Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

ATAQUE DE RANSOMWARE SACUDE A PROVEEDOR DE INTERNET TIGO

08 / 01 / 2024

CONTENIDO

INTRODUCCIÓN

En un giro impactante, el reconocido proveedor de internet Tigo se encuentra en el epicentro de un ciberataque masivo de ransomware, desencadenando una alerta nacional paraguaya de ciberseguridad. La división empresarial, Tigo Business, ha sido el blanco de la amenaza, atribuida al grupo de ciberdelincuentes Black Hunt. El incidente ha desencadenado respuestas rápidas tanto de la empresa como de las autoridades, generando preocupación sobre la seguridad digital en un mundo cada vez más conectado. En este contexto, exploraremos los detalles del ataque, las acciones tomadas por las autoridades y la importancia de la prevención en un escenario de crecientes amenazas cibernéticas.

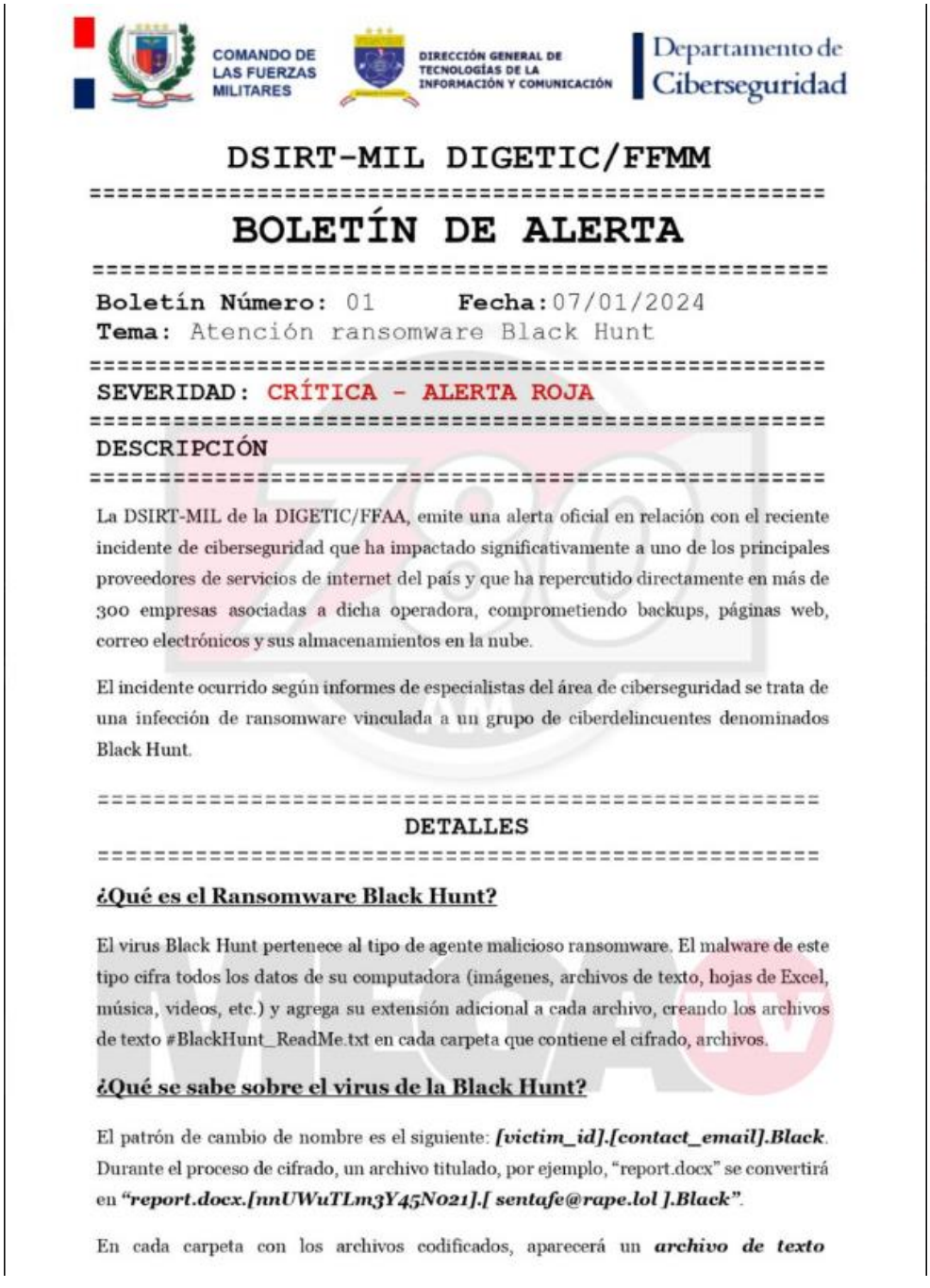
ATAQUE DE RANSOMWARE SACUDE A PROVEEDOR DE INTERNET TIGO

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2024_01_08_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	08/01/2024
Es día cero (0 day):	No

RESUMEN

En un impactante incidente de ciberseguridad, la reconocida empresa proveedora de internet, Tigo, ha sido víctima de un ataque de ransomware que ha afectado significativamente a su división empresarial, Tigo Business. La amenaza, vinculada al grupo de ransomeware conocido como “Black Hunt”, ha generado una alerta roja por parte de las Fuerzas Armadas de la Nación de Paraguay.



COMANDO DE LAS FUERZAS MILITARES

DIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Departamento de Ciberseguridad

DSIRT-MIL DIGETIC/FFMM

==========

BOLETÍN DE ALERTA

==========

Boletín Número: 01 **Fecha:** 07/01/2024

Tema: Atención ransomware Black Hunt

==========

SEVERIDAD: CRÍTICA - ALERTA ROJA

==========

DESCRIPCIÓN

==========

La DSIRT-MIL de la DIGETIC/FFAA, emite una alerta oficial en relación con el reciente incidente de ciberseguridad que ha impactado significativamente a uno de los principales proveedores de servicios de internet del país y que ha repercutido directamente en más de 300 empresas asociadas a dicha operadora, comprometiendo backups, páginas web, correo electrónicos y sus almacenamientos en la nube.

El incidente ocurrido según informes de especialistas del área de ciberseguridad se trata de una infección de ransomware vinculada a un grupo de ciberdelincuentes denominados Black Hunt.

==========

DETALLES

==========

¿Qué es el Ransomware Black Hunt?

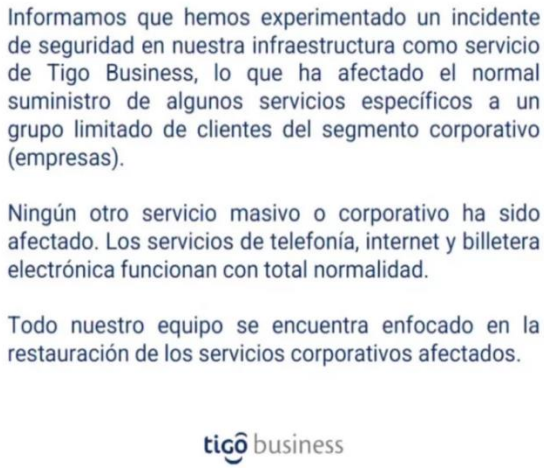
El virus Black Hunt pertenece al tipo de agente malicioso ransomware. El malware de este tipo cifra todos los datos de su computadora (imágenes, archivos de texto, hojas de Excel, música, videos, etc.) y agrega su extensión adicional a cada archivo, creando los archivos de texto #BlackHunt_ReadMe.txt en cada carpeta que contiene el cifrado, archivos.

¿Qué se sabe sobre el virus de la Black Hunt?

El patrón de cambio de nombre es el siguiente: ***[victim_id].[contact_email].Black***. Durante el proceso de cifrado, un archivo titulado, por ejemplo, “report.docx” se convertirá en ***“report.docx.[nnUWuTLm3Y45N021].[sentafe@rape.lol].Black”***.

En cada carpeta con los archivos codificados, aparecerá un ***archivo de texto***

El domingo 7 de enero, Tigo emitió un comunicado informando a sus clientes sobre un incidente de seguridad que ha afectado la infraestructura de sus servicios empresariales. La compañía aseguró que está trabajando incansablemente con equipos locales y regionales, con el respaldo de expertos técnicos, para restaurar los servicios afectados.



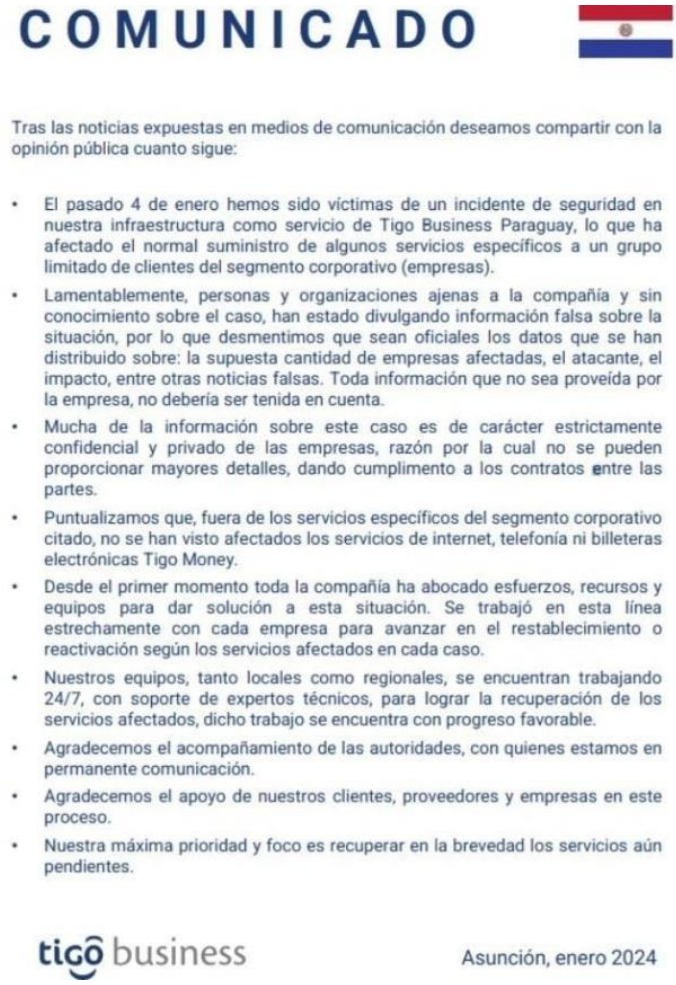
COMUNICADO

Informamos que hemos experimentado un incidente de seguridad en nuestra infraestructura como servicio de Tigo Business, lo que ha afectado el normal suministro de algunos servicios específicos a un grupo limitado de clientes del segmento corporativo (empresas).

Ningún otro servicio masivo o corporativo ha sido afectado. Los servicios de telefonía, internet y billetera electrónica funcionan con total normalidad.

Todo nuestro equipo se encuentra enfocado en la restauración de los servicios corporativos afectados.

tigo business



COMUNICADO

Tras las noticias expuestas en medios de comunicación deseamos compartir con la opinión pública cuanto sigue:

- El pasado 4 de enero hemos sido víctimas de un incidente de seguridad en nuestra infraestructura como servicio de Tigo Business Paraguay, lo que ha afectado el normal suministro de algunos servicios específicos a un grupo limitado de clientes del segmento corporativo (empresas).
- Lamentablemente, personas y organizaciones ajenas a la compañía y sin conocimiento sobre el caso, han estado divulgando información falsa sobre la situación, por lo que desmentimos que sean oficiales los datos que se han distribuido sobre: la supuesta cantidad de empresas afectadas, el atacante, el impacto, entre otras noticias falsas. Toda información que no sea proveída por la empresa, no debería ser tenida en cuenta.
- Mucha de la información sobre este caso es de carácter estrictamente confidencial y privado de las empresas, razón por la cual no se pueden proporcionar mayores detalles, dando cumplimento a los contratos entre las partes.
- Puntualizamos que, fuera de los servicios específicos del segmento corporativo citado, no se han visto afectados los servicios de internet, telefonía ni billeteras electrónicas Tigo Money.
- Desde el primer momento toda la compañía ha abocado esfuerzos, recursos y equipos para dar solución a esta situación. Se trabajó en esta línea estrechamente con cada empresa para avanzar en el restablecimiento o reactivación según los servicios afectados en cada caso.
- Nuestros equipos, tanto locales como regionales, se encuentran trabajando 24/7, con soporte de expertos técnicos, para lograr la recuperación de los servicios afectados, dicho trabajo se encuentra con progreso favorable.
- Agradecemos el acompañamiento de las autoridades, con quienes estamos en permanente comunicación.
- Agradecemos el apoyo de nuestros clientes, proveedores y empresas en este proceso.
- Nuestra máxima prioridad y foco es recuperar en la brevedad los servicios aún pendientes.

tigo business

Asunción, enero 2024

Según la empresa, el ataque se limita a un grupo específico de clientes empresariales, y no ha afectado otros servicios masivos o corporativos como telefonía, internet y billetera electrónica, que siguen operando con normalidad. La información falsa circulante sobre la cantidad de empresas afectadas, el atacante y el impacto real fue desmentida en un comunicado posterior.

El Departamento de Ciberseguridad de las Fuerzas Armadas de Paraguay emitió una alerta oficial ante posibles consecuencias derivadas de la infección de ransomware. Posteriormente, la Dirección General de Tecnologías de la Información y Comunicación del Comando de las Fuerzas Militares de Paraguay emitió un comunicado señalando el impacto directo en más de 300 empresas asociadas a Tigo, comprometiendo backups, páginas web, correos electrónicos y almacenamientos en la nube.

Aunque inicialmente se proporcionaron detalles sobre la infección de ransomware vinculada al grupo Black Hunt, la Dirección posteriormente eliminó el boletín de su página web, aclarando que los boletines cumplen una función informativa general y no están vinculados a casos específicos.

"SESQUICENTENARIO DE LA EPOPEYA NACIONAL 1864 – 1870"

COMANDO DE LAS FUERZAS MILITARES
DIRECCIÓN GENERAL DE TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN
DSIRT-MIL
_***_

Se informa que el boletín 01/2024, así como todos los boletines emitidos por el DSIRT-MIL, cumplen con una función meramente informativa y no está vinculado a algún caso en particular.

Es relevante resaltar que estos boletines forman parte de una labor continua de vigilancia y prevención. Estos son elaborados en base a múltiples fuentes informativas y se distribuyen a las distintas entidades de las Fuerzas Armadas, Fuerzas Singulares y Direcciones Generales, a través del sitio web de la DIGETIC, asegurando así una comunicación eficiente y oficial.

"Al mantenernos alerta y proactivos frente a amenazas emergentes, fortalecemos la integridad de nuestra infraestructura tecnológica."

El viceministro de Tecnologías del Ministerio de Tecnologías de la Información y Comunicación (MITIC) de Paraguay, Juan Ardissone, destacó la importancia de la prevención de ciberataques y ofreció el respaldo del Estado a empresas privadas en eventos de esta naturaleza. Aunque el Estado paraguayo no tiene información detallada sobre el ataque interno de Tigo, el MITIC está dispuesto a ofrecer ayuda según sea necesario.

"Nosotros no estamos hoy en día trabajando para hacer la recuperación de los datos porque ellos justamente nos dijeron que están trabajando en base al protocolo y con los técnicos de la empresa. Lo importante aquí es que cuando ocurre, existan los protocolos de recuperación", dijo Juan Ardissone, viceministro del Mitic, Paraguay, recordando que los ataques cibernéticos no son inevitables en todo momento, por lo cual resulta ideal siempre trabajar sobre esas posibilidades de manera constante y actualizada.

Ardissone aprovechó la oportunidad para recordar la importancia de medidas preventivas, tanto para instituciones públicas como para empresas y particulares, incluyendo el uso de antivirus, evitar programas piratas y tener precaución al abrir archivos adjuntos de correos electrónicos no esperados.

En un desarrollo colateral, se informó que el ataque también afectó uno de los servicios ofrecidos por la Cancillería Nacional, siendo el único caso dentro del sector público. Sin embargo, se ha confirmado que el servicio ya ha sido restablecido.

El incidente de ciberseguridad en Tigo Business destaca la creciente amenaza que enfrentan las empresas ante ataques de ransomware. La colaboración entre el sector privado y el respaldo gubernamental se vuelve crucial en la lucha contra estas amenazas digitales. El caso continúa siendo monitoreado de cerca, y la recuperación de los servicios afectados sigue en progreso.

RECOMENDACIONES

- Identificación de los Indicadores de compromiso como direcciones IP y dominios maliciosos.
- Implemente un plan de recuperación que mantenga y conserve múltiples copias de datos confidenciales o de propiedad y servidores en una ubicación segura, segmentada y separada físicamente (es decir, disco duro, dispositivo de almacenamiento o la nube).
- Implemente la segmentación de la red y mantenga copias de seguridad fuera de línea de los datos para garantizar una interrupción limitada de la organización.
- Realice copias de seguridad de los datos con regularidad y proteja con contraseña las copias de seguridad almacenadas sin conexión. Asegúrese de que las copias de los datos críticos no sean accesibles para su modificación o eliminación desde el sistema donde residen los datos.
- Mantenga actualizado todos los sistemas operativos, y software.
- Instale, actualice periódicamente y habilite la detección en tiempo real del software antivirus en todos los hosts.
- Audite las cuentas de usuarios con privilegios administrativos y configure los controles de acceso, con el principio de privilegios mínimos.
- Desactive los puertos no utilizados.
- Deshabilite las actividades y permisos de línea de comandos y scripting.
- Asegúrese de que todos los datos de copia de seguridad estén encriptados, sean inmutables
- Examine el tráfico de red entrante y saliente, en busca de actividad sospechosa dentro de su red.

INDICADORES DE COMPROMISO

https://github.com/develgroup/SOC_IOCs/tree/main/20240108_01_BlackHuntRansomeware

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente