NEOSECURE
SABEMOS DE SEGURIDAD

2021

TENDENCIAS EN SEGURIDAD

INTRODUCCIÓN

Es poco lo que se puede agregar a todo lo que se ha dicho de la singularidad del 2020 en relación a las vidas de miles de millones de seres humanos y de las organizaciones en las que trabajan; aceleró un futuro de distancia y teletrabajo, rompiendo los ya erosionados límites de las redes corporativas. De todas las temáticas de ciberseguridad, fue la más abordada durante gran parte del año.

Pero el año 2020 fue también un recordatorio de que lo impensable sucede, lo que Taleb denomina un Cisne Negro, un evento que escapa de lo que predecimos a partir de eventos del pasado. Ya habíamos tenido un año activo, dónde el Ransomware y los ataques dirigidos habían logrado una sinergia tal, que daba para un caso de negocios; pero fue sólo hacia finales del 2020 cuando nuestra comunidad vivió su propio Cisne Negro. SolarWinds y otras organizaciones diligentes y sofisticadas pudieron ser vulneradas por ataques de alta sofisticación, utilizando técnicas nuevas e ingeniosas, en un recordatorio más de la vitalidad que tiene la legión de organizaciones de cibercriminales, ciber-guerreros y ciber-activistas.

Hoy, generales, tras la batalla, podremos enumerar todas las cosas que no hicieron estas organizaciones. Lo concreto es que pudieron ser atacadas con éxito. Es posible que resulte desalentador, pero si volvemos a los fundamentos de nuestra disciplina, podremos recordar que sólo podemos disminuir nuestro riesgo al incorporar tecnologías, prácticas y experiencia, pero nunca lo haremos desaparecer.
Estos ataques, nos debe recordar la fluidez de este mundo, la velocidad con que cambia y la exigencia que nos obliga a mantenernos actualizados, entender y estudiar, revisar nuestros supuestos e innovar, incluso en lo que no habíamos considerado aún.

Nuestras tendencias 2021 tiene ese espíritu, revisar temas que hemos estado impulsando desde hace algún tiempo; profundizar en ellos y buscar la forma de aproximarnos sistemáticamente, sin ser excesivamente pretenciosos, pero con alta convicción y decisión.

NEOSECURE
SABEMOS DE SEGURIDAD

TENDENCIAS DE LA AMENAZA

Ilustración 1: Nivel de complejidad de las amenazas

A nivel operacional, un centro de monitoreo de seguridad debe concentrar sus esfuerzos en analizar los eventos que podrían materializarse en un incidente. La clasificación de la ilustración Nº 1, ayuda a comprender las amenazas que tienen mayor probabilidad de impactar en el negocio y a su vez, permite determinar la complejidad en la detección, análisis y la respuesta basado en dos ejes:

Sutileza: cantidad de rastros en el tiempo que genera la amenaza. Por ejemplo, una baja sutileza, nos deja muchos eventos en los controles de seguridad.

Evasión: características presentes en las amenazas que evaden la detección en los controles de red. Una amenaza que es altamente evasiva, requerirá de otros datos que no están presentes en los controles de seguridad.

A menor nivel de complejidad, se tendrán más antecedentes (logs/eventos), por lo tanto, es más sencilla la automatización de los procesos de detección, análisis y respuesta. En el polo opuesto, nos encontramos con las amenazas más complejas, donde tendremos datos menos específicos, que usualmente se confunden con actividad considerada normal.

Dicho de otro modo, los cuadros 1 a 3 corresponden a actividad reiterativa, probablemente muy masiva que requiere de baja intervención humana en el análisis, en comparación a los cuadros 7-9, donde se requiere de análisis manual. En los cuadros 4-6 se encontrarán las amenazas que pueden abordarse mediante automatización y otras requerirán análisis.

Se ha visto que la complejidad de las amenazas, ha ido aumentando progresiva y sostenidamente en el tiempo, sobre todo, en el 2020 donde tuvimos una expansión generalizada de la superficie de ataque, abriendo la puerta a las más sutiles, usualmente relacionadas con las botnets y puertas traseras, para posteriormente dar paso a las amenazas evasivas y disruptivas, como el Ransomware, y la extorsión, basados en la masiva exfiltración de información.

Es muy importante comprender este fenómeno que va en alza en el transcurso del 2021, donde las amenazas serán cada vez más sutiles y tendrán mayores capacidades de evasión.

Según el MITRE, a octubre de 2020 se contabilizaban 352 técnicas de ataque, un 24% superior al año anterior. Además, 4 tácticas de ataque han subido considerablemente y requieren de nuestra atención, ya que están directamente relacionadas con el modelo de complejidad de la amenaza de la ilustración Nº 1: un 36% de aumento en técnicas de evasión, un 27% de aumento en técnicas de comando y control, un 60% de aumento en técnicas para escalar privilegios y un 38% de aumento en las técnicas para robar y operar con credenciales válidas.

En otro ámbito, según el resultado de una encuesta realizada por Proofpoint, el 57% de las organizaciones enfrentaron un ataque exitoso de phishing y un 34% paga el rescate de un Ransomware, donde esta amenaza representa el 81% de los ataques con motivo financiero. Sin lugar a duda, estos números están relacionados con lo sutil que puede llegar a ser el Ransomware, utilizando un único punto de entrada a la red y comprometiendo todo el negocio.

Según Crowdstrike, el 51% de los ataques no utliliza malware, lo que representa un crecimiento del 22% con respecto al año anterior. En las respuestas a incidentes y Threat Hunting realizados por NeoSecure, se encontró que el 68% de las víctimas son atacadas en una segunda oportunidad y un 40% de los incidentes presentaron una falla de un control tradicional como el AV.

Según un informe de amenazas de Sentinelone, representado en la ilustración Nº 2, podemos visualizar que Linux está siendo blanco de ataque en el 23% de las instancias, en línea con los hallazgos e investigaciones de nuestro grupo de respuesta a incidentes, donde es habitual encontrar y analizar piezas de malware y criptominería, como principales objetivos del atacante.

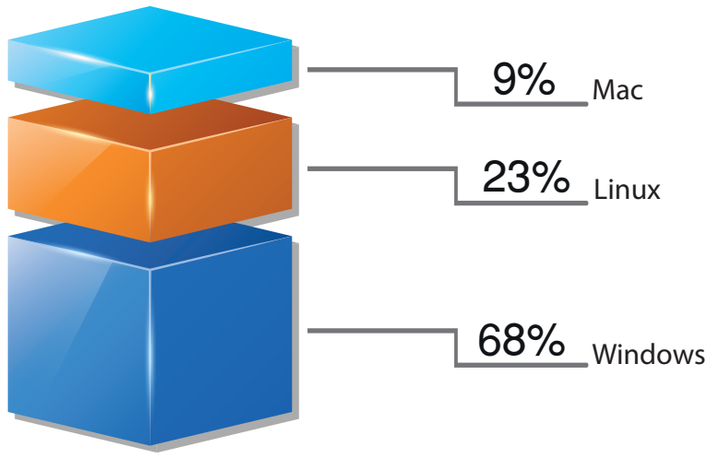


Ilustración 2:
Ataques por sistema operativo

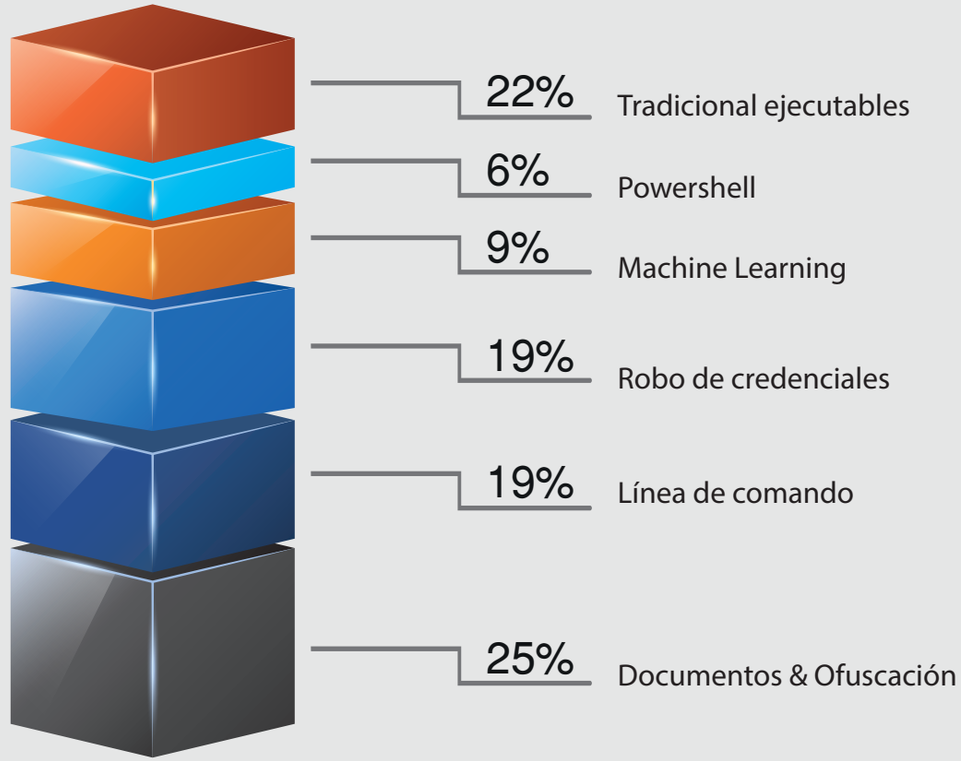


Ilustración 3:
Tipo de Intrusión

Según la ilustración Nº 3, que nos entrega Crowdstrike, sólo en el 22% de los incidentes se ha observado la presencia de malware en estado de ejecutable binario, es decir, como en la vieja escuela. Por otro lado, un 78% está compuesto por técnicas avanzadas que buscan evadir los controles de seguridad.

Interesante, el 9% de las amenazas utilizan machine learning para evadir la detección, es algo que, sin duda, aumentará en el 2021.

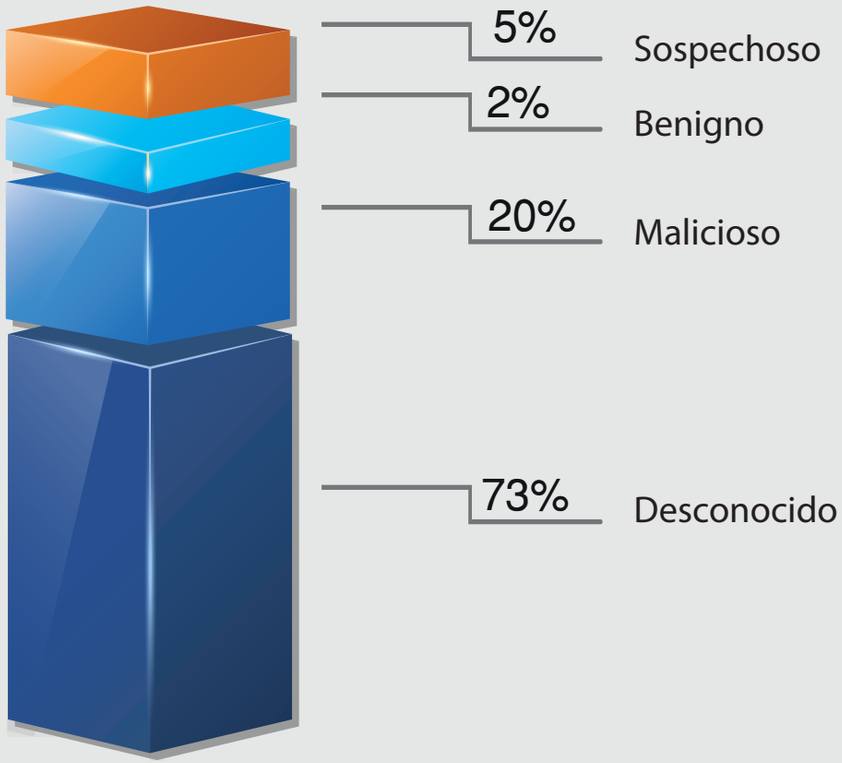


Ilustración 4:
Total detecciones v/s reputación

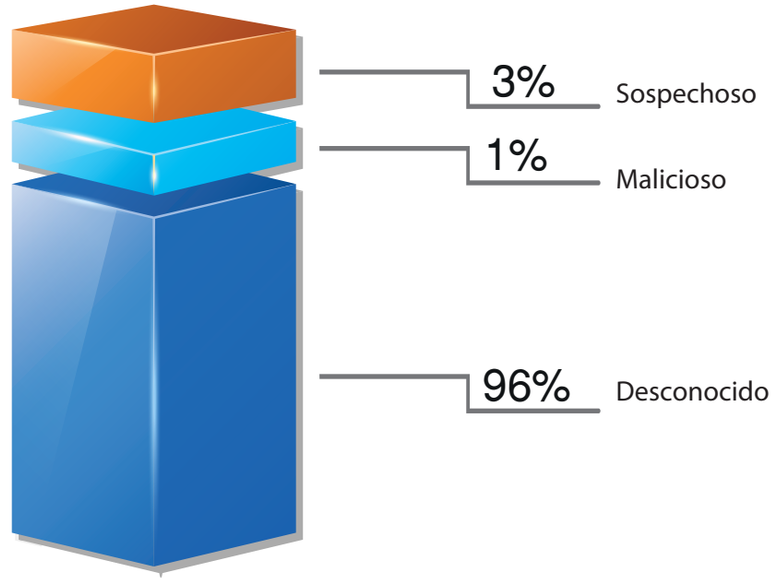


Ilustración 5:
Detección documentos y scripts v/s reputación

El uso de los Indicadores de Compromiso (IoC's) para protegernos de las amenazas está sufriendo un final anticipado. Como se aprecia en la ilustración Nº 4, al buscar la reputación de cualquier observable sospechoso, la positividad es de solo un 20%. Esto nos da luces de lo evasiva que es y de un patrón que se repite en el tiempo. Las amenazas o armas digitales, se van armando a medida y se utilizan por única vez y sólo sirven por minutos. Este escenario queda aún más claro con la ilustración Nº 5, donde el uso de la reputación sobre archivos del tipo documento office y scripts, resultan en una bajísima coincidencia o positividad.

TENDENCIAS
DE LA AMENAZA

Excepciones, listas blancas y más excepciones

Industrialización del acceso no autorizado

No es Ransomware, es APT

Botnets

¿Qué podemos esperar para el 2021?

EXCEPCIONES

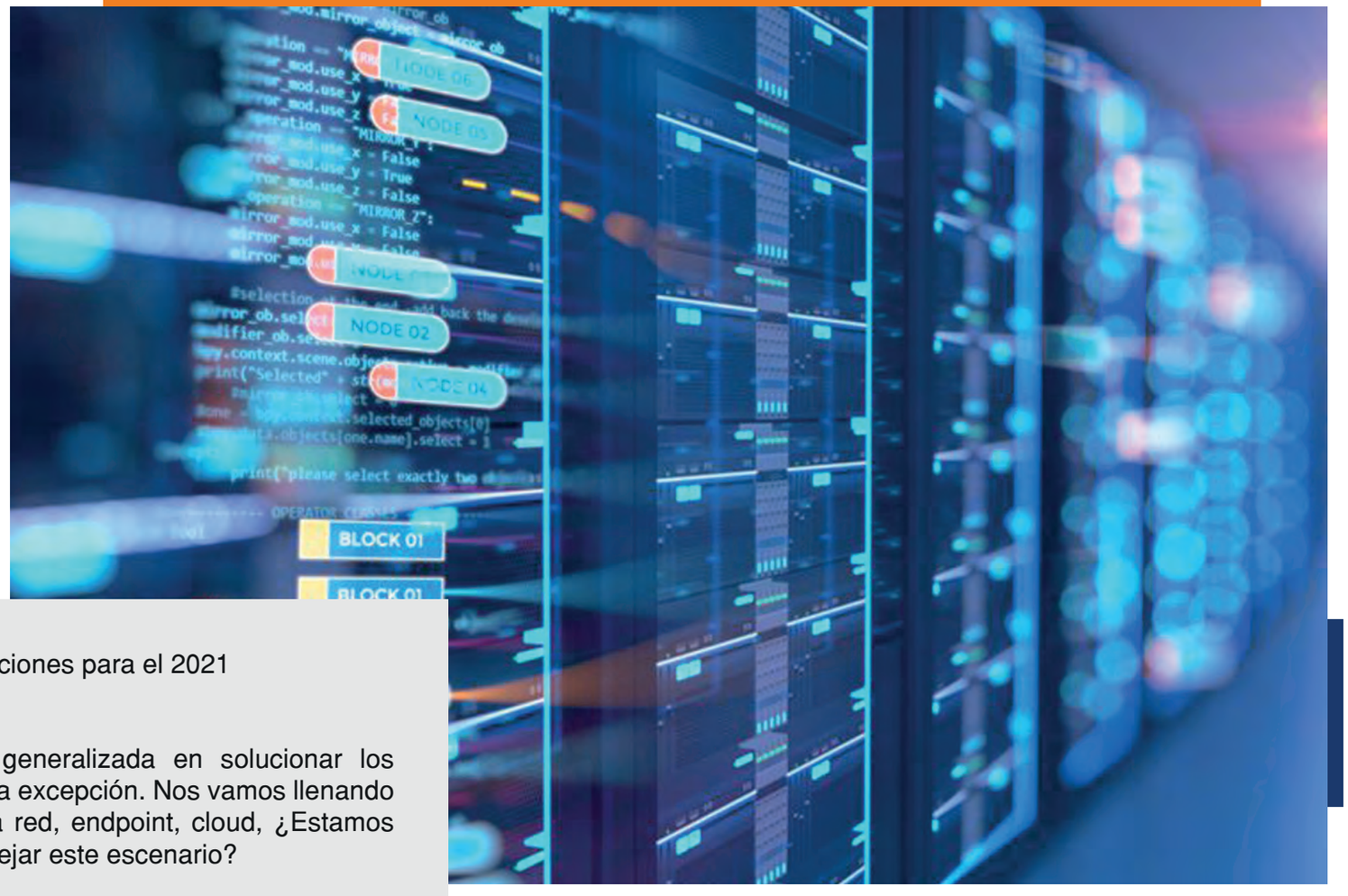
LISTAS BLANCAS Y MÁS EXCEPCIONES

La instalación de controles de seguridad en toda la red y endpoints conlleva un riesgo para la disponibilidad del negocio, hay un balance entre seguridad y productividad. Dependiendo de qué tan invasivo sea el control, podría darse, por ejemplo, el bloqueo de un proceso crítico, por considerarse comportamiento malicioso cuando no lo es. Esto se soluciona fácilmente mediante las listas blancas o excepciones a la regla, que permiten a los administradores solucionar problemas de compatibilidad o evitar los temidos falsos positivos.

A nivel de los firewalls de red, el problema está altamente relacionado con quien solicita el acceso, y el escaso tiempo que dispone el administrador para el diseño de las reglas, por lo que termina otorgando mayor acceso del que se requiere. Cuando las cosas no funcionan como se esperaba, se generan excepciones y listas blancas para privilegiar la operación del negocio; más adelante se soluciona el inconveniente, o quizás nunca, mientras ingresan otros requerimientos prioritarios.

En el caso de los firewalls aplicativos, la realidad es un tanto abrumadora, ya que este tipo de controles generan una alta tasa de falsos positivos que, por lo general, son excepcionados. El administrador de la plataforma, usualmente, no tiene conocimiento detallado de las aplicaciones que el WAF protege, sumado a la presión del negocio por disponibilidad y buen funcionamiento resulta en más excepciones aplicadas sin el suficiente análisis de impacto en la "in-seguridad".

Toda esto, resulta complejo si lo vemos desde la perspectiva de la aceptación del riesgo, ya que todo proceso formal de revisión atenta con el negocio, que requiere de un esquema ágil, apoyado con ejercicios de redteam y tecnología que permita acelerar la búsqueda de los agujeros de seguridad que las excepciones van dejando.



Tendencias de las excepciones para el 2021

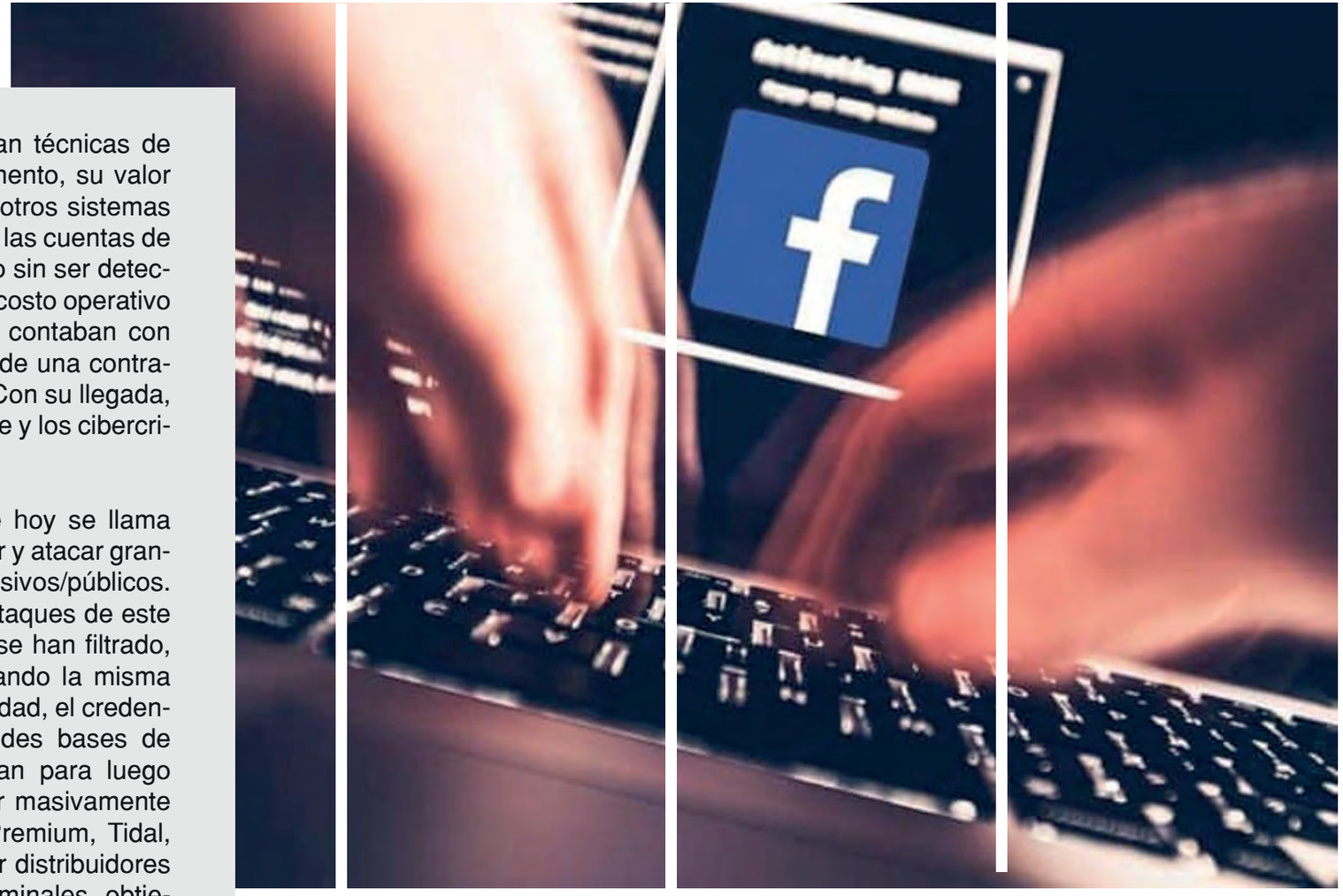
- Hay una tendencia generalizada en solucionar los problemas mediante la excepción. Nos vamos llenando de excepciones en la red, endpoint, cloud, ¿Estamos preparados para manejar este escenario?

INDUSTRIALIZACIÓN
DEL ACCESO NO AUTORIZADO

El mercado de credenciales robadas no ha parado de crecer y lo que inició, hace años, como algo novedoso y con altos precios, hoy se ha transformado en un commodity y el precio de las credenciales robadas está por el piso. Sólo basta con revisar la gran cantidad de grupos en Telegram, Facebook y otras redes sociales que ofrecen acceso clandestino a servicios de streaming pagos, para darse cuenta de esta realidad. La pregunta es, ¿cómo llegamos a esto?, A continuación, un resumen de lo que podría ser la industrialización del acceso no autorizado.

En una primera fase, los cibercriminales utilizaban técnicas de phishing para capturar credenciales. En ese momento, su valor radicaba en el acceso al homebanking, Paypal y otros sistemas similares que les permitían a los atacantes "vaciar" las cuentas de sus víctimas. El uso de mulas para mover el dinero sin ser detectados por los sistemas antifraude representaba un costo operativo no menor. Esto resultaba sencillo, porque no se contaban con mecanismos de protección de credenciales fuera de una contraseña; faltaba un segundo factor de autenticación. Con su llegada, el negocio sufrió un revés, ya no siendo tan rentable y los cibercriminales emigraron a otras especialidades.

En una segunda fase llegó la masividad, lo que hoy se llama credential leakage, que no es nada más que buscar y atacar grandes repositorios de credenciales en servicio masivos/públicos. Linkedin, Facebook, Google y otros, han sufrido ataques de este estilo y las credenciales de millones de usuarios se han filtrado, mayormente, porque los usuarios terminan utilizando la misma contraseña para todo. De aquí surge otra especialidad, el credential stuffing. Los cibercriminales descargan grandes bases de datos de fugas de credenciales y las almacenan para luego cargarlas en sistemas automatizados para probar masivamente los accesos a servicios como Spotify, Youtube Premium, Tidal, Netflix, Apple TV, etc, para luego ser vendidos por distribuidores en foros especializados. Es así como los cibercriminales, obtienen un mayor margen de ganancias con credenciales validadas en contraste con el modus operandi anterior con un costo de "producción" bajo al utilizar automatización.



Una tercera fase, está ocurriendo desde el 2020, con el aumento en el uso de botnets de phishing, en conjunto con el mecanismo de la fase 2, para acopiar credenciales validadas de acceso VPN, Escritorio Remoto y otros sistemas de acceso corporativos. Estas bases de datos tienen un valor superior ya que el comprador busca tener un pie dentro de las empresas para la ejecución de Ransomware, Extorsión, o APT.

Tendencias del acceso no autorizado en el 2021

- Mercado que ya es un commodity.
- Múltiples grupos en Telegram, Facebook y otras RRSS ofrecen acceso clandestino a servicios de streaming de pago a mitad de precio.
- La primera fase fue a través de phishing.
- En una segunda instancia obtuvieron credenciales de las grandes clouds mediante leakage.
- La fase actual, está muy automatizada y apunta a acopiar credenciales de VPN, escritorio remoto, y otros sistemas de empresas.

NO ES RANSOMWARE
ES APT

Desde el primer Ransomware han pasado 30 años y sigue evolucionando. Los primeros códigos maliciosos eran escritos y luego lanzados por sus propios autores, de hecho, hasta cierto punto las técnicas de cifrado que se utilizaban eran desarrolladas a medida. Luego, se lanzaron campañas mediante phishing masivo, algo muy similar al spam, que rápidamente fue controlado por los dispositivos antispam.

A partir de ahí se generaron campañas más complejas de spear-phishing, con envío de email controlado, para evadir controles antispam. Llegamos a un punto en que el negocio lucrativo generó toda una industria compuesta por proveedores de kits, Ransomware como servicio (RaaS), programas de afiliados, que en conjunto mueven varios millones de dólares. El Ransomware ha pasado de ser una amenaza pensada para individuos para llegar a afectar a cualquier entidad.

Los programas de afiliados al RaaS, han generado una suerte de amenaza híbrida entre los grupos cibercriminales asociados al Ransomware y a otros que, por ejemplo, buscan defraudar a grandes compañías mediante la captura de datos confidenciales asociados a propiedad intelectual o incluso de los propios consumidores, como información de tarjetas de crédito, bancaria e información personal en general. Este híbrido está compuesto por grupos que manejan grandes botnets, que ya tienen un acceso remoto en sus víctimas (un bot), el proveedor del RaaS, y usualmente otro grupo que busca lucrar con la captura de los datos. La eficacia que se ha visto de este trabajo mancomunado durante el 2020, nos hace pensar que no estamos solo frente a un Ransomware; claramente estamos frente a una amenaza del tipo APT (Advanced Persistent Threat).

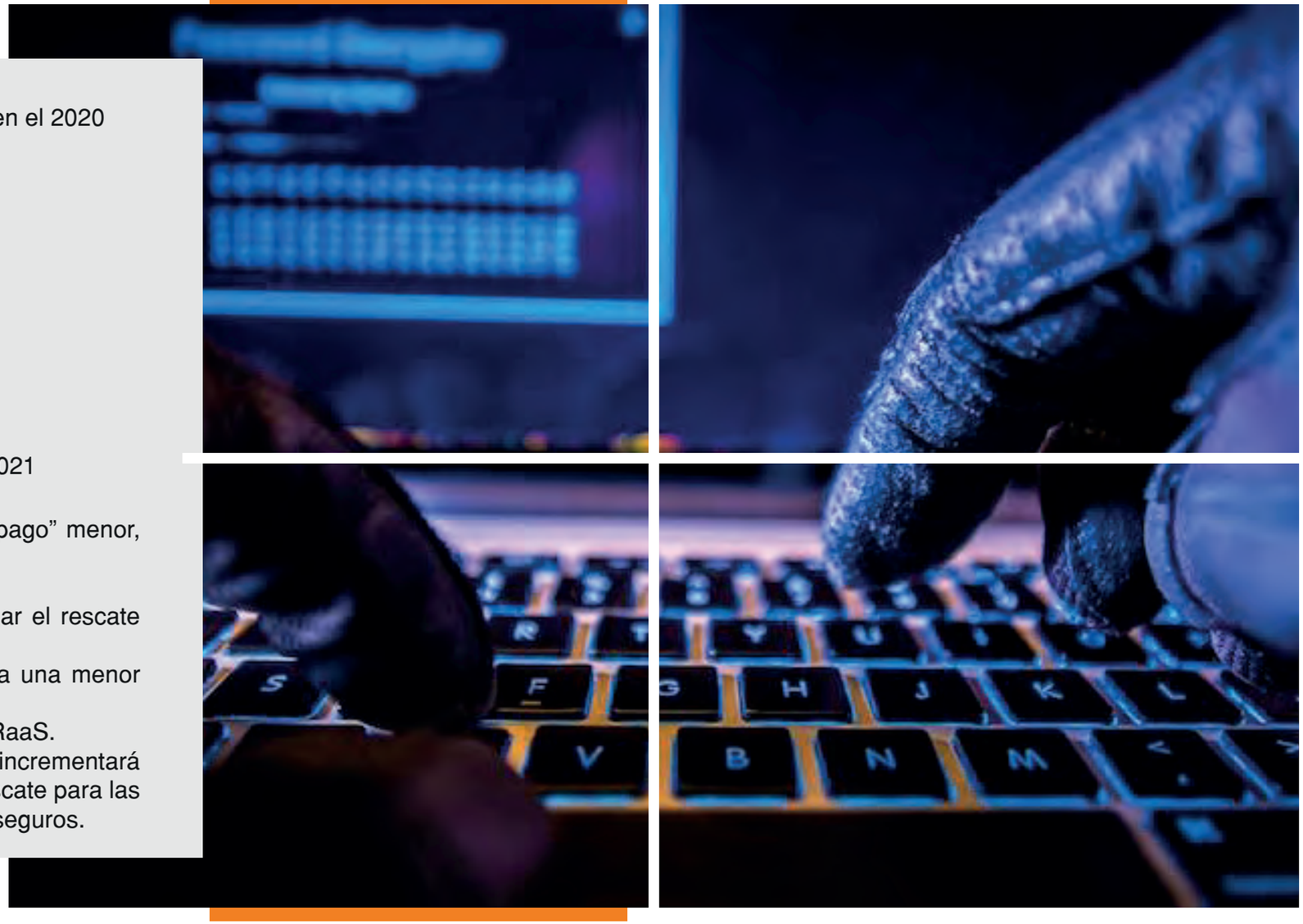
Nuestros esfuerzos para combatir el Ransomware deben apuntar a tratar esta amenaza mediante una estrategia anti APT, utilizando múltiples controles, metodologías y sobre todo teniendo en cuenta la concientización del factor humano con el que podremos mitigar el principal vector de ingreso que es el phishing.

Principales Ransomware de la región en el 2020

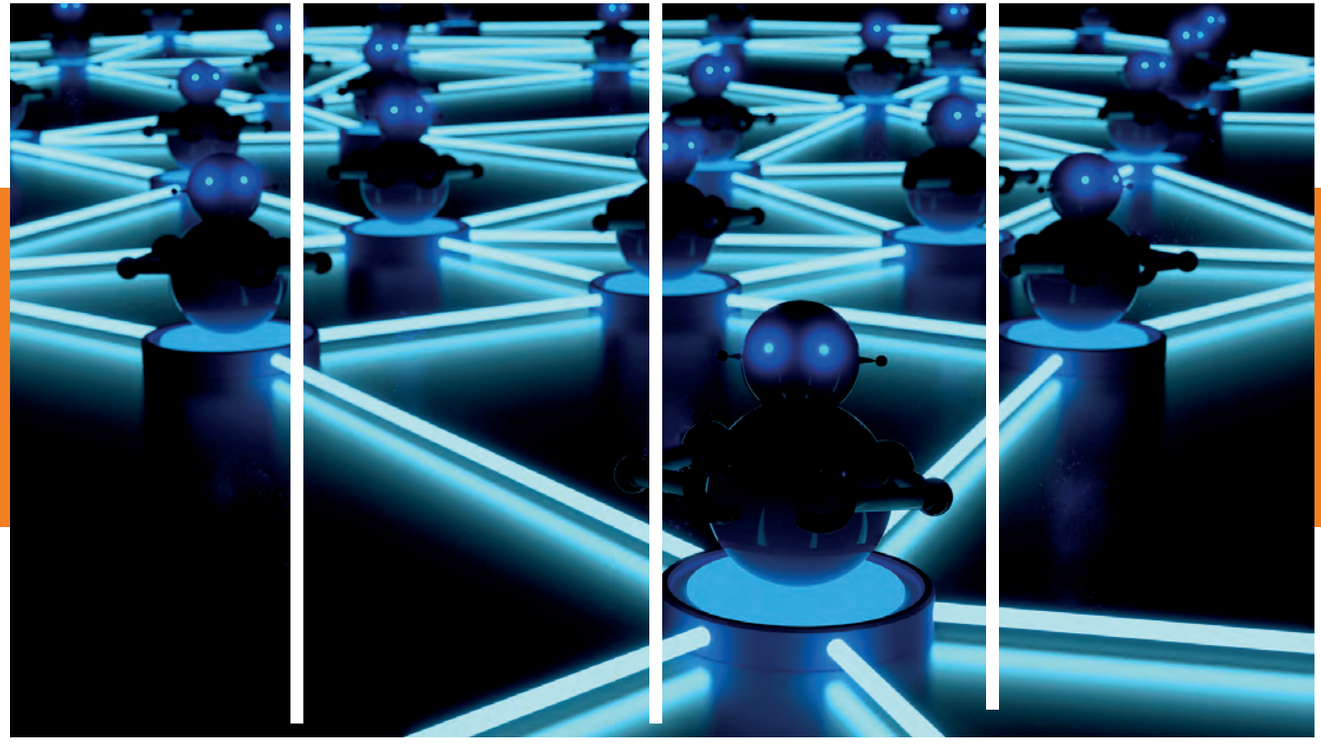
- Egregor
- Ryuk
- Ragnar
- Dharma
- Revil/Sodinokibi
- Maze
- Locky
- Doppelpaymer

Tendencias del Ransomware para el 2021

- Mayor velocidad y un “ciclo de pago” menor, más eficiente.
- Mayor frecuencia de ataques.
- Mejoras en el sistema para pagar el rescate (sin Darknet).
- Mayor acceso a RaaS, debido a una menor sofisticación de las consolas.
- Menores costos en el acceso a RaaS.
- El esquema de ciber-seguros incrementará las posibilidades de pago por rescate para las empresas que contraten dichos seguros.



BOTNETS



Las botnets son otro nicho de mercado del Cibercrimen, con un gran poder de ataque y en el tiempo se han hecho muy resilientes, transformándose en la columna vertebral para el resto de los ataques, incluso apoyando el ingreso de los APT.

Hoy, existe una preocupación general por el bajo precio de acceso a los servicios que proveen estas botnets, El bajo precio de acceso a los servicios de botnets debe ser un indicador más para los CISO's: está directamente relacionado con la frecuencia de los ataques. Según un estudio de PrivacyAffairs del 2020, el precio del arriendo de una botnet para realizar ataques de denegación de servicio rondó USD 10 la hora y USD 60 por 24hrs. El mismo estudio indica que el precio de un malware con un 70% de efectividad para 1000 blancos es de USD 80. Sin lugar a dudas son indicadores a considerar, entendiendo que por menos de USD 100, los cibercriminales pueden acceder a 1000 blancos, obteniendo una rentabilidad promedio entre 10 y 100 veces superior.

Las botnets no sólo están asociadas a ataques de denegación de servicio distribuido (DDoS), también están involucradas en el envío de correo phishing, criptominería, distribución de otros códigos maliciosos, interceptación y redirección de tráfico, puentes para búsqueda de equipos vulnerables y expansión hacia estos nodos, etc.

Tendencias de las botnets para el 2021

- Aumentarán los bots linealmente con los IoT's, dispositivos Edge, Contenedores en la nube y similares.
- El costo de acceso a las botnets como servicio, hoy en USD 10 la hora, bajará considerablemente.
- Por menos de USD 100 se tendrá acceso a 1000 blancos de ataque, con una puerta previamente abierta, para inyectar cualquier tipo de malware.

¿QUÉ PODEMOS ESPERAR PARA EL 2021?

- Aumento en el alcance del Ransomware, dificultando la recuperación del negocio, en combinación con APT.
- Más data/credential leaks debido a la proliferación de las botnets que buscan e indexan este tipo de información.
- Más fraude en línea, debido a mayores skills en los cibercriminales, el aumento en los sistemas de pagos y transferencia móviles.
- Entrada a la región de grupos cibercriminales de mayor escala (Rusos y Chinos).
- Aumento en la sofisticación de la amenaza en “Capa 8”, el factor humano, en combinación con malware automatizado (Los imitadores de Emotet).
- Automatización del acceso no autorizado y el movimiento lateral (compromiso del AD automático).

NEOSECURE
SABEMOS DE SEGURIDAD

EJES DE SEGURIDAD

EJES DE SEGURIDAD

EJE #1
Observabilidad -
Nuevas estrategias
de detección

EJE #2
El nuevo
SOC

EJE #3
El nuevo perímetro
en la nube

EJE #4
Zero Trust,
comencemos
microsegmentando

EJE #5
Una mirada más
amplia del estado
de la seguridad

EJE #6
Gestión de
usuarios privilegiados
universal

OBSERVABILIDAD

NUEVAS ESTRATEGIAS DE DETECCIÓN

La observabilidad, parte de la necesidad de tener visibilidad profunda en los diversos ambientes de la organización como respuesta a la sofisticación y evolución de los ataques dirigidos y de los APTs. Estos se caracterizan por tener una alta adaptabilidad, capacidad de evasión y requieren desde la perspectiva de la defensa un repertorio de datos más amplio y sobre todo más profundo que permita detectar técnicas más sutiles y sofisticadas.

Un mayor grado de observabilidad se logra recolectando no solamente los logs de los sistemas tradicionales de seguridad, tales como FW, AV, IPS, WAF, etc., sino también incorporando datos de diversos tipos de variables como Endpoint, tráfico interno de la red, tráfico DNS, o actividad del AD y de la nube entre otros.

Sistemas como los EDR y NDR amplían de manera relevante la capacidad de detección y análisis, al procesar gran cantidad de telemetría y proporcionar eventos de más alto nivel en este sentido, proveen un potente primer nivel de observabilidad. Aún estos sistemas podrían requerir de mayor contexto para poder confirmar adecuadamente los eventos que generan.

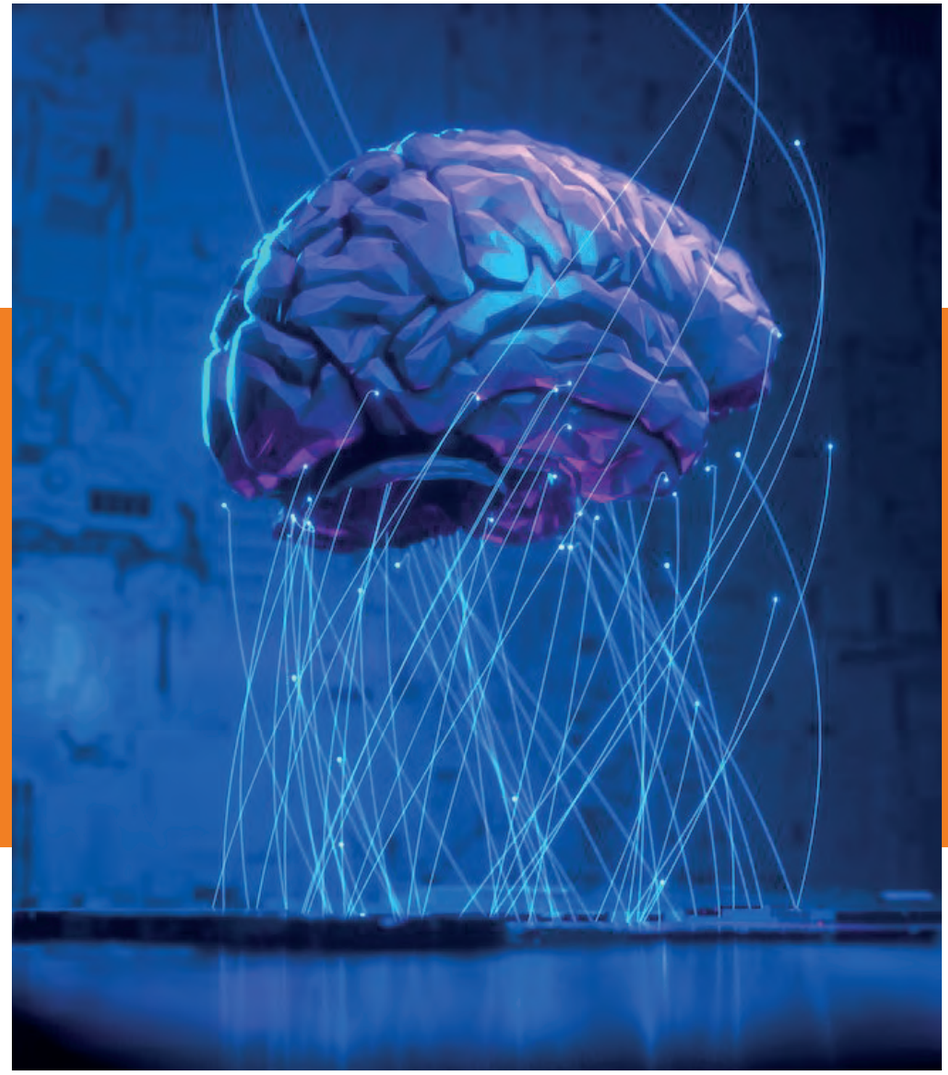
La observabilidad, entendida como la recolección masiva de datos sobre los activos que integran una red es relevante y necesaria para las tareas de investigación o la adopción de prácticas de Threat Hunting que buscan descubrir indicios sutiles que permitan identificar un ataque.

La observabilidad, apoya también las tareas de respuesta a incidentes, al generar una fuente de información que puede ser utilizada para una evaluación de compromiso o un análisis forense.

NEOSECURE RECOMIENDA

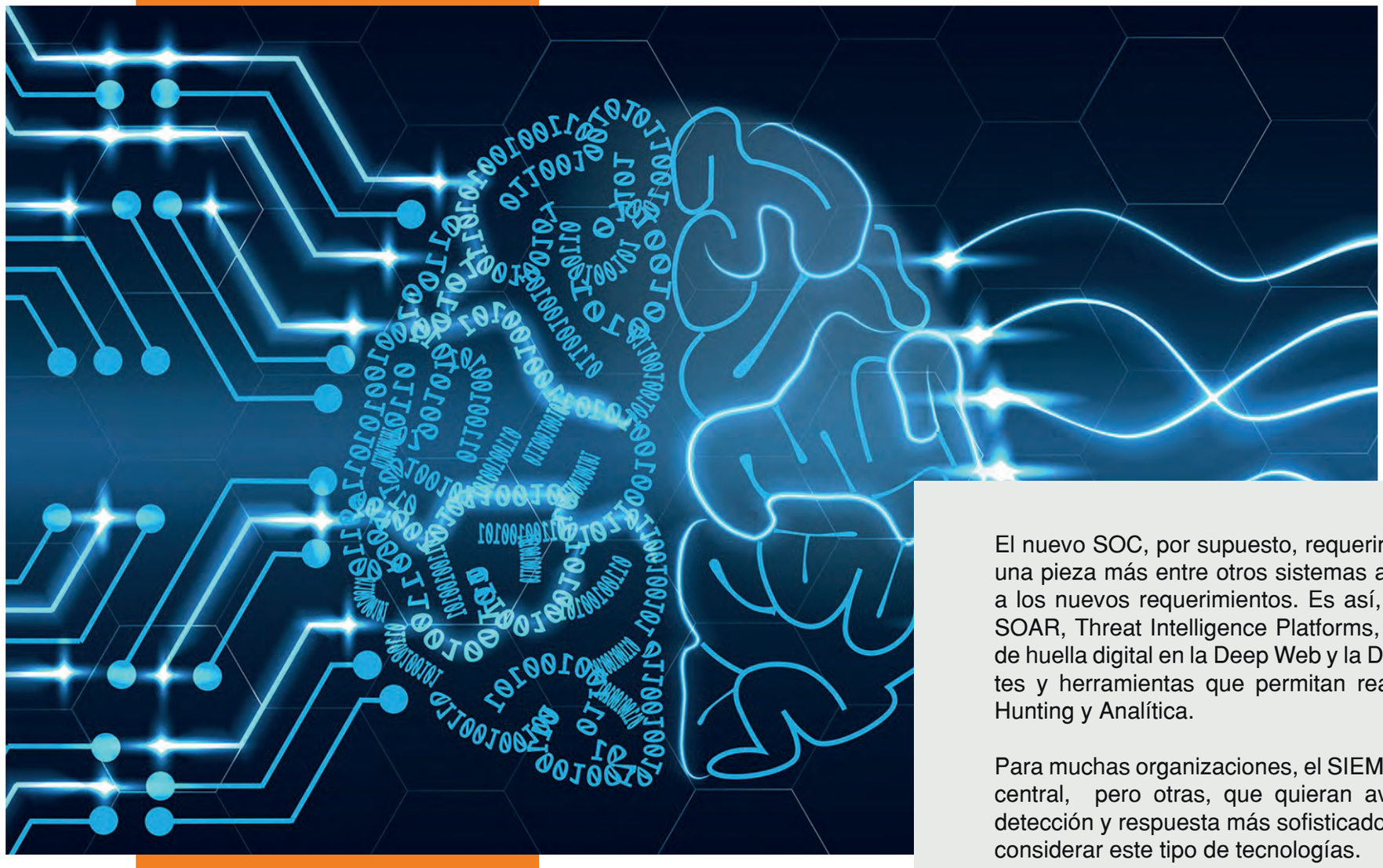
- La implementación de sistemas de tipo EDR o NDR.
- Iniciar un programa de recolección centralizada de información de activos relevantes de la red como Endpoints, DNS, AD, tráfico de red y cualquier otro sistema que permita sumar contexto de análisis.
- Incorporar prácticas de Threat Hunting dentro de la red y asegurar que el análisis de herramientas de monitoreo como EDR o NDR sean llevadas a cabo por analistas con preparación adecuada.

EL NUEVO SOC



El SOC, que ha sido el corazón de la Operación de Seguridad durante mucho tiempo ha sufrido una transformación radical durante los últimos años. Estamos observando, una tendencia a un modelo mucho más desentralizado. El SIEM, centro neurálgico del SOC tradicional, tiene a varios competidores en la disputa por la corona de este reino.

La necesidad de colectar cada vez más datos, de enriquecerlos con información de inteligencia, de contar con herramientas de investigación, de analítica, y de automatizar los procesos, tanto para lograr eficiencia como eficacia, están dándole una nueva forma.



El nuevo SOC, por supuesto, requerirá del SIEM, pero como una pieza más entre otros sistemas adicionales que aporten a los nuevos requerimientos. Es así, que deberá incorporar SOAR, Threat Intelligence Platforms, servicios de monitoreo de huella digital en la Deep Web y la Dark WebNet, o ambientes y herramientas que permitan realizar tareas de Threat Hunting y Analítica.

Para muchas organizaciones, el SIEM seguirá siendo la pieza central, pero otras, que quieran avanzar en modelos de detección y respuesta más sofisticados, deberán comenzar a considerar este tipo de tecnologías.

NEOSECURE RECOMIENDA

- La implementación de tecnologías SOAR para automatizar procesos de triage, de investigación y de respuesta a incidentes.

- La implementación de tecnologías TIP (Threat Intelligence Platforms) que automaticen el tratamiento de IoCs y aumenten la capacidad de investigación.

EL NUEVO

PERÍMETRO EN LA NUBE

La pandemia distribuyó a los equipos de trabajo de las organizaciones fuera de las oficinas comerciales y desarmó con eso uno de los más antiguos controles de seguridad: el de las defensas perimetrales. Sin este control, la navegación de los usuarios a través de Internet se ha convertido en una actividad mucho más riesgosa, donde aumenta la probabilidad de navegar en un sitio malicioso o en aquellos que fueron atacados y contaminados.

Si bien el perímetro tradicional ha sido sostenidamente sobrepasado por ataques de phishing, ataques a la cadena de suministro y otros, su utilidad para detener una miríada de amenazas, y contribuir a la detección de ataques más sofisticados, sigue vigente. Esto obliga a recomponer la estructura de controles de seguridad perimetrales de una organización que difícilmente, volverán a ser como antes de la pandemia.

La respuesta de la industria ha situado el nuevo perímetro de la organización en la nube. Las tecnologías SASE, (Secure Access Service Edge) proveen una capa de variados controles de seguridad en la nube, desde la cual los usuarios navegarán no sólo a los recursos de la red interna, también, a las nubes públicas dónde la organización tenga recursos o a la misma Internet.

Las soluciones SASE han incorporado en esta capa, controles de acceso, detección de tráfico anómalo, identificación de malware, análisis de reputación de sitios, cifrado, detección de fuga de información, control de acceso a las nubes públicas y aislación del browser entre otros, expanden las capacidades de la organización generando nuevos casos de uso, como la navegación protegida que permite a los usuarios tener un perímetro de seguridad local cuando viajan, trabajan desde un café como así también la integración a la red de oficinas remotas, en este punto único y escalable.

NEOSECURE RECOMIENDA

- Implementar una arquitectura SASE que sea punto de acceso a la navegación, acceso a recursos internos y acceso a la nube pública, que cuente con capacidades de control de seguridad como URL Filtering, detección de malware, detección de tráfico anómalo entre otros.
- Implementación de tecnologías de CASB para acceso a la nube SAAS.

ZERO TRUST

COMENCEMOS MICROSEGMENTANDO

Zero Trust, es el modelo de ciberseguridad con el que la industria se ha alineado con rapidez. Zero Trust, provee una mirada dónde debemos desconfiar de los accesos aún cuando estos provengan de zonas confiables como la red interna. Zero Trust, nos pide localizar controles lo más cerca posible de los datos y activos a proteger para monitorear, controlar y validar cada acceso dentro de otras cosas.

El problema del modelo Zero Trust, es lograr su implementación integral. Al ser una estrategia que considera variados elementos en todo el ambiente de una organización, implica, por un lado, la expansión de controles en mayor escala y nuevas capacidades que no necesariamente se encuentran disponibles dentro de los controles ya existentes. En estricto rigor, casi cualquier control de seguridad aporta un grano de arena al modelo Zero Trust, pero son pocos los que ayudan a implementar de manera amplia y profunda esta filosofía de protección.

La microsegmentación, es uno de los controles que hace una diferencia profunda en una estrategia Zero Trust, pero su implementación requiere algunas capacidades que no todas las tecnologías de control de acceso proveen.

Una tecnología de microsegmentación debe proveer la capacidad de identificar las interacciones entre sistemas (tráfico este-oeste). Adicionalmente, debe proveer la capacidad de construir políticas entre sistemas individuales o grupos de sistemas. Dichas políticas, deben mantenerse, aún cuando modifiquemos la localización lógica del activo. Finalmente, debe forzar el cumplimiento de dichas políticas.

Para que la microsegmentación tenga el efecto que se busca, debe poder implementarse sin tener que hacer profundos cambios en la red de la organización y debe cubrir además los mundos del datacenter y la nube.

La microsegmentación limitará, seriamente, el movimiento lateral de un atacante, su exploración, la propagación de malware y el acceso a sistemas críticos dentro de su cadena de ataque. Igualmente reducirá el abuso interno y limitará el efecto que puede tener el robo de credenciales de un usuario, contribuyendo a la implementación de la estrategia Zero Trust de manera relevante y sobre todo a disminuir el riesgo de la organización.

NEOSECURE RECOMIENDA

- Desarrollar una estrategia para adoptar el modelo Zero Trust.
- Implementar la microsegmentación a nivel de servidores en la nube y en el datacenter.
- Implementación de microsegmentación a nivel de Endpoint.

UNA MIRADA MÁS
AMPLIA DEL ESTADO DE LA SEGURIDAD

Si bien, gran cantidad de los controles de seguridad que implementamos se dirigen hacia las capacidades de detección y bloqueo de amenazas, un paso de higiene es el conocimiento de lo que tenemos y el nivel de seguridad de nuestra infraestructura. Este ejercicio comprende un abanico diverso de miradas.

Conocer el ambiente a proteger y sus debilidades, es uno de los aspectos más antiguos en ciberseguridad. Sin embargo, después de la adopción de los sistemas de detección de vulnerabilidades, muchas organizaciones parecieron conformarse con la limitada visibilidad que tienen de sus sistemas y sus debilidades.

Frente al aumento de incidentes de seguridad, la capacidad de tener la claridad permanente de la robustez de la plataforma tecnológica y poder mirar cada rincón, se convierte en un objetivo importante.

Preguntas como ¿Cuántos Endpoints Windows existen en la organización?, ¿En qué sistemas se está haciendo escaneos?, ¿Qué controles se encuentran implementados en el firewall aplicativo? ¿Cuáles sistemas cuentan con un EDR? ¿Cuáles no lo tienen? ¿Fueron escaneados todos los servidores del perímetro? ¿Cuándo? ¿Qué vulnerabilidades tienen? ¿Está configurada la capacidad de mirar tráfico cifrado en el firewall? ¿qué aplicaciones se encuentran instaladas en los equipos personales? ¿qué nivel de parchado tienen? Son algunas de las preguntas que tienen respuestas parciales o no las tienen directamente y aparecen apremiantes en medio de un incidente que requieren respuestas rápidas.

Obtener esta visibilidad requiere de varias capacidades tecnológicas. En primer lugar, la identificación de los activos de la red. Esto comprende un inventario acabado, desde la perspectiva de seguridad, que contenga sistemas del negocio, de seguridad y la cobertura que dichos sistemas ofrezcan de cara a proteger activos.

Podemos tener un EDR, pero si sólo cubre un 60% de la infraestructura, tenemos un 40% sin visibilidad ni protección.

La nube y los ambientes OT, así como el IoT deben ser parte integral de este mapa, permitiendo tener información amplia de nuestra red. Modernos sistemas de inventarios orientados a la seguridad, así como los sistemas de CSPM (Cloud Security Posture Management) apoyan en esta función.

Luego, convertido ya en un clásico, contar con visibilidad de las vulnerabilidades existentes con capacidad de priorización que contemple variables de localización y existencia de un Exploit; la explotabilidad de la vulnerabilidad, relevante para el negocio y el riesgo que implica, entre otras.

Otro aspecto son las configuraciones de seguridad de los sistemas de negocio, como servidores y Endpoints: el estado de sus políticas de clave, permisos, credenciales, etc. Los CSPM, proveen valiosa información de la seguridad de las configuraciones en la nube.

Finalmente, debemos tener visibilidad de las configuraciones de los variados sistemas de seguridad de la organización como firewalls, EDR, PAM, firewall aplicativo, AD, etc., que son el muro destinado a defender nuestra red y generalmente han significado inversiones cuantiosas para la organización. Tenerlos mal o insuficientemente configurados, genera una falsa sensación de seguridad que puede costar caro al momento de un ataque.

El conjunto de estas miradas nos permitirá contar con una panorámica completa de lo que debemos defender, de los controles que tenemos y del estado en que ambos se encuentran para acometer la misión.

NEOSECURE RECOMIENDA

- Implementar un sistema de inventario centralizado de activos (seguridad, OT, nube, TI, IoT) ojalá con foco en los aspectos de cobertura de seguridad.
- Contar con un esquema de gestión de vulnerabilidades con fuerte énfasis en la priorización de las mismas.
- Contar con sistemas de CSPM que permitan tener visibilidad, sobre las algunas veces complejas, configuraciones de los ambientes de nube.
- Contar con un sistema de relevamiento de configuraciones de los sistemas de seguridad.

GESTIÓN DE USUARIOS
PRIVILEGIADOS UNIVERSAL

Las tecnologías de PAM (Privileged Access Management) nos acompañan desde hace más de diez años y han mostrado ser un valioso aporte al control de los accesos y acciones de usuarios privilegiados dentro de la red. Han provisto la capacidad de centrar a los usuarios privilegiados, estableciendo reglas claras de hacia dónde y cómo pueden acceder, eventualmente limitado las acciones que pueden ejecutar.

Desde la aparición de los PAM, nuestro ecosistema tecnológico se ha hecho más amplio. La presencia de la(s) nube(s), el mundo OT, el mundo de DevOps y el mismo Endpoint son todos espacios dónde un adversario experimentado puede ejecutar ataques a nuestras organizaciones aprovechando los altos privilegios que algunos usuarios de la organización poseen.

El robo de credenciales, utilizado como mecanismo casi omnipresente en los Ataques Dirigidos y APT, apuntan principalmente a estos usuarios, justamente para acceder a sistemas críticos de la organización.

Esto, da lugar a situaciones dramáticas si un atacante logra acceder a los sistemas de control de una planta industrial, una central de generación o de distribución de energía eléctrica, situaciones que ya han ocurrido en el pasado. Si el atacante accede a sistemas críticos de gestión de la nube, el poder puede llegar a niveles mayores que los que habría tenido accediendo a los sistemas de la red interna. Pero en el mundo del DevOps, la situación puede llegar a ser explosiva si el atacante accede al código, permitiendo, eventualmente, un ataque del tipo cadena de suministro, como el realizado contra la empresa SolarWinds.

Por otro lado, el mundo del Endpoint ha sido largamente desatendido en este sentido y muchas de las acciones de una atacante que requieren privilegios, son posibles debido a que no existe una adecuada gestión de los privilegios de administrador.

El nivel de desarrollo de nuestras infraestructuras requiere de una estrategia de control de usuarios privilegiados amplia, que cubra los mundos OT, Nube, DevOps y Endpoint. Los sistemas de PAM proveen estas capacidades.

A través de esto lograremos reducir el impacto de abusos, de fallas y del posible robo de credenciales de estos usuarios.

NEOSECURE RECOMIENDA

- Implementar sistemas de control de usuarios privilegiados (PAM) en un espectro amplio, considerando ambientes OT, acceso a sistemas de gestión de nube, ambientes DevOps y Endpoints.

PRESENCIA LOCAL EN:

CHILE
SUECIA 0155 PISO14
PROVIDENCIA, SANTIAGO
CENTRAL +56 2 22905900

ARGENTINA
CERRITO 1186, PISO 7
BUENOS AIRES
CENTRAL +54 11 48190100

PERÚ
AV. DEL PINAR 152 OF. 1102
CHACARILLA DEL ESTANQUE,
SANTIAGO DE SURCO, LIMA
CENTRAL + 51 1 2084800

COLOMBIA
AV CALLE 26 #69D - 91 OF 504
TORRE DORADO, BOGOTÁ
CENTRAL +57 1 432 0700

BRASIL
AV. PRESIDENTE JUSCELINO
KUBITSCHEK, 1455, 4º ANDAR -
VILA NOVA CONCEIÇÃO –
SÃO PAULO -CEP 04543-011