

# CYBER **SECURITY** **NEWS**

SECURITY OPERATIONS CENTER

## **RANSOMWARE WHITE RABBIT CIFRA ARCHIVOS DE FORMA SIGILOSA**

11 / 12 / 2023

## CONTENIDO

INTRODUCCIÓN .....	3
RESUMEN .....	4
RECOMENDACIONES .....	6
NOTICIA COMPLETA .....	6
INDICADORES DE COMPROMISO .....	6
CONTACTOS DE SOPORTE .....	7

## INTRODUCCIÓN

En un preocupante desarrollo en el panorama de la ciberseguridad, el ransomware "White Rabbit" ha emergido como una amenaza sigilosa y difícil de detectar. Con un tamaño reducido y comportamiento discreto, este intruso malicioso cifra archivos de manera eficiente, desafiando los sistemas de detección. La comunidad en línea se encuentra en alerta ante la capacidad de este ransomware para eludir medidas de seguridad convencionales.

## RANSOMWARE WHITE RABBIT CIFRA ARCHIVOS DE FORMA SIGILOSA

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

ID de alerta:	DSOC-CERT_2023_12_12_2
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	<b>CLEAR</b>
Fecha de publicación:	11/12/2023
Es día cero (0 day):	No

## RESUMEN

RansomHouse es un grupo de amenazas pertenecientes a la familia Babuk que ha estado activo en el panorama del ransomware desde al menos 2021. Este grupo se ha destacado por llevar a cabo campañas de cifrado dirigidas a instancias de Linux y máquinas virtuales VMware ESXi, utilizando variantes de ransomware como Mario Locker o WhiteRabbit, siendo este último el más presente.

La primera vez que se detectó el ransomware "White Rabbit", según informó Threatpost, fue utilizado en un ataque contra un banco local no identificado en Estados Unidos. Se anunció que un equipo de investigadores forenses respondió a un cliente cuyo entorno se vio afectado por White Rabbit el 14 de diciembre de 2021.


En cuanto a la propagación de "White Rabbit", al igual que otros malwares, se introduce en los sistemas a través de correos electrónicos de phishing. En estos correos, se adjunta un archivo que, al ser abierto por el usuario, inicia la propagación del ransomware en el sistema.

Según Trend Micro, la detección de White Rabbit puede ser difícil debido al tamaño del archivo, que es de alrededor de 100 KB. Sin embargo, se puede identificar su presencia en cadenas de registro.



El comportamiento de este ransomware es difícil de observar, pero se puede monitorear a través de alertas de comando y control. Una vez que se ejecuta, White Rabbit escanea todas las carpetas del dispositivo y cifra archivos específicos. Además, crea un mensaje de rescate para cada archivo cifrado. A continuación, se muestra un ejemplo del mensaje de rescate.

```

-----
                                HELLO 
If you are reading this message, means that:
- your network infrastructures have been compromised,
- critical data has leaked,
- files are encrypted

a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"
a"t welcome to the Ransom House a"t
a"t You are locked by a"t
a"t W H I T E R A B B I T a"t
a"t Knock, Knock. Follow the white Rabbit... a"t
a"t { \ / a"t
a"t { -. - } a"t
a"t { " ) ( " } a"t
a"t a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"

The best and only thing you can do is to contact us
to settle the matter before any losses occurs.

-----
                                1. THE FOLLOWING IS STRICTLY FORBIDDEN
1.1 DELETION THIS NOTE.
Each note carries the encryption key
needed to decrypt the data,
don't lose it

1.2 EDITING FILES OR HDD.
renaming, copying or moving any files
could DAMAGE the cypher and
decryption will be impossible.

1.3 USING THIRD-PARTY SOFTWARE.
Trying to recover with any software
can also break the cipher and
file recovery will become a problem.

1.4 SHUTDOWN OR RESTART THE PC.
Boot and recovery errors can also damage the cipher.
Sorry about that, but doing so is entirely at your own risk.

1.5 HIRING THE FBI AND OTHERS
Cooperating with the FBI/CIA and so on
and involving their officers in negotiations
will end our communication with you
and we will share all the leaked data for free.

-----
                                2. EXPLANATION OF THE SITUATION
2.1 HOW DID THIS HAPPEN
The security of your IT perimeter has been compromised (it's not perfect at all).
We encrypted your workstations and servers to make the fact of the intrusion visible and to prevent you from hiding critical
data leaks.
We spent a lot of time for researching and finding out the most important directories of your business, your weak points.
We have already downloaded a huge amount of critical data and analyzed it. Now it's fate is up to you, it will either be deleted
or sold, or shared with the media.

2.2 VALUABLE DATA WE USUALLY STEAL:
- Databases, legal documents, billings, clients personal information, SSN...
- Audit reports
- Any financial documents (Statements, invoices, accounting, transfers etc.)
- work files and corporate correspondence
- Any backups

2.3 TO DO LIST (best practies)
- Contact us as soon as possible
- Contact us only in our chat, otherwise you can run into scammers.
- Purchase our decryption tool and decrypt your files. There is no other way to do this.
- Realize that dealing with us is the shortest way to the success and secrecy.
- Give up the idea of using decryption help programs, otherwise you will destroy the system
permanently
- Avoid any third-party negotiators and recovery groups. They can allow the event to leak.

-----
                                3. POSSIBLE DECISIONS
3.1 NOT MAKING THE DEAL
- After 4 days starting tomorrow your leaked data will be published or sold.
- We will also send the data to all interested supervisory organizations and the media.
- Decryption key will be deleted permanently and recovery will be impossible.
- Losses from the situation will be measured based on your annual budget

3.2 MAKING THE WIN-WIN DEAL
- You will get the Decryption Tool and the Manual how-to-use.
- You will get our guarantee and log of non-recoverable deletion of all your data.
- You will get the guarantee of secrecy and deletion of all traces of the deal in internet.
- You will get the security report on how to fix your security breaches.
-----

```

Las víctimas son amenazadas con la publicación o venta de datos confidenciales si no cumplen con las demandas de los ciberdelincuentes dentro de los cuatro días. La eliminación de la clave de descifrado se anuncia como consecuencia inevitable si no se realiza el pago.

## 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.

## NOTICIA COMPLETA

<https://devel.group/blog/ransomware-white-rabbit-cifra-archivos-de-forma-sigilosa/>

## INDICADORES DE COMPROMISO

[https://github.com/develgroup/SOC\\_IOCs/tree/main/20230307\\_02\\_RansomHouse](https://github.com/develgroup/SOC_IOCs/tree/main/20230307_02_RansomHouse)

## CONTACTOS DE SOPORTE



Correo electrónico: [cert@develsecurity.com](mailto: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>