



Nro. Alerta:	EC-2022-56	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS <b>ALERTA DE SEGURIDAD</b>	
TLP:	 <b>TLP:BLANCO</b>		
Fecha:	01-abril-2022	<b>Ransomware HIVE</b>	Versión 1.0

## I. DATOS GENERALES:

<b>Clase de alerta:</b>	Contenido Malicioso
<b>Tipo de incidente:</b>	Malware
<b>Nivel de riesgo:</b>	Alto

## II. ALERTA

Ransomware HIVE ha implementado mejoras en su software de cifrado; dificultando aún más, el proceso de análisis y recuperación de información.





Figura 1. Ilustración relacionada a ransomware  
Fuente: Google

## III. INTRODUCCIÓN

El grupo de ciberdelincuentes que desarrollaron el código malicioso “Hive ransomware”; se dio a conocer a mediados del 2021 implementando funciones de cifrado de la información en el equipo de la víctimas y operando como una pandilla de ransomware basada en afiliados, utiliza una variedad de técnicas y tácticas que son difíciles de defender y mitigar para los profesionales de la seguridad.

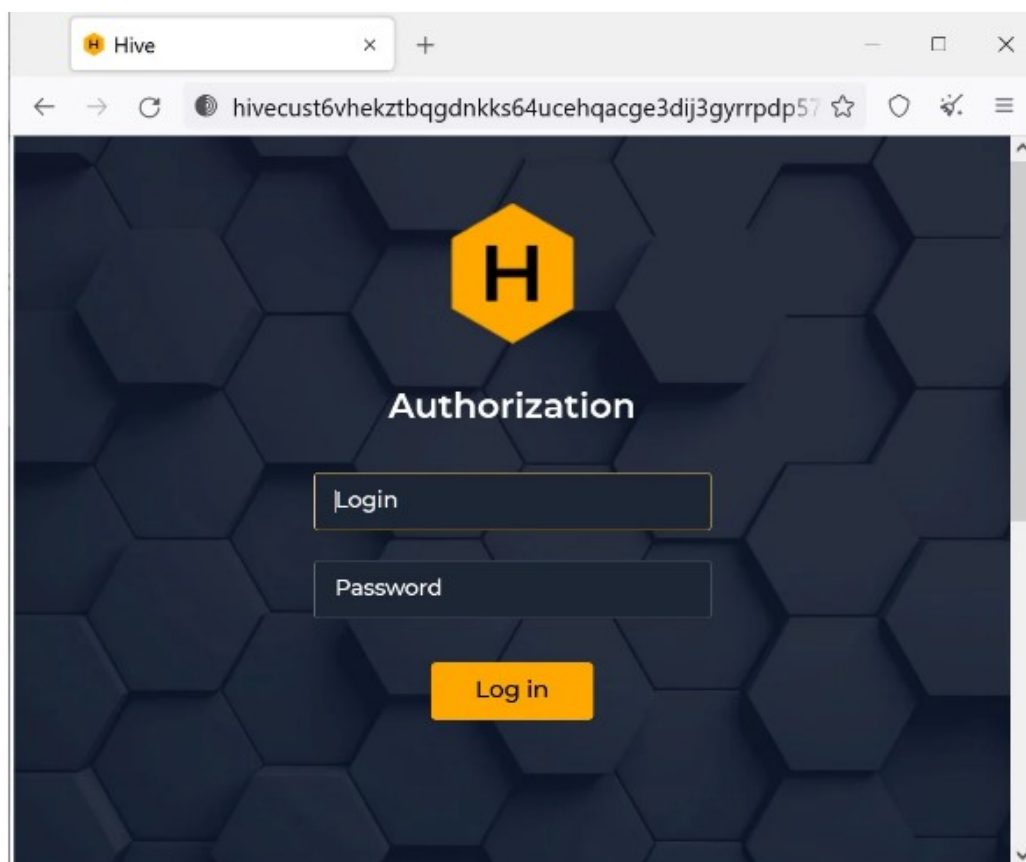
Es considerado uno de los grupos más agresivos y al igual que otros grupos de atacantes, HIVE extorsiona a las víctimas, exigiendo un pago y amenazando con publicar la información robada en el caso de que no se realice el pago.



Nro. Alerta:	EC-2022-56	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS <b>ALERTA DE SEGURIDAD</b>	
TLP:	 <b>TLP:BLANCO</b>		
Fecha:	01-abril-2022	<b>Ransomware HIVE</b>	Versión 1.0

El software de cifrado empleado por ransomware HIVE evoluciona día a día y en la actualidad ha convertido su encriptador VMware ESXi Linux al lenguaje de programación Rust; dificultando a investigadores recuperar la información.



En este sentido, HIVE ransomware ataca tanto a sistemas operativos Windows como en entornos Linux y más aún; se dirige a plataformas de virtualización VMware ESXI.



**Figura 2.** Imagen relacionada a HIVE ransomware  
Fuente: Bleepingcomputer

Además de ejecutar el cifrado de datos, roba datos confidenciales de las redes provocando una doble extorsión hacia la víctima. Según reportes de investigación, hasta octubre el 2021; este grupo de ciberdelincuentes; había atacado a 355 empresas y se encontraba en el octavo lugar entre las 10 principales cepas de ransomware por ingresos en 2021, según la empresa de análisis de cadenas de bloques Chainalysis.



Nro. Alerta:	EC-2022-56	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS <b>ALERTA DE SEGURIDAD</b>	
TLP:	 <b>TLP: BLANCO</b>		
Fecha:	01-abril-2022	<b>Ransomware HIVE</b>	Versión 1.0

#### IV. VECTOR DE ATAQUE:

El procedimiento de infección de HIVE es mediante **phishing** o **spear phishing**<sup>1</sup>; posteriormente se establece la persistencia a través herramientas como Cobalt Strike o ConnectWise, acompañada de movimientos laterales para posteriormente ejecutar el software de cifrado.

Una vez que las víctimas obtienen las credenciales y realizada su autenticación; encontrarán una pantalla en donde observarán:

1. Nombre de la organización infectada.
2. Chat en vivo para interactuar con los ciber delincuentes.
3. Sitio para enviar archivos.
4. En el caso de pagar el rescate, existe un sitio para descargar la información comprometida.

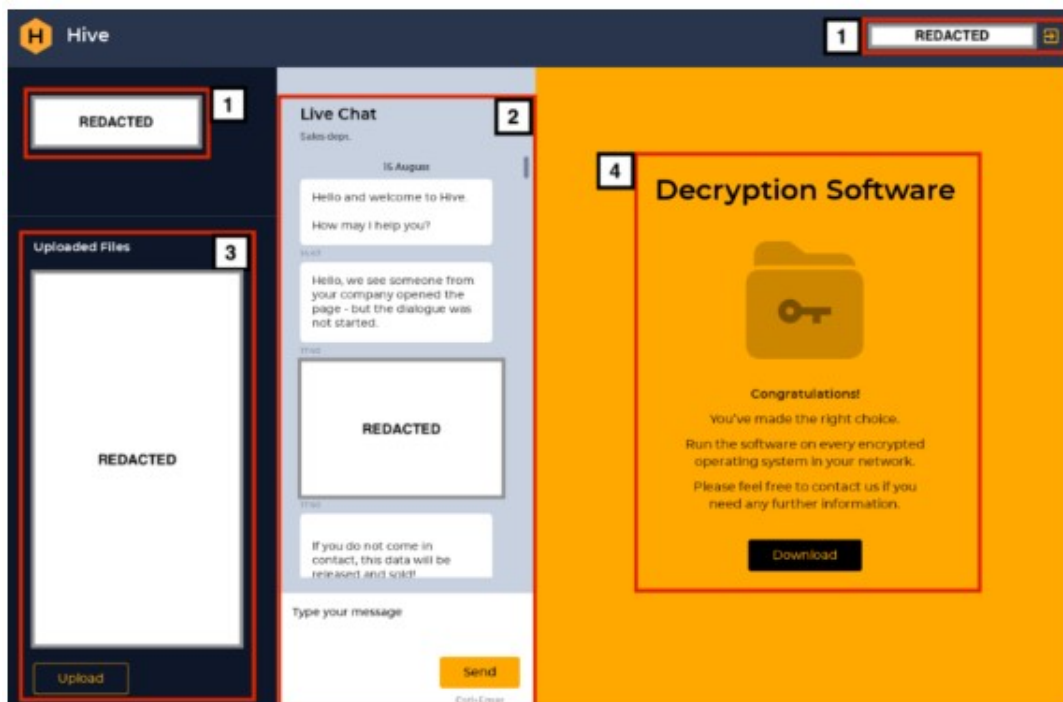



Figura 3. Imagen relacionada a HIVE ransomware  
Fuente: NETSKOPE

<sup>1</sup> Estafa de correo electrónico o comunicaciones dirigida a personas, organizaciones o empresas específica

Nro. Alerta:	EC-2022-56	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS <b>ALERTA DE SEGURIDAD</b>	 <p>CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS <b>ECUCERT</b></p>
TLP:	 <b>TLP: BLANCO</b>		
Fecha:	01-abril-2022	<b>Ransomware HIVE</b>	Versión 1.0

Cabe señalar que, la nueva variante del ransomware HIVE; transfiere el cifrador de Linux de Golang al lenguaje de programación Rust, provocando:

- Cifrado “seguro”, rápido y eficiente.
- Mantener las operaciones y las negociaciones con las víctimas en secreto; provocando que las tomas de muestras del ransomware sean escasas y dificultando el análisis de ingeniería inversa.

## V. Indicadores de compromiso:

A continuación, se menciona indicadores de compromiso asociados a HIVE:

	Parámetro	Descripción
1	<b>SHA256</b>	321d0c4f1bbb44c53cd02186107a18b7a44c840a9a5f0a78bdac06868136b72c1e21c8e27a97de1796ca47a9613477cf7aec335a783469c5ca3a09d4f07db0ff3a402af7a583471187bf9fc7872560aaacf5e3d8c99ca5404c3f157c06fba454b214c1bbcc7b0c2a4a47134d6009594a4d30bd7d5e363a41603de6b5b8de18ca
2	<b>Dominios</b>	hxxp://hiveleakdbtnp76ulyhi52eag6c6tyc3xw7ez7iqy6wc34gd2nekazyd[.]onion/ hxxp://hivecust6vhkzbtbqgdnkks64ucehqacge3dij3gyrrpdp57zoq3ooqd[.]onion/auth

Tabla 1. IOC relacionados a HIVE ransomware



Fuente: NETSKOPE

## VI. RECOMENDACIONES:

El EcuCert recomienda a su comunidad objetivo:

- En el caso de que la Organización/Institución se vea afectada por un ransomware, lo más importante es NO PAGAR el rescate.
- Realizar copias de respaldo de seguridad periódicas, de la información crítica para evitar la pérdida de la misma.
- No abrir, manipular, o interactuar, con correos electrónicos altamente sospechosos que lleguen a las bandejas de correo o mensaje en redes sociales.
- Implemente la segmentación de la red, de modo que todas las máquinas de su red no estén accesible desde cualquier otra máquina.
- No otorgue privilegios administrativos a todos los usuarios.
- Implementar técnicas de navegación segura en toda la Institución/Organización, como por ejemplo visita únicamente de sitios con certificados SSL y de origen no sospechoso.
- Descargar programas, archivos y actualizaciones, solamente desde fuentes oficiales y verificadas.



Nro. Alerta:	EC-2022-56	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS <b>ALERTA DE SEGURIDAD</b>	 <p>CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS <b>ECUERT</b></p>
TLP:	 <p><b>TLP:BLANCO</b></p>		
Fecha:	01-abril-2022	<b>Ransomware HIVE</b>	Versión 1.0

- Cerrar todo tipo de conexión/protocolo de acceso remoto a infraestructuras críticas en la Organización/Institución, en el caso de requerir su implementación, realizarlo bajo estrictas normas de seguridad apalancados en plataformas de seguridad perimetral y, uso de una VPN.
- Tener actualizado y utilizar un software anti-virus
- Mantener actualizados, y, bajo licenciamiento, (ya sea a nivel de software libre o de paga, de ser el caso), todos y cada uno de los sistemas y subsistemas de software y hardware de toda la infraestructura de IT y OT de la Institución, esto es, incluido a nivel de Firmware de todos los componentes.
- Capacitar a todos los usuarios, mediante la concientización y simulaciones para reconocer e informar sobre intentos de phishing e ingeniería social.
- Implementar un plan de respuesta a emergencias de la Organización/Institución.
- En el caso de que la Organización/Institución se vea afectada por un ransomware, visita los siguientes enlaces; a fin de establecer un panorama de la situación: <https://www.nomoreransom.org/es/decryption-tools.html#LockFile> (herramientas de des encriptado en el caso de existir) / <https://id-ransomware.malwarehunterteam.com/> (identificación de tipo de Ransomware y herramienta de des encriptado en el caso de existir una)
- En el caso de sufrir un ataque de proporciones mayores, contacte a las Autoridades competentes en base a la Normativa Legal Vigente a nivel Nacional.

## VII. REFERENCIAS:

- Abrams, L. (27 de 03 de 2022). *Bleepingcomputer*. Obtenido de Bleepingcomputer: <https://www.bleepingcomputer.com/news/security/hive-ransomware-ports-its-linux-vmware-esxi-encryptor-to-rust/>
- blog.segu-info. (29 de 03 de 2022). *blog.segu-info*. Obtenido de blog.segu-info: <https://blog.segu-info.com.ar/2022/03/ransomware-hive-todo-lo-que-necesitas.html>
- CERT, I. (12 de 2021). *Estudio del Análisis de HIVE*. Obtenido de Estudio del Análisis de HIVE: [https://www.incibe-cert.es/sites/default/files/contenidos/estudios/doc/incibe-cert\\_estudio\\_analisis\\_hive\\_2021\\_v1.pdf](https://www.incibe-cert.es/sites/default/files/contenidos/estudios/doc/incibe-cert_estudio_analisis_hive_2021_v1.pdf)
- FreeBSD. (s.f.). *FreeBSD*. Obtenido de FreeBSD: <https://www.freebsd.org/es/>
- GitHub. (s.f.). *GitHub*. Obtenido de GitHub: <https://github.com/netskopeoss/NetskopeThreatLabsIOCs/tree/main/Hive/IOCs>
- Kaspersky. (s.f.). *kaspersky*. Obtenido de kaspersky: <https://latam.kaspersky.com/resource->



Nro. Alerta:	EC-2022-56	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS <b>ALERTA DE SEGURIDAD</b>	 CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS <b>ECUCERT</b>
TLP:	 <b>TLP:BLANCO</b>		
Fecha:	01-abril-2022	<b>Ransomware HIVE</b>	Versión 1.0

[center/definitions/spear-phishing](#)

Palazolo, G. (8 de 9 de 2021). *Netskope*. Obtenido de Netskope:

<https://www.netskope.com/es/blog/hive-ransomware-actively-targeting-hospitals>

