Nro. Alerta:	EC-2022-067	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	11-mayo-2022	**RANSOMWARE QUANTUM LOCKER**	V 1.1

I. DATOS GENERALES:

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

II. ALERTA

Quantum Locker es un tipo de ransomware que ha venido cambiando de denominación desde su detección en 2020; así mismo, se caracteriza por tener un TTR[1] inferior al de las otras sepas de ransomware.

Figura 1.- lustraciones distintivas de Ransomware Quantum Locker
Fuente: Cybereason

III. INTRODUCCIÓN

Las primeras muestras de este ransomware se remontan a julio de 2021; sin embargo, correspondería a otro cambio de marca del ransomware "MountLocker"[2], el mismo que ha

[1] Tiempo de Rescate
[2] Fecha de lanzamiento estimada septiembre de 2020.

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

venido cambiando de nombres de operación como: AstroLocker y XingLocker. En la siguiente gráfica se indica los nombres que ha venido adquiriendo este ransomware.

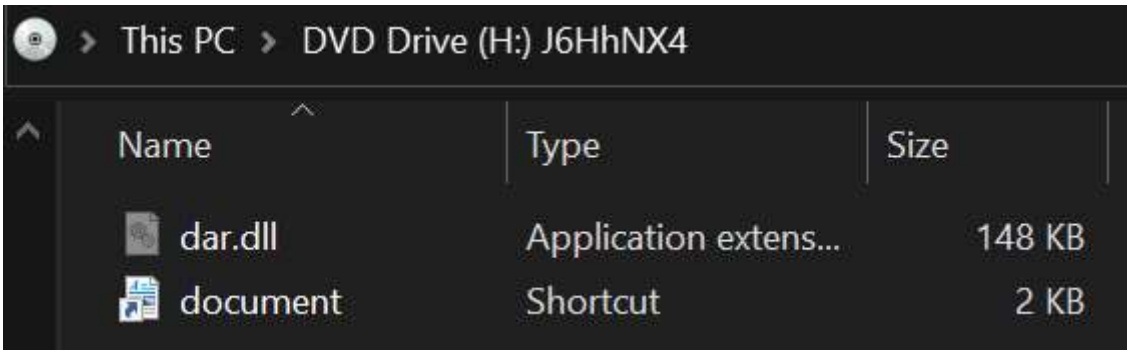
Figura 2.- Cambios de nombre del ransomware
Fuente: Propia, adaptada de Cybereason

IV. VECTOR DE ATAQUE: Phishing

La infección inicia con la descarga de una imagen ISO, que contiene una carga útil del malware IcedID[3]. La imagen ISO fue descargada a través de correo electrónico.

V. IMPACTO:

Al montar la imagen .iso; la víctima observa en su equipo el archivo de acceso directo llamado "documento", posterior a hacer clic en este acceso directo; se ejecuta la DLL de IcedID, la misma que se carga en memoria y se comunica con el C2. En la siguiente gráfica, se observan los archivos descargados y las propiedades de "documento".



[3] Inició como troyano bancario en el 2017 y es empleado por CONTI, REvil, Xing Locker.

Nro. Alerta:	EC-2022-067	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	11-mayo-2022	**RANSOMWARE QUANTUM LOCKER**	V 1.1

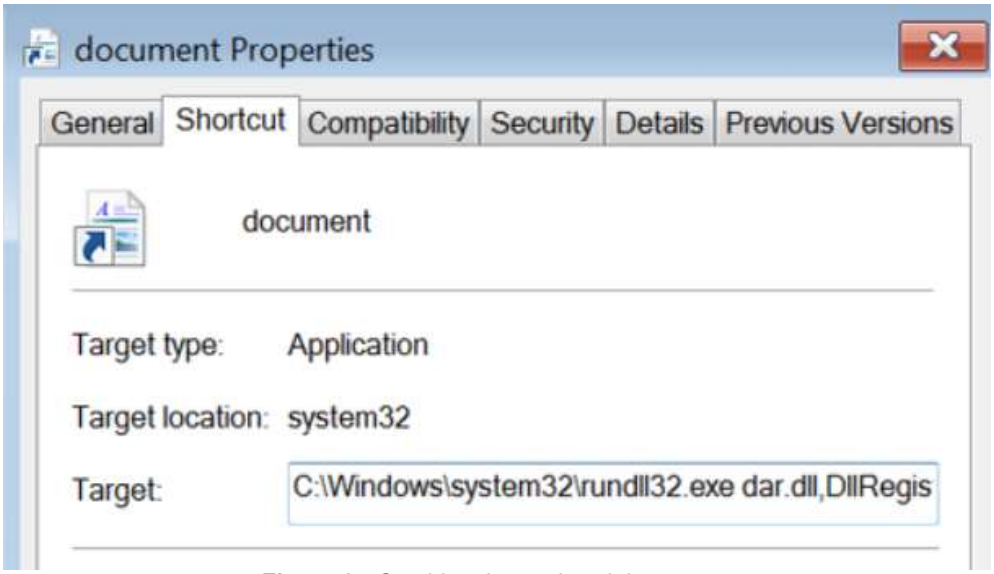


Figura 3.- Cambios de nombre del ransomware
Fuente: Cybereason

Establecida la comunicación con el C2, IcedID ejecuta los comandos de descubrimiento, extrae los resultados y los ciberdelincuentes definen si es una organización de interés o no para lanzar la siguiente fase de ataque.

En el caso de que el ataque continúe, se realiza una actividad de reconocimiento adicional y más profundo; así mismo se ejecuta un script llamado "adfind.bat"[4] a fin de recopilar información sobre Active Directory.

Para moverse lateralmente en el equipo de la víctima, interrumpe el proceso de LSASS[5] (Local Security Authority Subsystem Service); obteniendo las credenciales; posteriormente realiza conexiones RDP a otros servidores para verificar las credenciales obtenidas.

Una vez validada las credenciales, **empieza el despliegue de Quantum Locker;** en este caso los actores de amenazas copian el binario del ransomware en la carpeta: c$\windows\temp\ para posteriormente ejecutar de manera remota, a través de WMI y PsExec.

Previo a iniciar el cifrado de archivos, el ransomware verifica la ejecución de diferentes procesos relacionados con: antivirus, software de seguridad, herramientas de análisis de malware,

[4] Se coloca en el directorio %temp%, junto con el binario AdFind.exe y el binario 7Zip llamado 7.exe.
[5] Proceso responsable de hacer cumplir la política de seguridad del sistema.

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-2022-067	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:	TLP:BLANCO	**ALERTAS DE SEGURIDAD**	ecucert
Fecha:	11-mayo-2022	**RANSOMWARE QUANTUM LOCKER**	V 1.1

Microsoft Office, navegadores y bases de datos; en el caso de que se estén ejecutando se procederá a eliminar dichos procesos. En la siguiente tabla se indican los procesos a terminar.

Tabla 1. Lista de procesos a terminar

msftesql.exe	agntsvc.exe	firefoxconfig.exe	mysqld-opt.exe
sqlbrowser.exe	isqlplussvc.exe	firefoxconfig.exe	dbeng50.exe
sqlwriter.exe	xfssvccon.exe	mydesktopqos.exe	sqbcoreservice.exe
oracle.exe	sqlservr.exe	ocomm.exe	excel.exe
ocssd.exe	encsvc.exe	mysqld.exe	infopath.exe
dbsnmp.exe	ocautoupds.exe	sqlagent.exe	msaccess.exe
synctime.exe	mydesktopservice.exe	mysqld-nt.exe	mspub.exe
onenote.exe	QBW32.exe	procmon64.exe	
Outlook.exe	QBW64.exe	procexp.exe	
powerpnt.exe	ipython.exe	procexp64.exe	
sqlservr.exe	wpython.exe	thebat.exe	
visio.exe	python.exe	vapor.exe	
winword.exe	dumpcap.exe	thebat64.exe	
wordpad.exe	procmon.exe	Thunderbird.exe	

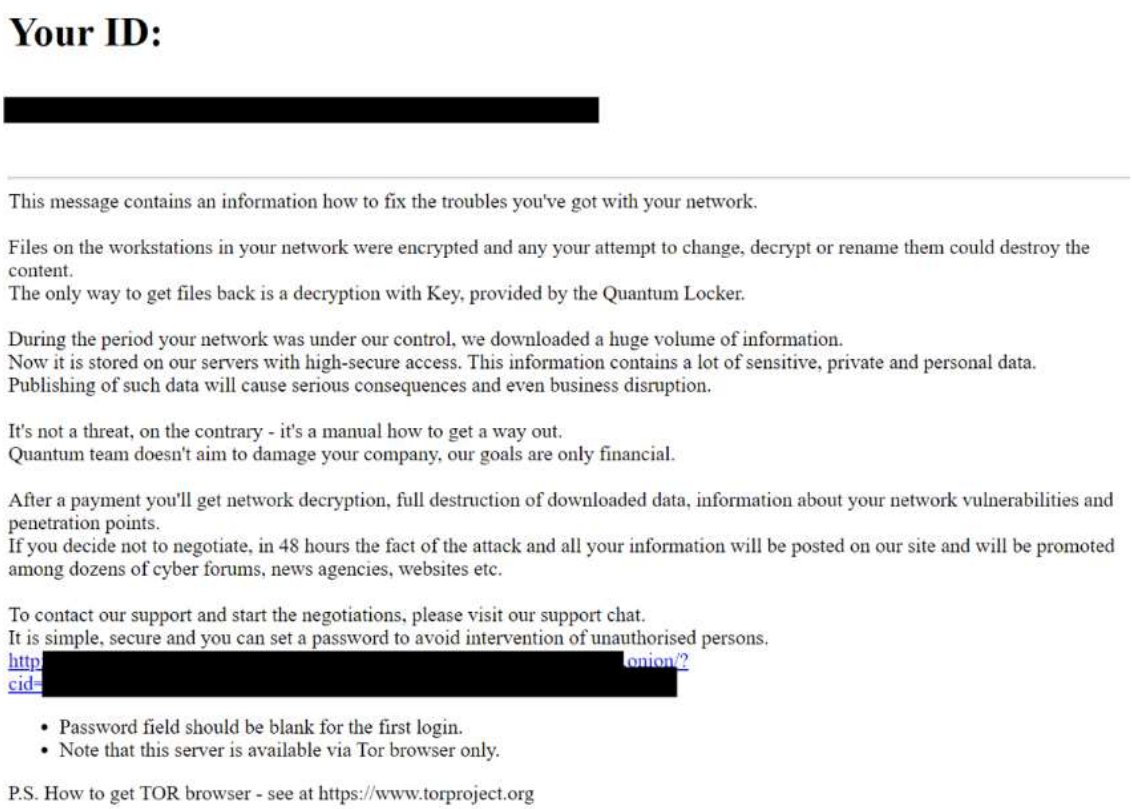
Fuente: Propia, adaptada de Cybereason

En la siguiente gráfica se observan los archivos encriptados por Quantum Locker, los mismos que poseen una extensión ".quantum"

Figura 4.- Archivo encriptados.
Fuente: Cybereason

A través del archivo "Readme" se dan a conocer las demandas de rescate que van desde miles de dólares, por ejemplo $150000 hasta demandas multimillonarias. En la siguiente gráfica se observa la nota de rescate generada.

Nro. Alerta:	EC-2022-067	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	11-mayo-2022	**RANSOMWARE QUANTUM LOCKER**	V 1.1



Your ID: [redacted]

This message contains an information how to fix the troubles you've got with your network.

Files on the workstations in your network were encrypted and any your attempt to change, decrypt or rename them could destroy the content.
The only way to get files back is a decryption with Key, provided by the Quantum Locker.

During the period your network was under our control, we downloaded a huge volume of information.
Now it is stored on our servers with high-secure access. This information contains a lot of sensitive, private and personal data.
Publishing of such data will cause serious consequences and even business disruption.

It's not a threat, on the contrary - it's a manual how to get a way out.
Quantum team doesn't aim to damage your company, our goals are only financial.

After a payment you'll get network decryption, full destruction of downloaded data, information about your network vulnerabilities and penetration points.
If you decide not to negotiate, in 48 hours the fact of the attack and all your information will be posted on our site and will be promoted among dozens of cyber forums, news agencies, websites etc.

To contact our support and start the negotiations, please visit our support chat.
It is simple, secure and you can set a password to avoid intervention of unauthorised persons.
http[redacted]onion/?cid=[redacted]

- Password field should be blank for the first login.
- Note that this server is available via Tor browser only.

P.S. How to get TOR browser - see at https://www.torproject.org

Figura 5.- Archivo Readme
Fuente: Thedfirreport

Al igual que otros tipos de ransomware como Conti o BlackCat; Quantum Locker emplea una doble extorsión y publica la información en su sitio en TOR. Una particularidad de este ransomware es el tiempo de pago de rescate antes de que toda la información sea publicada, la víctima cuenta 72 horas.

Nro. Alerta:	EC-2022-067	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	11-mayo-2022	**RANSOMWARE QUANTUM LOCKER**	V 1.1

En la siguiente gráfica se observa una ventana de interacción con los ciberdelincuentes.

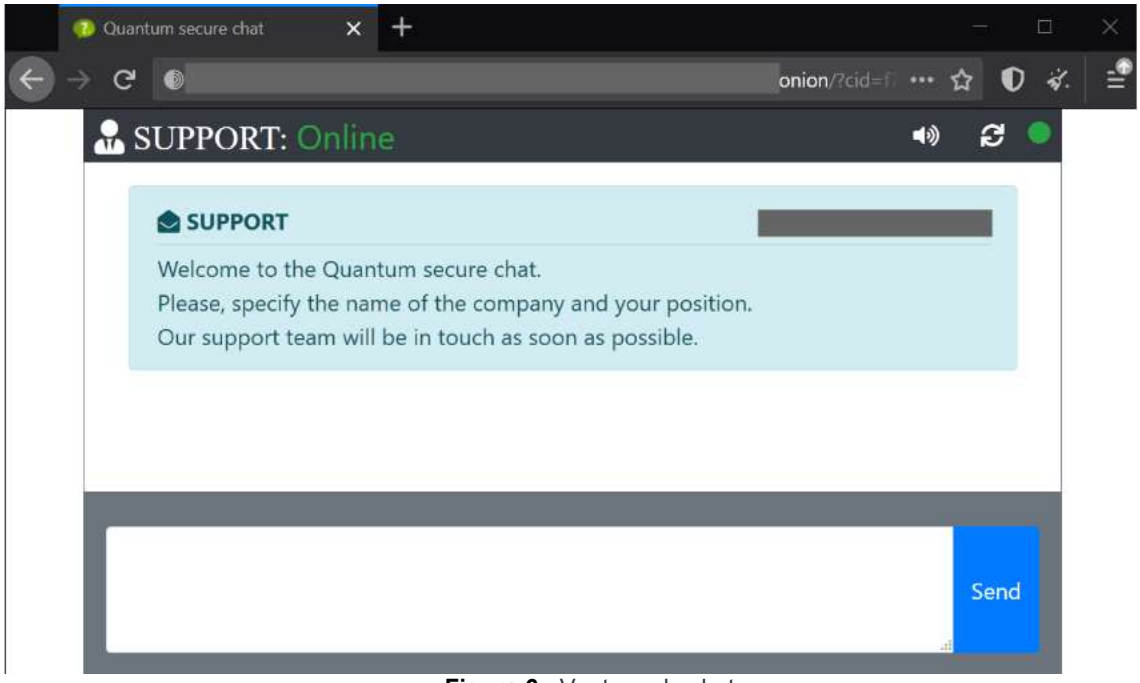


Figura 6.- Ventana de chat
Fuente: Thedfirreport

VI. INDICADORES DE COMPROMISO:

En la siguiente tabla, se indican los IOC asociados.

Tabla 2. IOC

SHA256	b63e94928da25e18caa1506305b9ca3dedc267e747dfa4710860e757d2cc8192
	1d64879bf7b1c7aea1d3c2c0171b31a329d026dc4e2f1c876d7ec7cae17bbc58
	511c1021fad76670d6d407139e5fef62b34ca9656fb735bd7d406728568fa280
	faf49653a0f057ed09a75c4dfc01e4d8e6fef203d0102a5947a73db80be0db1d
	0f3bb820adf6d3bba54988ef40d8188ae48b34b757277e86728bdb8441d01ea2
	0789a9c0a0d4f3422cb4e9b8e64f1ba92f7b88e2edfd14b7b9a7f5eee5135a4f
	8d30ab8260760e12a8990866eced1567ced257e0cb2fc9f7d2ea927806435208
	2c84b5162ef66c154c66fed1d14f348e5e0054dff486a63f0473165fdbee9b2e

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-2022-067	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	11-mayo-2022	**RANSOMWARE QUANTUM LOCKER**	V 1.1

	116e8c1d09627c0330987c36201100da2b93bf27560478be4043c1a834ad8913
	99a732c0512bc415668cc3a699128618f02bf154ff8641821c3207b999952533
	f72c47948a2cb2cd445135bc65c6bf5c0aaacc262ee9c04d1483781355cda976
	f8136eb39ee8638f9eb1acf49b1e10ce73e96583a885e4376d897ab255b39bd6
	79e25568a8aeec71d18adc07cdb87602bc2c6048e04daff1eb67e45f94887efc
	d44c065f04fe13bd51ba5469baa9077efb541d849ad298043739e08b7a90008f
	239d1c7cfd5b244b10c56abbf966f226e6a0cb91800e9c683ba427641e642f10
	7522b6de340a68881d11aa05e2c6770152e2d49ca5b830821ffce533fad948fd
	5bc00ad792d4ddac7d8568f98a717caff9d5ef389ed355a15b892cc10ab2887b
IP	138[.]68.42.130
	157[.]245.142.66
	188[.]166.154.118:80
Dominio	dilimoretast[.]com
	antnosience[.]com
	oceriesfornot[.]arriba
	sonlyevennot[.]superior

Fuente: Propia, adaptada de Cybereason

VII. RECOMENDACIONES:

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

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

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-2022-067	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	11-mayo-2022	**RANSOMWARE QUANTUM LOCKER**	V 1.1

- 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.

VIII. 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-2022-067	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	11-mayo-2022	**RANSOMWARE QUANTUM LOCKER**	V 1.1

IX. REFERENCIAS:

- Cybereason. (10 de 05 de 2022). *Cybereason*. Obtenido de Cybereason: https://www.cybereason.com/blog/cybereason-vs.-quantum-locker-ransomware
- itsecuritynews. (27 de 04 de 2022). *itsecuritynews*. Obtenido de itsecuritynews: https://www.itsecuritynews.info/quantum-ransomware-was-detected-in-several-network-attacks/
- Kiguolis, U. (13 de 04 de 2022). *2-spyware*. Obtenido de 2-spyware: https://www.2-spyware.com/remove-quantum-locker-ransomware.html
- Thedfirreport. (25 de 04 de 2022). *Thedfirreport*. Obtenido de Thedfirreport: https://thedfirreport.com/2022/04/25/quantum-ransomware/