SECURITY REPORT

LATINOAMÉRICA 2023

ESET Digital Security
Progress. Protected.

CONTENIDOS

INTRODUCCIÓN

El **ESET Security Report** (ESR) es un informe que se publica cada año en el cual se aborda el estado de la ciberseguridad corporativa en la región y se exponen los resultados obtenidos a partir de diversas investigaciones relacionadas con campañas de ciberataques y operaciones criminales. Además de esta información se tienen en cuenta datos de la telemetría de ESET, tendencias y noticias relacionadas al ámbito de la ciberseguridad, tanto a nivel regional como global, e información obtenida de más de 1800 encuestas realizadas a profesionales de tecnología y gerencias de compañías en eventos realizados por ESET -principalmente en formato digital- en 17 países de América Latina.

Uno de los eventos más relevantes en materia corporativa durante 2022 fue la **"salida" del teletrabajo como una realidad instaurada durante 2020 y 2021**. Esto provocó una relajación de las medidas de aislamiento impuestas por la pandemia del COVID-19 que regían el año anterior, lo cual significó un abandono del trabajo remoto como obligación dando lugar nuevamente a la presencialidad paulatina y el formato de trabajo hibrido. Si la esta situación se sigue discutiendo, esta realidad laboral da lugar a diversos escenarios en materia de ciberseguridad, tanto a nivel corporativo como de usuarios particulares, que veremos más adelante en este documento.

Durante 2022, lejos de atenuarse, las tendencias en ciberseguridad y cibercrimen en el ámbito corporativo estuvieron en gran medida **orientadas a grandes ataques y caídas de bandas de ransomware**, así como al impacto de vulnerabilidades de gran criticidad y con importante presencia desde hace algún tiempo, como Log4Shell. También se observó un aumento desmedido de ataques dirigidos a la cadena de suministros.

Los datos presentados ofrecen una mirada amplia. Desde el lado ofensivo, reflejado en las preocupaciones manifestadas por las compañías y los incidentes que sufrieron, sumado al análisis de diversas investigaciones relacionadas con operaciones cibercriminales apuntando a diferentes industrias. Desde el lado defensivo, la evaluación sobre los activos de las compañías, como tecnologías de seguridad implementadas y medidas en materia de gestión. Como complemento se incluye información vinculada al presupuesto destinado a ciberseguridad, así como indicadores relacionados al trabajo remoto; dos variables que todavía hoy son importantes a la hora de analizar la estrategia de seguridad.

HALLAZGOS

A nivel global, los países de la región con mayor porcentaje de detecciones de códigos maliciosos en campañas de Phishing son **Ecuador** 8%, seguido por Costa Rica 7,2%, **Colombia** 5,7%, **Guatemala** 5,2% y **El Salvador** 5,1%.

Dos tercios de los encuestados señaló el **robo o fuga de información** como su mayor preocupación en materia de ciberseguridad. A esta le sigue la preocupación por el **acceso indebido a sistemas** (64%).

El **69%** de los encuestados **afirmó haber sufrido algún incidente de seguridad** durante el último año.

El **65%** de los encuestados asegura que el **presupuesto asignado** al área de ciberseguridad no es suficiente.

La adopción de soluciones de seguridad para **dispositivos móviles**, que el año pasado marcaba un **10%**, registró un aumento considerable y pasó a ser **21%**, aunque todavía podemos considerar que es un porcentaje bajo en relación con el total de los encuestados y la relevancia que tienen estos dispositivos entre los usuarios y también a nivel corporativo.

Las detecciones de vulnerabilidades rompieron un récord en 2022, con **más de 25 mil reportes**, lo que representa un aumento del **26%** sobre el año anterior.

Se destaca en Latinoamérica la presencia de **ransomware y troyanos** que buscan robar información y que son distribuidos mediante técnicas de ingeniería social como el spearphishing. También el uso de otras técnicas, como extensiones maliciosas para los navegadores web más populares.

PERCEPCIÓN DE LAS COMPAÑÍAS

PREOCUPACIONES

Si bien las preocupaciones en materia de ciberseguridad dependen mucho del tipo de organización, la información recopilada en las encuestas es de gran ayuda para entender los aspectos abordados posteriormente en este informe. Por ejemplo, una mayor preocupación en cuanto al **robo o la fuga de información y los accesos indebidos a sistemas** puede traducirse en la necesidad de implementar tecnologías de protección y acciones de educación. Teniendo esto en cuenta, creemos que poder comparar de forma generalista la forma en que las empresas de la región gestionan sus incidentes y acompañar esta información con datos que nos aporta la telemetría en investigaciones de ESET puede ser de ayuda para las organizaciones a la hora de realizar un análisis y evaluar su capacidad de detección de amenazas y el nivel de autoconocimiento, sobre todo teniendo en cuenta las características de los ataques más comunes en la región.

Vale destacar que estas preocupaciones pueden estar condicionadas por una multitud de factores, ya que cada organización tiene sus particularidades y varía la infraestructura tecnológica que utiliza y las medidas de protección adoptadas.

Como resultado de las encuestas realizadas a personal de compañías en Latinoamérica, la principal preocupación para las organizaciones es el **robo/fuga de información** (66%), indicador que se acompaña con la pérdida o destrucción de información manifestado por los encuestados como el punto de mayor impacto.

GRÁFICO 1. *PRINCIPALES PREOCUPACIONES DE LAS EMPRESAS DE AMÉRICA LATINA EN CIBERSEGURIDAD.*

En segundo lugar se encuentran los **accesos indebidos a sistemas**, con el **64%**. Esta preocupación, que involucra campañas que buscan realizar tareas de espionaje o el robo de archivos confidenciales, probablemente esté relacionada con el aumento de ataques que buscan explotar vulnerabilidades, que utilizan backdoors, o por el uso de códigos malicio-

sos como el ransomware o troyanos de acceso remoto (RAT, por sus siglas en inglés). En tercer lugar entre las principales preocupaciones está el **uso de recursos e infraestructura con fines maliciosos (56%)**.

Finalmente, la preocupación por la **falta de disponibilidad de servicios críticos** sufrió un ligero aumento con respecto a la edición 2022. Esto puede deberse, en parte, a la vuelta a la presencialidad en los espacios de trabajo y cómo las organizaciones fueron redefiniendo sus estrategias y arquitecturas de TI. En este sentido, si bien el 67% de los encuestados aseguró que las organizaciones en las que trabajan están preparadas para llevar adelante su trabajo de manera hibrida, muchas de ellas han ido reconfigurado esta modalidad de trabajo que presenta diversos desafíos tanto para los equipos de tecnología como para los de seguridad.

INCIDENTES REPORTADOS

En un mundo atravesado por la tecnología es lógico que los incidentes de seguridad que afectan a los activos de una organización tengan consecuencias de alto impacto. Estos incidentes pueden provocar desde la interrupción de la operatoria de servicios críticos para un país, la ruptura de la confianza de los clientes de una empresa, hasta la pérdida de dinero de manera directa.

Existen varias formas para medir la variable de incidentes provocados y una de ellas es la consulta directa a las organizaciones dentro de la región. Sin embargo, **no podemos olvidar que esto solo nos da una percepción subjetiva del estado de la ciberseguridad**, ya que la capacidad de detección de incidentes de manera interna es distinta entre las organizaciones. En este sentido, es inevitable que solo un porcentaje de los intentos de ataque que recibe una organización sean detectados.

Este porcentaje dependerá de varios factores, como la complejidad de los ataques, pero principalmente recaerá en las herramientas tecnológicas, humanas y de gestión que se utilicen dentro de la organización. En otras palabras, una organización tiene conocimiento de tantos incidentes en su red como buenas son sus capacidades de detección, más aun considerando que los ataques dirigidos aumenta año tras año.

Según las encuestas realizadas a las organizaciones de la región, el 70% considera que el phishing se presenta como un ataque de alta probabilidad de ocurrencia, seguido de la infección con códigos maliciosos (63%) y el robo de credenciales de acceso (56%). Por otro lado, el 30% de los encuestados aseguró haber sufrido algún incidente de seguridad en los últimos 12 meses.

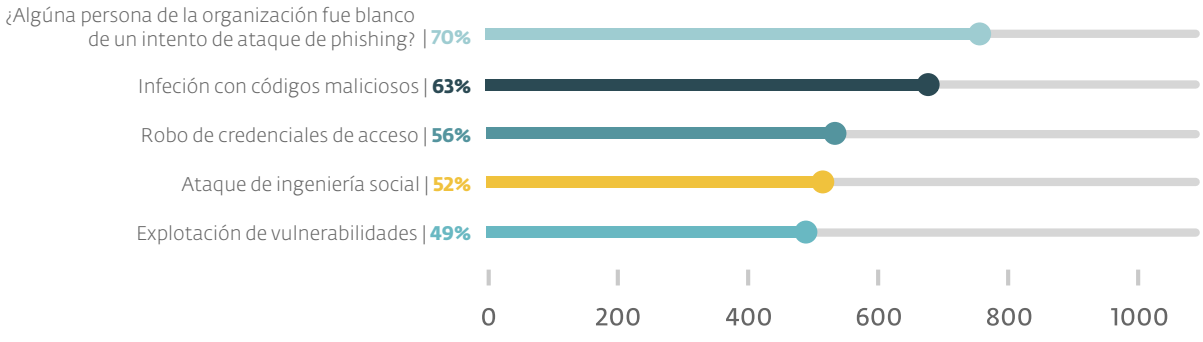

GRÁFICO 2. *CIFRAS QUE ARROJARON LAS ENCUESTAS AL CONSULTAR LOS TIPOS DE ATAQUES QUE RECIBIERON LAS ORGANIZACIONES EN 2022.*

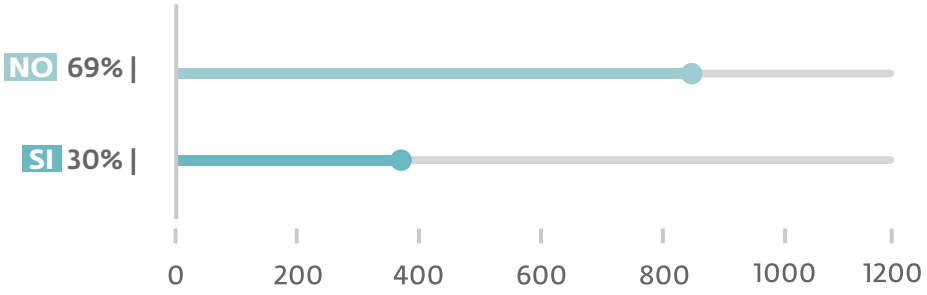

GRÁFICO 3. *USUARIOS QUE HAN SUFRIDO INCIDENTES DE SEGURIDAD EN LOS ÚLTIMOS 12 MESES*

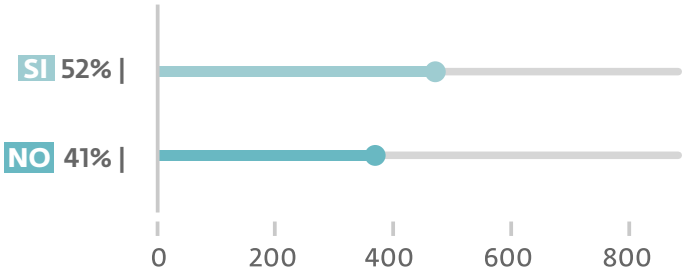

GRÁFICO 4. *USUARIOS QUE NO HAN SUFRIDO INCIDENTES Y CUENTAN CON TECNOLOGÍA SUFICIENTE.*

Si analizamos los datos de las encuestas, la mitad aseguró no haber sufrido incidentes de seguridad durante el último año y afirman contar con tecnología suficiente para gestionarlos. Sin embargo, si consideramos que año tras año aumenta la cantidad de detecciones maliciosas la lectura podría ser que la mitad de los encuestados no reconoció incidentes de seguridad en los activos de su organización, más allá de efectivamente haberlos sufrido o no.

INCIDENTES

A la hora de hablar del estado de la ciberseguridad de una organización es importante conocer no solo lo que sucede dentro de la misma, sino también incorporar una visión integral que contemple el contexto regional. Al analizar campañas maliciosas en América Latina y revisar los métodos de infección más utilizados podemos encontrar factores comunes que aportan a las compañías información útil a la hora de proteger una organización.

Como ya mencionamos en años anteriores, **cada vez son más las facilidades que existen para cometer ciberataques**, tanto por actores independientes como por grupos cibercriminales que deciden aceptar u ofrecer empleo para ampliar su red de ciberataques y de este modo ganar más dinero en menos tiempo. Los objetivos preferidos por los ciberatacantes son las empresas y organismos públicos, ya que son blancos con gran potencialidad en cuanto a los réditos económicos que pueden obtener.

Uno de los vectores de propagación más utilizados y que es el punto de partida de muchos de los ataques que afectan a las organizaciones es el phishing. Según los datos de la telemetría de ESET en Latinoamérica, los países con mayores niveles de detección de este tipo

de amenaza son Ecuador, Costa Rica, Colombia, Guatemala y El Salvador:

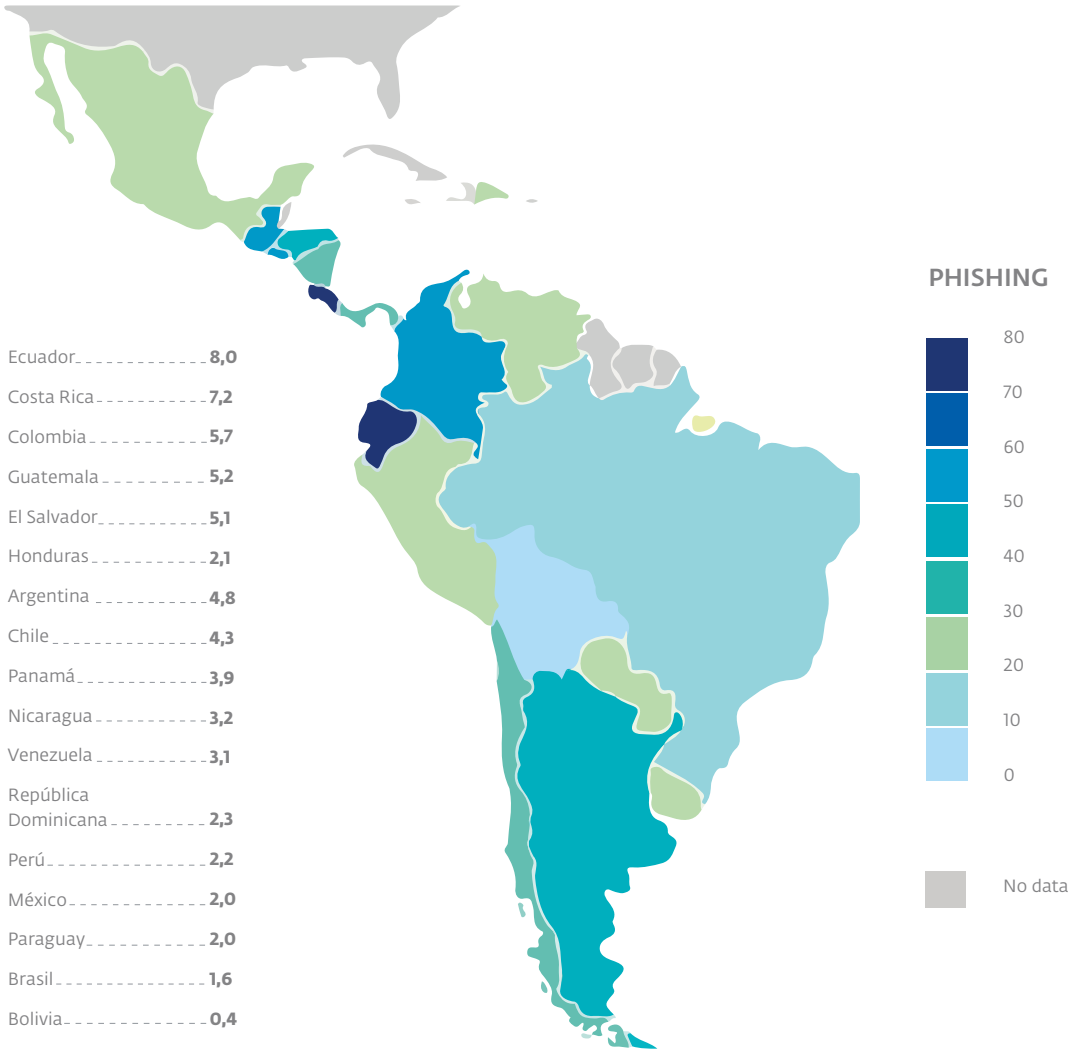

Gráfico 5. *Países de América Latina con mayor cantidad de detecciones de phishing en 2022*

Los datos corresponden al índice de detección, que toma valores entre 1 y 10 y que es calculado a partir de la relación entre la cantidad de detecciones de campañas de phishing y la cantidad de detecciones por territorio, normalizado de acuerdo al tamaño de cada país. Teniendo este tipo de medición, Ecuador resulta ser el país con mayor índice de detección de este vector de compromiso.

RANSOMWARE

Según las encuestas realizadas, el 96% de los organizaciones manifiesta una especial preocupación por el ransomware como amenaza informática, y solo el 21% reconoce haber sido blanco de un ataque de ransomware en los últimos dos años. Dentro de este último grupo, el 77% asegura haberse recuperado utilizando backups, mientras que solo el 4% afirma haberse recuperado pagando un rescate. Sin embargo, el 84% de los encuestados totales niega estar dispuesto a negociar el pago de un rescate.

Durante el año 2022 el ransomware ha sido el protagonista de varios incidentes de seguridad en la región. La situación incluso ha llegado a poner en jaque a gobiernos enteros, como el de Costa Rica, donde se declaró la emergencia nacional tras una serie de ataques protagonizados por los grupos de ransomware Conti y Hive. Tras este incidente, el gru-

po Conti pareció esfumarse o, más bien, cambiar de identidad, algo muy común entre los grupos de ransomware como servicio (RaaS) cuando notan que están atrayendo demasiada atención por parte de las autoridades.

EN 2022 UNA OLA DE ATAQUES DE RANSOMWARE QUE AFECTARON A ORGANISMOS GUBERNAMENTALES DE COSTA RICA LLEVARON AL PAÍS A DECLARAR LA EMERGENCIA NACIONAL.

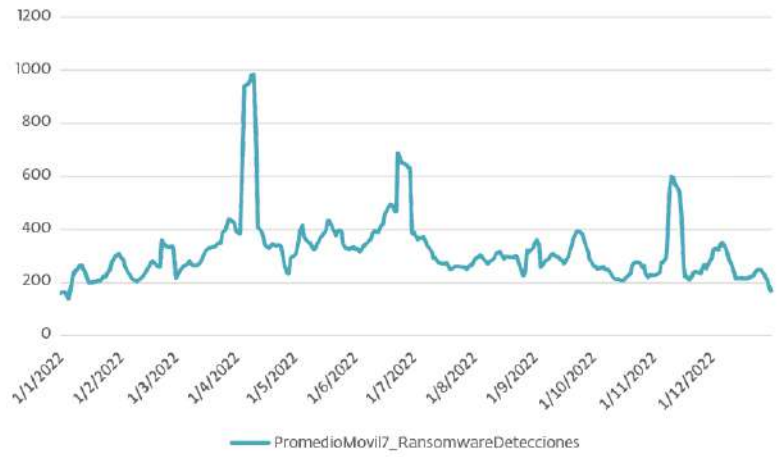

Gráfico 6. *Promedio móvil (7 días) de detecciones de ransomware durante 2022*

Actualmente el ransomware continúa siendo una amenaza con gran presencia en la escena de los ciberataques y probablemente lo siga siendo en el corto y mediano plazo. Los datos de la telemetría de ESET muestran un incremento considerable de detecciones durante 2022, año en el que se registró un nuevo récord en materia de detecciones sobre este tipo de malware.

Por otra parte, es importante entender que muchas campañas que distribuyen ransomware son complejas, ya que comienzan con la distribución de otros tipos de malware que una vez que comprometen los equipos de las víctimas descargan un ransomware. **Varios de estos ataques comienzan con un correo de phishing y son interrumpidos por tecnologías de seguridad, como las soluciones de ESET**, por lo que no siempre llegan a desplegar el ransomware final, sino que se detectan y detienen otros códigos maliciosos utilizados en etapas previas. Hablamos de exploits de vulnerabilidades, droppers, downloaders o botnets. De las más de 400 familias de ransomware distintas que fueron detectadas durante 2022,

Gráfico 7. *Top 10 familias de ransomware con mayor cantidad de hashes detectados durante 2022*

el 70% de las detecciones corresponden a solo 10 familias de este tipo de malware. Estas detecciones incluyen campañas de distribución masiva que **infectan a sus víctimas mediante descargas de cracks o programas fraudulentos**, comunicaciones maliciosas vía correos electrónicos o aplicaciones de mensajería instantánea.

Muchos de estos códigos maliciosos del tipo ransomware suelen ser genéricos y solo cuentan con la capacidad para cifrar archivos y extorsionar a la víctima para obtener una ganancia monetaria. En este sentido, Filecoder.STOP.A lidera la cantidad de detecciones y **refiere a un típico ransomware que cifra los archivos del sistema infectado pidiendo una remuneración a su víctima para descifrar los archivos comprometidos**, y es lógica la gran cantidad de detecciones ya que no se distribuye en campañas altamente dirigidas, sino todo lo contrario: se propagan a través de cracks o keygens. Esta situación demuestra claramente la falta de madurez y de conciencia por parte de las personas que optan por descargar software pirata.

Por otra parte, las detecciones de WannaCry (Filecoder.WannaCryptor) corresponden a la mitad de las detecciones y agrupan diferentes variantes de este popular ransomware. Esta es otra muestra más de la existencia de equipos tanto personales como corporativos que no son actualizados periódicamente, situación que se puede relacionar también con la falta de madurez y concientización a la hora de llevar adelante políticas de seguridad robustas y consecuentes.

SPYWARE

La incorporación de nuevas aplicaciones para resolver tareas tanto domésticos como profesionales también implica mayor cantidad de información que se vuelca a medios digitales, lo cual incluye datos financieros, accesos a cuentas, información gubernamental o de salud. Este aumento de la superficie de ataque es aprovechado por los actores malintencionados que ven cómo se amplían sus posibilidades para llevar adelante ataques que amplifican los volúmenes de información robada que se ofrece en mercados clandestinos, las extorsiones a las víctimas para no revelar la información o la ejecución de otros ataques usando datos previamente robados.

Ante este contexto, cada vez es más frecuente encontrar amenazas diseñas específicamente para el robo de datos y el espionaje utilizando malware del tipo spyware. En esta categoría encontramos a los keyloggers, RAT (o herramientas de acceso remoto), troyanos bancarios, infostealers, entre otras amenazas que contienen alguna funcionalidad para el espionaje.

CADA VEZ ES MÁS FRECUENTE ENCONTRAR AMENAZAS DISEÑADAS ESPECÍFICAMENTE PARA EL ROBO DE DATOS E INFORMACIÓN

Desde el laboratorio de investigación de ESET Latinoamérica hemos analizado distintas campañas dirigidas a compañías y organismos públicos de la región con el objetivo de robar información.

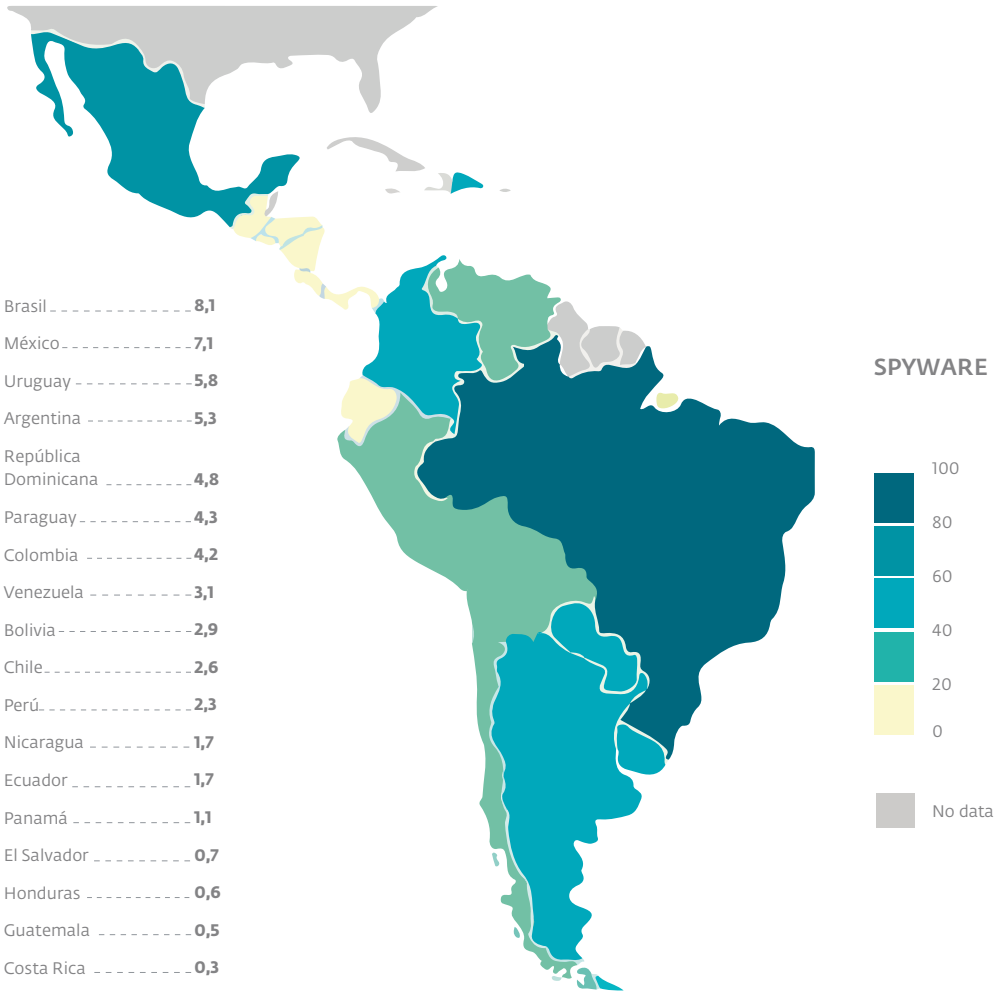

Gráfico 8. *Países con más detecciones de spyware en América Latina durante 2022*

Según los datos de la telemetría de ESET, el país con un mayor índice de detección de este tipo de amenaza es Brasil, con 8,1, muy cercano al nivel máximo 10. Le sigue México, con el 7,1. Esto, sin embargo, representa una parte de las piezas de código malicioso que roban información, ya que la gran mayoría suele contener solamente módulos secundarios con funcionalidades de espionaje y robo de información, pero no es su objetivo primordial, como el ransomware y cierta clase de troyanos.

TROYANOS

El 2022 fue un año en el que no solo se alcanzaron cifras record en cuanto al descubrimiento de vulnerabilidades en diferentes aplicaciones y sistemas, sino también en la cantidad de ataques y las pérdidas económicas como consecuencia de ellos.

Gran parte de los ataques dirigidos el último año involucraron el uso de familias más genéricas de troyanos, como son los dropper o downloader. **Estos se encargan de ingresar a los sistemas de la víctima y descargar una segunda amenaza en el equipo**, además de generar persistencia. De esta manera los cibercriminales logran eludir reglas o controles de seguridad que sean demasiado estrictas. Además, utilizar códigos maliciosos genéricos para la primera etapa de los ataques es una estrategia que permite revelar menos información de los actores maliciosos y de su intención detrás de los ataques.

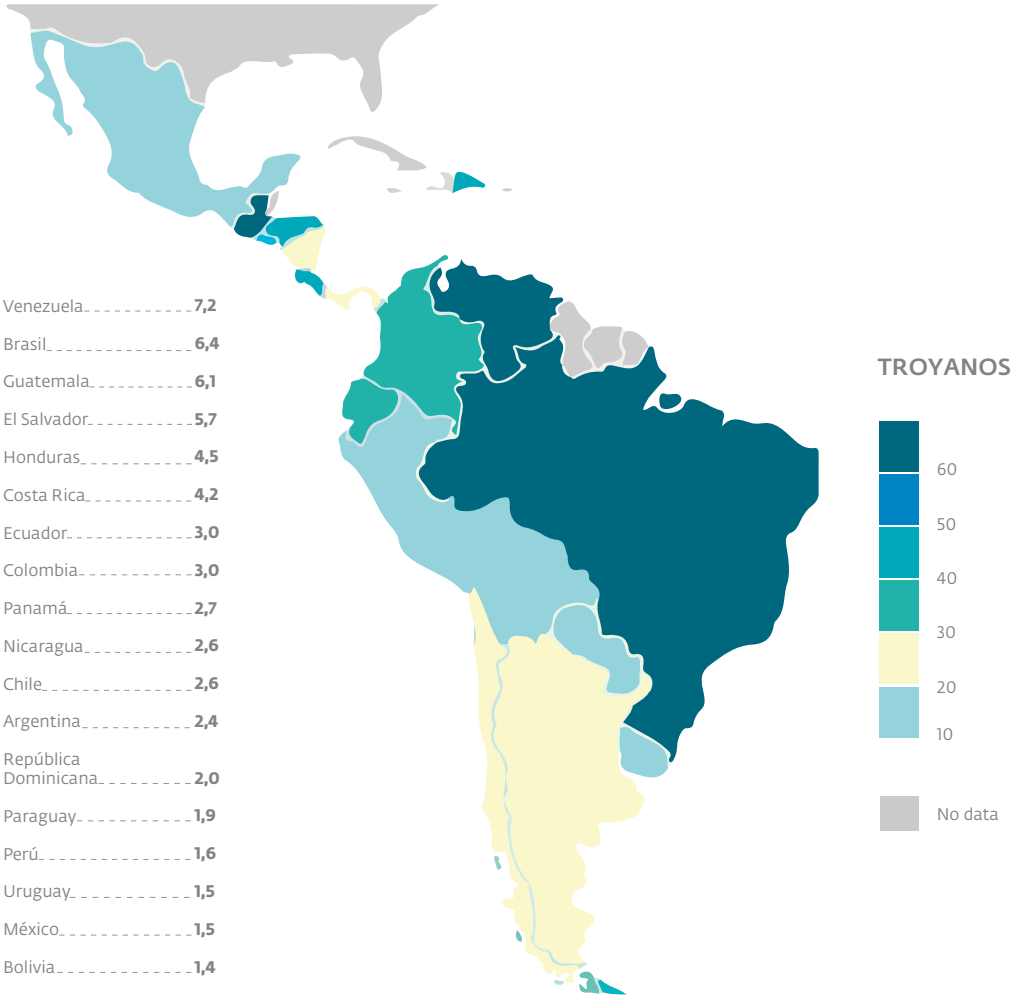

Gráfico 9. *Países con más detecciones de spyware en América Latina durante 2022*

CONTROLES

La protección de los activos de las compañías en Latinoamérica es una preocupación cada vez más creciente y las organizaciones buscan establecer medidas para combatir las distintas amenazas que pueden exponerlas a riesgo. A la hora de establecer controles podemos diferenciar aquellos basados en tecnología, como una solución de firewall, y aquellos relacionados con la gestión, centrados en concientizar o generar procesos en materia de protección de información, entre otros aspectos.

SOLUCIONES DE SEGURIDAD

Las medidas de protección más conocidas y adoptadas se componen por programas, reglas y monitoreo tecnológico. Estas ayudan a prevenir o detectar ataques complejos, que no necesariamente requieren de interacción humana, como lo podría ser una explotación de vulnerabilidad o una denegación de servicio distribuida (DDoS). En este sentido, las modalidades de empleo como el teletrabajo y el trabajo híbrido han modificado las estrategias de seguridad y las tecnologías necesarias, dado que los límites de la seguridad de las organizaciones se han corrido.

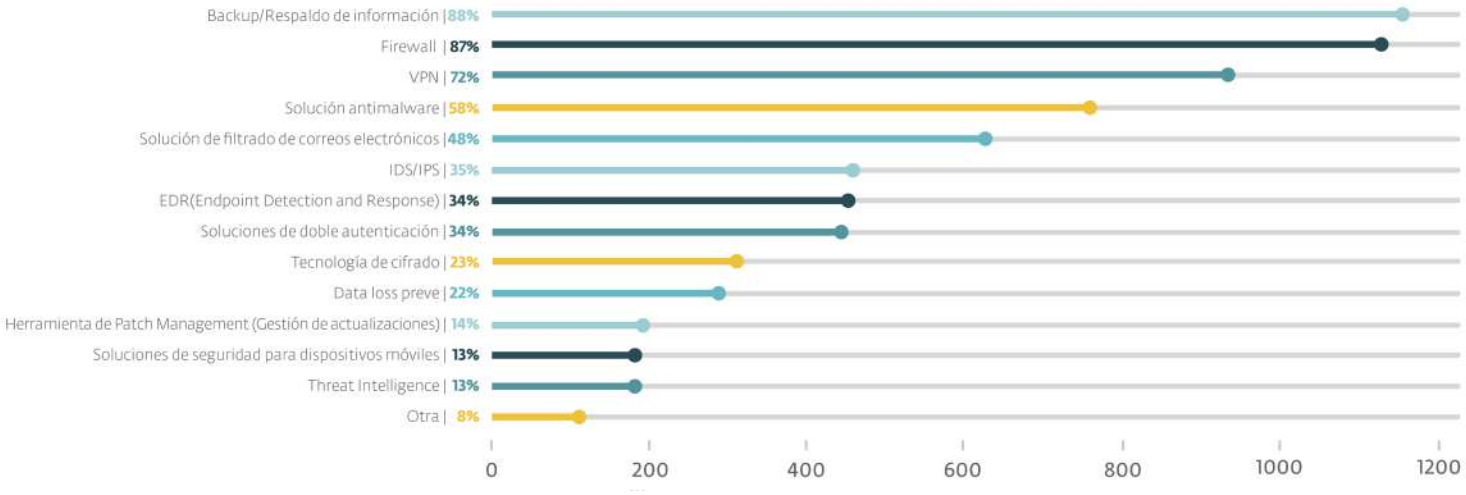

Gráfico 10. *Tecnologías de seguridad más implementadas en las empresas de América Latina en 2022*

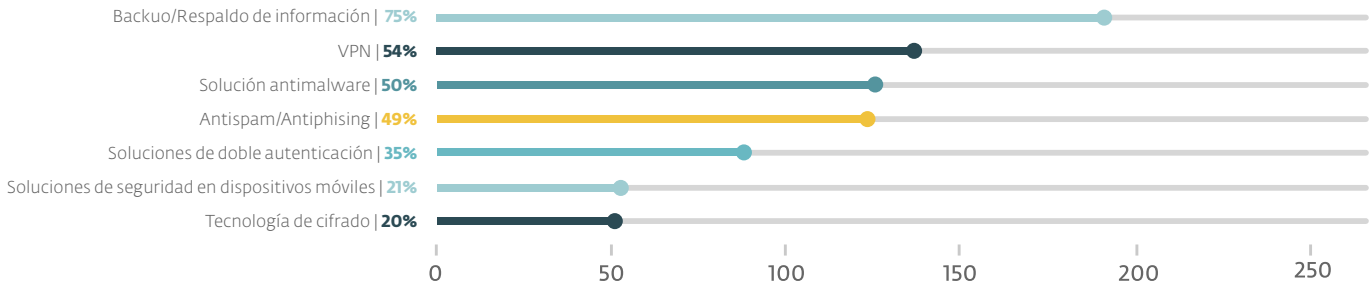

Gráfico 11. *Herramientas de seguridad más implementadas en los dispositivos de trabajo en 2022*

Probablemente, debido a que una gran cantidad de organizaciones fue víctima de ataques de ransomware y de otras amenazas que afectaron directamente a la información, el 2022 marco una nueva tendencia en cuanto a las prioridades. **La tecnología de seguridad más implementada en los entornos de las organizaciones fueron los sistemas de Backup (88%) en el 75% de los dispositivos de trabajo**. La segunda tecnología más implementada fue el Firewall (86%) y en tercer lugar las soluciones VPN. Esta últiima ha sido adoptada por el 72% de las organizaciones y el 54% de los equipos de trabajo utilizan este tipo de soluciones.

Las soluciones antimalware (60%) son la cuarta tecnología más implementada por las organizaciones y vale mencionar que en años anteriores ocupaba el primer puesto. Esta situación tal vez esté relacionada con el rediseño que muchas organizaciones han estado atravesando debido al teletrabajo y el trabajo híbrido que han difuminado el perímetro corporativo. Pero además de las soluciones tecnológicas, establecer un modelo definido de trabajo resulta vital para proteger los activos con una buena estrategia de seguridad.

Si bien 2022 rompió muchas de las tendencias que se venían sosteniendo durante los úl-

timos años, como fue la mayor adopción de soluciones de Backup, vale la pena mencionar que esta no es la única solución disponible. **Es importante que se complementen este tipo de soluciones en un esquema de seguridad que tenga en cuenta los distintos puntos de fuga que puede tener una organización**. En este sentido, el acompañamiento con herramientas como DLP (Data Loss Prevention) o tecnologías de cifrado, que todavía siguen presentando un bajo porcentaje de adopción, podría ser una gran opción.

Finalmente, la adopción de soluciones de seguridad para dispositivos móviles sigue siendo baja con apenas el 13%. Las organizaciones deben prestar atención a este dato, ya que el interés de los cibercriminales por los dispositivos móviles corporativos está en aumento y cada vez hay más amenazas dirigidas a dispositivos móviles que buscan robar credenciales bancarias.

PRÁCTICAS DE GESTIÓN

Como complemento a las herramientas tecnológicas implementadas se encuentran las prácticas y políticas de gestión de la ciberseguridad en las compañías. Estas no solo son cruciales para prevenir incidentes, sino también para restaurar la operativa luego de un ataque informático.

Según las encuestas realizadas por ESET dentro de Latinoamérica, el 81% de las organizaciones cuenta con una política de seguridad, lo que representa un aumento del 10% con respecto al 2022, mientras que el 41% de las organizaciones cuenta con un plan de respuesta a incidentes, cifra que representa un 4% más que el año anterior. Este aumento en las prácticas de gestión adoptadas se podría interpretar como una puesta en acción por parte de las organizaciones en relación a sus preocupaciones.

EL 81% DE LAS ORGANIZACIONES CUENTA CON UNA POLÍTICA DE SEGURIDAD

Las auditorias permiten evaluar diferentes aspectos de una organización y permiten luego tomar decisiones y armar estrategias de negocio y seguridad. Según las encuestas, solo el 33% de las organizaciones realiza auditorías de seguridad al menos una vez al año y un 20%

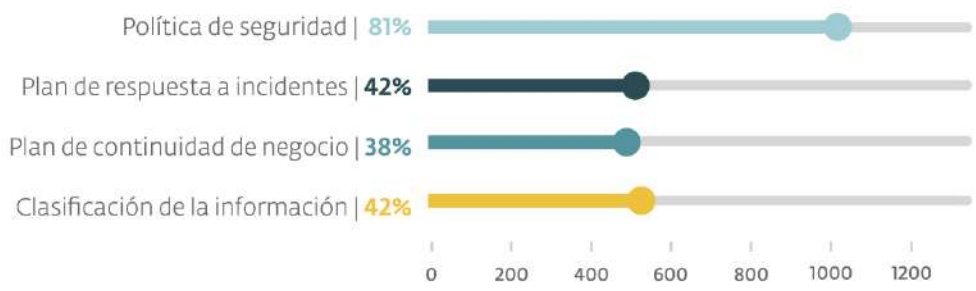

Gráfico 12. *Prácticas de gestión más adoptadas por las organizaciones de la región en 2022*

asegura nunca haber realizado una. En ambos casos los porcentajes son bajos.

Respecto a las auditorias de tipo pentesting solo 8% asegura realizarlas más de una vez al año y el 36% asegura nunca haberlas realizado. **En cuanto a los análisis de vulnerabilidades, 25% de las organizaciones asegura realizar este tipo de evaluaciones una vez al año y el 17% nunca**.

Es importante comprender que este tipo de auditorías son un punto de partida para tomar otras acciones y deben ejecutarse con periodicidad para poder hacer un seguimiento de los cambios tecnológicos y de seguridad que se quieren implementar dentro de la organización.

Con respecto a la aplicación de parches de seguridad, el 45% de las empresas asegura realizar actualizaciones de seguridad más de dos veces al año, mientras que el 27% asegura haber contratado un seguro contra riesgos cibernéticos.

Con respecto a las acciones de capacitación y concientización, solo el 28% de los encuestados afirma tener capacitaciones dentro la organización. De ese porcentaje, el 51% afirma que las capacitaciones se desarrollan de manera esporádica y solo el 24% afirma recibirlas de manera periódica.

PRESUPUESTO

El 65% de los profesionales encuestados manifiesta que necesitan mayor inversión en seguridad. Todo esto en un contexto global donde la economía se ha visto afectada durante el año 2022.

Si bien las economías más afectadas vieron en 2022 un resurgimiento de su actividad, también es cierto que las organizaciones han tenido que cambiar tanto a nivel infraestructura

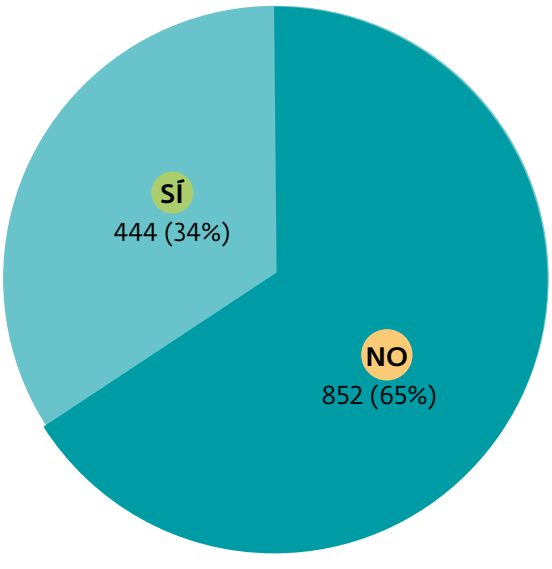

Gráfico 13. *Respuesta de las empresas ante la consulta de si consideran que el presupuesto asignado a ciberseguridad es suficiente o no*

física como tecnológica. Esto provocó inestabilidad traducida no solo en falta de dinero, sino también en perdida de toma de decisiones ya que la situación en sí genera la necesidad de repensar las estrategias de negocio a partir de la incertidumbre que provoca para los negocios la redefinición de un nuevo modelo de vida a nivel mundial.

VULNERABILIDADES, UNA VÍA DE ENTRADA ESENCIAL

Por el hecho de estar creada por humanos, toda pieza de software puede presentar errores en su desarrollo que dan lugar a vulnerabilidades o fallas que luego son aprovechadas por ciberatacantes para comprometer los sistemas de una empresa. De hecho, el 2022 fue histórico en la cantidad de vulnerabilidades detectadas en diversas aplicaciones y sistemas. En este sentido, los ciberatacantes siempre están buscando vulnerabilidades en las aplicaciones más utilizadas por las organizaciones y usuarios con la intención de sacar réditos sobre ellas a partir de la explotación mediante la inyección de códigos maliciosos y robar información. Como podemos apreciar en la imagen anterior, 10 familias de exploits cubre el 85% de detecciones totales de este tipo de amenaza en LATAM. Estos exploits apuntan a vulnerabilidades que fueron detectadas en programas ampliamente utilizados en el mundo corporativo. Por ejemplo:

EL 2022 FUE HISTÓRICO EN LA CANTIDAD DE VULNERABILIDADES DETECTADAS

Detecciones

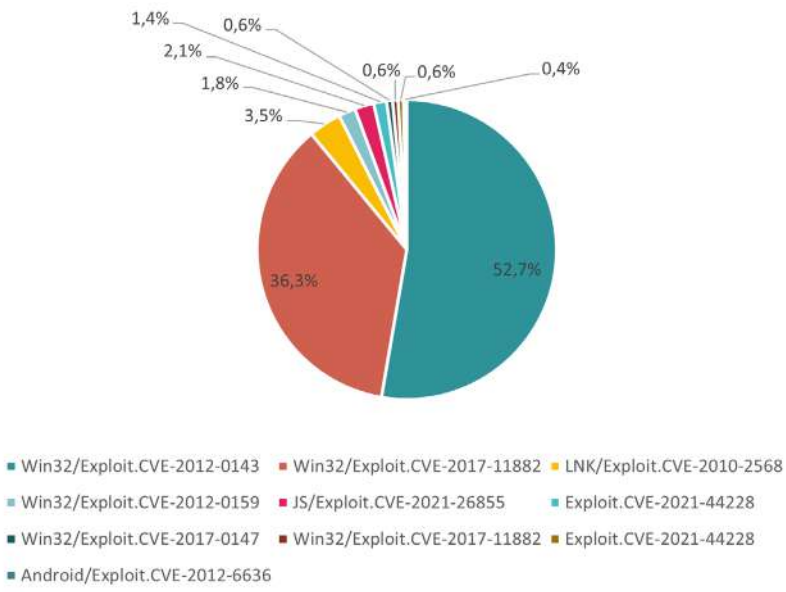

Gráfico 14. *Inversión en seguridad de las empresas de América Latina.*

CVE-2012-0143: Disponible en versiones 2003 (Windows) y 2008 (Mac) de aplicaciones de manejo de documentos de ofimática. Permite la ejecución de código remoto y toma de control del dispositivo.

CVE-2010-2568: disponible en Windows 7, Server 2003 y Server 2008. Permite la ejecución de código remoto y toma de control total del dispositivo, con criticidad alta. Fue utilizada en una campaña del gusano Stuxnet durante el año 2010.

CVE-2012-0159: disponible en versiones 2003, 2007 y 2010 de productos de Windows Office. Permite la ejecución de código remoto.

CVE-2021-26855: disponible en versiones 2019 de Microsoft Exchange. Permite la ejecución de código remoto, sin requerir autenticación previa.

Algo que vale la pena destacar es que algunas de estas vulnerabilidades fueron reportadas hace más de 10 años. De hecho, **todas las que figuran en el top 10 cuentan con parches disponibles que las enmiendan**. Esto indica una falta de uso de software actualizado, ya sea por no realizar las actualizaciones correspondientes, por el uso de software pirata o por falta de personal capacitado.

CAMPAÑAS DE CIBERCRIMEN EN LA REGIÓN

Como resultado de diversas investigaciones desarrolladas por el Laboratorio de ESET Latinoamérica, en los últimos años detectamos una tendencia que se mantiene constante. Hablamos de campañas dirigidas a empresas privadas y organismos gubernamentales que utilizan un modus operandi similar en cuanto al tipo de malware empleado, los blancos de ataque, los países, o el hecho que sean ataques dirigidos. Veamos a continuación un resumen de las campañas más destacadas.

LUXPLAGUE

Tipo de malware	RAT - njRAT
Modo de propagación	Spear Phishing
Sistema que afecta	Windows
Foco de propagación	Usuarios corporativos y entidades de gobierno
Países afectados	Argentina
Periodo de propagación	Actividad detectada desde el 2018 , relacionado con Operación Spalax y Janeleiro, familia de troyanos bancarios fuerte impacto entre 2020 y 2022
Técnicas MITRE ATT&CK	**T1071** - Indicator Removal on Host **T1105** - Ingress Tool Transfer **T1056** - Input Capture: Keylogging

Más información sobre la campaña LUXPLAGUE

OPERACIÓN DISCORDIA

Tipo de malware	RAT - njRAT
Modo de propagación	Spear Phishing
Sistema que afecta	Windows
Foco de propagación	Empresas de distintas industrias, organizaciones sin fines de lucro y organismos gubernamentales
Países afectados	Colombia 96% - Argentina 2% - Otros paises 2%
Periodo de propagación	Febrero 2022 - Marzo 2022
Técnicas MITRE ATT&CK	T1071 - Indicator Removal on Host T1105 - Ingress Tool Transfer T1056 - Input Capture: Keylogging

Más información sobre la campaña OPERACIÓN DISCORDIA

PULPO ROJO

Tipo de malware	RAT - Remcos
Modo de propagación	Spear Phishing
Sistema que afecta	Windows
Foco de propagación	Usuarios de alto perfil de sectores como salud, organismos gubernamentales y empresas de distintas industrias
Países afectados	Ecuador 90% - Estados Unidos 3% - Perú 3% - Guatemala 2% - Colombia 1% Brasil 1%
Periodo de propagación	Junio 2022 - Julio 2022
Técnicas MITRE ATT&CK	T1586.002 - Compromise Accounts: Email Accounts T1608.001 - Stage Capabilities: Upload Malware T1566.002 - Phishing: Spearphishing Link

Más información sobre la campaña OPERACIÓN PULPO ROJO

Como podemos apreciar, la mayor parte de estas campañas están dirigidas a usuarios corporativos de distintos sectores y las metodologías de propagación utilizadas siempre son técnicas de ingeniería social desplegadas por medio de phishing, spearphising o simplemente sistemas de mensajería instantánea.

Una característica común de todas estas campañas es el uso de commodity malware, lo cual dificultad las posibilidades de identificar a los actores detrás de ellas. Por otra parte, el hecho de que todas estas campañas utilicen códigos maliciosos que son ampliamente conocidos evidencia por parte de las compañías de la región la falta de soluciones de seguridad o de buenas tecnologías para detectar y bloquear estos códigos. **Esto permite que este tipo de ataques continúe siendo redituable para los cibercriminales** que no necesitan crear malware más sofisticado o nuevo para lograr evadir las detecciones.

La tendencia en el uso de commodity malware podría hacer pensar a muchas personas que los cibercriminales no cuentan con los recursos suficientes para crear herramientas propias, sin embargo, lo que en realidad muestra es cómo a partir de una baja inversión logran obtener grandes cifras de dinero en información lanzando campañas dirigidas al sector privado y público.

CONCLUSIONES

Sin dudas que el último año estuvo marcado por un nuevo record en materia de detección de vulnerabilidades, pero también muestra los diferentes desafíos que tienen por delante muchas organizaciones de diferentes industrias que aún están en búsqueda de un horizonte más sólido en cuanto al modelo de trabajo que debieran establecer para proteger sus activos. Si bien el trabajo remoto demostró a muchas compañías que la productividad no se ve afectada por esta modalidad de trabajo y que los colaboradores encuentran un mejor balance entre la vida laboral y personal, el 32% de las organizaciones considera que no están suficientemente preparadas para trabajar de forma remota o híbrida de manera segura.

SOBRE ESET

+ 110 millones de usuarios en todo el mundo	**13** centros en el mundo de investigación y desarrollo
+ 400 mil clientes corporativos	**200** países y territorios

Para conocer más información acerca de ESET visite: www.eset.com/latam

Para estar actualizado sobre todas las noticias relacionadas con la seguridad informática visite: www.welivesecurity.com/es/

Digital Security
Progress. Protected.