Nro. Alerta:	AL-2025-021	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	26-may-2025	Ransomware VanHelsing	Pág.: **1** of **8**

I. DATOS GENERALES:

Clase de alerta: Incidente
Tipo de Incidente: Ransomware
Nivel de riesgo: Alto

II. ALERTA

Figura 1.- Ransomware ValHelsing - figura referencial

Ransomware VanHelsing cifra archivos del sistema Microsoft Windows, adicionando las extensiones .vanlocker o .vanhelsing, exfiltra datos sensibles del usuario antes de proceder con el cifrado (de doble extorsión) y amenaza con publicarlos si no se paga por su rescate.

III. INTRODUCCIÓN

Este malware opera bajo el modelo de Ransomware as a Service (RaaS) y emplea una estrategia de doble extorsión. Primero, exfiltra los datos sensibles de la víctima antes de cifrarlos, con el fin de amenazar con su publicación en sitios web controlados por los atacantes si no se realiza el pago. Posteriormente, cifra los archivos locales y exige un segundo pago para restaurar el acceso a ellos.

VanHelsing destaca por ser multiplataforma afectando a sistemas Windows, Linux, BSD, ARM y VMwareSXi. Para entornos Windows está escrito en lenguaje C y utiliza los algoritmos Curve25519 como protocolo de intercambio de claves y ChaCha20 como

algoritmos de cifrado adjuntando extensiones .vanlocker o .vanhelsing a los archivos afectados.

Este Ransomware contiene dos imágenes, vhlocker.png para cambiar el fondo de escritorio y vhlocker.ico para asociarse a los archivos que han sido cifrados en las maquinas infectadas.

Figura 2.- Dispositivo infectado – Ransomware VanHelsing

Para la nota de rescate crea un archivo de nombre README.txt en él informa a sus víctimas que su red ha sido comprometida con el cifrado de archivos, archivos de interés y datos sensibles que para reestablecer el acceso a ellos espera el pago en bitcoins y en caso de no hacerlo, los datos robados serán publicados en foros, sitios web propios de VanHelsing, en el archivo se encuentran los links de contacto en la dark web para establecer la comunicación.


README - Notepad

File Edit Format View Help

--- No news is a good news ! ---

Your network has been breached and all your files Personal data, financial reports and important documents has been stolen , encrypted and ready to publis

If you willing to continue your bussines and make more money and keep bussines secret safe you need to restore your files first, And to restore all your fil
don't bother your self and wast your time or make it more harder on your bussines , we developed a locker that can't be decrypted using third part decrypter

making your self geek and trying to restore the files with third part decrypter this will leads to lose all your date ! and then the even you pay the ransom

to chat with us :

1 - Download tor browser https://www.torproject.org/download/
2 - go to one of these links above
http://vanhelcbxqt4tqie6fuevfng2bsdtxgc7xxlo2yo7n5taacdfrlpxnqd.onion
http://vanhelqmjstkvlterjwzgjzpqd22ikufwlggiz5y5r3rmfdeiajlljaid.onion
http://vanhelsokskrlaaclly fmtuqqa5haikubsjaokw47f3pt3uolvh6cgad.onion
http://vanheltarnbfjhuzggbncn1ap56dscnzz5yf6yjmxqivqmb5r2gmllad.onion

3 - you will be asked for your ticket id to enter the chat this for you : TICKET ID [redacted]

useful links :
#OUR TOR BLOG :
http://vanhelvuuo4k3xs1q626zkqvp6kobc2abry5wowxqyslbmqs5yjh4uqd.onion
http://vanhelwmbf2bwzw7gmseg36qqmekc5uuhqbsew4elhzcahyq7sukzad.onion
http://vanhelxjo52qr2ixcmtjeyqqrcodkuh36n7uq7q7xj2jggotyr3y72yd.onion

Figura 3.- Nota de rescate – Ransomware VanHelsing

Una de las señales más reveladoras del origen de VanHelsing es su norma explícita que prohíbe los ataques contra la Comunidad de Estados Independientes (CEI). Esto es un sello distintivo de grupos de Ransomware como LockBit, Conti, REvil y BlackCat/ALPHV, ya que muchas organizaciones cibercriminales de la región mantienen un acuerdo informal con ciertas autoridades para no atacar objetivos nacionales y entregar una parte de sus ganancias a cambio de que las autoridades ignoren sus actividades.

IV. VECTOR DE ATAQUE

AttackIQ describe el proceso de infección de VanHelsing con sus respectivos TTPs dividida en 2 etapas, ambas las realiza mediante funciones y comandos propios del API de Windows:

Primera Etapa

1. **Acceso inicial y descubrimiento - Reconocimiento del Sistema Local**

   Esta etapa comienza con la implementación del ransomware VanHelsing y realiza un reconocimiento inicial, como chequear la presencia de un depurador, recopilación de información local y del sistema de información para evitar infectar a las víctimas no deseadas.

Figura 4.- Grafica del proceso de acceso inicial y descubrimiento – Ransomware VanHelsing

2. **Transferencia de Herramientas de Entrada (T1105):**

   El despliegue de VanHelsing comienza con la descarga en memoria, se guarda en el disco en dos espacios separados para evaluar los controles de red y endpoint, así como su capacidad para evitar la entrega de muestras maliciosas conocidas.

3. **Evasión de Virtualización/Sandbox (T1497):**

   Ejecuta la función **IsDebuggerPresent** para detectar la presencia de un depurador en ejecución al proceso actual y evadirlo en su entorno de análisis.

4. **Descubrimiento de Ubicación del Sistema (T1614):**

   Funciones a ejecutar

   - **GetUserDefaultLCID** para obtener el ID de configuración regional predeterminado (LCID) del usuario en el sistema local.
   - **GetUserDefaultLocaleName** para obtener el nombre de la configuración regional predeterminada del usuario en el equipo local.
   - **GetLocaleInfoA** para obtener el código de país de la configuración regional predeterminada del usuario en el equipo local.

5. **Descubrimiento de Información del Sistema (T1082):**

   Funciones a ejecutar

   - **GetEnvironmentStrings** para descubrir variables de entorno, comúnmente utilizadas para identificar características del sistema o buscar contraseñas y secretos almacenados.
   - **GetNativeSystemInfo** para recuperar información asociada al sistema.

Segunda Etapa

1. **Descubrimiento e Impacto – Cifrado de Archivos por Ransomware VanHelsing**

   En esta etapa comienza con la eliminación de shadow copies de Windows para obstaculizar los esfuerzos de recuperación, luego procede a identificar las acciones y unidades de red accesibles para facilitar el movimiento lateral. Finalmente, se recorre el sistema de archivos sistemáticamente para identificar archivos de interés, que posteriormente se cifran utilizando una Curve25519 y ChaCha20.

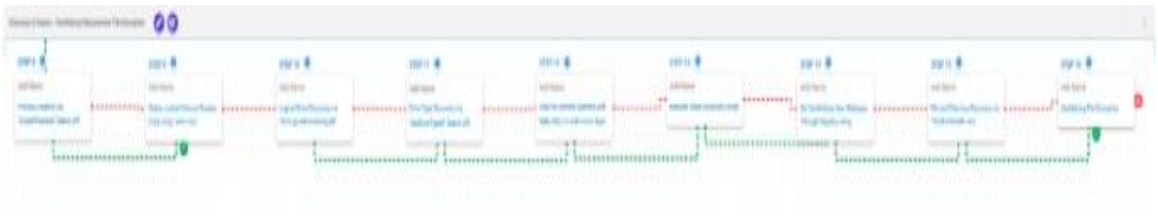

Figura 5.- Grafica del proceso de descubrimiento e impacto – Ransomware VanHelsing

2. **API Nativa (T1106):**

   Ejecuta la función **CreateProcessA** para crear un nuevo proceso de payload ejecutable.

3. **Inhibir el Sistema de recuperación (T1490):**

   Ejecuta el comando **wmic shadowcopy delete** para eliminar el *volume shadow copies* creadas por la emulación.

4. **Descubrimiento de Dispositivos Periféricos (T1120):**

   Funciones a ejecutar:

   - **GetLogicalDriveStringsW** para recuperar información sobre las unidades de disco físicas del sistema.

   - **GetDriveTypeW** para recuperar información sobre los discos físicos del sistema mediante la función de Windows.

5. **Descubrimiento remoto del sistema (T1018):**

   Realiza un escaneo de la red local en busca de cualquier sistema accesible remotamente por el puerto 445 (abierto).

6. **Descubrimiento de Redes compartidas (T1135):**

   Ejecuta el comando **net share** para listar todas las redes compartidas en el sistema.

7. **Modificar Registro (T1112):**

   Modifica la clave del registro **HKEY_CURRENT_USER\Control Panel\Desktop** para cambiar el fondo de escritorio.

8. **Descubrimiento de archivos y directorios (T1083)**:

   Ejecuta el **FindFirstFileW** y **FindNextFileW** para enumerar el sistema de archivos.

9. Data Encrypted for Impact (T1486):

Realiza las rutinas de cifrado de archivos utilizadas por las familias comunes de ransomware.

Los archivos que coinciden con una lista de extensión se identifican y cifran en su lugar utilizando algoritmos de cifrado similares utilizados por VanHelsing ransomware.

V. IMPACTO

VanHelsing destaca por ser multiplataforma, pero es predominantemente un malware para Windows.

VI. INDICADORES DE COMPROMISOS

Nombres de detección
W32/Filecoder_VanHelsing[.]A!tr[.]ransom
W32/PossibleThreat

Tabla 1. Nombres de Alerta – Ransomware VanHelsing

MD5 - VanHelsing Ransomware IOCs
5c254d25751269892b6f02d6c6384aef
3e063dc0de937df5841cb9c2ff3e4651

Tabla 2. MD5 – Ransomware VanHelsing

SHA-1 VanHelsing Ransomware Archivos IOCs
79106dd259ba5343202c2f669a0a61b10adfadff
e683bfaeb1a695ff9ef1759cf1944fa3bb3b6948

Tabla 3. Hashes de archivos – Ransomware VanHelsing

SHA-256 VanHelsing Ransomware Archivos IOCs
86d812544f8e250f1b52a4372aaab87565928d364471d115d669a8cc7ec50e17
99959c5141f62d4fbb60efdc05260b6e956651963d29c36845f435815062fd98

Tabla 4. Hashes de archivos 256 – Ransomware Vanhelsing

Indicadores de Compromiso	
Loader	4211cec2f905b9c94674a326581e4a5ae0599df9
Negotiation Onion Pages	vanhelcbxqt4tqie6fuevfng2bsdtxgc7xslo2yo7nitaacdfrlpxnqd[.]onion vanhelqmjstkvlhrjwzgjzpq422iku6wlggiz5y5r3rmfdeiaj3ljaid[.]onion vanhelsokskrlaacilyfmtuqqa5haikubsjaokw47f3pt3uoivh6cgad[.]onion vanheltarnbfjhuvggbncniap56dscnzz5yf6yjmxqivqmb5r2gmllad[.]onion
RaaS Onion Pages	vanhelvuuo4k3xsiq626zkqvp6kobc2abry5wowxqysibmqs5yjh4uqd[.]onion

	vanhelwmbf2bwzw7gmseg36qqm4ekc5uuhqbsew4eihzcahyq7sukzad[.]onion vanhelxjo52qr2ixcmtjayqqrcodkuh36n7uq7q7xj23ggotyr3y72yd[.]onion
Bitcoin Wallet	bc1q0cuvj9eglxk43v9mqmyjzzh6m8qsvsanedwrru
TOX	FEE914521FB507AB978107ACE3B69B4CA41DA89859408BAE23E1512E8C2E614A26C5FFD482A3

Tabla 5. IoCs – Ransomware Vanhelsing

VII. RECOMENDACIONES:

- Registre y analice los Indicadores de Compromiso (IoCs), validando previamente si han impactado sus servicios o infraestructura.
- No se recomienda ceder al pago del rescate, ya que no garantiza la restauración de la información comprometida.
- Mantenga actualizados los sistemas operativos, herramientas de ciberseguridad y soluciones antivirus.
- Capacite a su personal sobre los riesgos asociados a la ingeniería social, correos de phishing y la descarga o apertura de archivos sospechosos. Además, evite el acceso a sitios web no confiables.
- Analice archivos de origen desconocido utilizando tecnologías de análisis dinámico, como sandboxing.
- Implemente soluciones avanzadas de seguridad para correo electrónico, que permitan detectar amenazas como phishing y malware antes de que lleguen al usuario final.
- Aplique el principio de privilegios mínimos para reducir el riesgo de escalamiento de privilegios.
- Refuerce las políticas de acceso remoto, incluyendo el uso seguro de VPN con credenciales seguras y actualizadas.
- Elimine cuentas inactivas y revise regularmente los privilegios de usuario para asegurar el acceso adecuado.
- Habilite autenticación multifactor (MFA) en todos los sistemas y plataformas críticas.
- Restringa el acceso remoto mediante el uso de firewalls, listas blancas de IP y limitación de protocolos como RDP.
- Desactive todos los servicios y protocolos innecesarios, especialmente aquellos asociados a administración remota, para minimizar las superficies de ataque.
- Implemente un plan de respaldo y recuperación, asegurándose de contar con múltiples copias seguras y actualizadas de los datos sensibles, almacenadas en ubicaciones separadas.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

Fortinet (2025). Ransomware Roundup – VanHelsing. https://www.fortinet.com/blog/threat-research/ransomware-roundup-vanhelsing

AttackIQ (2025). Emulating the Terrorizing VanHelsing Ransomware. https://www.attackiq.com/2025/05/15/emulating-vanhelsing-ransomware/

Cyble (2025). Threat Actor Profile: VanHelsing Ransomware Group. https://cyble.com/threat-actor-profiles/vanhelsing-ransomware-group/

BleepingComputer (2025). VanHelsing ransomware builder leaked on hacking forum. https://www.bleepingcomputer.com/news/security/vanhelsing-ransomware-builder-leaked-on-hacking-forum/

Check Point Research (2025). VanHelsing, new RaaS in Town. https://research.checkpoint.com/2025/vanhelsing-new-raas-in-town/

CyFirma (2025). VanHelsing Ransomware. https://www.cyfirma.com/research/vanhelsing-ransomware/