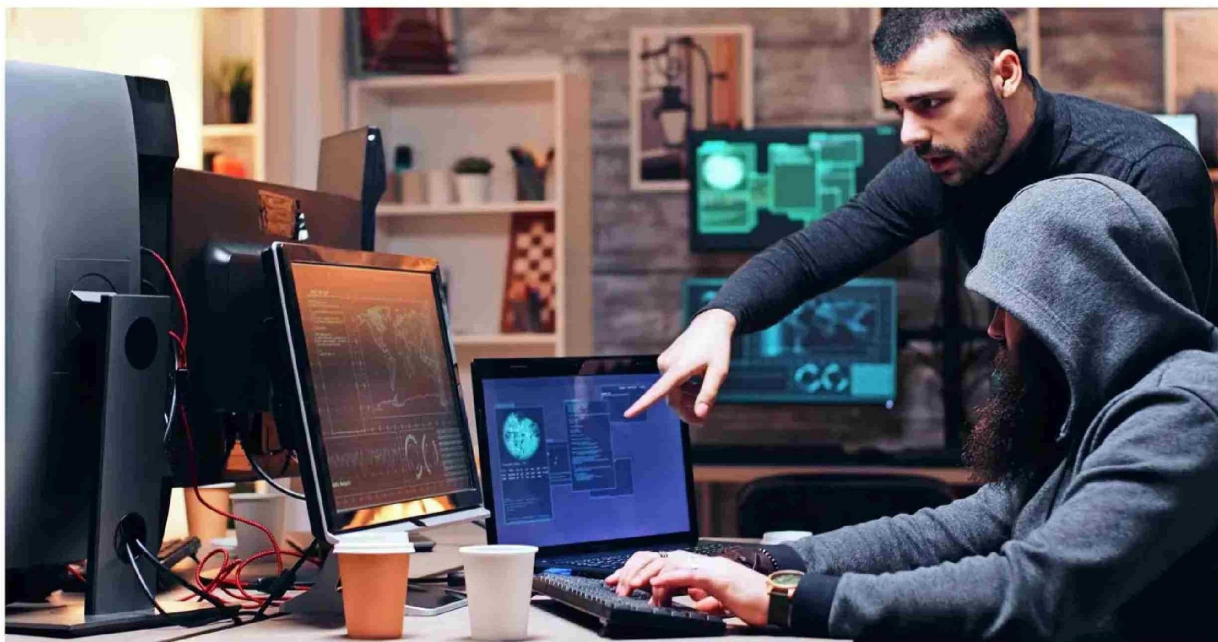


HACKERS QUE OFRECEN SUS SERVICIOS A CAMBIO DE NO VOLVERLAS A ATACAR

Consultoría criminal: La nueva técnica que amenaza la ciberseguridad de las empresas chilenas



Expertos aseguran que compañías medianas y pequeñas son las más expuestas a este nuevo tipo de ciberdelito, en parte, por la falta de cortafuegos en sus sistemas. Además, apuntan a que se debe contar con mejores lineamientos para definir el denominado "hackeo ético".

MAGDALENA ESPINOSA

Una nueva táctica criminal aterrizó en Chile en materia de ciberseguridad. Desde hace algunos meses, las empresas ya no solo se enfrentan al robo, secuestro y extorsión de información sensible, sino que las mafias virtuales sumaron otro plato al menú: el ofrecimiento de entregar informes técnicos para mejorar sus barreras de seguridad, después de amenazar a las compañías.

Parece insólito, pero es un fenómeno que comenzó hace unos años a nivel mundial y en Chile, aparecieron los primeros casos a fines de 2023. Hasta el momento, ninguno es público, porque recién a partir de este año las firmas están obligadas a reportar estos incidentes.

Herwin Cajamarca, gerente de Ingeniería de Negocios del data center IFX Chile, explica que lo "novedoso" es que los atacantes ofrecen consultorías posincidentes para "ayudar" a las empresas con información y consejos que les permitan evitar futuras infecciones.

"Hace un tiempo atrás escuché de un banco en Ecuador que sufrió un ataque de ransomware (se-
questró de datos) y los mismos ciberdelin-
cuales les ofrecieron que si se les contrataba como asesores,
no volverían a ser atacados. En ese momento
pareció un caso aislado, casi de estudio, pero hoy

está siendo cada vez más común", comentó el ingeniero. El modo de acción de los delin-
cuales digitales consiste en atacar las
redes y solicitar un rescate me-
diante bitcoins. Luego, a los afecta-
dos se les da un número de call cen-
ter para agendar la entrega del in-
forme técnico, con el objetivo de "ayudar"
mediante una consultoría.

OFERTA ALARMANTE

Jorge Atrón, exsubsecretario de Telecomunicaciones y exase-
sor presidencial en ciberseguri-
dad, conoce de cerca la técnica y la
califica como "alarmante". "Los delin-
cuales ingresan a las redes y luego
amenazan con atacar o filtrar infor-
mación sensible si no contratan sus
servicios de ciberseguridad". Esta oferta a me-
nudo se presenta como una con-
sultoría o una evaluación de ries-
gos, pero en realidad es un inten-
to de extorsión. Lo que realmente
necesitan las empresas es un in-
forme técnico de daños y una e-
valuación honesta de sus vulnera-
bilidades, cosa que no propor-
cionan este tipo de "hackers éticos",
sino que buscan asegurar un be-
neficio económico a través del
miedo y la coacción".

Andrés Corón, gerente de ciber-
seguridad de Entelgy Chile,
coincidió con Atrón y aseguró que
"esta estrategia no solo busca
maximizar el beneficio económi-

co, sino también reducir la expo-
sición directa de los atacantes, de-
legando la ejecución a afiliados y
ampliando su alcance global".

Los ataques a entidades como
bancos o retailers hicieron que las
grandes compañías nacionales
tomaran rápidamente medidas
para protegerse. Sin embargo, los
delinquentes centraron su aten-
ción en los eslabones más débiles
de la cadena: medianas y peque-
ñas empresas.

Luis Porta, director ejecutivo de
Accenture Chile, advirtió que "en
un ecosistema digital interconec-
tado, las brechas en ciberseguridad
en empresas de menor tamaño o
menor madurez tecnológica pue-
den representar un punto de en-
trada para amenazas que afecten a to-
do el sistema. Además, la accele-
rada adopción de nuevas tecnolo-
gías como la inteligencia artificial (IA),
sin procesos adecuados de e-
valuación de riesgos, está generando
nuevas vulnerabilidades".

FACTOR SORPRESA

Luis Porta explicó que de acuer-
do a un informe del Foro Econó-
mico Mundial, el 42% de los encues-
tados en América Latina declaró
que sus países no están prepara-
dos para enfrentar incidentes gra-
ves en infraestructura crítica.

El elemento sorpresa es la prin-
cipal punta de lanza de estas or-
ganizaciones, pues no existe una es-

trategia única para perseguirlos. De
hecho, el ejecutivo de IFX Chile
explicó que nunca las empresas
están 100% a salvo de estos inci-
dentes, por lo que es crucial contar
con un plan multicapas, dinámico y
adaptativo.

Consultoras, empresas de tec-
nología y el mundo académico
coinciden en que la estrategia de
ciberseguridad nacional debe con-
tar con una "visión sistémica".

El ejecutivo de Accenture puso
énfasis en que no basta con pro-
teger solo los data centers, sino que
se debe contar con una estrategia
que abarque desde la educación y
conciencia de los clientes, incluya
la cadena de proveedores, y arme
gobernanzas y planes de respuesta
a incidentes. "Chile tiene talento y
capacidades, pero debemos cerrar
brechas, especialmente en secto-
res más expuestos y con menos
recursos", agregó.

En materia de consultoría, el de-
bate no está exento de acaloradas
discusiones. Incluso, cuando se
discutió la Ley Marco de Ciberse-
guridad, vigente desde este año, el
denominado "hacker ético" fue un
punto de divergencia entre los ex-
pertos.

Uno de sus defensores es Ale-
jandro Hevia, director del Labora-
torio de Criptografía Aplicada y Ciber-
seguridad de la Universidad de Chi-
le, quien explicó que el hackeo ético
es un proceso hecho por un
profesional de la ciberseguridad,
registrado, que avisa de las fallas me-

42%
DE LOS ENCUESTADOS
EN AMÉRICA LATINA
por el Foro
Económico
Mundial declaró
que sus países no
están preparados
para enfrentar
incidentes graves
en infraestructura
crítica.

Un hacker ético
comparte las
fallas apenas
son
encontradas y
no exige
recompensa a
cambio, pero
puede ser
contratado
posteriormente
para un
análisis.

El elemento
sorpresa es la
principal punta
de lanza de
estas
organizaciones,
pues no existe
una estrategia
única para
perseguirlos.

dante una notificación responsa-
ble. Y agregó: "Si una persona soli-
cita un monto de dinero, después
de vulnerar las barreras de segu-
ridad de una empresa para dar a co-
nocer el método de cómo lo logró,
es extorsión, no hackeo ético".

Bajo su mirada, un hacker ético
comparte las fallas apenas son en-
contradas y no exige recompensa
a cambio, pero puede ser contra-
tado posteriormente para un aná-
lisis. "La ley chilena da luces de
cómo se hace este procedimien-
to", añadió.

PUNTO CRÍTICO

Sin embargo, el mecanismo de
cómo se entrega la información es
un punto crítico. Juan Pablo Gon-
zález, director de datos personales y
ciberseguridad en HD Group, ex-
plicó que "es importante avanzar en
estándares y reglas claras. Eso no
ha sido discutido con profundidad.
En la práctica, el fenómeno que está
ocurriendo es que se detectan vul-
nerabilidades en las empresas y se
exigen beneficios económicos. Eso
empaña la labor de aquellos in-
vestigadores de 'sombrero blanco' y se
entra a un terreno gris".

A su parecer, "debemos definir
los espacios donde los profesiona-
les puedan detectar fallas, como
hackatones o, incluso, abrir proce-
sos en que las compañías definan
antes las recompensas en caso de
detectar fallas y promover la ge-
neración de incentivos", señaló.

Pese a que la ley está vigente,
González apuntó a que todavía fal-
tan lineamientos que detallen con
mayor definición el marco de ac-
ción en esta materia. "Es un tema
pendiente", remató.