La ciberguerra: riesgo del siglo XXI para las instituciones y empresas

Asael Villanueva | Redacción Nacional

Miles de empresas y organizaciones de todo el mundo reciben a diario **ataques cibernéticos**, ¿pero, **por qué no nos enteramos** o no escuchamos qué suceda tan comúnmente?

La razón: **los equipos de ciberseguridad**.

Pablo Tamez es ***Chief Information Security Officer*** en el **Tec de Monterrey** y desde hace 2 años es el **líder de la estrategia** de ciberseguridad. Además se encarga de este rubro en **TecSalud, Tecmilenio y Sorteos Tec.**

En entrevista con **CONECTA,** Pablo detalló algunos **puntos clave de ciberseguridad** de la institución de los que él y su equipo se encargan.

*“Los países de donde provienen la mayoría de los ataques [al Tec] son **Brasil, China, Estados Unidos y Rusia**”*

¿REALMENTE HAY ATAQUES?

Pablo afirma que esa es **una de las preguntas más recurrentes** que le hacen las personas a quienes les **resulta increíble** que este tipo de amenazas sucedan.

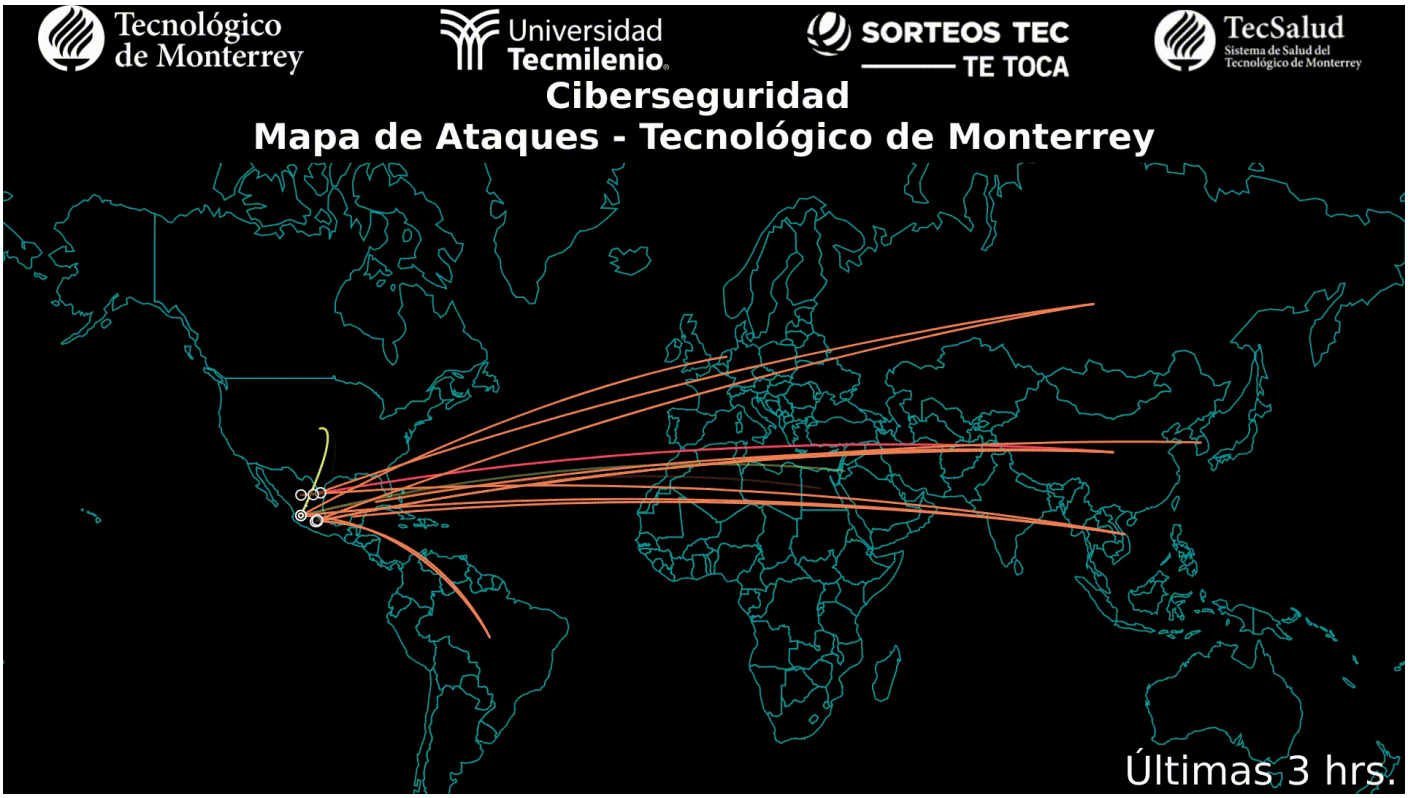
/>>

*"**Apenas publiques algo en Internet va a ser atacado.** No porque lo conozcan, sino porque hay robots que están automáticamente buscando"*, comentó.

"Que no lo sepamos no quiere decir que no esté pasando", recalcó Tamez quien menciona que, por ejemplo, **el Tec de Monterrey recibe en promedio 2 millones de ataques cibernéticos al mes,** los cuales son detenidos por el equipo de ciberseguridad.

*"Los países de donde provienen la mayoría de los ataques [al Tec] son **Brasil, China, Estados Unidos y Rusia**"*, afirmó Pablo.

En el Tec, estos ataques pueden ser observados en monitores en tiempo real, mostrando de dónde provienen y qué están intentando atacar.



/>>

LOS DEFENSORES DE LA INFORMACIÓN EN LÍNEA

Para Tamez, que las **instituciones cuenten ahora con este tipo de infraestructura es como un seguro de auto: lo tienes para que te proteja, pero esperas no utilizarlo.**

Explica que, dentro de los **ataques más comunes**, podemos encontrar **dos tipos**:

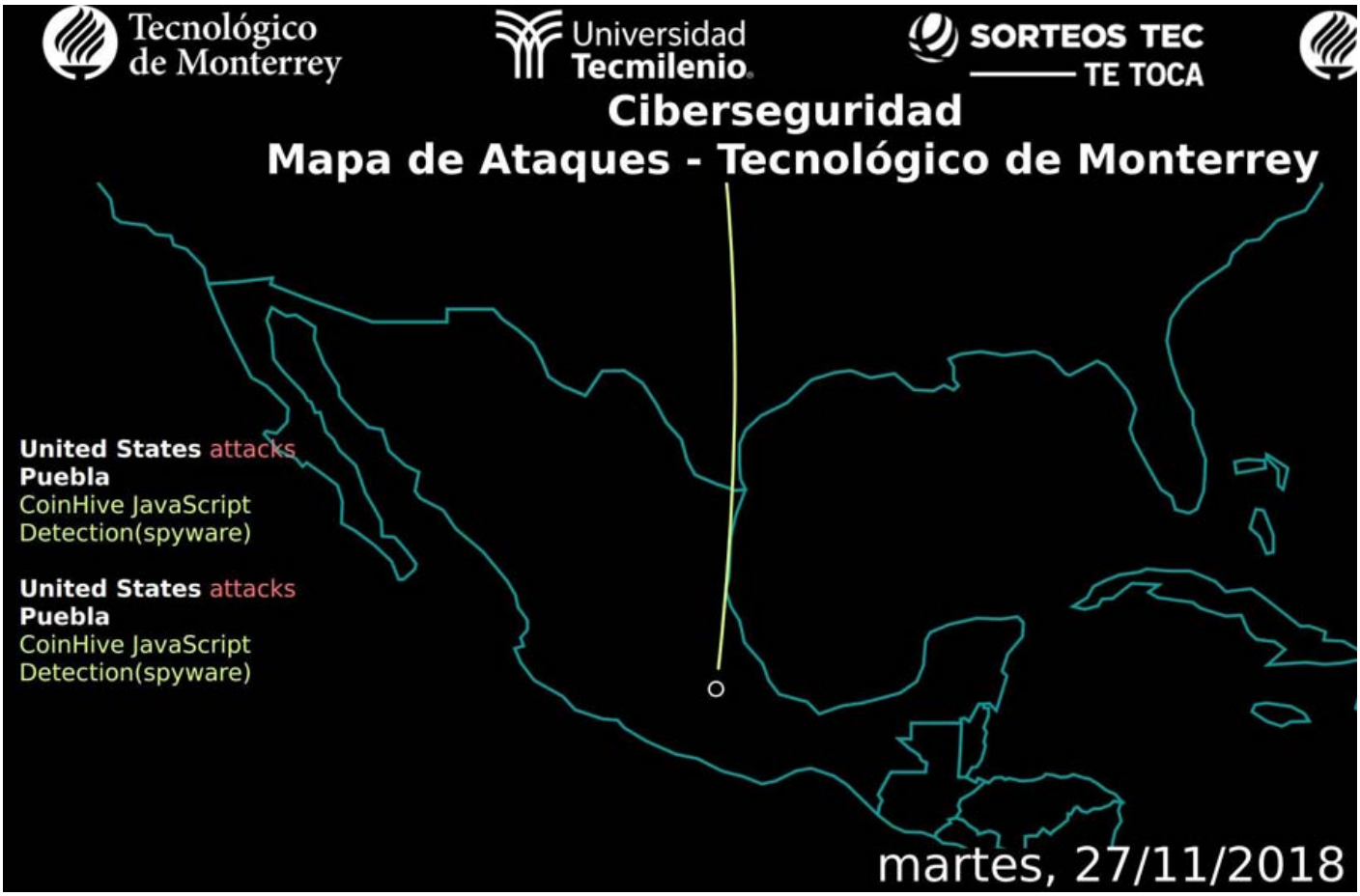
- ***Ataques al azar****. Es un ataque común y se realiza de manera automática o manual buscando encontrar alguna falla en un sistema para ingresar, robar datos o realizar ataques desde esos servidores.*

- ***Ataques dirigidos****. Tienen un objetivo en específico, ya sea un servidor, un lugar físico o el robo de datos de una persona en especial.*

Estos ataques pueden provocar la **caída de algunos servicios**, el **mal funcionamiento de algunos sitios** o incluso el robo de datos sensibles.

/>>

Uno de los **casos más comunes**, según Tamez, es la **suplantación de identidad o *phishing,*** en el que alguien se hace pasar por otra persona o una institución (ya sea bancaria o de otro tipo) y donde **el usuario ingresa sus datos pensando que está en el sitio real.**

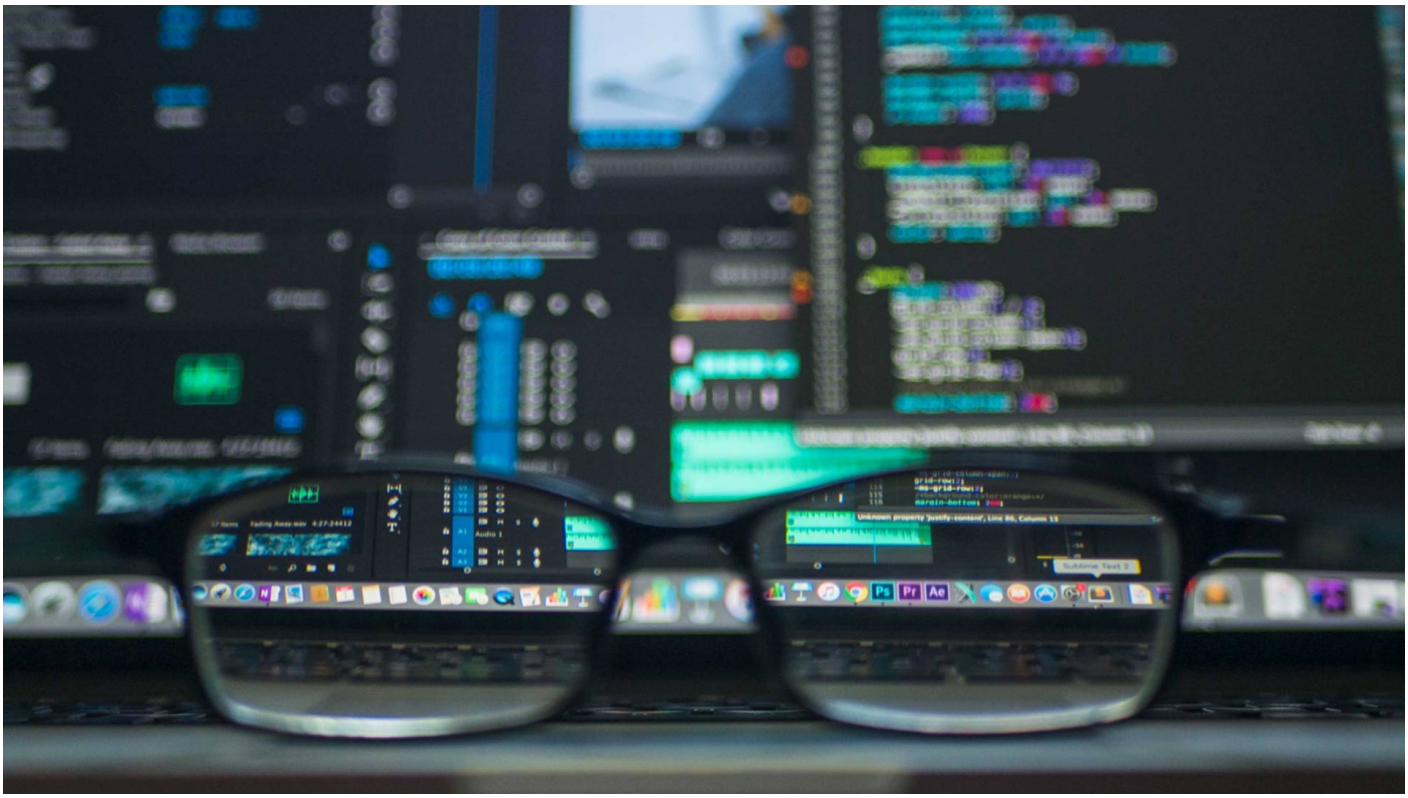


/>>

¿POR QUÉ ATACAN?

Tamez además comenta que **entre los motivos de los ataques** está el tema de la **reputación** entre la comunidad de hackers.

“Hay plataformas donde los hackers presumen sus logros y se retan entre ellos a hackear información sensible de una organización o persona”**,** aseveró.


/>>

Otro de los motivos es el **abuso de recursos.** En instituciones con **recursos muy grandes de enlaces y servidores**, los hackers pueden generar ataques o minar bitcoins, por mencionar algunos.

*“Otro, **de los más peligrosos** es obviamente el **robo de información**”*, afirmó el experto.

Frente a los riesgos que representan estas amenazas en el terreno virtual, **Tamez considera que instituciones y personas deben prestar atención a la información que se publica en internet.**

*“**Es muy importante cuidar la información** que otorgan en las redes sociales, y número dos, la verificación en dos pasos es muy improbable que puedas ser vulnerado, porque aparte del password ya tienes otro filtro de seguridad”,* finalizó.

.

LEE TAMBIÉN: