THREATSCOUT®

N.04
Marzo, 2021

ESPIONAJE COMERCIAL

"Evaluación y proyección de impacto en tiempos de digitalización acelerados"

WWW.TEKIUM.MX

Extracto

El espionaje comercial es la actividad encubierta que busca adquirir información específica sobre una estrategia, producto, diseño, fórmula o en general cualquier elemento de nuestros activos críticos que permitan una ventaja comercial/industrial a la competencia nacional o extranjera. En este papel de trabajo realizaremos una aproximación a los riesgos -post pandemia- de esta actividad en momentos de creciente digitalización.

Introducción:

Nadie quiere hablar de espionaje dentro de una organización. ¿Por qué vamos a gastar tiempo en un tema del cuál no tenemos indicadores?; ¿Eso es un tema de las grandes corporaciones, eso no sucede acá en Monterrey, Toluca o Querétaro cierto?

Nadie -tampoco- quiere hablar de la desestabilización que puede sufrir una organización vía daño reputacional, exposición pública de clientes, accionistas y/o nómina, campañas de desinformación dirigidas o robo de activos críticos por nombrar algunas de las pesadillas que mantienen despiertos en las madrugadas a los jefes de seguridad corporativos.

De acuerdo con varios líderes de negocios consultados, la naturaleza de lo que ellos consideran la amenaza de espionaje está clara y en general, aseguran que sus medidas de protección contra esta actividad son las correctas.
Sin embargo, al hurgar un poco más sobre esas ‘medidas de contraespionaje’, podemos observar que están poco o nada actualizadas en relación con la dinámica de globalización de riesgos. En otras palabras, están desfasadas y su efectividad no ha sido comprobada contra vulnerabilidades actuales.

Ahora bien, ¿cuán extendido está el espionaje comercial en la región? Según Kaspersky, desde el 2018 hasta el 2020 vienen detectando ataques selectivos de espionaje contra industrias mexicanas a través de un conjunto de herramientas denominados MT3 y bautizado como MontysThree por el mismo equipo de investigadores de Kaspersky.[1]

Pero ¿de cuántas empresas estamos hablando? Eso es un poco más delicado. Muy pocas organizaciones están dispuestas a aceptar que han sido víctimas de espionaje porque ello significaría que fueron vulneradas y eso -a su vez- nos llevaría a preguntar: ¿cómo y en qué forma?

1 https://bit.ly/3w7weh6

Imagínese que usted sea la persona encargada de protección patrimonial o seguridad corporativa de una empresa y ante una mínima sospecha de espionaje comercial/industrial usted tenga que realizar un análisis de vulnerabilidades para disipar o profundizar esa sospecha. Considere lo siguiente:

a. ¿Cuántos de nuestros empleados participan en blogs privados o públicos dónde se divulgue información técnica propietaria o relacionada con la organización?
b. ¿Cuántos de nuestros empleados postean sus capacidades y/o cursos ofrecidos por nuestra organización en sus perfiles?
c. ¿Cuántos de nuestros empleados postean sus afiliaciones técnicas o profesionales en las redes junto con el nombre o logo de la organización?
d. ¿Cuántas imágenes de eventos de nuestra organización hay en la web que indiquen ubicación?
e. ¿Cuántas imágenes tienen nuestros corporativos en redes sociales? ¿Se aprecian lugares, casas, tienen geo-data?
f. Cuántas publicaciones hay en las redes sociales que apunten a eventos futuros de nuestra organización (aniversarios, lanzamientos, etc.)
g. ¿Qué información hay en internet sobre nuestros socios comerciales y/o proveedores?
h. ¿Hemos revisado qué información postean nuestros socios comerciales y/o proveedores sobre nosotros?

Si al obtener toda (o parte) de estas respuestas usted todavía cree que su organización no es vulnerable a una operación de espionaje, entonces el elefante puede salir de la cristalería sin contratiempos y con los ojos vendados.

Digitalización y espionaje:

La pandemia nunca fue la razón por la cual se comprendió la importancia de la digitalización de los procesos; el COVID19 fue el catalizador de esa aceleración que ya venía gestándose en muchas áreas, especialmente con la modernización del sector financiero.

Sin embargo, varias compañías se vieron obligadas –cómo una medida de supervivencia- a acelerar la digitalización de sus procesos sin que necesariamente el 'back office' haya estado a la par de esa transformación.

Estos desniveles (converger la necesidad de digitalizar procesos con la integración de data de calidad en el back office para apoyar el trabajo remoto), deja entreabierta una serie de puertas que podrían facilitar, entre otras, la exfiltración de información sensible para la organización.

Súmenle a eso un crecimiento en la procura de trabajos de INTELIGENCIA COMPETITIVA[2] en los últimos meses en áreas tales cómo: solicitudes de información sobre fusiones y adquisiciones, análisis de potenciales nuevas regulaciones, evaluación y análisis de blogs sobre la competencia, análisis de redes sociales, análisis de sentimiento sobre determinados productos, servicios y/o impacto (o falta de) respecto a estrategias de mercadeo.

Cómo podemos observar, tanto las reorganizaciones internas producto de más de un año de pandemia y trabajo remoto, amén de este -inusual- crecimiento en solicitudes de inteligencia competitiva, debería llamarnos la atención, aunque fuese para revisar nuestro estatus con respecto a las defensas de los activos críticos de la organización.

Pero vayamos nuevamente a la génesis del espionaje comercial, ¿cuáles son las tres categorías principales para esta actividad?:

a. Cuando grupos especializados en falsificación y/o bandas de crimen organizado tienen como objetivo principal el producto de una compañía u organización.
b. Cuando un infiltrado (ìnsider) o una empresa en competencia directa tiene como objetivo principal los procesos y activos de otra compañía u organización.
c. Cuando un Estado o un grupo apoyado por un Estado (APT)[3] tiene como objetivo principal los secretos industriales o comerciales de una compañía u organización.

Por lo menos en Latinoamérica, el espionaje basado en inteligencia sobre productos y/o procesos es mayor que el espionaje amparado o ejecutado por un Estado extranjero contra industrias y organizaciones científicas y/o comerciales...pero ese fenómeno podría cambiar muy rápido.

Ciertamente el espionaje comercial entre competidores, nacionales o extranjeros, de un mismo ramo es común y la mala noticia es que se perfila un crecimiento precisamente por el avance en los procesos de digitalización que se observan a raíz de la pandemia.

¿Cuál será la próxima estrategia de mercadeo de la cerveza X?; ¿Qué nuevo producto están desarrollando en la industria de panificación Y?; ¿Cómo son las condiciones

2 Proceso estructurado, 'legal', diseñado para reunir, evaluar y/o proyectar datos, e informaciones sobre competidores, actuales o futuros, para la toma de decisiones estratégica, generar prácticas comerciales eficientes y elevar la seguridad interna -contrainteligencia- para la protección de información crítica de interés para otros en el mercado o sector comercial/industrial.

3 APT : Advanced Persistent Threat o Amenaza Avanzada Persistente. Generalmente se refieren a grupos de hackers muy avanzados con especializaciones particulares en su accionar.

de la fusión de marcas R y M que se están negociando?; ¿Qué información comprometedora podrá haber de los directivos U y K de X organización?

Las respuestas a este tipo de preguntas se negocian con frecuencia con compañías especializadas en espionaje comercial/industrial en México y en la región. La pandemia aceleró los procesos de digitalización, pero también aceleró la necesidad de arreciar la competitividad en sectores que anteriormente convivían en cierta armonía. Por ello, los riesgos derivados de esta nueva competencia por sobrevivir también varían según el entorno empresarial (número de competidores y share del mercado) y cuán fuerte haya golpeado la pandemia.

La disrupción de la interacción social, los cambios en el comportamiento de los consumidores, la desigualdad digital, el tele-working y la dificultad para planificar estratégicamente por la incertidumbre sanitaria son algunas de las consecuencias, oportunidades y riesgos que moldearán el ecosistema comercial e industrial en los meses por venir.

No duden que hay individuos y organizaciones ávidas en conocer, replicar y de ser necesario, entorpecer, los esfuerzos de crecimiento de una organización en esta época. El resguardo de la información sensible (estrategias, planes, activos, etc.) es una de las principales prioridades que se debería reforzar. La reacción normal ante una situación anormal es una reacción anormal. No subestimen la capacidad de espionaje del entorno.

2021–2025 Latinoamérica como campo de batalla alterno:

4 años parece poco en el desarrollo de una organización, pero esos mismos 4 años son un salto cuántico respecto a los avances en materia de inteligencia artificial (AI) que se verán. Por ejemplo, buena parte del comercio global es digital, las grandes compañías tecnológicas obtienen, mediante esas transacciones (nombres, números, direcciones, empleos, registros de seguros, inventarios, costos, etc.) grandes cantidades de data cuyo uso final generalmente se cruza entre bases de datos con destinos poco transparentes tanto para el consumidor, como para muchos entes oficiales.

De acuerdo con el Internet Security Threat Report de la compañía Symantec del 2019: “La razón más probable que una organización sufra un ataque específico (o dirigido) es por la obtención de inteligencia previa que hayan podido captar; esto motiva al 96 por ciento de los grupos de actores adversariales (o APT) a iniciar con operaciones de espionaje antes del ciberataque”[4].

La geopolítica cibernética está generando profundas divisiones en el uso (y mal uso) de la data que se obtiene cada segundo. La batalla por la supremacía del campo cibernético que protagonizan los Estados Unidos y China está generando una bifurcación del uso y reserva de la data obtenida, que poco a poco se hará más evidente en áreas como la militar.

La necesidad de inteligencia, más allá, de coadyuvar a la defensa del perímetro digital de las organizaciones, se traduce -hoy por hoy- en conocimiento de la competencia, del mercado y el último caso, de la posibilidad de anticipar patrones de conducta del consumidor y/o las reacciones a cambios -vía software de análisis de sentimientos- en las redes. En otras palabras, aquellos que producen, analizan y generan conocimiento con ese tipo de data, están sentados sobre un tesoro... con muchos pretendientes.

Ese es el caso actual de muchas de las organizaciones que analizan y cruzan la data que obtienen vía redes sociales, ventas, bases de datos, etc. Gracias a la evaluación de esa información, se obtiene inteligencia que nos permite: desde tomar decisiones, hasta generar estrategias. ¿Imagínense que nuestra competencia tenga la misma data?; ¿Cómo cambiaría eso nuestra estrategia de mercadeo, de distribución o de inversiones a corto y mediano plazo?

En el futuro cercano, ese escenario podría ser común y la

4 https://bit.ly/3w9yOmE

respuesta sobre ¿quién se beneficia ante sets similares de data? (¿la competencia o mi organización?) podría depender más de la nacionalidad de mis aliados/asociados/inversionistas, que de la capacidad de agilidad gerencial o las cualidades de anticipación de mis ejecutivos.

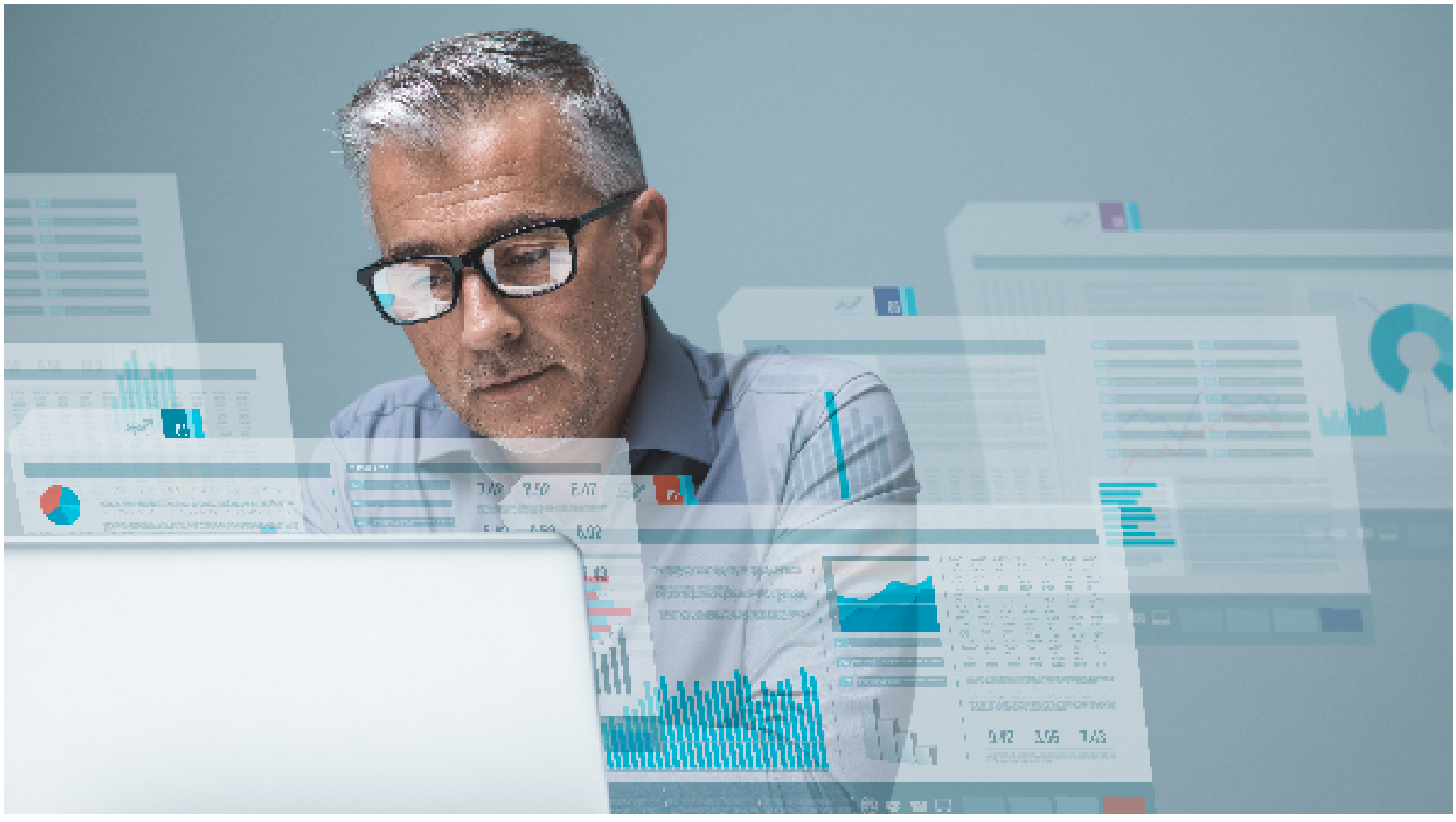
Por ejemplo, el Centro Nacional de Contrainteligencia y Seguridad de los Estados Unidos (NCSC) acaba de publicar un trabajo titulado: "Mitigación del riesgo de Infiltrado en las entidades de infraestructura crítica de los Estados Unidos": Guía para una perspectiva de Inteligencia[5]; más allá de la pertinencia del trabajo, un párrafo proyecta lo que el Centro de Contrainteligencia y Seguridad Nacional (NCSC) anticipa:

"La naturaleza descentralizada y digital de la infraestructura crítica mundial crea vulnerabilidades que pueden ser explotadas por entidades de inteligencia externas, así como están atacando las facilidades y redes que apuntalan la industria energética global, los mercados financieros, servicios de telecomunicaciones, gobierno y capacidades militares de defensa".

Lamentablemente, de una u otra forma, empresas e industrias de cualquier latitud del continente nos veremos afectados por la constante fuga de data a la que estamos expuestos, pero las consecuencias serán más perniciosas para aquellos que no hagan nada.

La creciente digitalización de los procesos empresariales genera presiones alternas a juntas directivas que ya están batallando por sobrevivir en una economía con obvios signos de recesión. Son momentos que definirán nuestras organizaciones en los años por venir. El espionaje es una herramienta más del arsenal de aquellos que se quieren beneficiar a costa de otros. Es una herramienta que evoluciona con la tecnología, que se abarata y se vuelve más efectiva cuando se combina con factores alternos cómo lo es el factor humano (infiltrado).

La evolución de la inteligencia artificial (AI) en los años por venir definirán nuevas avenidas para el uso de las data que generamos, por lo que el valor de las medidas de contrainteligencia cibernética que se tomen ahora, serán el mejor escudo de prevención ante un entorno que evoluciona hacia más vectores de riesgo que hacia una estabilización de los mismos.



5 https://bit.ly/3rwwFhw

Acerca de Nosotros

Somos un equipo de expertos en ciberseguridad, apasionados por innovar y desarrollar soluciones para contrarrestar retos y riesgos del entorno digital. Creemos en una evolución digital constante que, paralelamente, requiere de capacidades específicas para cerrar paso a quienes hacen el mal.

Nuestra manera de hacer esto, y lo que nos motiva a diario, es poder brindar a empresas la tranquilidad de dejar su ciberseguridad en nuestras manos.

TEKIUM

Avenida Patriotismo #767, piso 7. San Juan Mixcoac, C.P 03730. Ciudad de México.