Q&A: Estado actual de la seguridad en México y Latinoamérica

- **¿Cómo podemos contribuir para poder evitar ciberataques ya que son daños muy graves?**

La contribución depende del sector y de las habilidades. Por ejemplo, las empresas privadas suelen hacerlo a partir del desarrollo de tecnologías de seguridad que comercializan, impulsando campañas de concientización que buscan llegar a la mayor cantidad posible de usuarios, o bien, mediante la investigación; las instituciones educativas lo hacen formando profesionales en el área y también fomentando la investigación.
Por su parte, los gobiernos mediante políticas públicas o creando leyes y reglamentos que contribuyen a la seguridad en todos los ámbitos; como usuarios, podemos aplicar y difundir buenas prácticas de seguridad entre las personas que utilizan la tecnología y que podrían ser potenciales víctimas de atacantes; y estas prácticas no solo desde el ámbito personal, sino también en el laboral o en cualquier otro rol que desempeñemos.

- **¿Cuáles son los principales ciberataques en México?**

De acuerdo con el ESET Security Report (ESR) 2020, los códigos maliciosos continúan siendo la principal amenaza para las organizaciones y los usuarios. En el caso de México, el 59% de los encuestados afirmó haber sufrido una infección de malware, aunque también existen importantes detecciones de adware, de aplicaciones potencialmente no deseadas (PUA) y de aplicaciones potencialmente inseguras.
Durante 2019, los códigos maliciosos con mayor cantidad de registros fueron Ramnit (9,9%), seguido por ProxyChanger (9,6%), Emotet (8,9%), Bondat (8,3%) y Bundpil (4,1%).
EL top cinco está conformado de la siguiente forma, de acuerdo con la telemetría de ESET:

- Win32/Ramnit. Código malicioso utilizado principalmente para robar datos confidenciales relacionados con servicios bancarios de los usuarios. Se propaga a través de dispositivos extraíbles y una de sus principales características es que puede infectar el Master Boot Record (MBR) para mantener su persistencia en el sistema operativo.

- JS/ProxyChanger. Se trata de un malware del tipo troyano escrito en JavaScript. Tiene como función impedir al usuario acceder a sitios web para redirigir el tráfico hacia sitios web de atacantes.

- Win32/Emotet. Este código malicioso se encarga principalmente de la distribución de otras familias de troyanos bancarios. Es conocido por su arquitectura modular,

métodos de persistencia y auto propagación, así como por sus características polimórficas que intentan evadir la detección basada en firmas.

- JS/Bondat. Gusano informático escrito en JavaScript que tiene como función principal infectar sistemas Windows para unirlos a una botnet. Funciona como un vector de infección inicial, ya que también descarga otros archivos que pueden realizar más acciones maliciosas. Su medio de propagación es a través de medios extraíbles utilizando archivos LNK.

- Win32/Bundpil. Es un gusano diseñado para mejorar la persistencia de la botnet Wauchos (también conocida como Gamarue o Andrómeda), para dificultar la eliminación global de su red. Como características, es capaz de propagarse a través de medios extraíbles.

Vale la pena destacar que algunas familias y variantes van en aumento en cuanto a su actividad, mientras que otras han reducido su frecuencia, no así su impacto.
Ante este cambio de enfoques no debemos olvidar que el panorama de amenazas es amplio, aunque en ocasiones solamente se haga referencia a amenazas mediáticas. Por lo tanto, es importante conocer la diversidad de códigos maliciosos que se propagan por Internet para lograr implementar las medidas de protección adecuadas y necesarias.

- **¿En qué casos es recomendable que la detección de amenazas y ciberataques lo hagan herramientas con Inteligencia Artificial y/o Machine Learning?**

El Aprendizaje Automático o Aprendizaje Automatizado es un enfoque de la Inteligencia Artificial, que busca brindar la capacidad a un sistema de aprender de la experiencia.

Está pensado no solo para los objetivos de la IA (como imitar el comportamiento humano), sino también para reducir los esfuerzos y/o el tiempo empleado en diversas tareas. Por ejemplo, ML se puede utilizar para reconocer patrones, a partir de decisiones basadas en datos en lugar de algoritmos, por lo que el comportamiento cambia con el tiempo y con la información.

En ciberseguridad y en particular para la detección de malware, Machine Learning generalmente refiere a una de las tecnologías integradas en una solución que recibe grandes cantidades de muestras limpias y maliciosas correctamente etiquetadas, y ha aprendido a diferenciarlas. Debido al entrenamiento (aprendizaje automático supervisado), es capaz de analizar e identificar la mayoría de las amenazas potenciales para usuarios y de actuar proactivamente para mitigarlas.

La automatización de este proceso hace que la solución de seguridad sea más rápida y ayuda a los humanos expertos a manejar el crecimiento exponencial en el número de muestras que aparecen cada día. Los algoritmos que no tienen este entrenamiento (aprendizaje automático no supervisado), son prácticamente inútiles para la seguridad.

- **¿Existe algún lugar (repositorio, paper, etc.…) en donde se consulten datos más técnicos de los ciberataques?**

Existe referencias donde se detallan las investigaciones en torno a algunas amenazas informáticas identificadas y analizadas:
https://www.welivesecurity.com/la-es/articulos/white-papers/
https://www.welivesecurity.com/papers/white-papers/
https://www.virusbulletin.com/blog/
https://www.defcon.org/html/links/dc-torrent.html
https://www.blackhat.com/html/archives.html

- **¿Qué tanta experiencia necesito para adentrarme al framework?**

Si la pregunta hace referencia a MITRE, depende del modo de involucramiento. En caso de la contribución al framework son necesarias diversas habilidades, conocimientos y aptitudes para realizar investigación en torno a las amenazas y ataques informáticos.
Si se trata de consultar información, basta con tener una adecuada interpretación del modo en el que está organizado el navegador, aunque sin duda, también requiere de conocimientos previos y generales del funcionamiento de sistemas operativos, redes, lenguajes de programación, etc.

- **¿Cómo podemos ayudar para identificar los ataques en el Sistema Bancario en México?**

La banca se encuentra constantemente en la mira de atacantes, por lo que la novedad se presenta cuando un ataque es efectivo, esto tiene como consecuencia que, al identificar las vulnerabilidades del sector, haya más interés por parte de cibercriminales que buscan obtener algún tipo de beneficio, principalmente económico.
A pesar de que las instituciones se conducen de acuerdo con sus protocolos de seguridad, que sin duda son perfectibles, nunca se tienen las regulaciones suficientes, ya que tanto la tecnología como las amenazas avanzan con mayor rapidez que las legislaciones y las regulaciones, por lo que generalmente existe una brecha. Otro inconveniente relacionado con las regulaciones es que no se cumplen por completo, a pesar de que tienen el carácter de obligatorias; incluso algunas directrices se presentan como opcionales, y por tal razón no son acatadas.

Aunado a lo anterior, la seguridad al cien por ciento no existe, por lo tanto, todos los esfuerzos de protección se enfocan en mitigar riesgos hasta un nivel aceptable para las empresas. Por ello, mientras que las organizaciones requieren asegurar toda su infraestructura, para los atacantes basta un solo resquicio para lograr vulnerarlas.
Una forma de identificar amenazas es mediante las tecnologías EDR, detección y respuesta en los endpoints, así como tecnologías de inteligencia de amenazas, que permiten tener una detección temprana de amenazas, especialmente si otras instituciones ya han sido atacadas y los adversarios utilizan las mismas tácticas y técnicas.

- **¿Cuál sería la estrategia más eficiente para poder atender las vulnerabilidades por volumen que son detectadas por un área de seguridad en una empresa grande?**

Una estrategia recomendada es el uso de soluciones catalogadas como Client Management Tools (CMTs), que permiten automatizar tareas de administración en los sistemas.

Las soluciones de Patch Management o gestión de vulnerabilidades se incluyen en este grupo de herramientas, diseñadas para administrar grupos grandes de sistemas dentro de las redes corporativas, de tal forma que las tareas de corrección de vulnerabilidades de automaticen y se realicen con mayor rapidez.

- **¿Qué recomendaciones harías a los equipos de TI para el caso de BYOD?**

Debido al crecimiento y expansión de la tecnología, utilizar dispositivos móviles es algo cotidiano en muchos de los ámbitos de la vida, y el trabajo no es la excepción. Sin embargo, utilizar los dispositivos como herramientas laborales plantea retos y oportunidades.
Por esta razón, resulta necesario considerar las ventajas y desventajas de esta modalidad laboral, y estar preparados para garantizar la protección de la información corporativa. Los detalles relacionados con la seguridad BYOD pueden revisarlos en la siguiente guía que preparamos para WeLiveSecurity:
https://www.welivesecurity.com/wp-content/uploads/2014/01/documento_guia_byod_W.pdf

- **¿Cuál es tu apreciación del nivel de seguridad de la información que tenemos en México, respecto a otros Países?**

Una referencia para abordar este tema es el Índice Global de Ciberseguridad (GCI), que mide el nivel de compromiso de cada nación con la Agenda de Ciberseguridad Global de la UIT, con el objetivo de destacar las áreas potenciales para mejorar y llevar la ciberseguridad a la vanguardia de los planes nacionales.

En el último informe publicado, México no figura en los tres primeros lugares para América, lugares que son ocupados por Estados Unidos, Canadá y Uruguay. Esto nos muestra que existen brechas importantes por cubrir en diversos ámbitos, como el legal, organizacional, políticas públicas, etc. Tenemos un camino importante por recorrer.

- **¿Cuál es la probabilidad que detengan a las personas que lanzan ransomware?**

Lamentablemente la probabilidad es baja, y de forma lamentable también, es una amenaza que se reinventa continuamente. Nuevas modalidades de ransomware son aplicadas y adoptadas por los cibercriminales.

Por lo tanto, la postura es de no pagar el rescate, ya que no hay garantías de que al realizar el pago sea posible descifrar y recuperar los archivos. Además, tampoco se tiene la certeza de que luego del pago, la información comprometida no se haga pública, o bien, que pueda ser utilizada con otros propósitos maliciosos.

Aunado a lo anterior, con estas acciones se financia el modelo de negocio de los atacantes, que con más recursos pueden desarrollar más amenazas de este estilo, incluso otras que no conocemos en la actualidad; en consecuencia, se contribuye para que más usuarios u organizaciones se vean afectados.