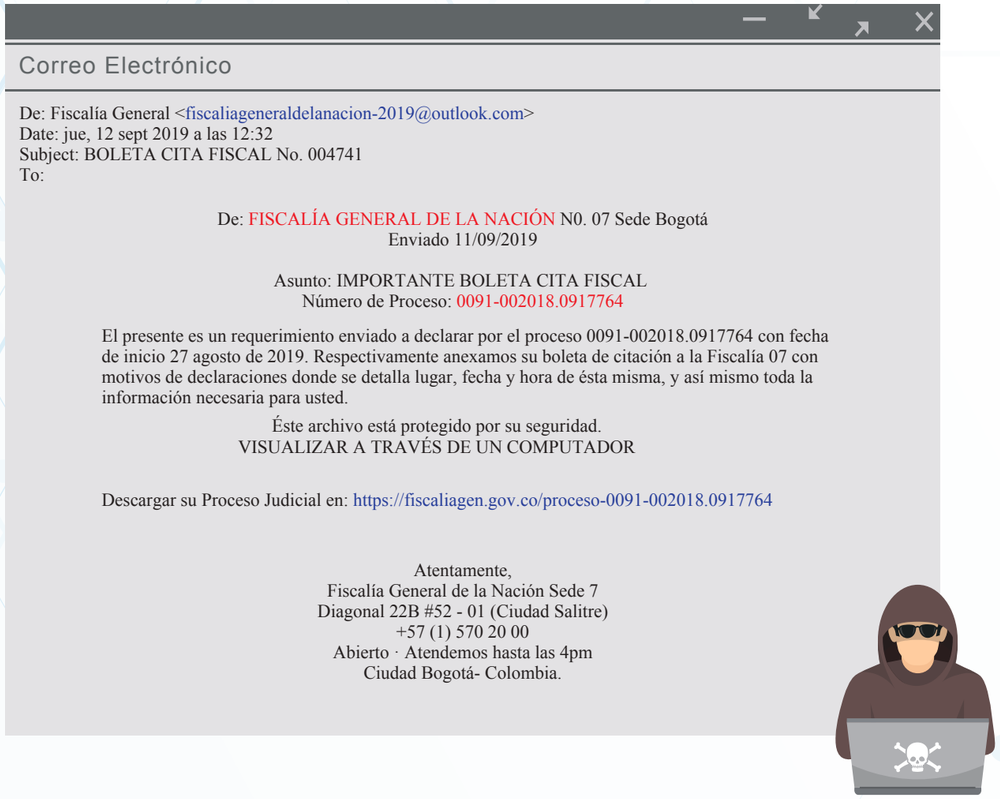


Muestras Analizadas por mes- Fuente Laboratorio Informática Forense

PRINCIPALES MEDIOS PARA PROPAGAR MALWARE:

El correo electrónico se ha convertido en el medio más utilizado por los ciberdelincuentes para realizar campañas masivas de distribución de Malware a través de la suplantación de entidades oficiales (Fiscalía General de la Nación y la Dirección de Impuestos y Aduanas Nacionales).

Mediante el uso de mensajes de engaño inducen al usuario a visitar lugares de dudosa reputación, evidenciado en la descarga de archivos de características ejecutables, que terminan vulnerando la seguridad del sistema para suplantar servicios legítimos del sistema operativo y robar todo tipo de datos.



Correo Electrónico

De: Fiscalía General <fiscaliageneraldelanacion-2019@outlook.com>
Date: jue, 12 sept 2019 a las 12:32
Subject: BOLETA CITA FISCAL No. 004741
To:

De: FISCALÍA GENERAL DE LA NACIÓN N0. 07 Sede Bogotá
Enviado 11/09/2019

Asunto: IMPORTANTE BOLETA CITA FISCAL
Número de Proceso: 0091-002018.0917764

El presente es un requerimiento enviado a declarar por el proceso 0091-002018.0917764 con fecha de inicio 27 agosto de 2019. Respectivamente anexamos su boleta de citación a la Fiscalía 07 con motivos de declaraciones donde se detalla lugar, fecha y hora de ésta misma, y así mismo toda la información necesaria para usted.

Éste archivo está protegido por su seguridad.
VISUALIZAR A TRAVÉS DE UN COMPUTADOR

Descargar su Proceso Judicial en: https://fiscaliagen.gov.co/proceso-0091-002018.0917764

Atentamente,
Fiscalía General de la Nación Sede 7
Diagonal 22B #52 - 01 (Ciudad Salitre)
+57 (1) 570 20 00
Abierto · Atendemos hasta las 4pm
Ciudad Bogotá- Colombia.

Durante los meses de Septiembre y Octubre se analizaron diversas muestras de Malware para Sistemas Operativos Android (.APKs), identificando un común denominador frente a los permisos cargados en memoria (android.permission.WRITE_EXTERNAL_STORAGE) el cual permite que se modifique la información almacenada en los dispositivos externos conectados (MicroSD), exponiendo la información del usuario e incrementado los índices de compromisos.

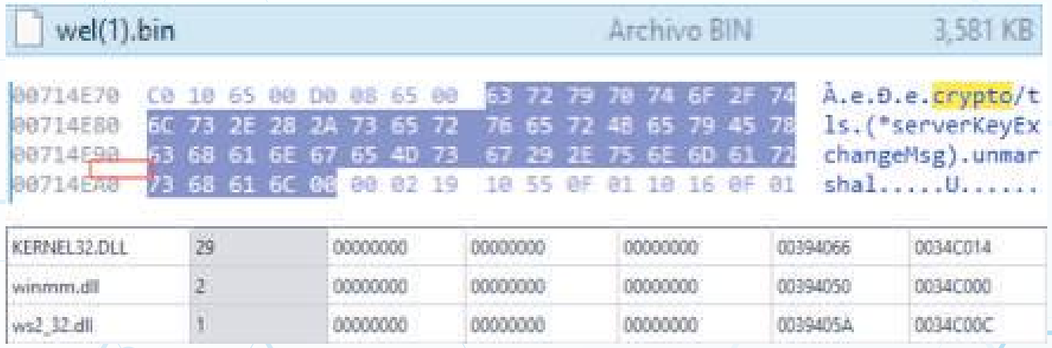
Es de aclarar que no todas las aplicaciones móviles necesitan utilizar almacenamiento interno para su funcionamiento, pero en su mayoría son usados como memoria secundaria.

MALWARE “ZEBROCY”:

“ET TROJAN APT28 / Sofacy Zebrocy Go Variant CnC Activity”

Mediante análisis realizado a un correo electrónico el cual contenía una dirección URL, se logró detectar la presencia del Malware Zebrocy de tipo Backdoor, potencialmente catalogado como peligroso, debido al alto nivel de sofisticación en su estructura, puesto que puede ocultar componentes maliciosos como Downloader´s y Troyanos en el sistema operativo Windows, además de contar con un tipo de inteligencia artificial que no le permite ejecutarse bajo ambientes controlados.

Este software permite tomar control de la máquina mediante comandos conocidos como (REG_GET_KEYS_VALUES, CMD_EXECUTE), los cuales envían al ciberatacante información sobre llaves de registro del sistema, en un lapso de entre 2 a 5 minutos, omitiendo los diferentes controles de seguridad de los diferentes antivirus.



wel(1).bin — Archivo BIN — 3,581 KB

```
00714E70  C0 10 65 00 D0 08 65 00  63 72 79 70 74 6F 2F 74  À.e.Ð.e.crypto/t
00714E80  6C 73 2E 28 2A 73 65 72  76 65 72 4B 65 79 45 78  ls.(*serverKeyEx
00714E90  63 68 61 6E 67 65 4D 73  67 29 2E 75 6E 6D 61 72  changeMsg).unmar
00714EA0  73 68 61 6C 00 00 02 19  10 55 0F 01 10 16 0F 01  shal.....U......
```

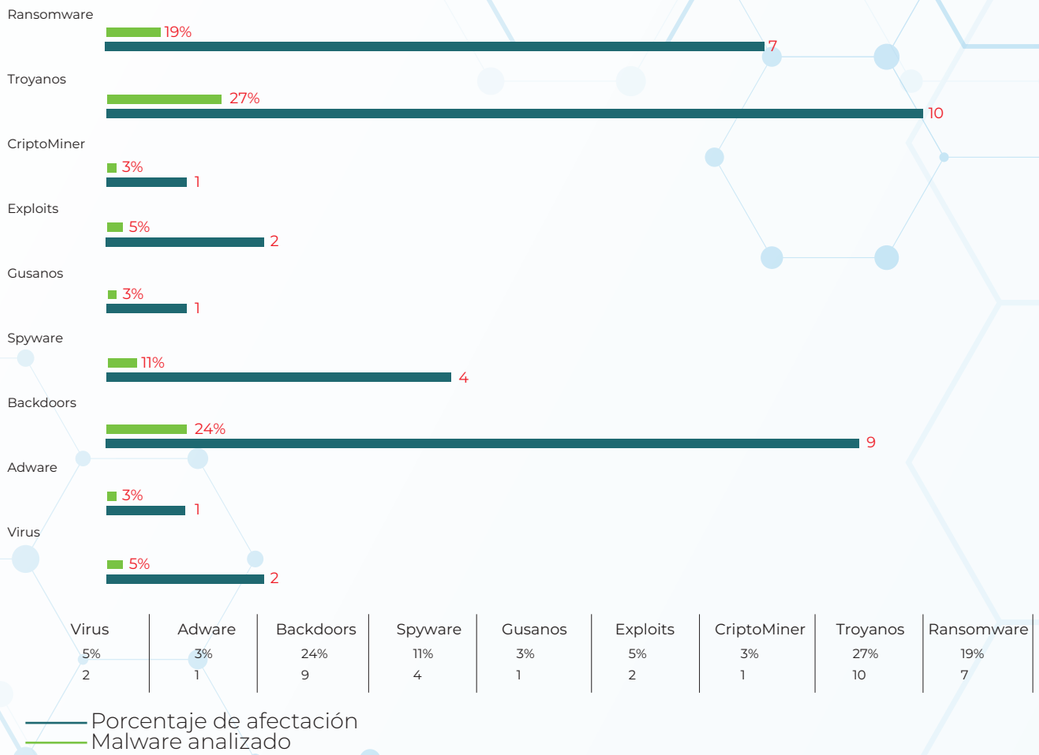
KERNEL32.DLL	29	00000000	00000000	00000000	00394066	0034C014
winmm.dll	2	00000000	00000000	00000000	00394050	0034C000
ws2_32.dll	1	00000000	00000000	00000000	0039405A	0034C00C

Tabla de Importaciones- Fuente Laboratorio de Informàtica Forense

La efectividad en que este malware logra múltiples .DLL (Bibliotecas de enlaces dinámicos), para poder realizar llamados a componentes maliciosos, demuestra una gran capacidad para escalar privilegios de usuario.

El archivo binario original utiliza packer UPX, para poder ofuscar la estructura de la tabla de importaciones, con el fin de ser indetectable por los antivirus.

37 MUESTRAS DE MALWARE ANALIZADAS



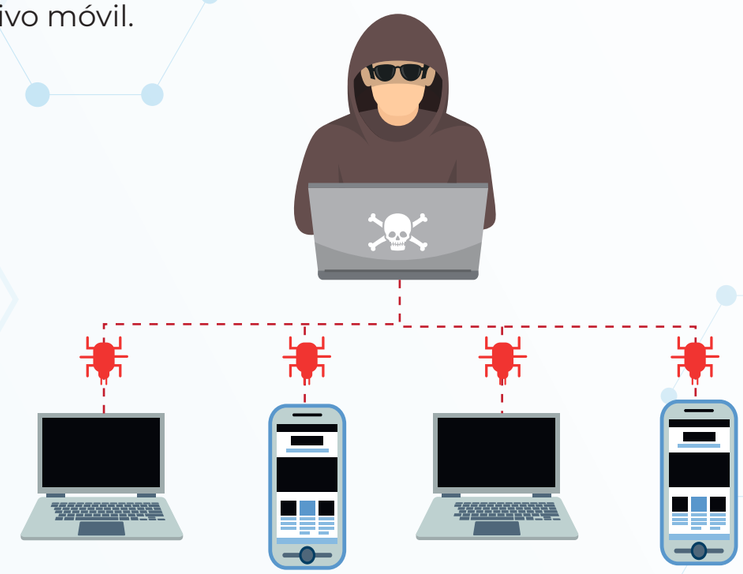
Muestras de Malware Analizadas - Fuente Laboratorio Informática Forense

Es de anotar que la muestra más analizada pertenece a Malware de tipo Troyano, siendo este un indicador de compromiso de alto riesgo, ya que por su comportamiento pueden poner en riesgo la infraestructura tecnológica de cualquier organización.

MUESTRAS MÁS ANALIZADAS:

Para el presente estudio se analizaron un total de *234 muestras* bajo la extensión APK. pertenecientes a Sistemas Operativos Android, hallando muestras positivas para Malware, de las cuales un **89%** llegan a ser Cryptominer y el otro **11%** Adware.

El método tradicional que utiliza el cibercriminal para infectar los dispositivos es el de propagar anuncios publicitarios fraudulentos por medio de las redes sociales y diferentes navegadores, con la finalidad de atraer la atención del usuario, para que ejecute la acción deseada y así lograr infectar el dispositivo móvil.



Este malware hace que se deteriore la vida útil del dispositivo, toda vez que requiere utilizar un 100% de los recursos físicos con que cuenta el mismo, para poder realizar procesos de minería en la creación de monedas virtuales.

En segundo puesto con un 27% le siguen los ejecutables con extensión .IPA con un total de 122 muestras analizadas propias de sistemas operativos iOS.

7.

SIM SWAPPING

Secuestro o cambio de SIM CARD

Este tipo de estafa explota una de las mayores vulnerabilidades de las tarjetas SIM: el hecho de que funcionan en cualquier plataforma. Lo hace gracias a lo que se conoce como "ingeniería social", la técnica de los cibercriminales para llevar a cabo el SIM swaping, el cual consiste en confundir a los vendedores de empresas de celulares y lograr que transfieran los números a tarjetas controladas por ellos.

Según datos de la Comisión Federal de Comercio de los EEUU FTC por sus siglas en inglés (Federal Trade Commission), los casos reportados por robo de identidad para la obtención de SIMCARD ante operadores de telefonía celular representan actualmente 9,8% del total de casos reportados en 2018.

Lo más complejo del asunto es que los criminales usan la "nueva" SIM CARD, para tener acceso a cuentas financieras que usan autenticación de dos factores a través de mensajes de texto (2FA).

99 *Celulares son reportados como robados en Colombia cada hora.*

30% *Hurto de celulares en Colombia en 2019.*

La autenticación de dos factores (2FA), proporciona seguridad adicional en el proceso de inicio de sesión. Utiliza la contraseña habitual para acceder a un correo electrónico o una cuenta, y además proporciona un código de verificación de un segundo dispositivo, normalmente un teléfono móvil.

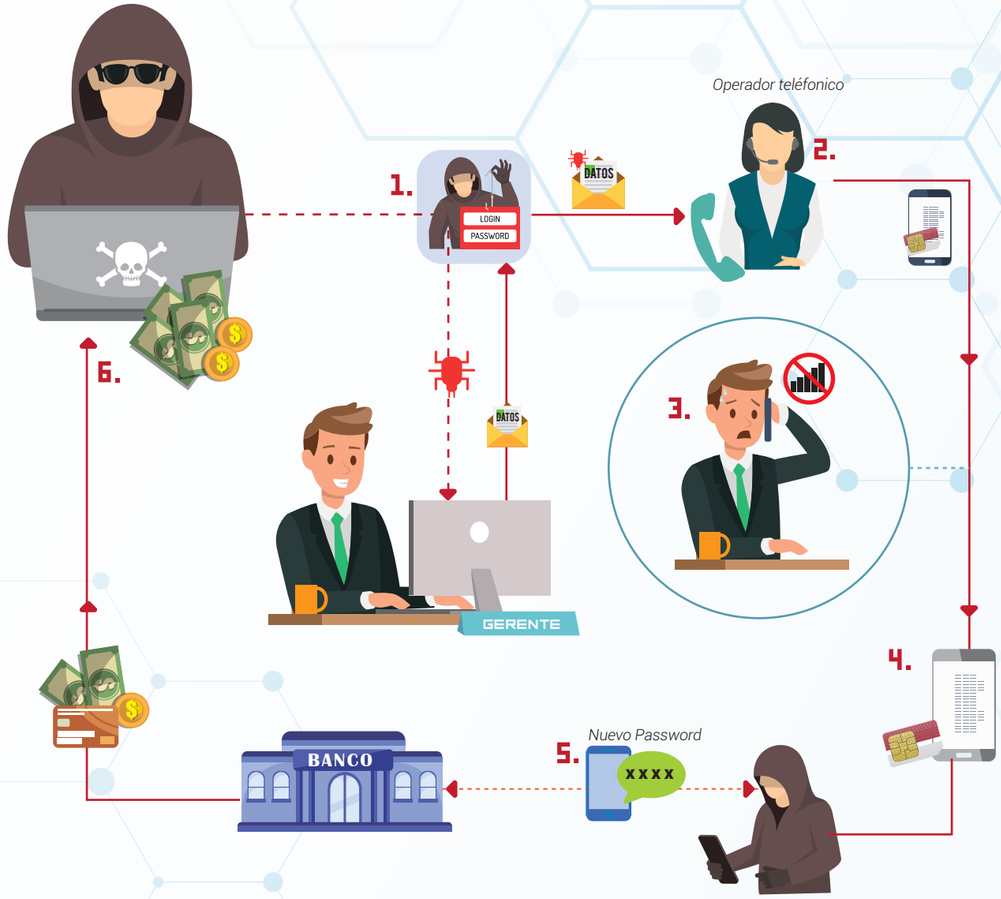
El 2FA es utilizado por servicios de correo electrónico, redes sociales, y muchas otras aplicaciones.

El duplicado de la tarjeta SIM es fundamental para obtener la doble verificación que muchos bancos utilizan para autorizar pagos y transferencias a sus clientes, generalmente un código es enviado vía SMS al teléfono celular del usuario para poder finalizar estas transacciones.

Las apps de los bancos son muy seguras, y disponen de claves de acceso, cifrado de las comunicaciones y teclados virtuales. Sin embargo, los ciberdelincuentes a través de ingeniería social, consiguen engañar por medio de técnicas de persuación y manipulación psicológica.

Cerca del 90% de los ciberataques que sufren las empresas en Colombia se deben a ingeniería social.

Los cibercriminales pueden conseguir datos de las víctimas en mercados ilegales en las darknet o bases de datos de usuarios infectados con Malware y víctimas suplantanción de identidad. Con esta información reportan como robado el teléfono ante el operador y consiguen obtener un duplicado de la tarjeta SIM de la víctima.



A continuación, consiguen suplantar al usuario en el sistema financiero y obtener el código 2FA para realizar transacciones y afectar los activos económicos de las empresas.

El SIM Swapping también es usado en la cadena criminal del BEC y permite crear chats falsos suplantando a gerentes ante las áreas financieras, consiguiendo mediante engaño la transferencia de activos a cuentas bajo control del criminal.

55% *De los ciberdelitos denunciados en Colombia son por hurto informático.*

SAFE

SIM SWAPPING

8.

CRYPTOJACKING

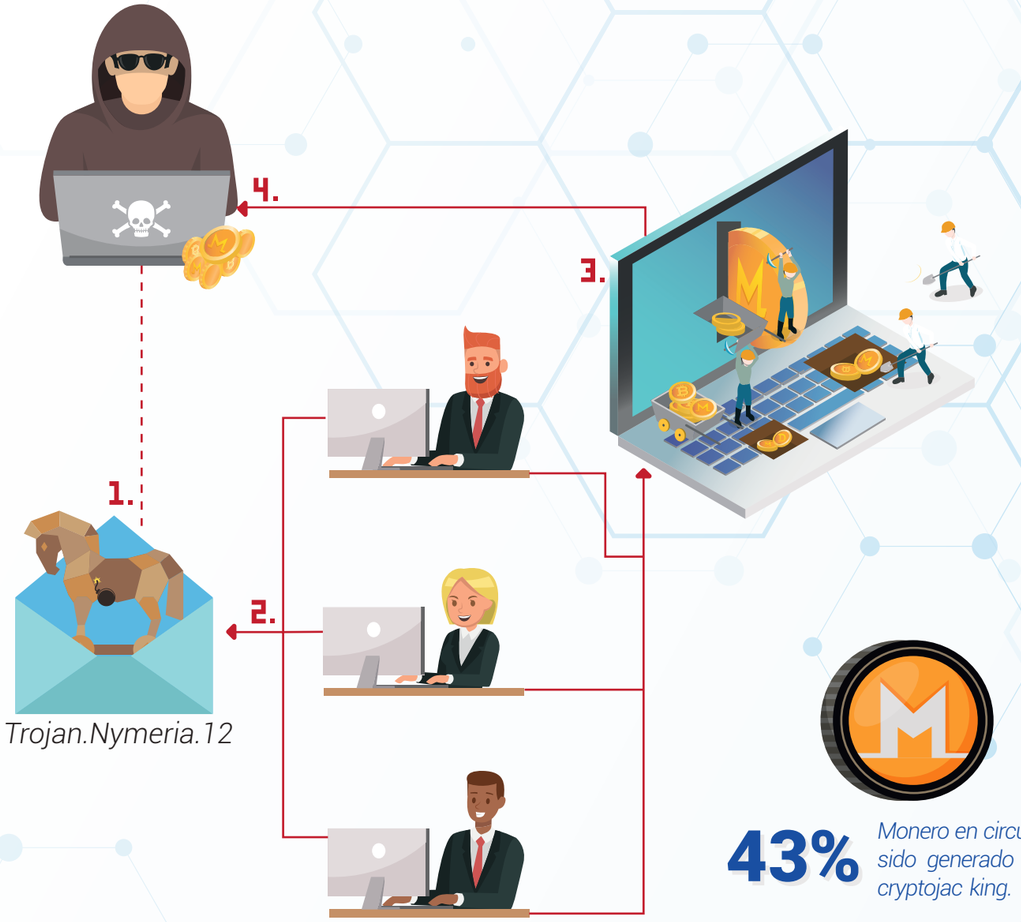
Minería de criptomonedas

El uso de un hardware del visitante de una página web sin su permiso, para minar criptomonedas es un problema para usuarios y compañías que se financian con la publicidad (el 90% de Internet). Y más ahora que el Bitcoin está batiendo récords.

Un ataque de cryptohacking tiene como objetivo generar criptomonedas por medio de comandos computacionales de un tercero.

Los cibercriminales utilizan al menos dos técnicas con las cuales se valen del poder computacional de servidores, equipos de computo e incluso teléfonos celulares de las víctimas.

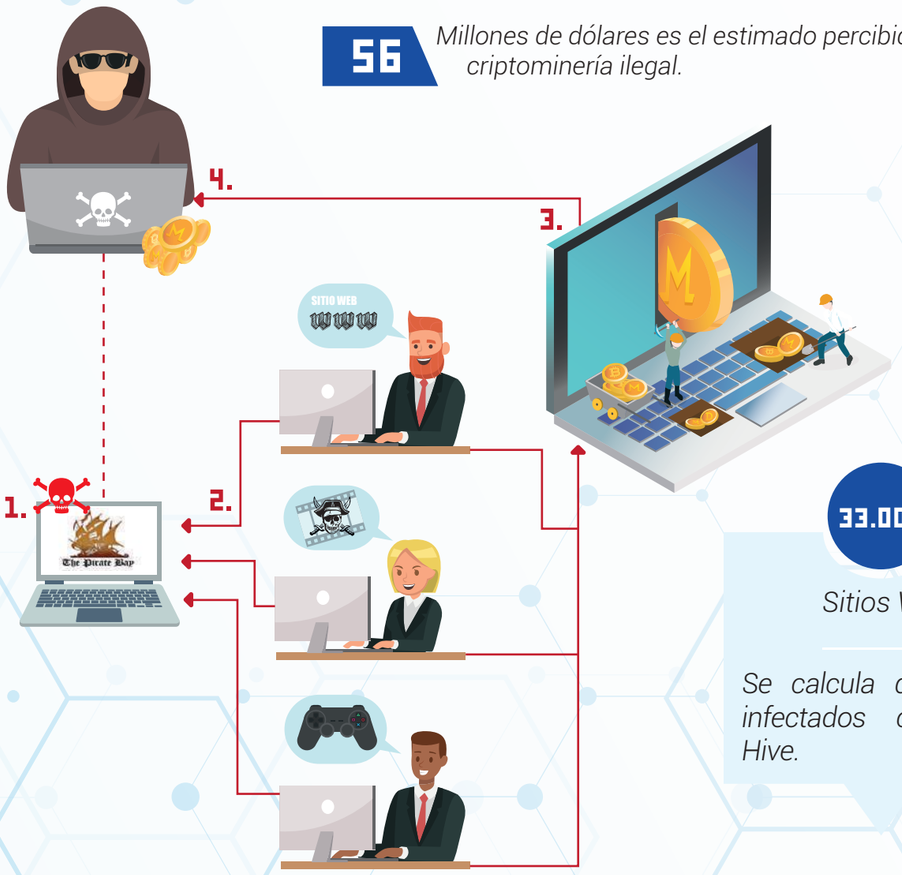
Las víctimas pueden ser objeto de ataques de Criptohacking cuando acceden a sitios web infectados. En este caso, las páginas visitadas por los empleados pueden contener un código javascript que transforma de manera pasiva y silenciosa el navegador del usuario en un criptominero. Como resultado los sistemas se ralentizan ya que la capacidad de procesamiento de la máquina afectada empieza a ser utilizada por el atacante.



Trojan.Nymeria.12

43% *Monero en circulación ha sido generado mediante cryptojac king.*

56 *Millones de dólares es el estimado percibido por la criptominería ilegal.*



33.000

Sitios WEB

Se calcula que están infectados con Coin Hive.

En una segunda modalidad, el Centro Cibernético Policial (CCP) analizó muestras de malware encontradas en correos electrónicos enviados a distintas empresas en Colombia. El resultado permitió identificar el malware “Trojan.Nymeria.12”, que se hace pasar por el Host de servicios nativos de Windows “Svchost.exe”, bajo el nombre de “Scvhost.exe”.

Las pruebas realizadas permitieron percibir un déficit del funcionamiento de la máquina, creando llaves de registro y consumo excesivo de recursos físicos usados para poder minar criptomonedas.

Este método sobrecarga los equipos y disminuye la producción de la empresa y puede sobrecargar el consumo de otros recursos.

SAFE

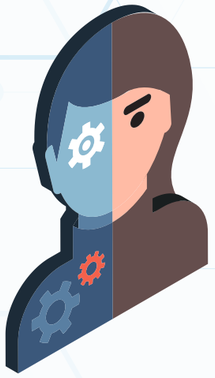
9.

TENDENCIAS CIBERCRIMEN 2020

Durante el 2020, se prevé un incremento en el número de ciberataques que utilizan inteligencia artificial, además de la automatización de ataques ya consolidados como phishing bancario a través de redes sociales.

2020 TENDENCIAS 2020

En 2020 el Cibercrimen seguirá sofisticando su actuar delictivo y utilizará las capacidades tecnológicas disponibles a su favor.



Inteligencia Artificial y Malware

El escaneo automatizado de vulnerabilidades por parte de los Cibercriminales facilitará la detección de víctimas potenciales. El Malware podrá detectar si un sistema de seguridad le está analizando (sandbox) y se auto eliminará.

Lo anterior supone un desafío adicional para los investigadores, porque estas técnicas antiforense eliminarán evidencia digital en los equipos y sistemas infectados de empresas y ciudadanos víctimas.

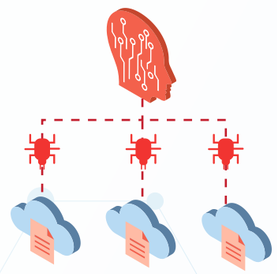
Uso de perfiles falsos en redes sociales para difusión de Malware

Cuentas falsas en redes sociales como Twitter y Facebook serán usadas para generar contenidos de manera automatizada masificando las cifras de infección de malware.

BEC basado en Deepfake

Las empresas en Colombia podrán recibir audios e incluso videos, en los cuales los cibercriminales suplanten a ejecutivos, clientes y proveedores para conseguir transferencias de dinero o despacho de productos.

La tecnología Deepfake es una técnica basada en Inteligencia Artificial, que coloca imágenes o videos sobre otro video, así como imitación de voces.



Uso de Botnet para difusión de correos extorsivos

Se prevé el incremento de casos de Sextorsión, basados en el envío masivo de mensajes por parte de los cibercriminales utilizando equipos controlados remotamente (Botnet). La tasa podrá alcanzar hasta 30 mil correos por hora.

Uso de mercados ilegales en DarkNet

El cibercrimen seguirá utilizando los foros de la DarkNet para la venta de datos bancarios en la internet Profunda. Aprovecharan creciente uso de Criptomonedas en Colombia para facilitar la dispersión de las ganancias de los Ciberataques.

SAFE

10.

RECOMENDACIONES

Para ayudar a las empresas en Colombia a poner en marcha los procesos internos con los que mejorar su ciberseguridad hemos preparado una serie de recomendaciones a implementar según el nivel de madurez y avance de su plan y marco de seguridad adoptado.

RECOMENDACIONES

El 60% de las pequeñas y medianas empresas, no pueden sostener sus negocios más de seis meses luego de sufrir un ciberataque importante.
Ésto demuestra que los factores en torno a los Ciberataques a PYMES en Colombia comprometen seriamente los activos económicos e impactan asuntos estrictamente legales y de cumplimiento de las compañías.

60%
PYMES

Recientemente fue presentado el Estándar **ISO/IEC 27701**, cuyo objetivo es proporcionar orientación sobre la protección de la privacidad, incluida la forma en que las organizaciones deben gestionar la información personal, además de ayudar a demostrar el cumplimiento de la normativa en privacidad, como el Reglamento General de Protección de Datos, en todo el mundo.

Las compañías que no dispongan de un **SGSI Sistema de Gestión de Seguridad de la Información** pueden implantar las normas ISO/IEC 27001 e ISO/IEC 27701 de manera conjunta.

Y es que la privacidad de la información sin duda es muy importante para todos los tipos de organizaciones, grandes, o pequeñas e incluso sin importar si son del sector público o privado o una entidad gubernamental o sin ánimo de lucro.

El uso del teléfono celular por parte de empleados y ejecutivos se ha convertido en otro factor de riesgo, al gestionarse desde allí **tareas tan sensibles para una organización** como el correo electrónico, puede perderse información valiosa o incluso necesitarse invertir altas sumas de dinero para recuperar datos y volver a proteger las plataformas y sistemas comprometidos.

Una **adecuada gestión del correo electrónico disminuye** la oportunidad que tienen los cibercriminales de afectar a las compañías, por lo que una adecuada política de almacenamiento de información en la nube seria de mucha utilidad establecerse por ejemplo que tipo información y durante que tiempo puede permanecer almacenada en estos repositorios virtuales.

Establecer pautas respecto a la **prohibición de uso de la cuenta de correo corporativo** para darse de alta en un servicio de interés personal tales como una aplicación de juegos, citas u ocio. Las empresas tardan meses e incluso años en enterarse que las contraseñas de correo de las cuentas de sus directivos y empleados han sido comprometidas y expuestas en foros de data leaks en internet, luego de que cibercriminales han conseguido robar información de servidores de terceros en los cuales se habían registrado empleados haciendo uso de credenciales corporativas.

SAFE

Otro aspecto para considerar en las compañías guarda una relación directa con la **política de proveedores y clientes y su relacionamiento con la Ciberseguridad empresarial**. El fraude BEC, aprovecha por ende cualquier duda o espacio que exista como punto débil de las comunicaciones entre una empresa y sus partes interesadas en la cadena productiva.

Esta ruptura o falla en el relacionamiento conlleva a que se generen por ejemplo pagos no autorizados, despachos a terceros sin validar o transferencias de activos hacia cuentas en poder de los cibercriminales. Por ello es muy importante que el **empresario defina todos los procedimientos** que se deben seguir en su organización para autorizar pagos u otros, siempre en aras de minimizar la oportunidad de fraude.

La tecnología entonces juega un papel muy importante pues **establecer mecanismos perimetrales de protección** ayuda a detectar de manera temprana muchas de las amenazas cibernéticas a las que se ven expuestas las compañías, por ejemplo, servicios antivirus, antimalware y anti-phishing deben ser considerados como esenciales a la hora de implementar la infraestructura para la operación del negocio.

Recuperarse de un ciberataque es muy importante, y las compañías deben desarrollar la ***capacidad de Ciberresiliencia*** *en un enfoque de extremo a extremo sobre tres áreas críticas: la seguridad de la información, la continuidad del negocio y la capacidad de recuperación de las redes de las empresas; para garantizar que las organizaciones sigan funcionando durante los ciberataques.*

La Ciberseguridad empresarial exige que las **organizaciones sean dinámicas e innovadoras** por ello cambiar las estructuras tradicionales puede ser una importante decisión a la hora de enfrentar amenazas, de acuerdo con su tamaño y activos a proteger las compañías deben estudiar la incorporación de la figura del CISO (Oficial o Director de Seguridad de la Información).

Cada empresa sigue un modelo organizativo diferente, por lo que las funciones del CISO pueden variar según la madurez o la actividad de la organización, pudiendo haber una fusión entre esta figura y otras como la del DPO (Data Protection Officer) o la del CSO (Chief Security Officer).

Sin importar el escenario del Ciberataque y la complejidad que este signifique para la empresa, todas las organizaciones deben prepararse para gestionar un incidente cibernético y esa labor previa involucra a todos los empleados y directivos, por lo que es muy importante **definir cuales son los roles y responsabilidades** que tiene cada uno de los actores involucrados en el plan de respuesta y gestión de un incidente cibernético.

La formación y concienciación en ciberseguridad contribuyen en esencia a que cada integrante de la organización identifique los riesgos y las amenazas a las que está expuesta la compañía y como se convierte en la primera barrera de contención de un ataque.

La Ciberseguridad es un compromiso de todos.

SAFE

GLOSARIO

GLOSARIO

ADWARE: (SOFTWARE PUBLICITARIO) Aplicaciones que durante su funcionamiento despliegan publicidad en ventanas emergentes o barras de herramientas a cambio de la gratuidad en su utilización.

ATAQUE: Explotación de una o varias vulnerabilidades utilizando un método de ataque con el fin de destruir, exponer, alterar o inhabilitar un sistema de información o la información que el sistema maneja.

BOTNET: Conjunto de ordenadores controlados remotamente por un atacante, los cuales pueden ser utilizados en conjunto para realizar actividades maliciosas como envío de spam, ataques de DDOS y códigos maliciosos.

CIBERATAQUE: Acción producida en el ciberespacio que compromete la disponibilidad, integridad y confidencialidad de la información mediante el acceso no autorizado, la modificación, degradación o destrucción de los sistemas de información y telecomunicaciones o las infraestructuras que los soportan.

CIBERDELITO: Actividad delictiva que emplea el ciberespacio como objetivo, herramienta o medio. Ejemplos: fraude, suplantación de identidad, hurto, crimen organizado, etc.

CÓDIGO MALICIOSO: Software capaz de realizar un proceso no autorizado sobre un sistema con un deliberado propósito de ser perjudicial.

DENEGACIÓN DE SERVICIO: Consiste en saturar con muchas peticiones de servicio un servidor, hasta que este no puede atenderlas todas y de esa manera provocar su colapso.

DENEGACIÓN DE SERVICIO DISTRIBUIDA: Ataque de denegación de servicio que se realiza utilizando múltiples puntos de ataque simultáneamente.

EXPLOIT: Tipo de software, fragmento de datos, o una secuencia de comandos que aprovecha un fallo o una vulnerabilidad en el sistema con el fin de tomar el control total, una escalada de privilegios o un ataque de denegación de servicio.

GESTIÓN DE VULNERABILIDADES: Proceso proactivo de seguridad consistente en identificar vulnerabilidades y reducirlas antes de que sean causa de un incidente de seguridad.

GUSANO INFORMÁTICO: Programa que puede autoaplicarse y enviar copias de así mismo de un ordenador a otro de una red. Tras su instalación en uno de éstos repite el proceso anterior, además de realizar alguna otra tarea indeseable, quizás hasta colapsar el sistema anfitrión.

PUERTA TRASERA: Tipo de software de control remoto que permite ingresar en un sistema operativo, página web o aplicación a una determinada parte de los mismos que usualmente está restringida a un usuario ajeno, evitando los métodos de autentificación usuales.

RANSOMWARE: El ransomware es un código malicioso para secuestrar datos, una forma de explotación en la cual el atacante encripta los datos de la víctima y exige un pago por la clave de descifrado.

El ransomware se propaga a través de archivos adjuntos de correo electrónico, programas infectados y sitios web comprometidos. Un programa de malware ransomware también puede ser llamado criptovirus, criptotroyano o criptogusano.

ROGUEWARE: Tipo de programa informático malintencionado cuya principal finalidad es hacer creer que una computadora está infectada por algún tipo de virus, induciendo a pagar una determinada suma de dinero para eliminarlo.

ROOTKIT: Es una herramienta que sirve para ocultar actividades ilegítimas en un sistema. Una vez que ha sido instalado, permite al atacante actuar con el nivel de privilegios del administrador del equipo. Está disponible para una amplia gama de sistemas operativos.

SANDBOX: Mecanismo de protección utilizado en algunos lenguajes o entornos de programación que limita el acceso que tiene un programa a los recursos del sistema. Un recinto restringe un programa a una serie de privilegios y comandos que le dificultan o imposibilitan el causar algún daño a la información del usuario.

SAFE

SCAM: Fraude destinado a conseguir que una persona o grupo de personas entreguen dinero, bajo falsas promesas de beneficios económicos (viajes, vacaciones, premios de lotería, etc.).

SCAREWARE: El scareware es un software malicioso que engaña a los usuarios de una computadora para que visiten sitios infestados de malware. Este scareware, que también se conoce como software de engaño, software de escaneo fraudulento o fraudware, puede darse en forma de ventanas emergentes.

SEGURIDAD DE LA INFORMACIÓN: La preservación de la confidencialidad, la integridad y la disponibilidad de la información. Puede, además, abarcar otras propiedades, como la autenticidad, responsabilidad, fiabilidad y prevención del repudio.

SPAM: Se denomina 'spam' a todo correo no deseado recibido por el destinatario, procedente de un envío automatizado y masivo por parte del emisor. El 'spam' generalmente se asocia al correo electrónico personal, pero no sólo afecta a los correos electrónicos personales, sino también a foros, blogs y grupos de noticias.

SPEAR PHISHING: Phishing dirigido de forma que se maximiza la probabilidad de que el sujeto objeto del ataque pique el anzuelo.

SEGURIDAD DE LA INFORMACIÓN: La preservación de la confidencialidad, la integridad y la disponibilidad de la información. Puede, además, abarcar otras propiedades, como la autenticidad, responsabilidad, fiabilidad y prevención del repudio.

SPYWARE: Tipo de software malicioso que al instalarse intercepta o toma control parcial de la computadora del usuario sin el consentimiento de este último.

TROYANO: Software malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero al momento de ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado.

VIRUS: Segmento de código que puede copiarse, tras la satisfacción de alguna condición lógica o temporal, para infectar otros programas, a los que ataca modificándolos, destruyéndolos, etc.

VULNERABILIDAD: Debilidad o falta de control que permitiría o facilitaría que una amenaza actuase contra un objetivo o recurso del Sistema.

ZOMBI: Es el nombre que se da a los ordenadores que han sido infectados de manera remota por un usuario malicioso con algún tipo de software que, al infiltrarse dentro del propio ordenador manipulado y sin consentimiento del propio usuario, un tercero puede hacer uso del mismo ejecutando actividades ilícitas a través de la Red.

SAFE

REFERENCIAS

Barret, B., “ATM Hacking Has Gotten So Easy, The Malware’s A Game”, https://www.wired.com/story/atm-hacking-winpot-jackpotting-game/, 2019.

Ciberresiliencia Organizacional, TicTac Tanque de análisis y creatividad del sector TIC en Colombia, http://www.ccit.org.co/estudios/ciberresiliencia-organizacional/ 2019.

Chainalysis, Crypto Crime Report: Decoding increasingly sophisticated hacks, darknet markets, and scams, 2019; CipherTrace, Cryptocurrency Anti-Money Laundering Report, 2018.

Europol, European Union Serious and Organised Crime Threat Assessment: Crime in the age of technology, 2017.

European Payments Council, 2018 Payment Threats and Fraud Trends Report, 2018.

Europol, “Authorities Across the World Going After Users of Biggest DDoS-for-hire Website”, https://www.europol.europa.

Federal Bureau of Investigation, “Business e-mail compromise the 12 billion scam”, https://www.ic3.gov/media/2018/180712.aspx, 2018.

Informe IOCTA 2019, Internet Organised Threat Assessment, EUROPOL https://www.europol.europa.eu/iocta-report, 2019.

Microsoft, “Attack inception: Compromised supply chain within a supply chain poses new risks”, https://www.microsoft.com/security/blog/2018/07/26/attack-i ception-compromised-supply-chain-within-a-supply-chain-poses-new-risks/, 2018.

SAFE

TENDENCIAS CIBERCRIMEN COLOMBIA

DATA

2019 - 2020