Nro. Alerta:	EC-2021-030	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	10-dic-2021	**RANSOMWARE ALPHV (BLACKCAT) BASADO EN RUST SE EMPIEZA A DESPLEGAR PELIGROSAMENTE**	V 1.0

I. DATOS GENERALES:

Clase de alerta: Encriptación de datos

Tipo de incidente: Ransomware

Nivel de riesgo: Alto

II. ALERTA

Investigadores de seguridad han descubierto esta semana la primera cepa de ransomware profesional que se codificó en el lenguaje de programación Rust y se implementó contra empresas en ataques del mundo real.

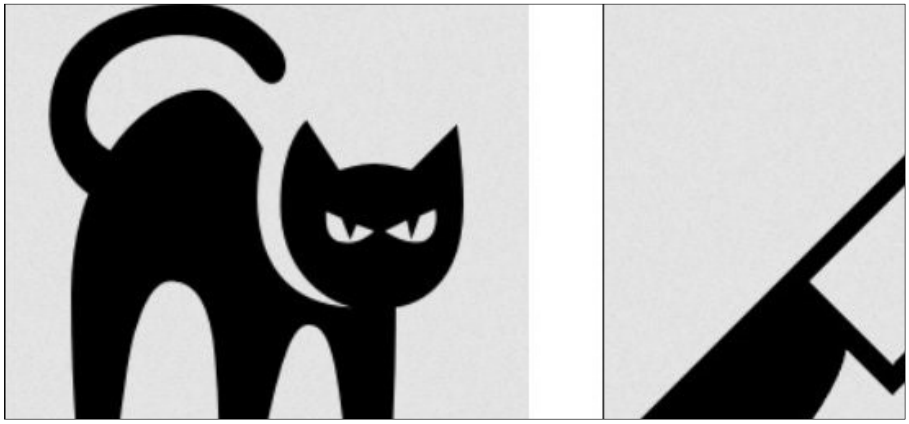

Figura 1.- lustraciones distintivas de Ransomware Alphv (Blackcat) **Fuente:** BleepingComputer

III.INTRODUCCIÓN

El ransomware, denominado BlackCat, fue revelado por MalwareHunterTeam. *"Las víctimas pueden pagar con Bitcoin o Monero",* dijeron los investigadores en una serie de tweets que detallan el malware de cifrado de archivos. Se evidencia que se están dando credenciales a intermediarios para las negociaciones.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2021-030	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	10-dic-2021	**RANSOMWARE ALPHV (BLACKCAT) BASADO EN RUST SE EMPIEZA A DESPLEGAR PELIGROSAMENTE**	V 1.0

BlackCat, similar a muchas otras variantes que han surgido antes, opera como un ransomware-as-a-service (RaaS), en el que los desarrolladores principales reclutan afiliados para violar los entornos corporativos y cifrar archivos, pero no sin antes robar dichos documentos en un esquema de doble extorsión para presionar a los objetivos para que paguen la cantidad solicitada o exponer al riesgo de los datos robados si las empresas se niegan a pagar.

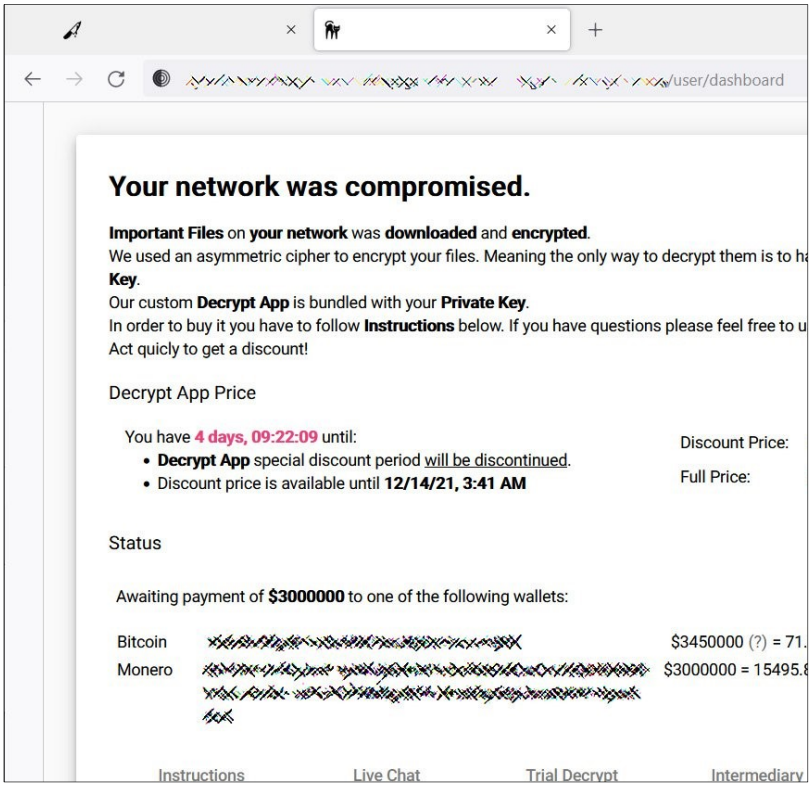

Figura 2.- Portal Web de pagos de Ransomware Alphv (Blackcat) **Fuente:** BleepingComputer

IV. VECTOR DE ATAQUE:

Hasta la fecha de publicación de esta alerta, se desconoce el vector de ataque utilizado para infectar una infraestructura de red con este nuevo

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2021-030	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	10-dic-2021	**RANSOMWARE ALPHV (BLACKCAT) BASADO EN RUST SE EMPIEZA A DESPLEGAR PELIGROSAMENTE**	V 1.0

Ransomware.

V. IMPACTO:

Entre las características de ALPHV/BlackCat, está la capacidad de cifrar datos en sistemas Windows, Linux y VMWare eSXI:

- Toda la línea de Windows desde 7 y superior (probado en 7, 8.1, 10, 11; 2008r2, 2012, 2016, 2019, 2022); XP y 2003.
- ESXI (probado en 5.5, 6.5, 7.0.2u)
- Debian (probado en 7, 8, 9);
- Ubuntu (probado en 18.04, 20.04)
- ReadyNAS, Synology

BlackCat no es la única operación de malware profesional que se ha trasladado a Rust, considerado un lenguaje de programación mucho más seguro en comparación con otros como C y C ++. En este momento, el grupo parece estar operando múltiples sitios de filtraciones, y cada uno de ellos aloja los datos de una o dos víctimas con ALPHV (BlackCat), creando uno nuevo para usar en nuevos ataques. A continuación se muestra una captura de pantalla de uno de estos sitios:

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2021-030	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	10-dic-2021	**RANSOMWARE ALPHV (BLACKCAT) BASADO EN RUST SE EMPIEZA A DESPLEGAR PELIGROSAMENTE**	V 1.0

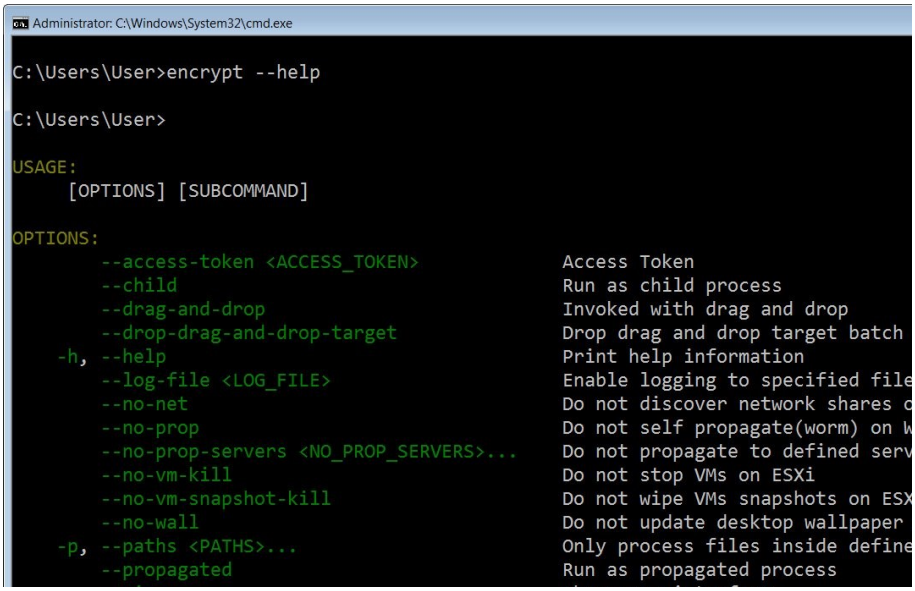

Figura 3: Argumentos de la línea de comandos del ransomware ALPHV BlackCat**Fuente:** BleepingComputer

VI. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo tomar en consideración lo siguiente:

- Respaldar toda la información y sistemas que se requiere restaurar en caso de sufrir un incidente cibernético.
- Hacer caso omiso a correos electrónicos y enlaces sospechosos.
- En caso de sufrir un ataque de ransomware, informe a las autoridades competentes en base a la normativa legal vigente a nivel Nacional.
- Mantener el control del uso de dispositivos de almacenamiento externos.
- Actualizar periódicamente las capas de seguridad implementadas en su red.
- Gestionar correctamente privilegios de usuarios.
- Deshabilitar el RDP (Protocolo de escritorio remoto).
- Fortalecer las políticas de seguridad para evitar la conexión de equipos personales tales como computadores, tabletas, celulares en la red institucional.
- Concientizar a todos los usuarios sobre los tipos de amenazas, formas de infección y consecuencias a los que estamos expuestos.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2021-030	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	10-dic-2021	**RANSOMWARE ALPHV (BLACKCAT) BASADO EN RUST SE EMPIEZA A DESPLEGAR PELIGROSAMENTE**	V 1.0

- intentos de phishing e ingeniería social.
- En caso de sufrir un ataque NO pagar el rescate y, contactar a las Autoridades competentes en base a la Normativa Legal Vigente a nivel Nacional.

VII. REFERENCIAS:

- Abrams, L. (9 de diciembre de 2021). *Bleeping Computer*. Obtenido de https://www.bleepingcomputer.com/news/security/alphv-blackcat-this-years-most-sophisticated-ransomware/
- Cimpanu, C. (09 de diciembre de 2021). *The Record by Recorded Future*. Obtenido de https://therecord.media/alphv-blackcat-is-the-first-professional-ransomware-gang-to-use-rust/
- Lakshmanan, R. (10 de diciembre de 2021). *The Hacker News*. Obtenido de https://thehackernews.com/2021/12/blackcat-new-rust-based-ransomware.html
- William. (10 de diciembre de 2021). *Mac Pro Tricks*. Obtenido de https://macprotricks.com/alphv-blackcat-this-years-most-sophisticated-ransomware/

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec