**INTENTO DE HACKEO A LA EMPRESA BIZLAND**

**ENSAYO VERSION 2.0**

***CARRERA: TECNICATURA EN DESARROLLO DE SOFTWARE***

***MATERIA: INTRODUCCION A REDES***

***ALUMNA :VANINA BELEN COSTILLA***

***EMAIL:COSTILLAVANINA@GMAIL.COM***

***FECHA DE ENTREGA 2/06/23***

**INTRODUCCION**

A nadie escapa la enorme influencia que ha alcanzado la informática en la vida diaria de las personas y organizaciones, y la importancia que tiene su progreso para el desarrollo de un país. Las transacciones comerciales, la comunicación, los procesos industriales, las investigaciones, la seguridad, la sanidad, etc. son todos aspectos que dependen cada día más de un adecuado desarrollo de la tecnología informática. Junto al avance de la tecnología informática ha surgido una serie de comportamientos ilícito como el intento de hackeo a la compañía Bizland..

La compañía Bizland que administra el sistema del boleto prepago de colectivo en provincias como Tucumán (CIUDADANA/METROPOLITANA),Córdoba(RED BUS), Salta(SAETA), La Rioja(SIRVE) sufrió un ataque por medio de un programa malicioso llamado LockBit que puso en crisis al sistema de transporte público generando problemas para cargar las tarjetas y una lenta solución provocando malestar entre miles de usuarios.

DESARROLLO

## ¿Qué es Bizland?

Bizland es una empresa especializada en soluciones de procesamiento transaccional,con más de 40 años en trayectoria de **sistemas** para el **transporte público.**



# INTENTO DE HACKEO DE LA COMPAÑÍA BIZLAND

La empresa Bizland confirmaron que la caída de los sistemas que afectan la carga de saldo en las tarjetas del transporte urbano de pasajeros capitalino –y de Tucumán, de Salta y de La Rioja– provocados por el programa malicioso LockBit.

¿Qué es LockBit? Es un programa informático que está hecho para bloquear el acceso a sistemas informáticos y pedir rescate. “Por eso se llama ‘ramsomware’. Ramsom es rescate en inglés”.

Para que se entienda aún mejor, “Es una evolución de un virus informático. Un programa que funciona igual que un virus biológico: infecta, hace un daño y contagia. Pero el ramsomware que encripta o cifra los archivos, ya no son más accesibles.

Lo que hace LockBit es impedir que se acceda a los archivos, y para poder volver a hacerlo, hay que pagar un rescate. Ese pago se suele realizar a través de billeteras virtuales de criptomonedas. Una vez que ese pago se realizó, se envía una herramienta que desencripta la información.

Al menos, así funciona un rasomware. “Pero en LockBit, hacen un daño más: además de encriptar, copian y roban cierta cantidad de archivos. Entonces, la extorsión es doble: para recuperar la información y para evitar que lo publiquen”.

Según pudo saber  hubo un pedido de rescate a Bizland, pero la empresa se negó a pagarlo.

“LockBit busca automáticamente objetivos valiosos, propaga la infección y cifra todos los sistemas informáticos accesibles en una red. Este ransomware se utiliza para lanzar ataques selectivos contra empresas y otras organizaciones. Como es un ciberataque auto pilotado, los atacantes de LockBit se caracterizan por amenazar a organizaciones de todo el mundo con interrumpir las operaciones por la detención repentina de las funciones esenciales, extorsionarlas para el beneficio financiero del hacker, y robar datos y publicación ilegal de estos como chantaje si la víctima no paga el rescate”

Está activo desde 2019, y uno de sus ataques más conocidos fue al servicio postal del Reino Unido, Royal Mail, a principios de este año.

En una entrevista se explico que los creadores diseñaron un malware “que cualquiera podía utilizar, con el que sólo señalas un objetivo y haces clic”.

“Actualizan su software, se fijan constantemente en la opinión de los usuarios y se preocupan por la experiencia de estos al emplearlo. También cazan furtivamente a gente de bandas rivales. En sí, lo dirige como un negocio y, por eso, es sumamente atractivo para los delincuentes”, remarca.

En esa misma línea, un “RaaS”: “Significa ‘ransomware as a service’, tienen el programa y tienen socios. Son proveedores de ese programa malicioso. Vos les pagas a ellos para que te den el ransomware, y luego reparten las ganancias de los rescates”.

En la lista de ataques hay sitios, empresas y organizaciones de todo el mundo. En febrero de este año, atacaron a la aseguradora La Segunda, a la empresa de medicina prepaga Osde y al Grupo Albanesi, proveedor de gas.

Se destaca que los objetivos viables “son aquellos que se sentirán tan obstaculizados por la interrupción, que preferirán una suma abundante, y que tendrán los fondos para hacerlo”, y que por eso, provocan ataques generalizados contra grandes empresas.

No se sabe quién está detrás, pero se señala que no atacan en Rusia ni en países con buena vinculación con el Kremlin.



Por su parte, Bizland explicó que este ataque no implicó el robo de datos sensibles de los usuarios ni fondos, pero sí afectó a la operatividad de su red de comunicaciones.

El ataque no pudo superar las barreras de contención para este tipo de intrusiones con que cuenta la empresa, pero sí llegó a impactar sobre los servidores de comunicaciones por lo que se está viendo afectada la posibilidad de acreditación de saldo por parte de los usuarios en algunos de los puntos de carga de la red.

La empresa realizará oportunamente la denuncia correspondiente para que la Justicia investigue este episodio delictivo y se pone a disposición de las autoridades para aportar todos los datos de interés para la investigación y trabajar de manera conjunta.

Los técnicos están trabajando para restablecer la normalidad de las comunicaciones a la mayor brevedad posible. A raíz de lo sucedido, la empresa informó que, como medida de contingencia frente al ataque informático, se duplicaron los viajes con saldo negativo para que los usuarios puedan evitar inconvenientes en el uso del transporte público.

Sin embargo, los pasajeros deberán compensar ese saldo cuando el sistema vuelva a la normalidad y la red de cargas funcione sin inconvenientes.

Finalmente luego de varios días se logro restablecer el sistema de boleto prepago habilitando los puntos de recarga de la tarjeta .



**CONCLUSION**

Se puede decir que este programa malicioso LockBit puede ocasionar grandes perdidas de dinero en pocos segundos y afectar la privacidad de las compañias sin que estas se percaten de ello.

Existe en el mundo un gran interés por contrarrestar e investigar este tipo de conductas que afectan a la operatividad de la red de comunicaciones, dónde pudimos concluir la deficiencia de sistema utilizado por Bizland. Creo que se debe fortalecer leyes para que sean efectivas además de ser dinámicas como lo son las mismas tecnologías de la información para evitar inconvenientes a futuro.

Debemos tomar conciencia de la importancia de aplicar métodos de seguridad Informática en los sistemas domésticos o empresariales para evitar al máximo sufrir las consecuencias de estas acciones ilegales.

**REFERENCIAS**

<https://www.lavoz.com.ar/ciudadanos/que-es-lockbit-el-programa-malicioso-que-provoco-las-fallas-en-red-bus-y-farmacias/>

<https://www.lagaceta.com.ar/nota/990876/sociedad/por-intento-hackeo-peligra-recarga-tarjetas-colectivos-tucuman.html>

<https://www.cronista.com/economia-politica/hackearon-la-barrera-de-seguridad-de-transporte-publico-y-peligra-el-sistema-funciona-la-tarjeta/>

<https://radiotucuman.com.ar/nota/25781/hoy-se-normalizaria-la-carga-de-las-tarjetas-ciudadana>