Nro. Alerta:	EC-2022-65	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	06-mayo-2022	**Ransomware CONTI**	Versión 1.0

I. DATOS GENERALES:

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

II. ALERTA

CONTI es un RaaS (Ransomware as a service) que fue detectado a finales de 2019, con ataques en Europa, América del Norte y en este último mes con ataques en países cercanos de la región, como: Costa Rica, Colombia y Perú.

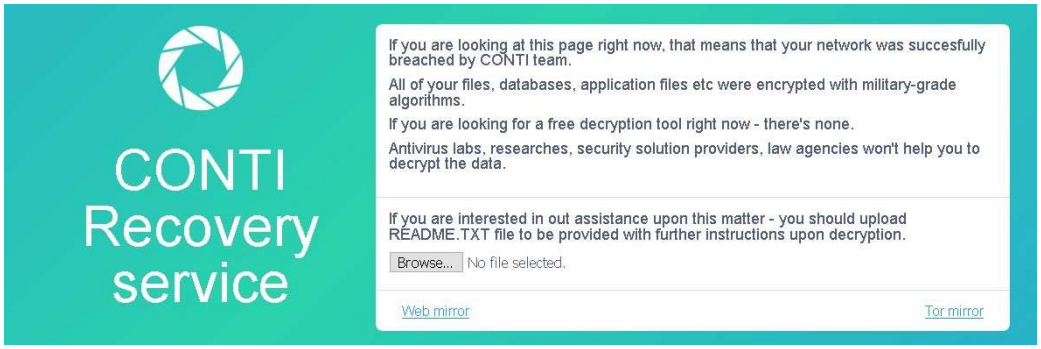

Figura 1. Ilustraciones relacionadas a ransomware CONTI
Fuente: WeLiveSecurity

III. INTRODUCCIÓN

CONTI es el nombre que emplea un grupo de ciberdelincuentes supuestamente de origen ruso, que distribuye ransomware como servicio RaaS; siendo detectado por primera vez entre octubre y diciembre de 2019. Así mismo, conforme señala el estudio realizado por Chainalysis titulado “The 2022 Crypto Crime Report”; CONTI fue el ransomware que obtuvo la mayor cantidad de recaudación por extorsión en el 2021 llegando alrededor de 180 millones de dólares.

Nro. Alerta:	EC-2022-65	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	06-mayo-2022	**Ransomware CONTI**	Versión 1.0

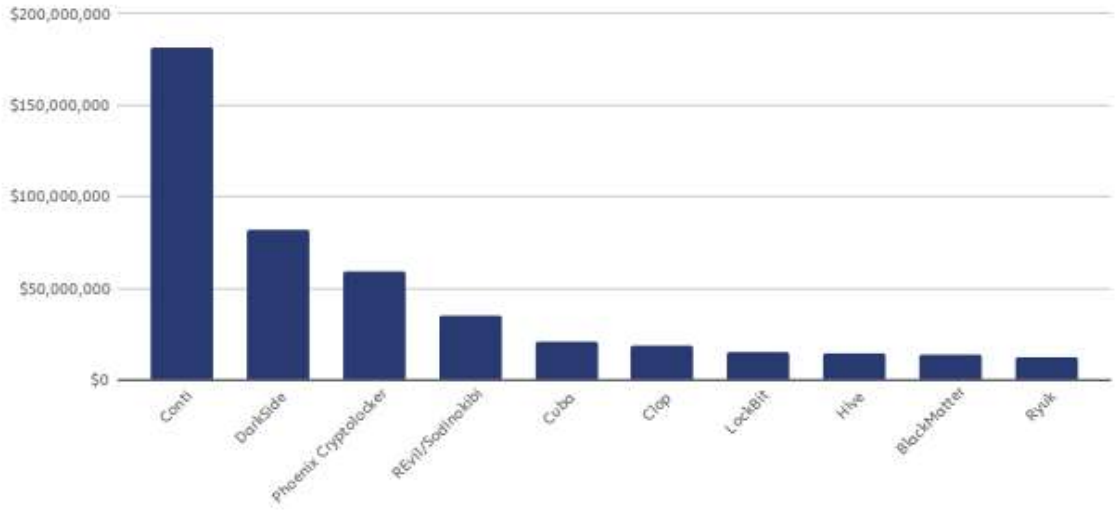

Figura 2. Valores recaudados por ransomware en el 2021.
Fuente: Chainalysis

CONTI emplea una modalidad de doble extorsión:

1. Filtrar información confidencial de sus víctimas previo al cifrado.
2. Extorsionar a las víctimas, amenazando con publicar información filtrada a menos que paguen el monto de dinero exigido.

Las víctimas de este ransomware se encuentran distribuidas a nivel mundial; por ejemplo, en el 2021 el ataque más recordado fue el perpetrado a Ireland's Health Service Executive (HSE), Ireland's Department of Health (DoH); en el cuál solicitaron un rescate de 20 millones de dólares; en américa latina también se hizo presente, afectando a organizaciones de Argentina, Brasil, Colombia, Nicaragua y República Dominicana.

En este sentido, en abril de 2022 se ha identificado ataques por parte de CONTI a Costa Rica, Colombia y Perú; en la siguiente imagen se indica las notas de rescate emitidas por CONTI.

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-2022-65	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	06-mayo-2022	**Ransomware CONTI**	Versión 1.0

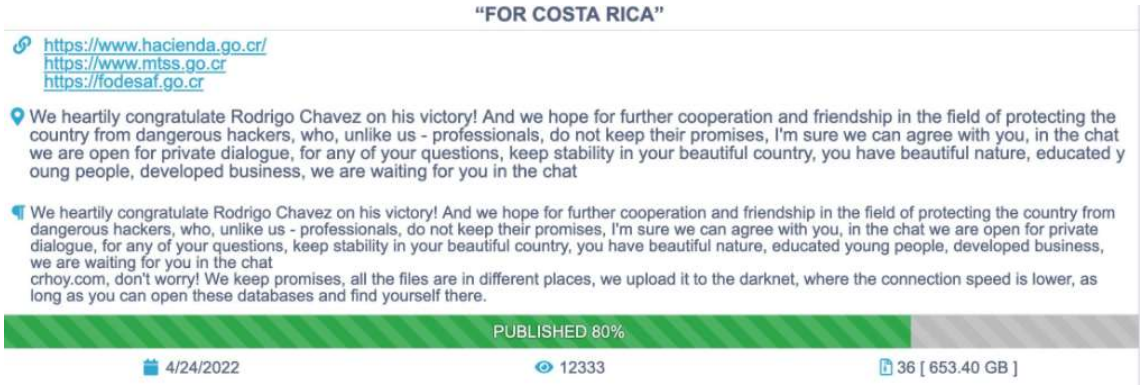

Figura 3. Nota de rescate emitida por Conti
Fuente: Tor

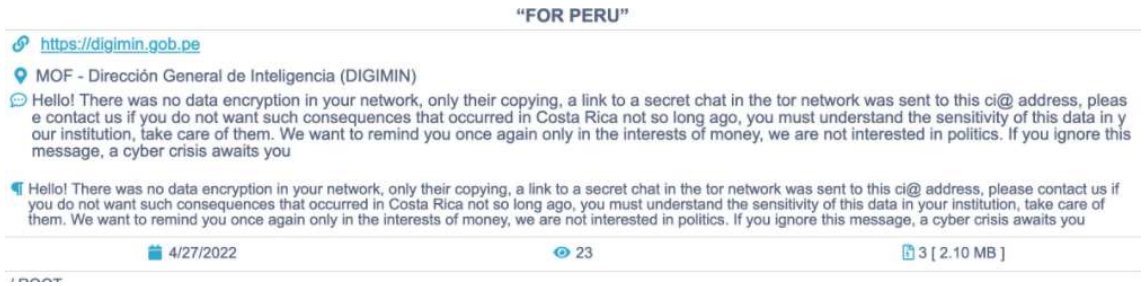

Figura 4. Nota de rescate emitida por Conti
Fuente: Tor

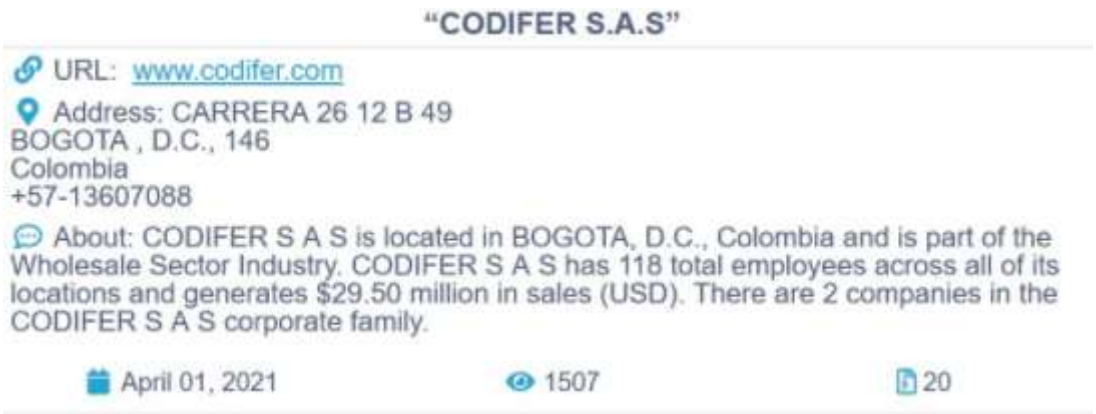

Figura 5. Nota de rescate emitida por Conti
Fuente: Tor

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-2022-65	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	06-mayo-2022	**Ransomware CONTI**	Versión 1.0

IV. VECTOR DE ATAQUE:

CONTI puede emplear diferentes técnicas:

- **Phishing**: A través de adjuntos maliciosos o enlaces maliciosos que permitirán la descarga de malware para realizar movimientos laterales dentro de la red y posteriormente descargara el correspondiente ransomware.
- **Explotación de vulnerabilidades:** De equipos expuestos a internet.

V. IMPACTO:

Para lograr la propagación en la red; CONTI, emplea varias herramientas, por ejemplo: Cobalt Strike, Mimikatz, PsExec; entre otras. Así mismo, el movimiento lateral emplea diferentes técnicas; por ejemplo:

- **Remote Windows Management Instrumentation (WMI):** Se utiliza para activar cargas útiles de forma remota mediante el proceso **/node:.. process call créate**
- **PsExec:** Tanto la herramienta Sysinternals como su implementación de Cobalt Strike se utilizan para la ejecución remota de la carga útil
- **Tarea remota programada:** Uso de la utilidad de línea de comandos SCHTASKS con el indicador /s para crear una tarea remota para ejecutar una carga útil colocada
- **WinRM:** Método de ejecución de código incorporado en Cobalt Strike.
- **EternalBlue:** Explotando una vulnerabilidad de ejecución remota de código en SMB.
- **BlueKeep**: Explotando una vulnerabilidad de ejecución remota de código en RDP.

En referencia a la recopilación de credenciales, CONTI emplea Mimikatz[1] y las herramientas:

- **Kerberoast:** Se utiliza para descifrar las contraseñas de usuario de servicio de Kerberos desde los tickets de servicio técnico
- **Zerologon:** Esta vez se utiliza como módulo posterior al ataque de Cobalt Strike para adquirir un inicio de sesión en el DC para ejecutar dcsync
- **Ladrón de credenciales:** Escanea el sistema de archivos local para buscar contraseñas de usuario almacenadas en archivos de texto y documentos

En la siguiente gráfica se observa el ciclo de infección empleado por CONTI.

[1] Aplicación de código abierto que permite robar datos de identificación de otros usuarios.

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-2022-65	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	06-mayo-2022	**Ransomware CONTI**	Versión 1.0

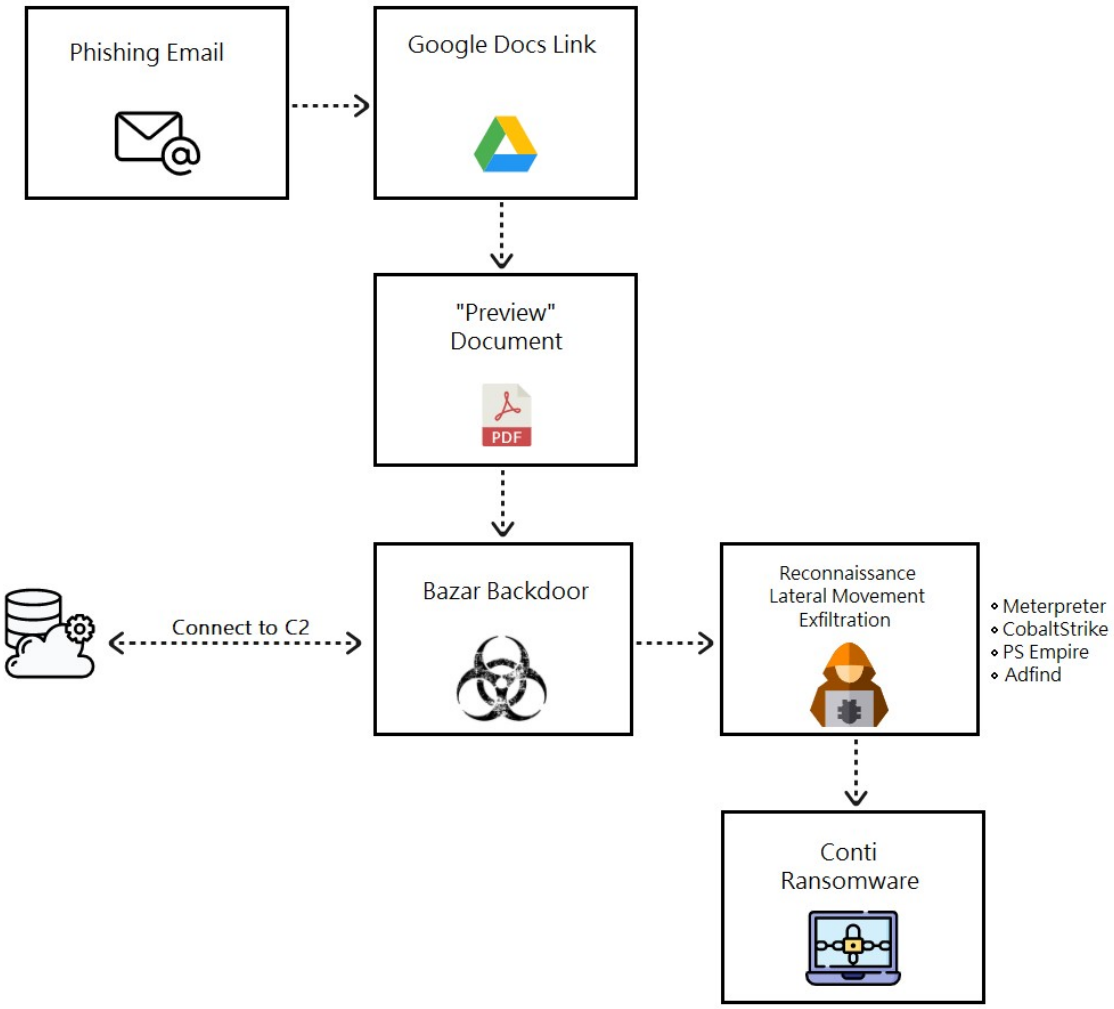

Figura 6. Ciclo de infección
Fuente: Blog Cyble

Una vez que la información ha sido comprometida, el archivo “CONTI_README” disponible en el escritorio de la víctima; señala las acciones a realizar.

Nro. Alerta:	EC-2022-65	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	06-mayo-2022	**Ransomware CONTI**	Versión 1.0

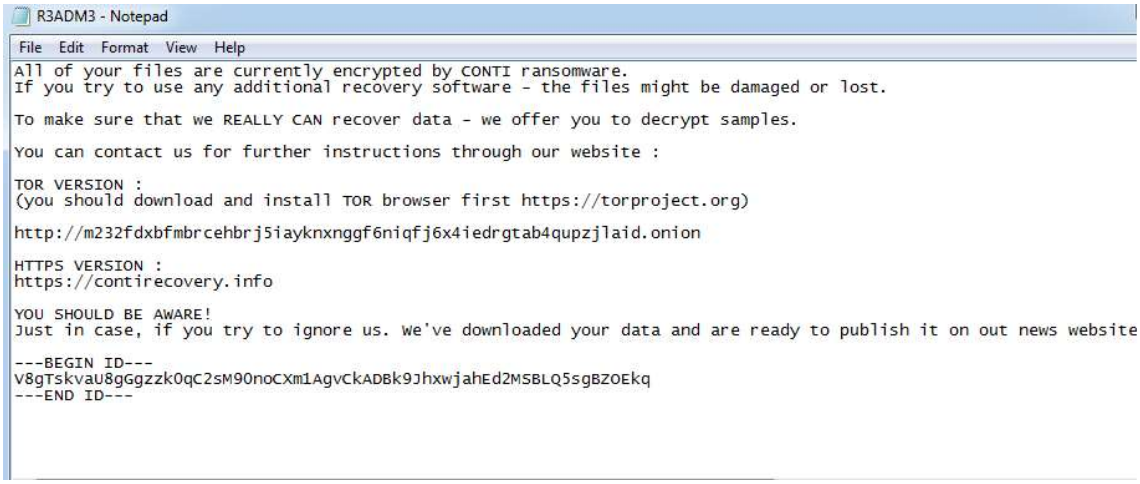

Figura 7. Nota de aviso
Fuente: Blog Cyble

A continuación, se presenta un resumen de las principales características de CONTI.

Resumen de la Amenaza	
Nombre	Virus CONTI
Tipo de Amenaza	Ransomware, Crypto Virus, Files locker.
Extensión de Archivos Encriptados	.CONTI
Mensaje de Rescate	CONTI_README.txt
Antivirus de Detección	Avast (Win32:Malware-gen), BitDefender (DeepScan:Generic.Ransom.AmnesiaE.634), ESET-NOD32 (una variante de Generik.EBKALVO), Kaspersky (Trojan.Win32.DelShad.cmo). En el siguiente enlace se mencionan los anti virus que detectan a CONTI: https://www.virustotal.com/gui/file/732e207d32fe4296e6cf0b4e874111e551a9490329e662fe42958e08ef3a9884/detection

Tabla 8. Resumen CONTI

VI. INDICADORES DE COMPROMISO

En la siguiente tabla se indica los IOC asociados a este ransomware:

Parámetro	Descripción				
Command and Control Server (C2)	162[.]244[.]80[.]235 85[.]93[.]88[.]165 185[.]141[.]63[.]120 82[.]118[.]21[.]1				
Hash	98ª9c760bb94d4d081271a3087ace8bed47fc4c8a38cdfe3f42b92bcdbee68e7 a64c3e0522fad787b95bfb6a30c3aed1b5786e69e88e023c062ec7e5cebf4d3e b93247a0efbbb9852d056e8cb655fc76d802928bf23586077ef0d73ba710e514 be8c5d07ab6e39db28c40db20a32f47a97b7ec9f26c9003f9101a154a5a98486 e09b43312a6b1622428a3d8bab0270673701d7d7a73c667dc3ee8940da0b96a1 e21fe7117b2bca120dec9f0bd970a6355b143a3b62207b480f93d1e35b70c0e5 efc85a4100dae0d3fa69cff22149a3f735ee34bb43c79524f379c44ac5814751 0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da 1b9a300d4e882a59e4bb15f7aa7069df6cc48057d1f89a71fff6df4e70d483f1 1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591 1d2a96013e4cc499cffab9000b9595e532a9feee425d3b4f536a5dc0695f381b 1ee21714bde9bf89cc6c55d7dac5686ad0e85f231c2ba7f91d575cb6a1f8092e 3c557727953a8f6b4788984464fb77741b821991acbf5e746aebdd02615b1767 4dc13bb83a16d4ff9865a51b3e4d24112327c526c1392e14d56f20d6f4eaf382 4e99e6b477daa5717a97f12a01ee8f2fa5aa8dce870982c7c45382c0e73aa1d1				
Dominios	badiwaw[.]com balacif[.]com barovur[.]com basisem[.]com bimafu[.]com bujoke[.]com buloxo[.]com bumoyez[.]com bupula[.]com	fipoleb[.]com fofudir[.]com fulujam[.]com ganobaz[.]com gerepa[.]com gucunug[.]com guvafe[.]com hakakor[.]com hejalij[.]com	kipitep[.]com kirute[.]com kogasiv[.]com kozoheh[.]com kuxizi[.]com kuyeguh[.]com lipozi[.]com lujecuk[.]com masaxoc[.]com	pihafi[.]com pilagop[.]com pipipub[.]com pofifa[.]com radezig[.]com raferif[.]com ragojel[.]com rexagi[.]com rimurik[.]com	tiyuzub[.]com tubaho[.]com vafici[.]com vegubu[.]com vigave[.]com vipeced[.]com vizosi[.]com vojefe[.]com vonavu[.]com

Tabla 9. IOC CONTI

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-2022-65	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	06-mayo-2022	**Ransomware CONTI**	Versión 1.0

VII. 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.
- Desconectar/aislar completamente de la infraestructura de red, ya sea interna o externa, cualquier dispositivo infectado o potencialmente infectado con ransomware.
- 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
- 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/

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

(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. REFERENCIAS:

Chainalysis. (02 de 2022). *Chainalysis*. Obtenido de Chainalysis: https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf

CISA. (21 de 09 de 2021). *CYBERSECURITY ADVISORY*. Obtenido de CYBERSECURITY ADVISORY: https://www.cisa.gov/uscert/sites/default/files/publications/AA21-265A-Conti_Ransomware_TLP_WHITE.pdf

Kupchik, S. (05 de 04 de 2022). *Akamai*. Obtenido de Akamai: https://www.akamai.com/es/blog/security/conti-hacker-manual-reviewed

Tavella, F. (29 de 11 de 2021). *Welivesecurity*. Obtenido de Welivesecurity: https://www.welivesecurity.com/la-es/2021/11/29/ransomware-conti-principales-caracteristicas/