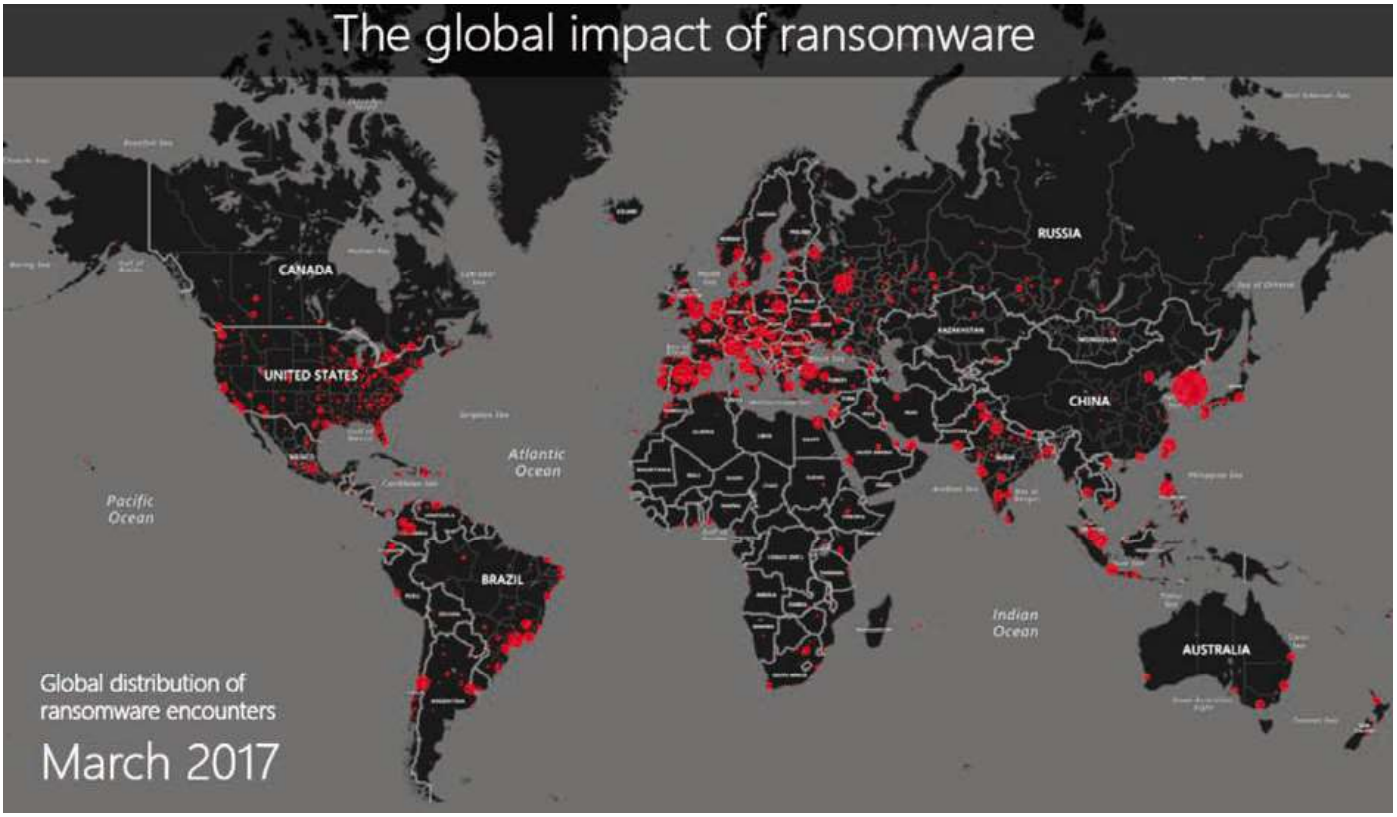
La verdad sobre el *ransomware*



Fuente: Microsoft Security Blog (https://goo.gl/vd88Mi)

Distribución global de encuentros de *ransomware* por mes. En el blog TechNet, de Microsoft, se puede consultar el mapa mes por mes, entre enero y junio del 2017.

La encriptación de datos para exigir rescate es un problema muy visible y que puede afectar a cualquier ciudadano, pero hay amenazas mucho más peligrosas, según Eddy Williems, evangelista principal de la firma alemana G Data, cuya función es explicar en palabras sencillas conceptos complejos de seguridad.

En la medida en que la gente se familiariza con las tecnologías conectadas a internet, ¿los riesgos para los ciudadanos son mucho mayores?

Sí, el problema con el internet de las cosas (IoT) es que los aparatos y objetos que se conectan a internet deberían ser seguros por diseño y por metodología, pero, desafortunadamente, y ese es el mayor riesgo de esos dispositivos, es que no se están desarrollando de forma segura.

¿Por qué sucede eso? ¿Porque los desarrolladores no están capacitados, porque no se invierte lo suficiente, porque el conocimiento tecnológico es insuficiente?

Es una combinación de factores. Integrar seguridad en los dispositivos podría demorar su salida al mercado o afectar sus precios. También es difícil encontrar la gente adecuada, pues el que sabe fabricarlos, probablemente no sabe asegurarlos, y cuando el fabricante busca ayuda en la industria de la ciberseguridad, se topa con que ella enfrenta sus propias limitaciones, porque faltan recursos humanos. Se requiere que la academia trabaje en la formación de ese tipo de expertos.

En su conferencia habló de contar la verdad sobre el *ransomware*, ¿a qué se refiere?

Mostré una imagen que evidencia las exageraciones de los medios de comunicación y de la industria de seguridad, porque se piensa que el *ransomware* es lo único; en realidad, en términos porcentuales es muy pequeño, pero, como es muy visible, nos olvidamos de amenazas como el *spyware* y el *adware* que espían nuestras actividades, o las que apuntan hacia nuestras cuentas bancarias o información personal. El *ransomware* está poniendo millones de dólares en los bolsillos de los cibercriminales y

no deberíamos subestimarlo, pero estas otras son más extendidas y potencialmente más peligrosas porque podrían afectar infraestructuras críticas o gobiernos y son las que realmente se constituyen en armas de guerra.

¿A quiénes van dirigidos los ataques de *ransomware*?

Son para obtener dinero fácil. Los bancos no son su objetivo real, las instituciones educativas sí, porque usualmente carecen de presupuesto suficiente para comprar defensas de calidad; es tentador atacarlas porque no pueden detenerse y son más proclives a pagar rescates costosos y sin mucha resistencia. Por otro lado, debemos separar dos tipos de *ransomware*: el indiscriminado cuyo fin es conseguir la mayor cantidad de dinero de las víctimas, y el que apunta directamente a alguna entidad. Un ataque dirigido es muchísimo más complicado y muchísimo más caro; para obtener dinero rápido es más fácil o eficiente lanzarlo al público general.

¿Qué tipo de información le encriptan al ciudadano y cuánto le piden en promedio para rescatarla?

Los costos dependen de variables como el precio del bitcóin, debido a que se exige el pago del rescate en moneda virtual, y también del poder adquisitivo de los países. Recuperar la información puede costar desde 100 dólares y el promedio es de 500 dólares. Lo que encriptan depende del *ransomware* en sí mismo; normalmente no se cifran programas, sino documentos de oficina, fotos, hojas de cálculo. También pueden

> "Los dispositivos que se conectan a internet deberían ser seguros por diseño y por metodología, pero no se están desarrollando de esa forma".
>
> Eddy Williems

tomar posesión del sistema e incluso las copias físicas de respaldo (*backups*) pueden ser cifradas. Probablemente, la mejor defensa reside en el uso de tecnologías muy nuevas como la supervisión de conducta, que consiste en analizar el comportamiento del *software* de cualquier aplicación que corra en el sistema, para, con base en criterios preestablecidos, determinar si se asemeja a un *ransomware*. También hay que contemplar productos específicamente diseñados contra esta amenaza y las tecnologías de protección contra *exploits* (fragmentos de *software* o datos que aprovechan vulnerabilidades de seguridad para que el sistema se comporte de manera errada).

¿Cómo sabe un ciudadano del común, que compra equipos y programas legales, si estos cuentan con esas protecciones?

Actualmente no existen pruebas comparativas especializadas en *ransomware*. Represento a la AMTSO (Anti-malware Testing Estándar Organization), una entidad independiente que fija los estándares para analizar los diferentes productos *antimalware* y ver cuáles funcionan bien, cuáles no y cuáles son mejores. Debido a su complejidad, es muy difícil simular el *ransomware,* estudiarlo para estandarizar pruebas, pero se está trabajando en eso.

Foto: Felipe Cazares

Eddy Williems, de G Data.

¿Qué recomendaciones puede darnos a los ciudadanos para protegernos?

El problema fundamental siempre será el factor humano. Los usuarios hacen clic irresponsablemente y una práctica sana es ser precavidos en el uso de los clics. Además, somos negligentes en la instalación de las actualizaciones en las aplicaciones; en gran medida si los sistemas operativos y las aplicaciones se mantuvieran al día, no habría que apoyar la responsabilidad en las soluciones antivirus. El aprendizaje es muy lento, pero las amenazas se hacen cada vez más sofisticadas y más rápidas.

¿Podemos vivir tranquilos conectados a internet?

Sí, podemos, pero hay tener ciertas precauciones básicas; la industria de la ciberseguridad está avanzando y cada vez es posible cubrir nuevos frentes. Es como caminar en el bosque: usted se aplica repelente porque los mosquitos pueden atacarlo; eso ayuda, pero siempre puede haber una serpiente y tenemos que ser muy cuidadosos. ■

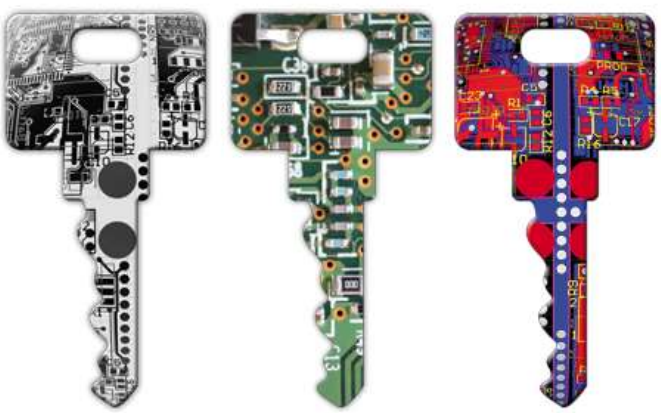


Imagen: Gerd Altmann (Geralt) en www.pixabay.com (https://goo.gl/H4Fj6P). Licencia CC0 Creative Commons.

Las llaves de la ciberseguridad están en manos de cada ciudadano. Prácticas sencillas como actualizar las aplicaciones ayudan a disminuir los riesgos.