Nro. Alerta:	EC-2022-64	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	29-abril-2022	**Ransomware DJVU/STOP**	Versión 1.1

I. DATOS GENERALES:

Clase de alerta: Malware
Tipo de incidente: Ransomware
Nivel de riesgo: Alto

II. ALERTA

En el mes de abril de 2022 se identificaron ataques por parte de ransomware DJVU/STOP que afectan a infraestructura tecnológica de instituciones públicas y privadas en Ecuador.

Figura 1. Imagen asociada a ransomware.

III. INTRODUCCIÓN

El término ransomware hace referencia a un tipo de malware; un software malicioso, que impide usar el dispositivo (ordenador, portátil) hasta que no se cancele el valor del rescate. Existen diferentes variantes de ransomware; sin embargo, en el mes de abril de 20202 a través del monitoreo continuo se ha identificado la presencia de código malicioso JHDD y HAJD pertenecientes a la familia de ransomware STOP/DJVU.

La manera en la que estos códigos maliciosos llegan a la infraestructura de la víctima es variada, por ejemplo:

- Visitar una página web maliciosa.
- Interactuar con un adjunto malicioso.
- Descargar software con agregados indeseables.

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

Una vez que el ransomware ha ingresado al equipo de la víctima; empieza el accionar para el cual fue diseñado. Existen dos clases de ransomware:

- Ransomware de bloqueo.
- Ransomware de cifrado.

JHDD

Pertenece a la familia de ransomware **STOP/DJVU[1];** siendo una de sus características el encriptar archivos y añadir la extensión ".jhdd" a los archivos comprometidos; así mismo, añade el archivo "**readme.txt**"

Es considerado uno de los virus con más extendido del 2022 y en el 2019 fue uno archivos de cifrado más peligroso; emplea el algoritmo de criptografía RSA y entre las variantes de esta familia se encuentran: DEWD, JHGN, JHBG, JHDD, DMAY, MSJD y YGVB.

HAJD

Código malicioso que encripta los archivos a cambio de un pago por la liberación y al igual que otros integrantes de la familia STOP/DJVU emplea algoritmo de criptografía RSA, emplea el archivo read.txt para dar a conocer la afectación y la manera de pago; de igual manera, los archivos comprometidos poseen la extensión ".hajd"

En la siguiente tabla se indica un resumen de las características de este tipo de ransomware.

Ítem	Parámetro	Descripción
1	Nombre	HAJD /JHDD
2	Familia de ransomware	STOP/DJVU
3	Extensión	.hajd .jhdd
4	Nota de ransomware	_readme.txt
5	Rescate	De $490 a $980 (en Bitcoins)
6	Detección3	MSIL/Spy.Agent.DSV , TrojanSpy:Win32/Delgent , Trojan.Ransom.Magniber
7	Síntomas	Cifrado la mayoría de los archivos (fotos, videos, documentos) y agrega una extensión particular ".hajd";
		Puede eliminar las instantáneas de volumen para hacer que los intentos de la víctima de restaurar los datos sean imposibles.

[1] Similar a otro de la misma familia: Koom, Wiot, Wiot.

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-2022-64	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	29-abril-2022	**Ransomware DJVU/STOP**	Versión 1.1

Ítem	Parámetro	Descripción
		Agrega una lista de dominios al archivo HOSTS para bloquear el acceso a ciertos sitios relacionados con la seguridad.
		Instala un troyano que roba contraseñas en el sistema, como Azorult Spyware.

Tabla 1. Características ransomware DJVU/STOP

IV. VECTOR DE ATAQUE:

Entre los métodos de ataque de STOP/DJVU se menciona:

- Descarga de software de sitios sospechosos.
- Archivo malicioso adjunto a un correo electrónico.
- Archivos ocultos en sitios web del proveedor (parches para programas o juegos, activadores para software, generadores de claves, archivos de almacenamiento regulares).

En un inicio, dichos archivos de instalación o de descarga pueden parecer legítimos; sin embargo, desencadenan un proceso de infección, el mismo que se representa en la siguiente figura.

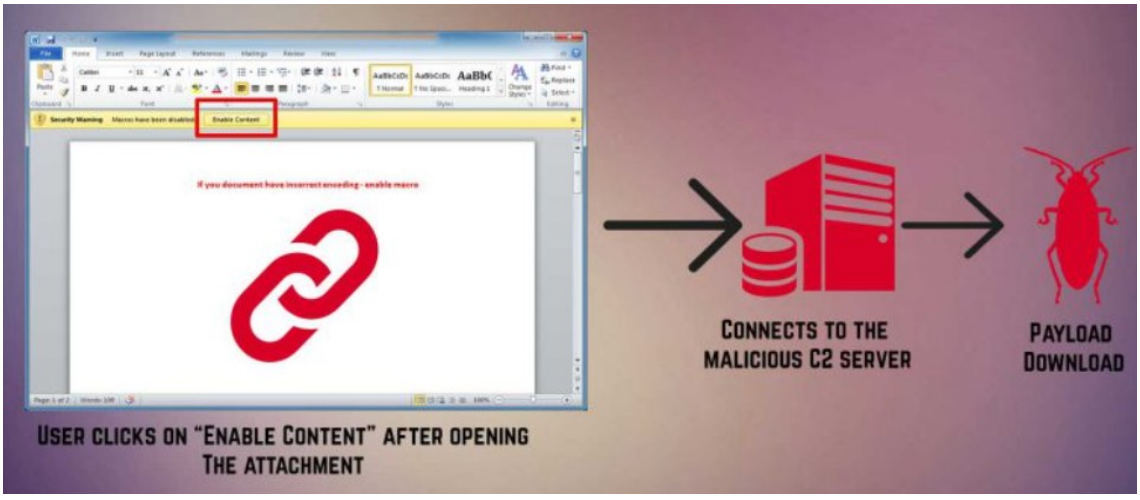

Figura 2. Cadena de infección DJVU ransomware

Considerando la anterior figura, se tiene que el código malicioso se conecta con el servidor C2 y descargar los respectivos archivos de módulo; los mismos que se encuentran ubicados

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

en los siguientes directorios:

- %AppData%
- %SystemDrive%
- %Local%
- %LocalLow%
- %windows%
- %Temperatura%
- %Sistema%
- %system32%

Entre los archivos que JHDD descarga se encuentra:

- **.TMP.EXE** es el ejecutable del ransomware.
- **1.exe** deshabilita y elimina las definiciones de virus de Windows Defender y cierra el análisis en tiempo real.
- **2.exe** modifica el archivo de host de Windows, inhabilitando la opción de una navegación segura.
- **Updatewin.exe** muestra en pantalla una supuesta venta de actualización de Windows mientras inicia el proceso de encriptación.

En la siguiente gráfica se indica la ventana falsa de actualización.

Figura 3. Ventana falsa de actualización.

Nro. Alerta:	EC-2022-64	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	29-abril-2022	**Ransomware DJVU/STOP**	Versión 1.1

V. INDICADORES DE COMPROMISO:

En la siguiente Tabla se indica las extensiones de archivo utilizadas por la familia de ransomware DJVU/STOP.

IOC	Descripción
Extensión de archivos	qewe, .mpal, .sqpc, .mzlq, .koti, .covm, .pezi, .zipe, .nlah, .kkll, .zwer, .nypd, .usam, .tabe, .vawe, .moba, .pykw, .zida, .maas, .repl, .kuus, .erif, .kook, .nile, .oonn .vari, .boop, .nord, .geno, .kasp, .ogdo, .npph, .kolz, .copa, lyli, .moss, .foqe, .mmpa, .efji, .nypg, .iiss, .jdyi, .vpsh, .agho, .vvoa, .epor, .sglh, .lisp, .weui, .nobu, .igdm, .booa, .omfl, .igal, .atek, .qlkm, .coos, .wbxd, .pola, .cosd, .plam, .ygkz, .cadq, .ribd, .reig, .tirp, .enfp, . ekvf, .ytbn, .fdcz, .urnb, .lmas, .wrui, .rejg, .pcqq, .igvm, .nusm, .ehiz, .paas, .pahd, .mppq, .qscx, .sspq, .iqll, .ddsg, .piiq, .leex, .neer, .miis, .zqqw, pooe, .lssr, .zzla, .wwka, .gujd, .ufwj, .moqs, .hhqa, .aeur, .guer, .nooa, .muuq, .reqg, .hoop, .orkf, .iwan, .lqqw, .efdc, .wiot, .koom, .rigd, .tisc, .nqsq, .irjg, .vtua, .maql, .zaps, .rugj , .rivd, .cool, .palq, .irfk, .stax,
ajd	1e051acde7df4de352ac28c78d730d6671dfe6f7e3e5118a92ce2ed00292cc05
	80b2d9c63eacfea597bfd6ec329d69fd8df2e8dbeae18a8f1ac114114ed41d43
	42e44fd8c26a24db695067da085562a6f2286f7db5cccb7d80afa9c09415a2fb
	caf00c219bedd62021b4578b03ec1b80f2006f6dfc4b2414df6578cc1801a0d9
	19deef8cbf60229277f45e96c1b02bb1a398a4d86d6421c309562625bbd34612
	e4a5c5299a3a51c8e6675ccf84e7ec3e328233079d7588434ef9530ca565aa95
	16bf7779a83306724b530bf0dd3d500446326c71cd272b19671d8eb6a89980c0
	c0448d733802bd6ebc97b099bdcb5744fcd6149c9075088e88eb0869a6d8d175
	59b745c35ab2e9da7112ac6b47a2e97a66c5592f14c55824f2c96b830247c2d6
	264896379166e6b349462dd06613a2a71f47316815256eb71f57aa4f11d9980c
	09d2fc99b2f5ab8868ee5c0f11644802996f30ae0bfdd2611ac0e7a604ff296e
	2b697dedde68e57f4ce0031983226e1db30f0e41e52e5307f1bb1eddc87ae7e7
	0a78ef97187a1415043026da3f215eab8ec3c4d3642df057ff0c5e35fc6b289e
	ad221a0e4b9b7a0a2da6f3c3fb059deda23076d897d7783835d9c39a354a2232
	0b8b3bf412cc14bd4d3460c40e2cdc1da7ed958a73ba25fa8d90b79cdc5a1f32
	8db8e0f0d7953453870d287debecb85a414b45ea809ab6508f45b25567c033fd
	5da2d0a1ea19e918a59358917d5f0ccb629b1ab3570dd48976f724104c3fcb83
	118fdc1f91f1d3ccd8afeed03bfbc1c51e6bc7e316d9b1c0d88640872ed3e17e
	770402cd3cd44132d6347cf6b18ae45d51e07cefa240f435359fcf821c3ba0a3
	e3bb53c048fc7ac736a6b0d1a5e757cd7dc0b4c2bc15e904b7a3e46f473db0f0

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-2022-64	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	29-abril-2022	**Ransomware DJVU/STOP**	Versión 1.1

IOC	Descripción
	19bbac767fb526749ae7b964b1dc526461c7ad405a4cb503cea07e9b7bcac801
	b27365d31a5639858d05f20e8df13feb1d2177245bc62d224fbafe0fa417e592
	8137226c9073ca173d35d539a512a986911ee9318cbc49fde02b5fd9e4be0321
	4baef09afa940e86cdb9651c83bb40b87674e507e5c4e697cd00997b4caed201
	38c1fd8ec20cf39d28f3fb6989b83598abaf0d3cc5c4b2945bdf9fbdf06f09fa
	7d1ed8cb8d29470eb02f40072bab23dcc60922579b52e4c5192cfd2735420444
	40827ec53c31bef7fb11bd4e087d0ec309dd52550d72890d75d94242e44015b3
	948956eae20714c6407522860bb3d10a9f10501f309d58d02707264d9ab1ab40
	ac436d556a1bde5ea6481bea8ca29bcc235a30b1dc62606eedf9b055d15993b9
	6be8676956e7628387a3061be007256d923bcb3289c1dd380ce7734a1fc07fa3
URL	https://crackithub[.]com/adobe-acrobat-pro/ https://crackithub[.]com/easyworship-7-crack/ https://kmspico10[.]com/ https://kmspico10[.]com/office-2019-activator-kmspico/ https://piratepc[.]net/category/activators/ https://piratepc[.]net/startisback-full-cracked/ https://es.howtofix.guide/jhdd-virus-file-2/

Tabla 2. IOC ransomware DJVU/STOP

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.
- Otorgar privilegios de usuario al mínimo dependiendo del tipo de labor a realizar.
- 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.
- Bloquear el acceso de usuarios, a dispositivos de almacenamiento externo, ajenos a la Institución/Organización, a través de políticas de seguridad adecuadas.
- Implementar y monitorear, plataformas de seguridad perimetral para identificar posible

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

tráfico malicioso tanto a nivel interno como externo a la infraestructura de red de la organización/Institución

- Descargar programas, archivos y actualizaciones, solamente desde fuentes oficiales y verificadas.
- 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. Descargo de responsabilidad

- La información en la presente alerta; se proporciona "tal cual" solo con fines informativos. EcuCERT no respalda ningún producto o servicio comercial, incluidos los sujetos de análisis.
- Cualquier referencia a productos, procesos o servicios comerciales específicos por marca de servicio, marca comercial, fabricante o de otro modo, no constituye ni implica respaldo, recomendación o favorecimiento por parte del EcuCERT.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

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-2022-64	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	29-abril-2022	**Ransomware DJVU/STOP**	Versión 1.1

VIII. REFERENCIAS:

Kaspesky. (s.f.). *Kaspesky*. Obtenido de Kaspesky: https://latam.kaspersky.com/resource-center/threats/ransomware

Krastev, V. (20 de 04 de 2022). *Sensor Tech Forum*. Obtenido de Sensor Tech Forum: https://sensorstechforum.com/es/jhdd-virus-files/

Malpedia. (s.f.). *Malpedia*. Obtenido de Malpedia: https://malpedia.caad.fkie.fraunhofer.de/details/win.stop

Smith, B. (s.f.). *How to Fix*. Obtenido de How to Fix: https://es.howtofix.guide/jhdd-virus-file-2/

TheratFox. (s.f.). *TheratFox*. Obtenido de TheratFox: https://threatfox.abuse.ch/browse/malware/win.stop/