IDENTIFICANDO a los autores del ransomware

JORGE CORONADO

III CONGRESO IMPULSO CIBERSEGURIDAD

¿Qué vamos a ver?

1. Autor
2. Conceptos básicos
3. CKC estandar
4. Grupos y situación actual
5. Investigación del grupo Vice Society
6. Conclusiones

¿Quién es Jorge Coronado?

Con una trayectoria de más de 10 años en forense informático y Open Source Intelligence (OSINT), este experto en ciberseguridad ha convertido su pasión por la programación en Python en una carrera fructífera. Desde sus inicios en la informática, ha ascendido rápidamente, culminando en la fundación de su propia empresa, QuantiKa14, que se especializa en Respuesta a Incidentes y Forensica Digital (DFIR), peritajes informáticos, desarrollo de aplicaciones y auditoría de seguridad.

Además de su extensa experiencia técnica, ha compartido su conocimiento a través de ponencias en prestigiosos congresos y eventos, incluyendo PyConEs, OpenExpo, Hack&Beers, EastMadHack y Sec/Admin. Activo en el ámbito profesional, es socio número 116 y vocal de la Asociación de Peritos Tecnológicos de Andalucía (APTAN) y socio 221 de la Asociación Profesional Española de Privacidad (PETEC).

Su compromiso con la divulgación de la ciberseguridad se extiende más allá de las conferencias. Ha sido colaborador durante cuatro años en Canal Sur Radio y ha escrito numerosos artículos de opinión e investigación que han sido publicados en ElPlural, lamarea.com, entre otros. También ha gestionado un blog activo con más de 400 publicaciones, y es el fundador de Happy Hacking Sevilla, la comunidad más activa de Sevilla en ciberseguridad, además de co-organizador del congreso OSINTCITY.

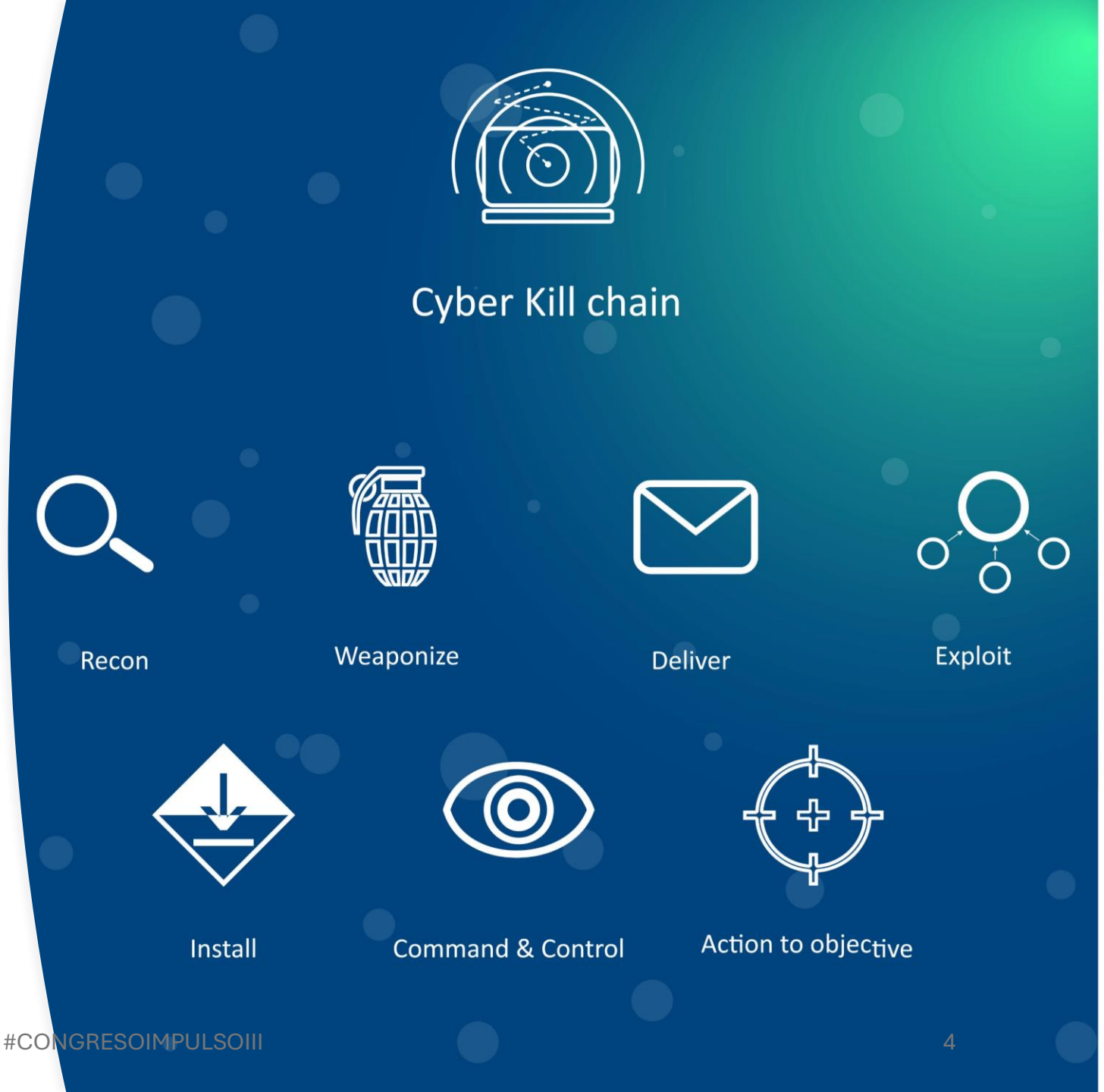
En el ámbito académico, fue director del curso de verano sobre ciberdelincuencia de género y profesor en el curso de detectives en investigación digital en la Universidad Pablo de Olavide en 2017. Ha impartido formación a cuerpos de seguridad a través de la Escuela Pública de Seguridad Pública de Andalucía (ESPA) y otros cursos.

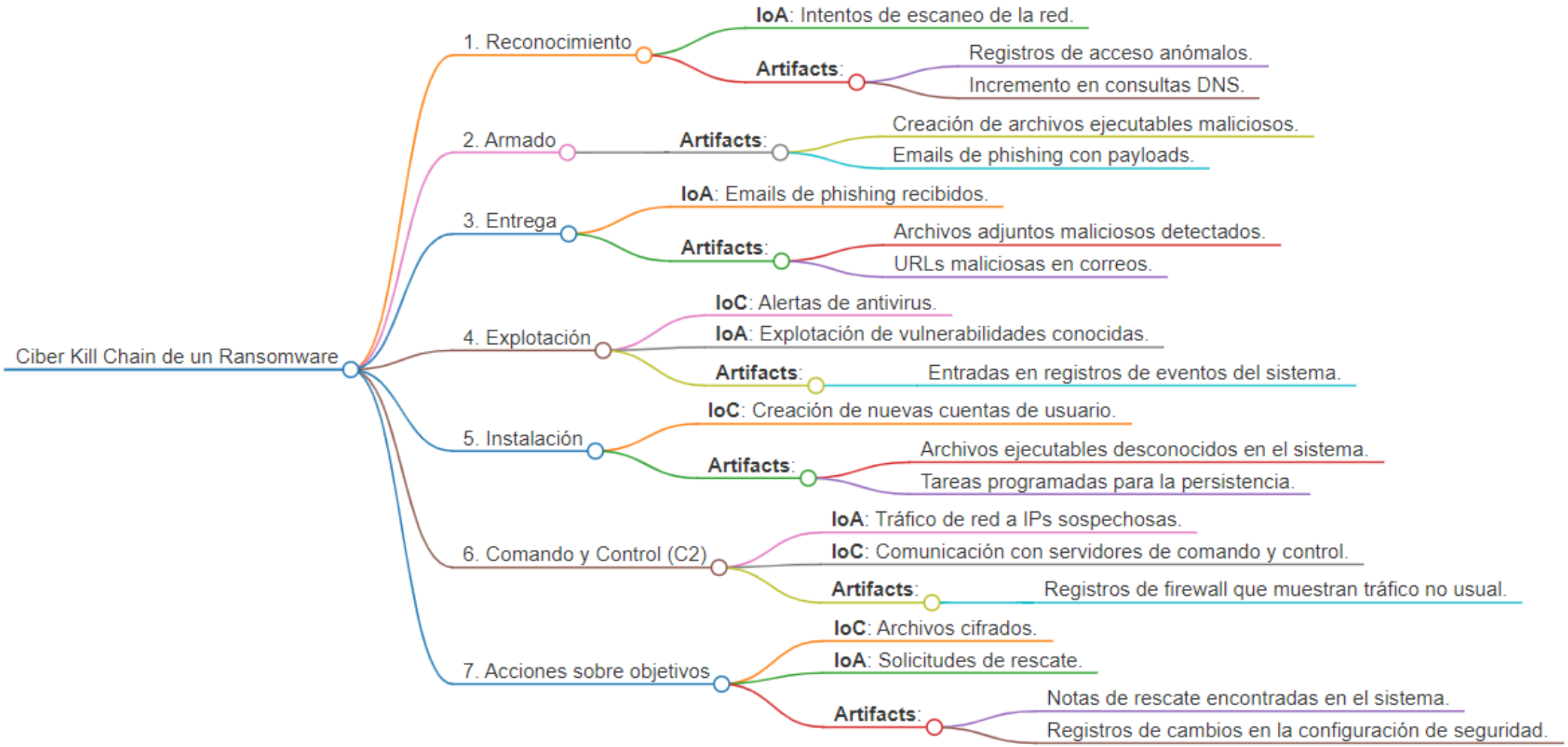
Como innovador en su campo, ha co-escrito el primer protocolo institucional en España contra la violencia de género en redes sociales en Andalucía y ha desarrollado un protocolo de actuación para la búsqueda de personas desaparecidas a través de las TIC.

Además, es el creador de aplicaciones innovadoras como INTELRTV y Dante's Gates, siendo esta última reconocida como el mejor producto de seguridad del 2023 por Red Seguridad.

Conceptos básicos

- Ransomware
- OSINT
- Cadena de Asesinato Cibernético (CKC)
- Técnicas, tácticas y procedimientos
- Indicadores de Ataque (IoA)
- Indicadores de Compromiso (IoC)
- Artifacts para Análisis Forense Informático




Ciber Kill Chain de un Ransomware
1. Reconocimiento
IoA: Intentos de escaneo de la red.
Artifacts:
Registros de acceso anómalos.
Incremento en consultas DNS.
2. Armado
Artifacts:
Creación de archivos ejecutables maliciosos.
Emails de phishing con payloads.
3. Entrega
IoA: Emails de phishing recibidos.
Artifacts:
Archivos adjuntos maliciosos detectados.
URLs maliciosas en correos.
4. Explotación
IoC: Alertas de antivirus.
IoA: Explotación de vulnerabilidades conocidas.
Artifacts:
Entradas en registros de eventos del sistema.
5. Instalación
IoC: Creación de nuevas cuentas de usuario.
Artifacts:
Archivos ejecutables desconocidos en el sistema.
Tareas programadas para la persistencia.
6. Comando y Control (C2)
IoA: Tráfico de red a IPs sospechosas.
IoC: Comunicación con servidores de comando y control.
Artifacts:
Registros de firewall que muestran tráfico no usual.
7. Acciones sobre objetivos
IoC: Archivos cifrados.
IoA: Solicitudes de rescate.
Artifacts:
Notas de rescate encontradas en el sistema.
Registros de cambios en la configuración de seguridad.

Grupos y situación actual

ÚLTIMOS 90 DÍAS

May 15Th, 2024

Currently tracking **191** groups across **338** relays & mirrors - ***68*** *currently online*

There have been **26** posts within the last 24 hours

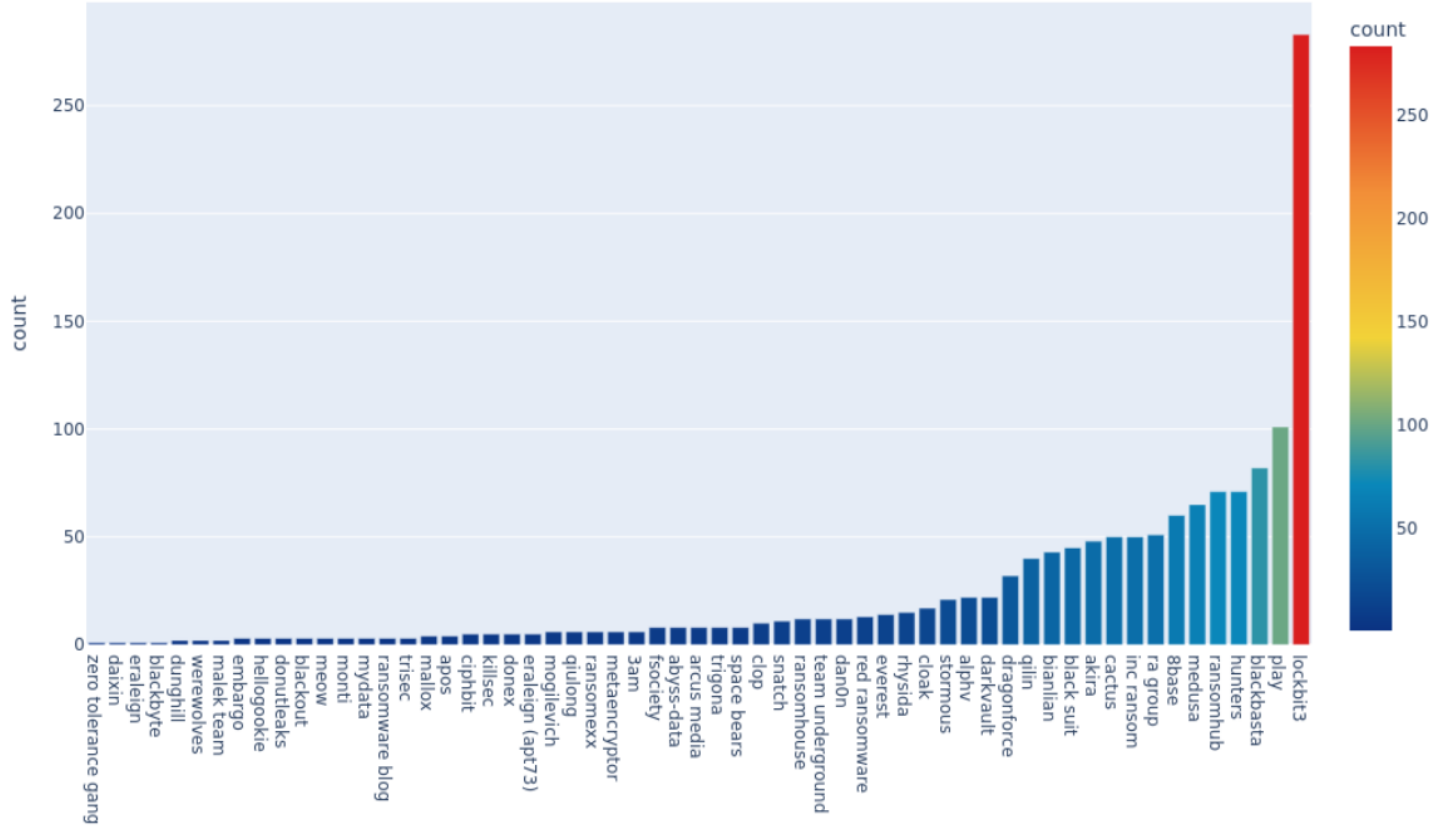
There have been **379** posts within the month of may

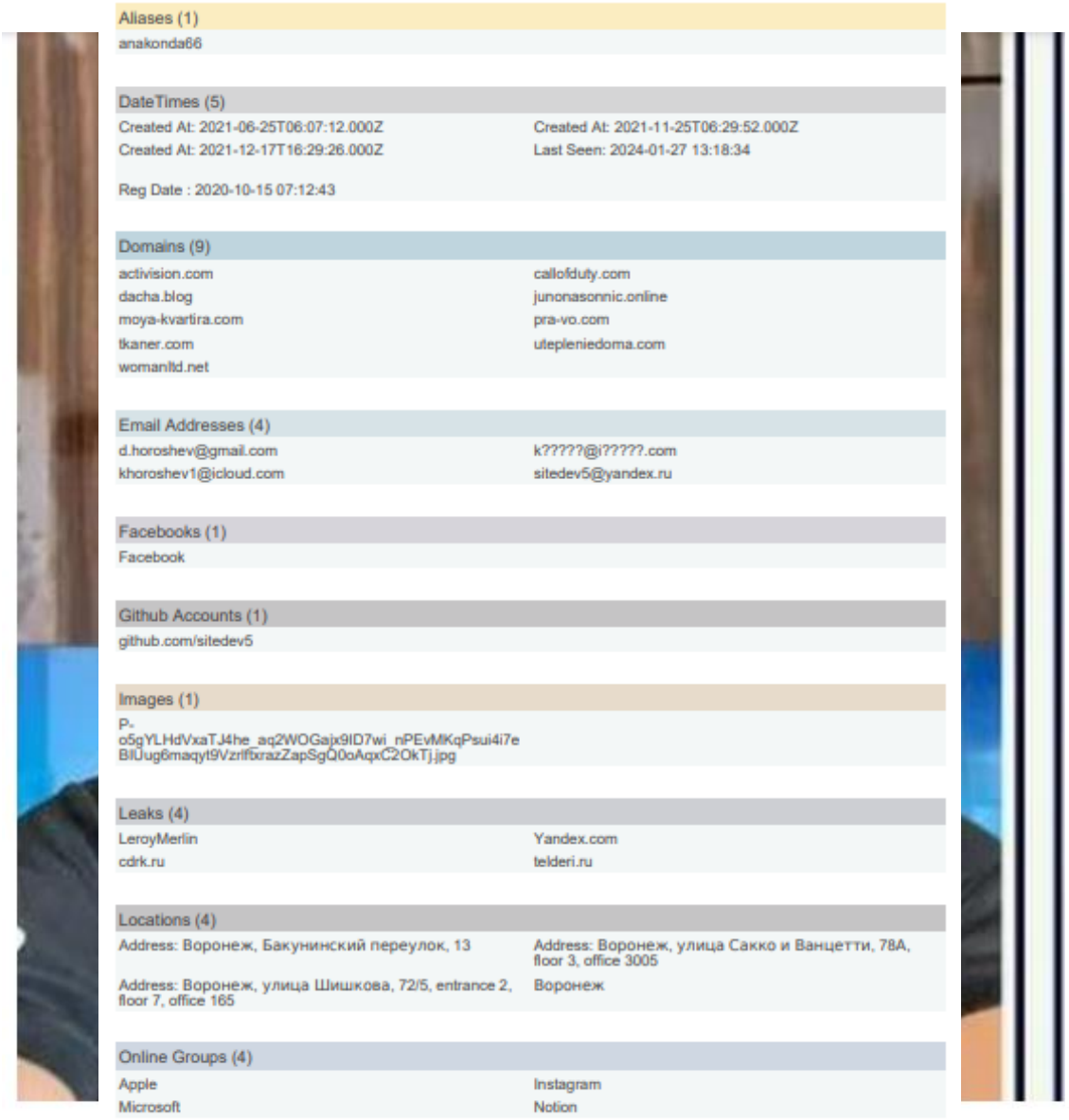
There have been **1408** posts within the last 90 days

There have been **1941** posts within the year of 2024

There have been **14011** posts since the dawn of ransomlook

There are **113** custom parsers indexing posts





Aliases (1)
anakonda66

DateTimes (5)
Created At: 2021-06-25T06:07:12.000Z
Created At: 2021-11-25T06:29:52.000Z
Created At: 2021-12-17T16:29:26.000Z
Last Seen: 2024-01-27 13:18:34
Reg Date : 2020-10-15 07:12:43

Domains (9)
activision.com
callofduty.com
dacha.blog
junonasonnic.online
moya-kvartira.com
pra-vo.com
tkaner.com
utepleniedoma.com
womanlld.net

Email Addresses (4)
d.horoshev@gmail.com
k?????@i?????.com
khoroshev1@icloud.com
sitedev5@yandex.ru

Facebooks (1)
Facebook

Github Accounts (1)
github.com/sitedev5

Images (1)
P-
o5gYLHdVxaTJ4he_aq2WOGajx9ID7wi_nPEvMKqPsui4i7e
BlUug6maqyt9VzrlfbrazZapSgQ0oAqxC2OkTj.jpg

Leaks (4)
LeroyMerlin
Yandex.com
cdrk.ru
telderi.ru

Locations (4)
Address: Воронеж, Бакунинский переулок, 13
Address: Воронеж, улица Сакко и Ванцетти, 78А, floor 3, office 3005
Address: Воронеж, улица Шишкова, 72/5, entrance 2, floor 7, office 165
Воронеж

Online Groups (4)
Apple
Instagram
Microsoft
Notion

Passwords (1)
O3x0flMWadd3bb04d1530ba15e418cbb1b720d06

People (1)
Дмитрий Хорошев

Phone Numbers (4)
+747 3241 4824
+795 2102 0220
+796 7341 5167
? (???) ???-??-20

Phrases (31)
2022-08-23 17:56:34
Address Comment: Вход будет слева, после металической двери и лестницы
Door Code: 165
Door Code: 3005
Expiry Date: 2024-06-22 00:00:00
Expiry Date: 2024-09-10 00:00:00
Expiry Date: 2024-09-11 00:00:00
Expiry Date: 2024-10-14 00:00:00
Expiry Date: 2024-10-22 00:00:00
Expiry Date: 2024-12-17 00:00:00
Expiry Date: 2025-04-01 00:00:00
ID: 498546248
ID: 667139228
ID: 687771007
Notion
Registration Date: 2013-06-22 00:00:00
Registration Date: 2013-10-22 00:00:00
Registration Date: 2016-10-14 00:00:00
Registration Date: 2018-12-17 00:00:00
Registration Date: 2020-04-01 00:00:00
Registration Date: 2020-09-10 00:00:00
Registration Date: 2020-09-11 00:00:00
The entrance will be on the left, after the metal door and the stairs.
Update Date: 2023-06-08 00:00:00
Update Date: 2023-08-26 00:00:00
Update Date: 2023-08-26 00:00:00
Update Date: 2023-08-31 00:00:00
Update Date: 2023-09-12 00:00:00
Update Date: 2023-12-03 00:00:00
Update Date: 2024-04-02 00:00:00
n2KvePcv71173f5198ddf937d9921fcf7abbb4de

URLs (1)
nationalcrimeagency.gov.uk

Vkontakte Id or Alias or URLs (1)
vk.com/d_khoroshev

Whatsapps (1)
Whatsapp

Dimitry Khoroshev, el creador ruso del programa malicioso LockBit. (Departamento de Justicia de Estados Unidos).

https://www.vice.com/en/article/n7nw8m/conti-ransomware-hackers-apologize-to-arab-royal-families-for-leaking-their-data

la oscura parte inferior de Internet.

VER MÁS →

Entre los datos filtrados por Conti, había archivos sensibles pertenecientes a celebridades como David Beckham, Oprah Winfrey y Donald Trump, según *El Daily Mail*. También había, según los propios hackers, información perteneciente a los Emiratos Árabes Unidos, Qatar y las familias reales sauditas.

Y los hackers realmente no quieren molestarlos.

"Encontramos que nuestros datos de muestra no se revisaron adecuadamente antes de ser subidos al blog," escribieron los hackers en un anuncio publicado el jueves. "Conti garantiza que cualquier información relacionada con los miembros de las familias de Arabia Saudita, Emiratos Árabes Unidos y Qatar se eliminará sin ninguna exposición y revisión."

"Nuestro Equipo se disculpa con Su Alteza Real el Príncipe Mohammed bin Salman y cualquier otro miembro de las Familias Reales cuyos nombres fueron mencionados en la publicación por cualquier inconveniente,"

En fecha 10 de octubre de 2023 se constata la recepción de la respuesta a la reiteración del requerimiento, de su análisis se extrae las siguientes afirmaciones relevantes para la investigación:

- El día 20 de abril de 2023 tuvieron problemas al intentar entrar en el sistema informático y acceder a los datos de pacientes, localizando un fichero que contenía un mensaje en el que se solicitaba rescate por los datos encriptados.

- Puesto que, el disco duro estaba encriptado, procedieron a sustituirlo en fecha 24 de abril de 2023, reinstalando el software necesario.

- La última copia de seguridad que disponían tenía una antigüedad de un mes aproximadamente y estaba guardada en un disco duro externo, esta copia sirvió para recuperar todos los datos de pacientes hasta esa fecha. Afirman lo siguiente: "*A partir de ahí se pudo comenzar a trabajar con normalidad, aunque con el inconveniente principal de haber perdido la agenda de citas de los pacientes…Los datos que se perdieron del último mes se han podido ir recuperando con normalidad, las citas con los pacientes han permitido recuperar la información de los tratamientos que se les habían realizado y darles continuidad*".
- En relación con el ordenador afectado afirman que: "*El ordenador servidor disponía de antivirus, pero la brecha se produjo a través de un puerto abierto para conexión remota, y no fue suficiente*".
- El ordenador disponía de antivirus, pero la brecha se produjo a través de un puerto abierto para conexión remota.
- Afirman que tras la brecha decidieron ***(…)***.
- El número de afectados aproximado es de 2500, todos ellos pacientes, con datos identificativos, de salud y económicos sobre pagos, pero sin existir números de cuenta bancaria o números de tarjetas de crédito.
- Afirman que no han recibido comunicación o quejas de pacientes alertando de la materialización de posibles consecuencias y que han monitorizado internet sin obtener exposición de datos.
- Se adjunta un informe del incidente redactado por la empresa informática que da soporte técnico a DENTALCUADROS, de su análisis se extrae:
    - El informe está redactado por la empresa JOSEP MOLINS SERVEIS INFORMATICS.
    - En el informe se afirma que la noche del 20 al 21 de abril de 2023 "*hackers consiguen entrar por la brecha del puerto 3389 abierto en el router para la conexión de escritorio remoto, procediendo a encriptar todos los ficheros de datos incluido Microsoft SQL…Cabe destacar que como el ataque se produce de madrugada, el resto de los ordenadores de la clínica están apagados con lo que no consiguen encriptar*".

¿Qué te puede suceder si no implementas medidas y actúas mal tras un ataque de ransomware?

De conformidad con lo dispuesto en el artículo 85 de la LPACAP, podrá reconocer su responsabilidad dentro del plazo otorgado para la formulación de alegaciones al presente acuerdo de inicio; lo que llevará aparejada una reducción de un 20% de la sanción que proceda imponer en el presente procedimiento. Con la aplicación de esta reducción, la sanción quedaría establecida en 16.000,00 euros, resolviéndose el procedimiento con la imposición de esta sanción.

Del mismo modo podrá, en cualquier momento anterior a la resolución del presente procedimiento, llevar a cabo el pago voluntario de la sanción propuesta, lo que supondrá la reducción de un 20% de su importe. Con la aplicación de esta reducción, la sanción quedaría establecida en 16.000,00 euros y su pago implicará la terminación del procedimiento, sin perjuicio de la imposición de las medidas correspondientes.

La reducción por el pago voluntario de la sanción es acumulable a la que corresponde aplicar por el reconocimiento de la responsabilidad, siempre que este reconocimiento de la responsabilidad se ponga de manifiesto dentro del plazo concedido para formular alegaciones a la apertura del procedimiento. El pago voluntario de la cantidad referida en el párrafo anterior podrá hacerse en cualquier momento anterior a la resolución. En este caso, si procediera aplicar ambas reducciones, el importe de la sanción quedaría establecido en 12.000,00 euros.

En todo caso, la efectividad de cualquiera de las dos reducciones mencionadas estará condicionada al desistimiento o renuncia de cualquier acción o recurso en vía administrativa contra la sanción.

En caso de que optara por proceder al pago voluntario de cualquiera de las cantidades señaladas anteriormente (16.000,00 euros o 12.000,00 euros), deberá hacerlo efectivo

agencia española protección datos

> "*Como ya se sabe que pretenden extorsionar económicamente y rechazándolo completamente se procede a buscar copias externas de los datos encriptados. Localizamos un disco externo donde se encuentre una copia de hace dos meses aproximadamente. Decidimos actuar con dicha copia*."
>
> "*No tenemos constancia de que los datos hayan sido robados, sino que han sido encriptados para pedir un rescate. En cualquier caso, en el programa de gestión hay fichas de pacientes y tratamientos dentales. No se guardan datos económicos como tarjetas de crédito, etc…así que la exposición solo afectaría a direcciones, teléfonos o direcciones de correo.*"

- Se afirma que procedieron de la siguiente forma: ***(…).***

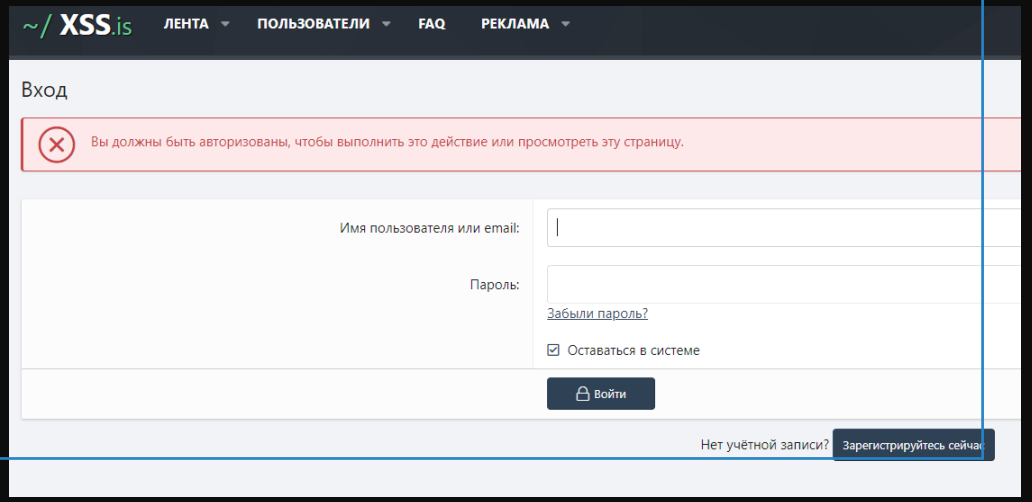
- Se adjunta el Registro de Actividades de Tratamiento (RAT) con la información de la actividad afectada por la brecha ("*Gestión de Pacientes*"), de su análisis se extrae:
  - Incluye los datos del Delegado de Protección de Datos, la empresa *SRCL Consenur SLU*.
  - Finalidad del tratamiento: *diagnosis, tratamiento e historial médico, gestión administrativa, contable y fiscal.*
  - Interesados: *pacientes, padres o tutores, representante legal.*
  - Datos: *DNI, nombre y apellidos, dirección, teléfono, firma, imagen, salud, datos biométricos, datos sobre categorías personales, datos económicos, financieros y seguros.*
  - Transferencias: *al prestador Align Technology Inc en EEUU a través de Normas Corporativas Vinvulantes.*
  - Plazos de conservación: *Historial clínico (Ley 41/2002) obliga a conservar historias clínicas un mínimo de 5 años. La Ley 21/2000 de Cataluña obliga a conservación durante 15 años de determinada información relacionada con la historia clínica.*
  - Descripción general de medidas de seguridad:
    - ***(…).***
  - Base jurídica: *prestación de servicio contratado y cumplimiento de obligación legal.*


Medidas para Evitar Ataques de Ransomware
1. Contra Ataques de Phishing
Educación y Concienciación de Empleados
Capacitaciones regulares sobre seguridad informática.
Simulaciones de phishing para mejorar la detección.
Filtros de Correo Electrónico
Implementar soluciones avanzadas de filtrado de spam.
Bloquear adjuntos de tipos de archivos riesgosos.
Verificación de URLs y Dominios
Herramientas para verificar la seguridad de enlaces en emails.
2. Contra Acceso Remoto a Servicios
Uso de VPNs Seguras
Implementar y obligar el uso de VPNs cifradas para todo acceso remoto.
Autenticación de Dos Factores (2FA)
Obligatoria para acceso a sistemas críticos y administrativos.
Políticas de Seguridad Estrictas
Restricciones de acceso según el principio de menor privilegio.
Sesiones de tiempo limitado para conexiones remotas.
3. Contra Vulnerabilidades en Sistemas Informáticos
Gestión de Parches
Programa regular de actualizaciones y parches para software y sistemas operativos.
Verificación y aplicación de parches de seguridad críticos con prioridad.
Herramientas de Detección de Intrusos
Sistemas de detección y prevención de intrusiones (IDS/IPS) en la red.
Respaldo y Recuperación de Datos
Implementar políticas de respaldo frecuentes y seguras.
Pruebas regulares de los planes de recuperación de desastres.
4. Medidas Generales
Auditorías de Seguridad
Evaluaciones de seguridad regulares por parte de terceros.
Segmentación de Red
Dividir la red en segmentos para limitar la propagación de ataques.
Monitorización Continua
Uso de herramientas de monitorización en tiempo real para detectar actividades sospechosas.

¿Investigamos?

¿Quién es Vice Society?

Zeppelin ransomware se ofrece como Ransomware-as-a-Service (RaaS) en varios foros de ciberdelincuencia de habla rusa (XSS, BHF, DarkMarket, IFUD).

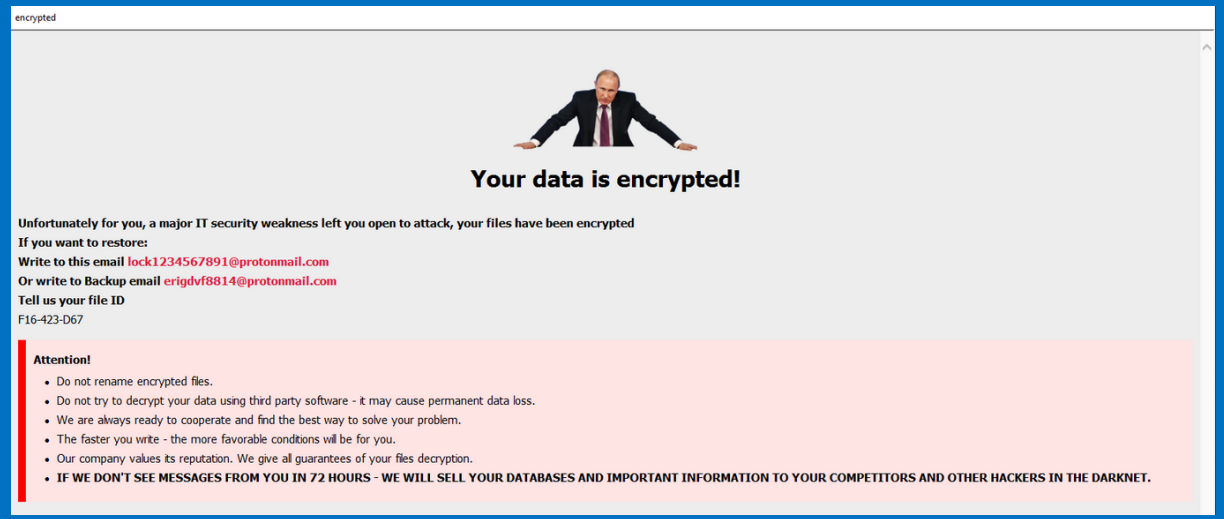


RAMAS DE VICE SOCIETY

“Vice Society is a threat group active since at least early June 2021, known for deploying multiple ransomware strains on their victims' networks, such as **Hello Kitty/Five Hands and Zeppelin ransomware.**”

“Vice Society es un grupo de amenazas activo desde al menos principios de junio de 2021, conocido por implementar múltiples cepas de ransomware en las redes de sus víctimas, **como Hello Kitty/Five Hands y Zeppelin ransomware**.”

https://www.bleepingcomputer.com/news/security/microsoft-vice-society-targets-schools-with-multiple-ransomware-families/



“On October 21, the FBI notified OAG that it had seized an account belonging to HelloKitty, a **Ukrainian hacking group**, which contained OAG patient and employee files,” the Oregon Anesthesiology Group said in a breach disclosure on December 6.

The FBI believes HelloKitty exploited a vulnerability in our third-party firewall, enabling the hackers to gain entry to the network,” it added.

While the HelloKitty ransomware, also known as FiveHands, has been active since January 2021, details about the gang’s possible location had not been previously shared or disclosed.

No mentions about their possible location were included in a CISA alert, an FBI IC3 alert, nor in reports from multiple security firms such as NCC Group, Cado Security, Malwarebytes, Palo Alto Networks, SentinelOne, and Mandiant.

With Ukrainian police successfully detaining members of the REvil, Clop, and LockerGoga gangs, along with others, over the past six months, it is now a real possibility that this slip-up from OAG might have tipped off HelloKitty’s Ukrainian operators to the need to move to a new jurisdiction.”

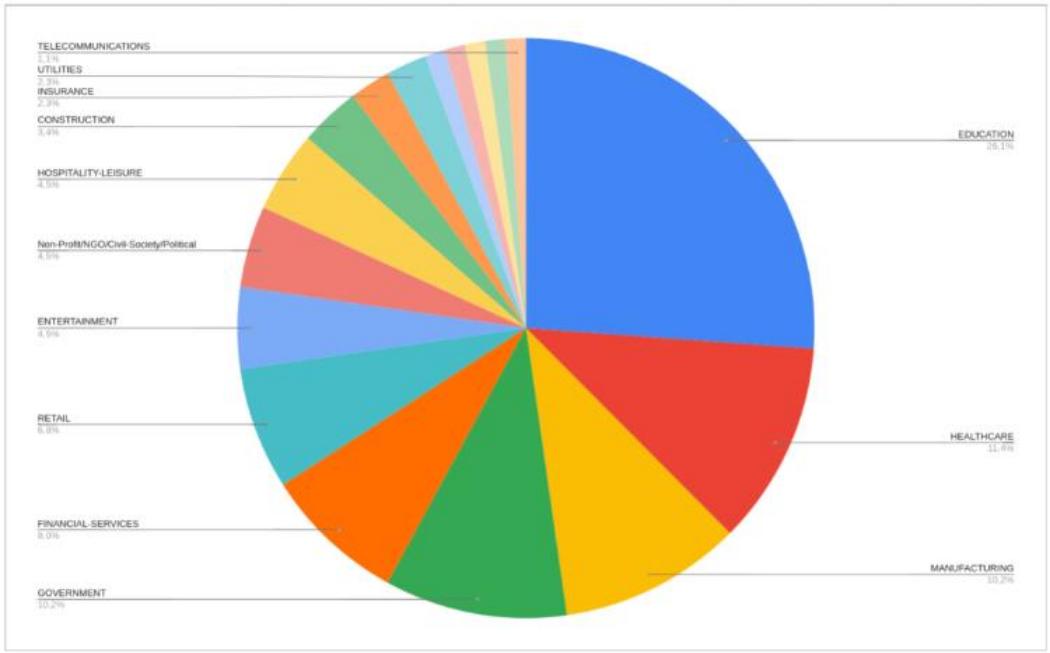
“Con la policía ucraniana deteniendo con éxito a miembros de las pandillas REvil, Clop y LockerGoga, junto con otros, en los últimos seis meses, ahora existe una posibilidad real de que este desliz de OAG podría **haber alertado a los operadores ucranianos de HelloKitty sobre la necesidad de trasladarse a una nueva jurisdicción**.”

https://therecord.media/the-fbi-believes-the-hellokitty-ransomware-gang-operates-out-of-ukraine

Analizamos el logo

Víctimas	URL
CSIC	http://www.csic.es/
Jealsa	https://www.jealsa.com
	https://www.rianxeira.com
Vygon	http://www.vygon.es/
Vectalia Group	http://www.alicante.vectalia.es/
Caldes Montbui	http://www.caldesdemontbui.cat/
Levantina Ing y construcción	http://www.lic-sl.com/
Maristes Hermitage	http://www.maristes.eu/
Amaveca Salud	https://amavecasalud.es/
Prosol	http://www.prosol.ca/

Empresas víctimas en España expuesto en la web



Analizamos sus víctimas

IoCs

- Fuente: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6690-ccn-cert-id-09-22-vice-society-neshta-1/file.html

Neshta		
Tipo	**Descripción**	**Valor**
Sistema de ficheros	Carpeta en la que los ficheros originales son guardados una vez se descifran. Previamente a su ejecución.	"%TEMP%\3582-490
Sistema de ficheros	Fichero que crea para hacer una copia de sí mismo.	%SystemRoot%\svchost.com
Sistema de ficheros	Indica el ultimo fichero infectado que ha sido ejecutado	%SystemRoot%\directx.sys
Sistema de ficheros	Creado una vez todos los ficheros han sido infectados	%TMP%\tmp5023.tmp
Clave de registro	Clave de registro creada para la persistencia	**Clave:** HKLM\SOFTWARE\Classes\exefile\shell\open\command **Valor de Registro:** (Default) **Valor:** %SystemRoot%\svchost.com "%1" %*
Mutex	Mutex creado para evitar que estén en ejecución múltiples instancias del virus	MutexPolesskayaGlush*.*

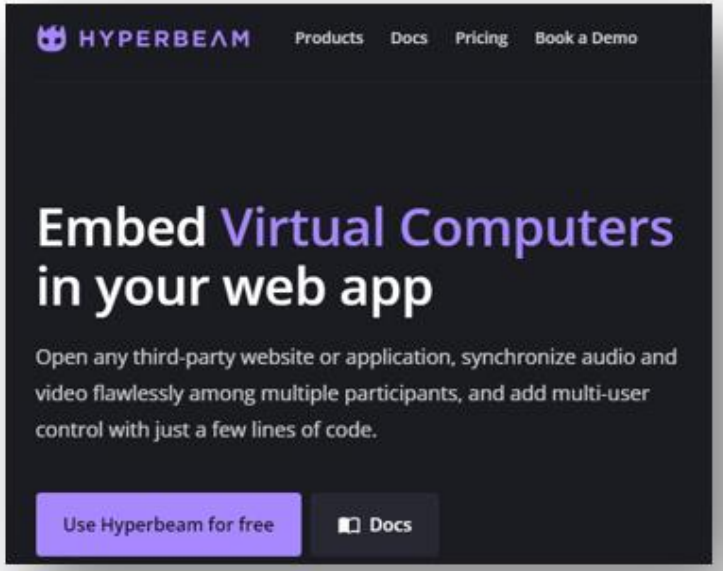
Ransomware		
Tipo	**Descripción**	**Valor**
Sistema de ficheros	Extensión de los ficheros cifrados	".xnxxx"
Sistema de ficheros	Nombre del fichero que contiene el mensaje de rescate	"ALL YOUR FILES ARE ENCRYPTED!!!
Sistema de ficheros	El nombre de este fichero es generado a raíz de la clave pública, y tiene un tamaño de 40 caracteres. Se utiliza para guardar información relacionada con el cifrado	**Caso genérico:** C:\Users\Public\[A-F0-9]{40} **Caso concreto de la muestra analizada:** C:\Users\Public\6F4B95343D2D76D10F87017F60B7235937F26A64
Clave de registro	Clave de registro creada para la persistencia	**Clave:** HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce **Valor de Registro:** LicChk **Valor:** {path_al_fichero_ejecutable_del_ransomware}

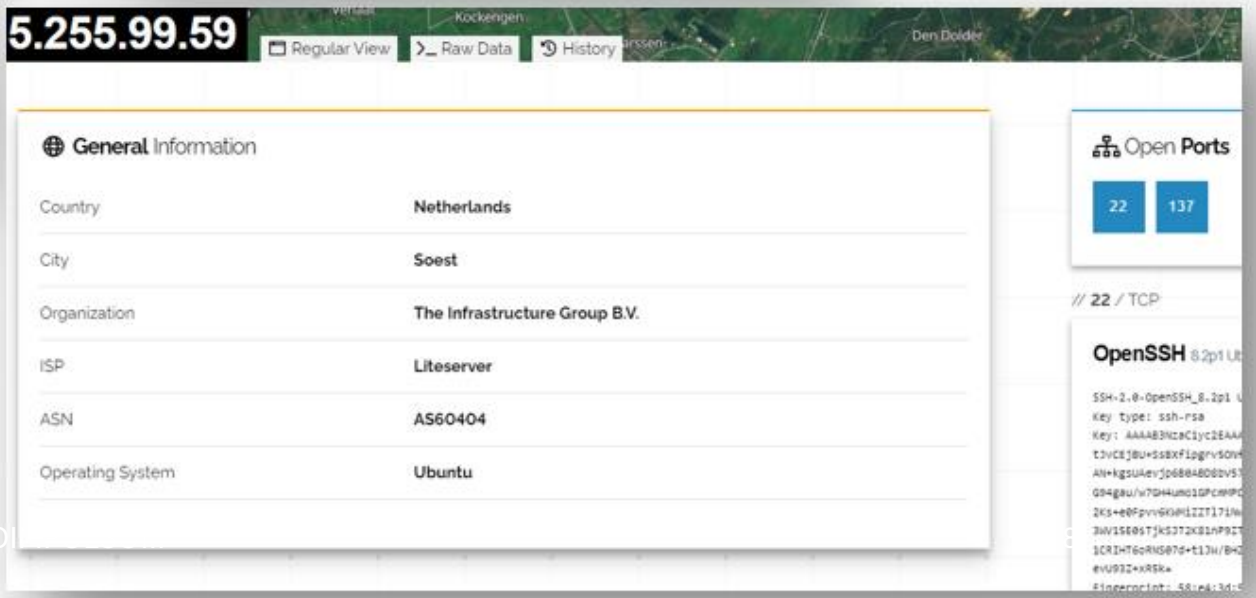
IOCs

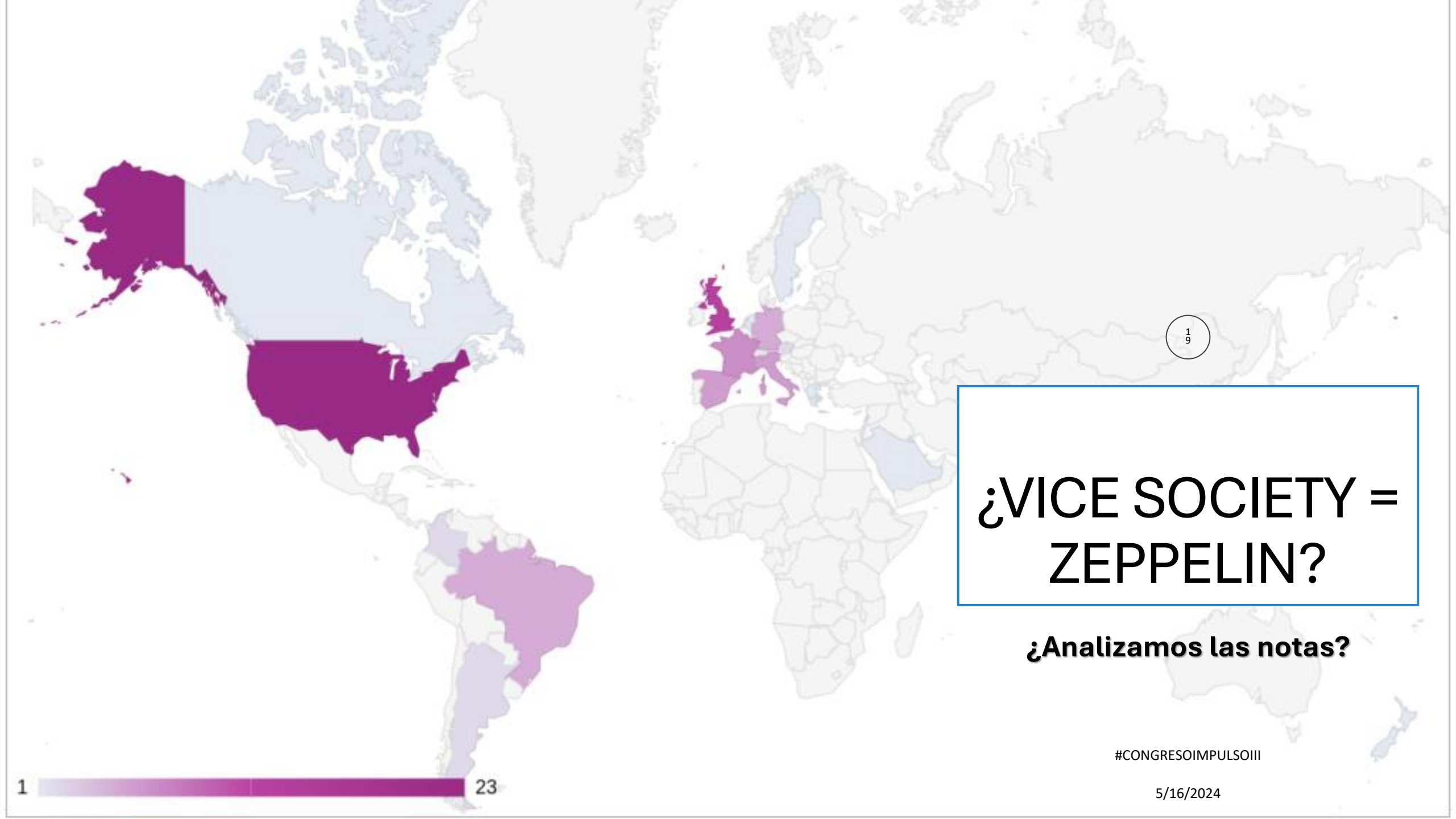
TYPE	VALUE
SHA1	a0ee0761602470e24bcea5f403e8d1e8bfa29832 3122ea585623531df2e860e7d0df0f25cce39b21 41dc0ba220f30c70aea019de214eccd650bc6f37 c9c2b6a5b930392b98f132f5395d54947391cb79
MD5	fb91e471cfa246beb9618e1689f1ae1d
IPV4	5.255.99[.]59 5.161.136[.]176 198.252.98[.]184 194.34.246[.]90
URL	hxxp[:]//vsociethok6sbprvevl4dlwbqrzyhxcxaqpvcqt5belwvsuxaxsutyad[.]onion
Email	v-society.official@onionmail[.]org ViceSociety@onionmail[.]org

Fuente: https://www.hivepro.com/wp-content/uploads/2022/09/Vice-Society-actors-target-K-12-institutions-in-US_TA2022194.pdf

5.161.136.176

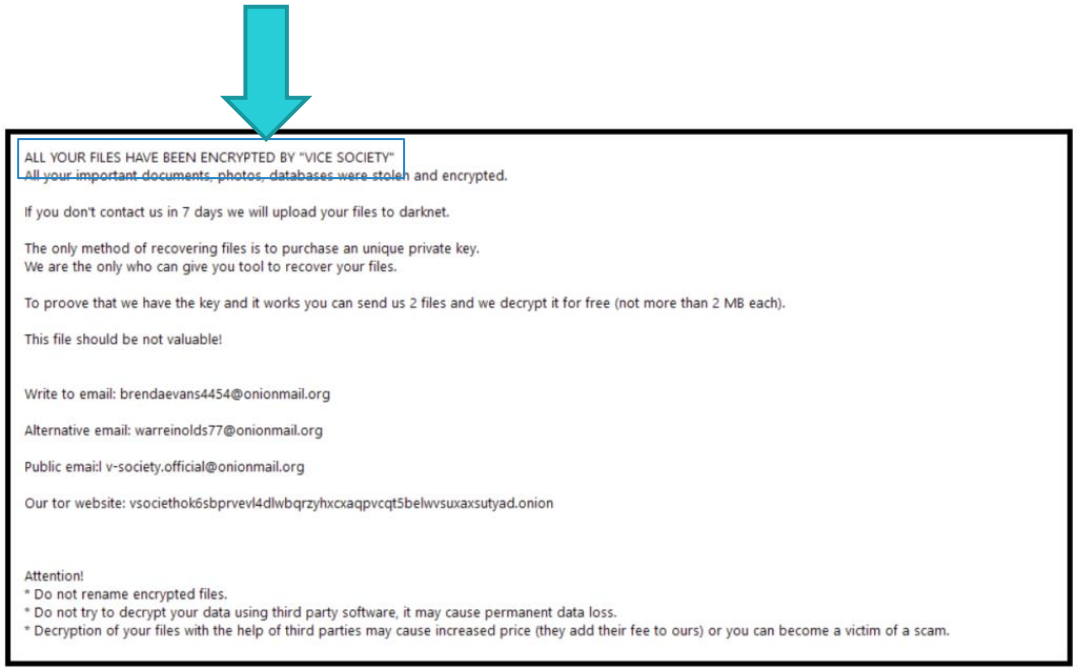


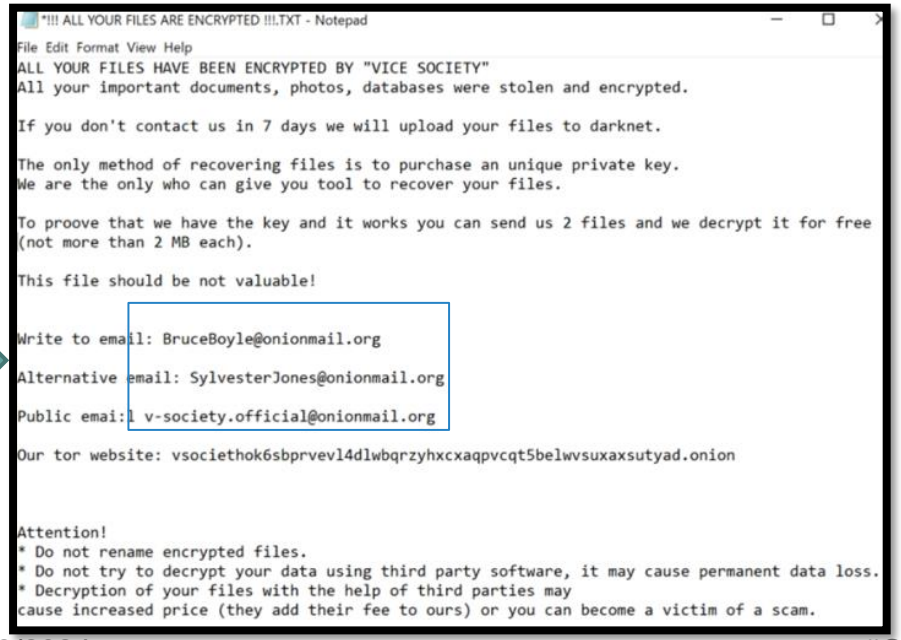


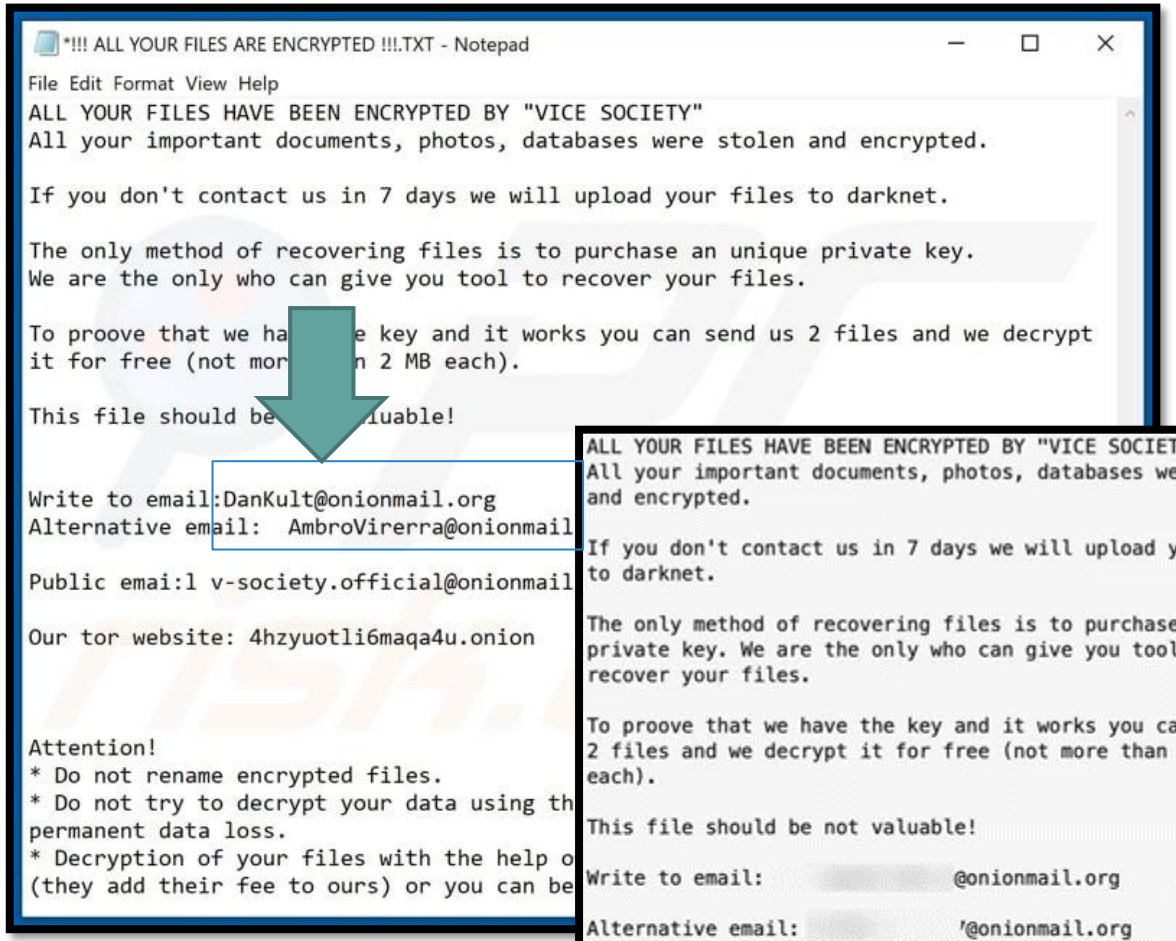


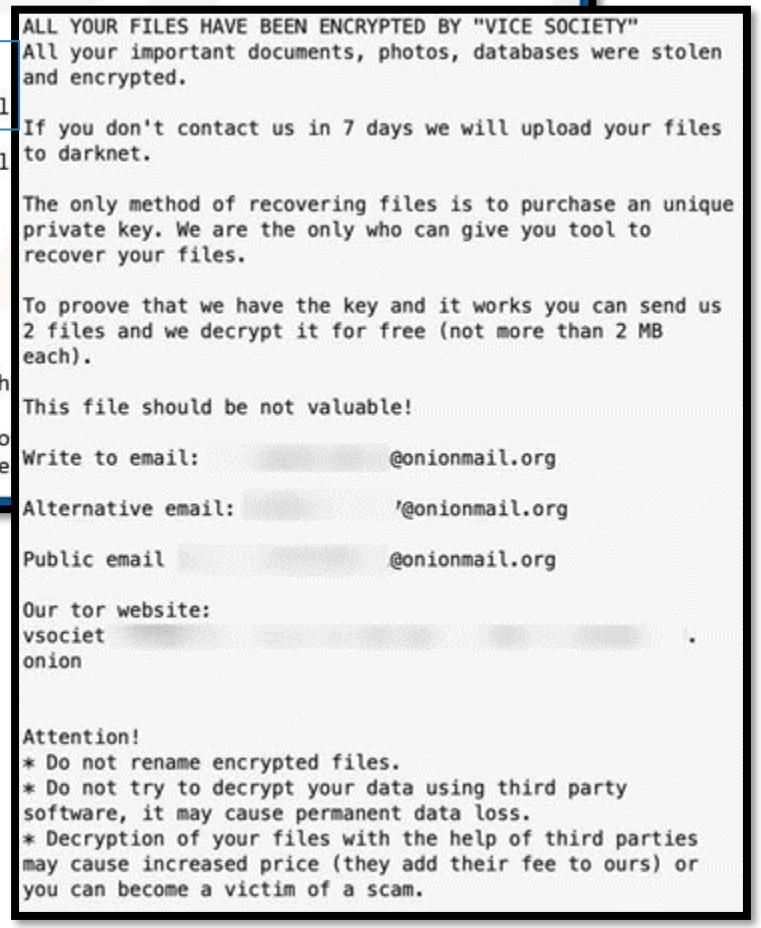
¿VICE SOCIETY = ZEPPELIN?

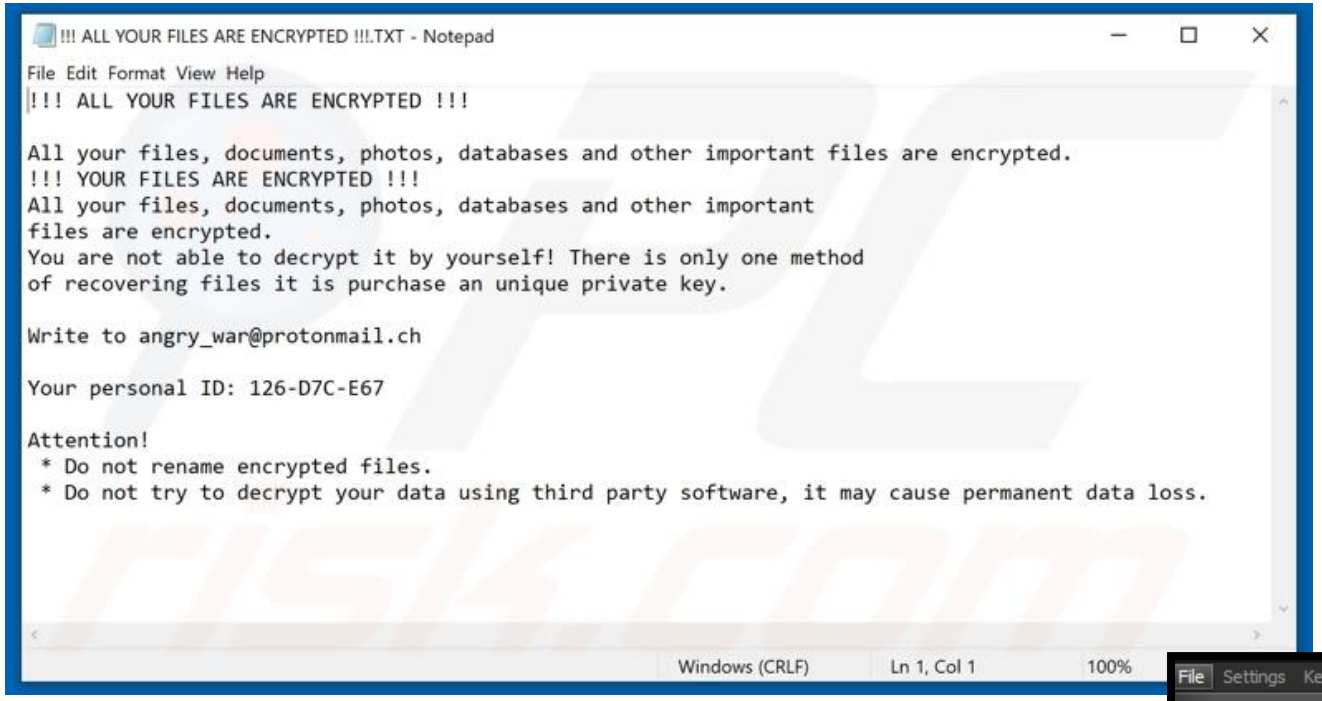
¿Analizamos las notas?

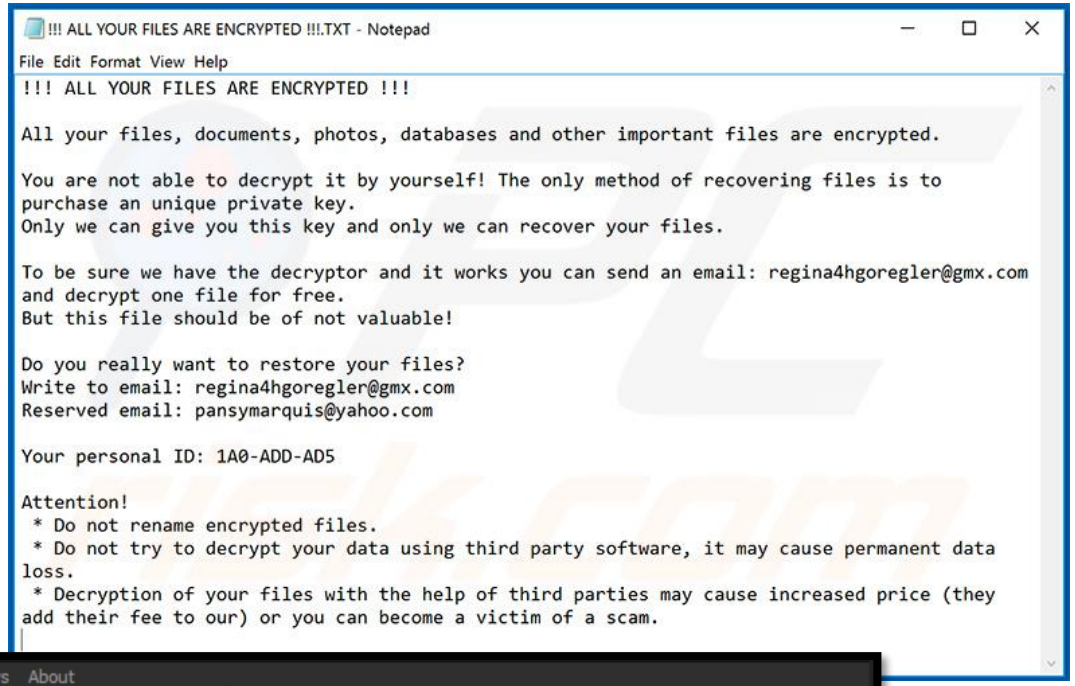

ALL YOUR FILES HAVE BEEN ENCRYPTED BY "VICE SOCIETY"
All your important documents, photos, databases were stolen and encrypted.
If you don't contact us in 7 days we will upload your files to darknet.
The only method of recovering files is to purchase an unique private key.
We are the only who can give you tool to recover your files.
To proove that we have the key and it works you can send us 2 files and we decrypt it for free (not more than 2 MB each).
This file should be not valuable!
Write to email: brendaevans4454@onionmail.org
Alternative email: warreinolds77@onionmail.org
Public email: v-society.official@onionmail.org
Our tor website: vsociethok6sbprvevl4dlwbqrzyhxcxaqpvcqt5belwvsuxaxsutyad.onion
Attention!
* Do not rename encrypted files.
* Do not try to decrypt your data using third party software, it may cause permanent data loss.
* Decryption of your files with the help of third parties may cause increased price (they add their fee to ours) or you can become a victim of a scam.

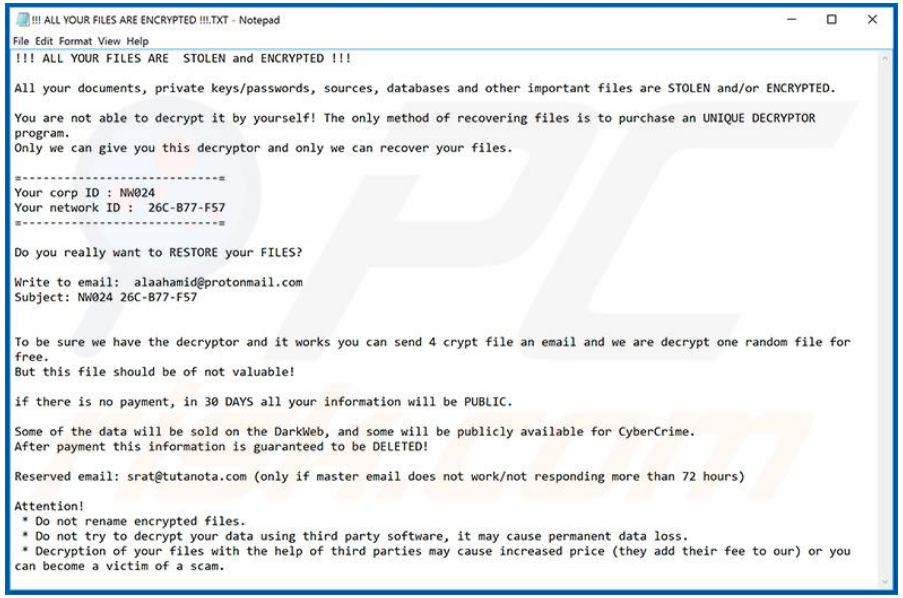

*!!! ALL YOUR FILES ARE ENCRYPTED !!!.TXT - Notepad
File Edit Format View Help
ALL YOUR FILES HAVE BEEN ENCRYPTED BY "VICE SOCIETY"
All your important documents, photos, databases were stolen and encrypted.
If you don't contact us in 7 days we will upload your files to darknet.
The only method of recovering files is to purchase an unique private key.
We are the only who can give you tool to recover your files.
To proove that we have the key and it works you can send us 2 files and we decrypt it for free (not more than 2 MB each).
This file should be not valuable!
Write to email: BruceBoyle@onionmail.org
Alternative email: SylvesterJones@onionmail.org
Public email: v-society.official@onionmail.org
Our tor website: vsociethok6sbprvevl4dlwbqrzyhxcxaqpvcqt5belwvsuxaxsutyad.onion
Attention!
* Do not rename encrypted files.
* Do not try to decrypt your data using third party software, it may cause permanent data loss.
* Decryption of your files with the help of third parties may
cause increased price (they add their fee to ours) or you can become a victim of a scam.

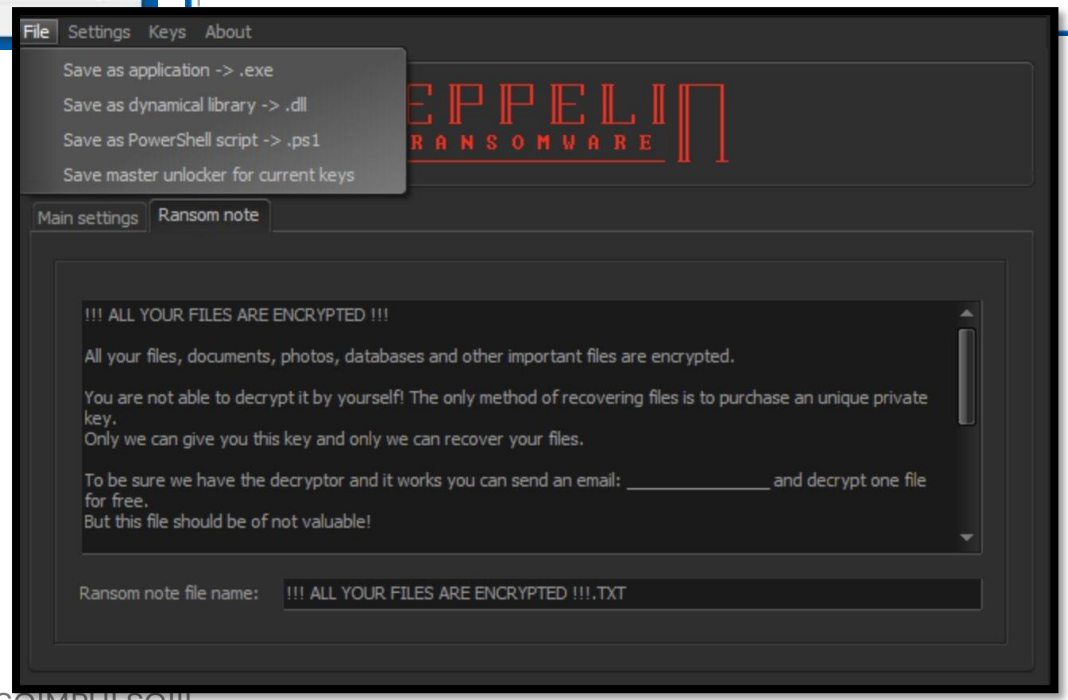

*!!! ALL YOUR FILES ARE ENCRYPTED !!!.TXT - Notepad
File Edit Format View Help
ALL YOUR FILES HAVE BEEN ENCRYPTED BY "VICE SOCIETY"
All your important documents, photos, databases were stolen and encrypted.
If you don't contact us in 7 days we will upload your files to darknet.
The only method of recovering files is to purchase an unique private key.
We are the only who can give you tool to recover your files.
To proove that we ha e key and it works you can send us 2 files and we decrypt it for free (not mor n 2 MB each).
This file should be uable!
Write to email:DanKult@onionmail.org
Alternative email: AmbroVirerra@onionmail
Public emai:l v-society.official@onionmail
Our tor website: 4hzyuotli6maqa4u.onion
Attention!
* Do not rename encrypted files.
* Do not try to decrypt your data using th
permanent data loss.
* Decryption of your files with the help o
(they add their fee to ours) or you can be


ALL YOUR FILES HAVE BEEN ENCRYPTED BY "VICE SOCIETY"
All your important documents, photos, databases were stolen and encrypted.
If you don't contact us in 7 days we will upload your files to darknet.
The only method of recovering files is to purchase an unique private key. We are the only who can give you tool to recover your files.
To proove that we have the key and it works you can send us 2 files and we decrypt it for free (not more than 2 MB each).
This file should be not valuable!
Write to email: @onionmail.org
Alternative email: '@onionmail.org
Public email @onionmail.org
Our tor website:
vsociet .
onion
Attention!
* Do not rename encrypted files.
* Do not try to decrypt your data using third party software, it may cause permanent data loss.
* Decryption of your files with the help of third parties may cause increased price (they add their fee to ours) or you can become a victim of a scam.


!!! ALL YOUR FILES ARE ENCRYPTED !!!.TXT - Notepad
File Edit Format View Help
!!! ALL YOUR FILES ARE ENCRYPTED !!!
All your files, documents, photos, databases and other important files are encrypted.
!!! YOUR FILES ARE ENCRYPTED !!!
All your files, documents, photos, databases and other important
files are encrypted.
You are not able to decrypt it by yourself! There is only one method
of recovering files it is purchase an unique private key.
Write to angry_war@protonmail.ch
Your personal ID: 126-D7C-E67
Attention!
* Do not rename encrypted files.
* Do not try to decrypt your data using third party software, it may cause permanent data loss.
Windows (CRLF)
Ln 1, Col 1
100%


!!! ALL YOUR FILES ARE ENCRYPTED !!!.TXT - Notepad
File Edit Format View Help
!!! ALL YOUR FILES ARE ENCRYPTED !!!
All your files, documents, photos, databases and other important files are encrypted.
You are not able to decrypt it by yourself! The only method of recovering files is to purchase an unique private key.
Only we can give you this key and only we can recover your files.
To be sure we have the decryptor and it works you can send an email: regina4hgoregler@gmx.com and decrypt one file for free.
But this file should be of not valuable!
Do you really want to restore your files?
Write to email: regina4hgoregler@gmx.com
Reserved email: pansymarquis@yahoo.com
Your personal ID: 1A0-ADD-AD5
Attention!
* Do not rename encrypted files.
* Do not try to decrypt your data using third party software, it may cause permanent data loss.
* Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.


!!! ALL YOUR FILES ARE ENCRYPTED !!!.TXT - Notepad
File Edit Format View Help
!!! ALL YOUR FILES ARE STOLEN and ENCRYPTED !!!
All your documents, private keys/passwords, sources, databases and other important files are STOLEN and/or ENCRYPTED.
You are not able to decrypt it by yourself! The only method of recovering files is to purchase an UNIQUE DECRYPTOR program.
Only we can give you this decryptor and only we can recover your files.
Your corp ID : NW024
Your network ID : 26C-B77-F57
Do you really want to RESTORE your FILES?
Write to email: alaahamid@protonmail.com
Subject: NW024 26C-B77-F57
To be sure we have the decryptor and it works you can send 4 crypt file an email and we are decrypt one random file for free.
But this file should be of not valuable!
if there is no payment, in 30 DAYS all your information will be PUBLIC.
Some of the data will be sold on the DarkWeb, and some will be publicly available for CyberCrime.
After payment this information is guaranteed to be DELETED!
Reserved email: srat@tutanota.com (only if master email does not work/not responding more than 72 hours)
Attention!
* Do not rename encrypted files.
* Do not try to decrypt your data using third party software, it may cause permanent data loss.
* Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.


File Settings Keys About
Save as application -> .exe
Save as dynamical library -> .dll
Save as PowerShell script -> .ps1
Save master unlocker for current keys
EPPELIN
RANSOMWARE
Main settings
Ransom note
!!! ALL YOUR FILES ARE ENCRYPTED !!!
All your files, documents, photos, databases and other important files are encrypted.
You are not able to decrypt it by yourself! The only method of recovering files is to purchase an unique private key.
Only we can give you this key and only we can recover your files.
To be sure we have the decryptor and it works you can send an email: _____ and decrypt one file for free.
But this file should be of not valuable!
Ransom note file name: !!! ALL YOUR FILES ARE ENCRYPTED !!!.TXT

Entrevistas

Sergiu Gatlan

Lawrence Abrams

Bill Toulas

Fuente: https://www.bleepingcomputer.com/tag/vice-society/

"Why not?

They always keep our private data open. You, me and anyone else go to hospitals, give them our passports, share our health problems etc. and they don't even try to protect our data. They have billions of government money. Do they steal that money?

USA president gave big amount to protect government networks and where is their protection? Where is our protection?

If IT department don't want to do their job we will do ours and we don't care if it hospital or university." - Vice Society ransomware.

de: **Thomas** [redacted] <[redacted]@onionmail.org>
para: Mauro [redacted]
fecha: 13 mar 2022, 19:56
asunto: Re: Re: Interview / Proposal
enviado por: onionmail.org
firmado por: onionmail.org
seguridad: Encriptación estándar (TLS) Más información
: Este es importante principalmente porque frecuentemente lees mensajes con esta etiqueta.

Mi interlocutor es Thomas, líder de Vice Society.

- ¿Cómo te decidiste a formar un grupo de ransomware? ¿Cómo nació Vice Society?

Por un grupo de amigos que estaban interesados en pentesting. Decidimos probar suerte.

- Argentina se caracteriza por ser una víctima fácil y también por ser un mal pagador (Caso REvil, Everest). ¿Por qué los eligieron? ¿Fue a propósito?

[Encriptar] al gobierno de cualquier país es un logro y además, siempre tienen documentos interesantes. Tardamos 6 horas para obtener acceso a cada pieza de infraestructura crítica y alrededor de 6 horas más para atacar. Seguro te acordarás que su página web estuvo caída más de 1 semana a mediados de enero.

- ¿Argentina intentó negociar o contactarlos? Si es así, ¿hicieron una oferta?

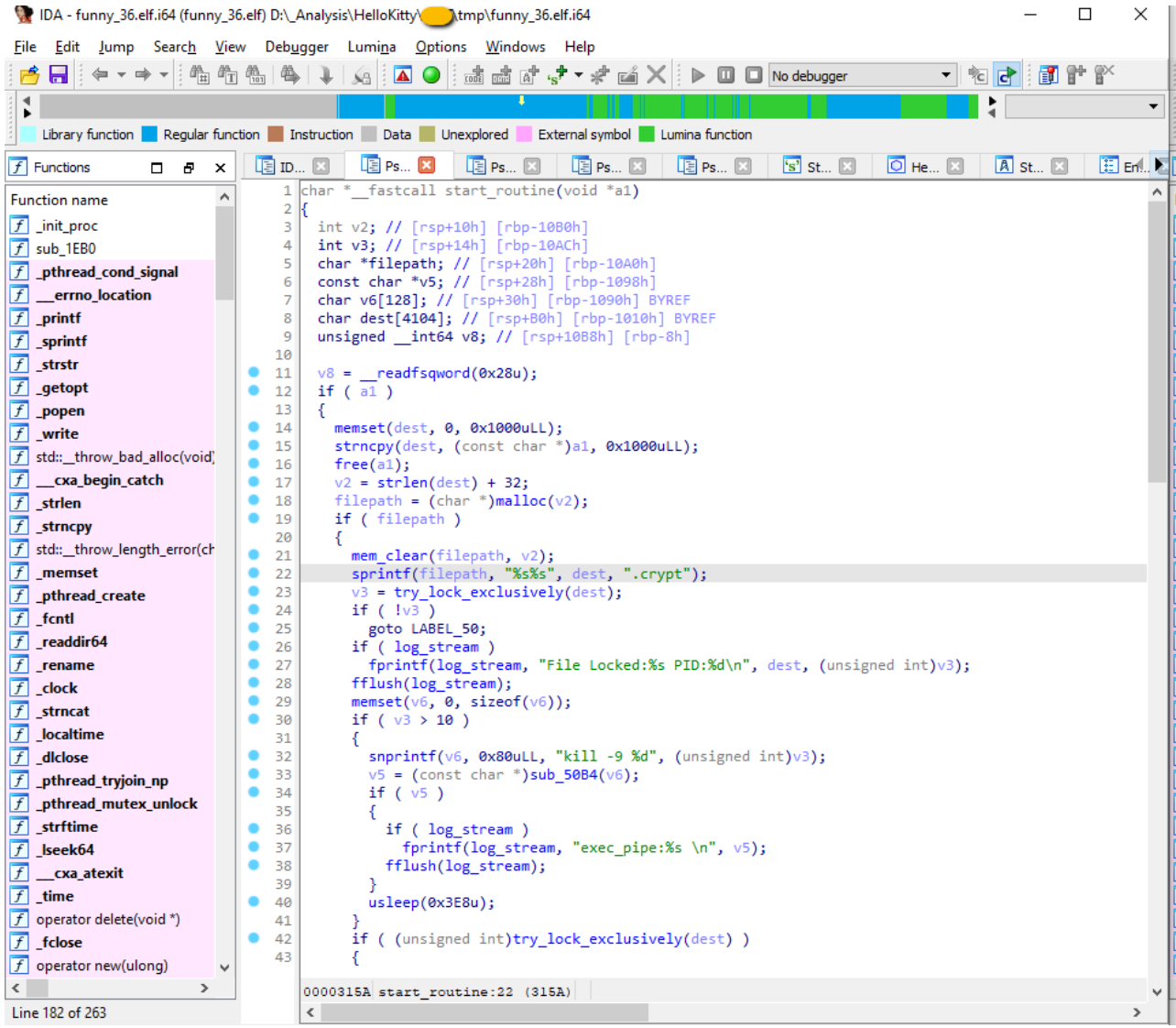
Hablamos con algunas organizaciones de Argentina en otras circunstancias pero no recordamos si pagaron.

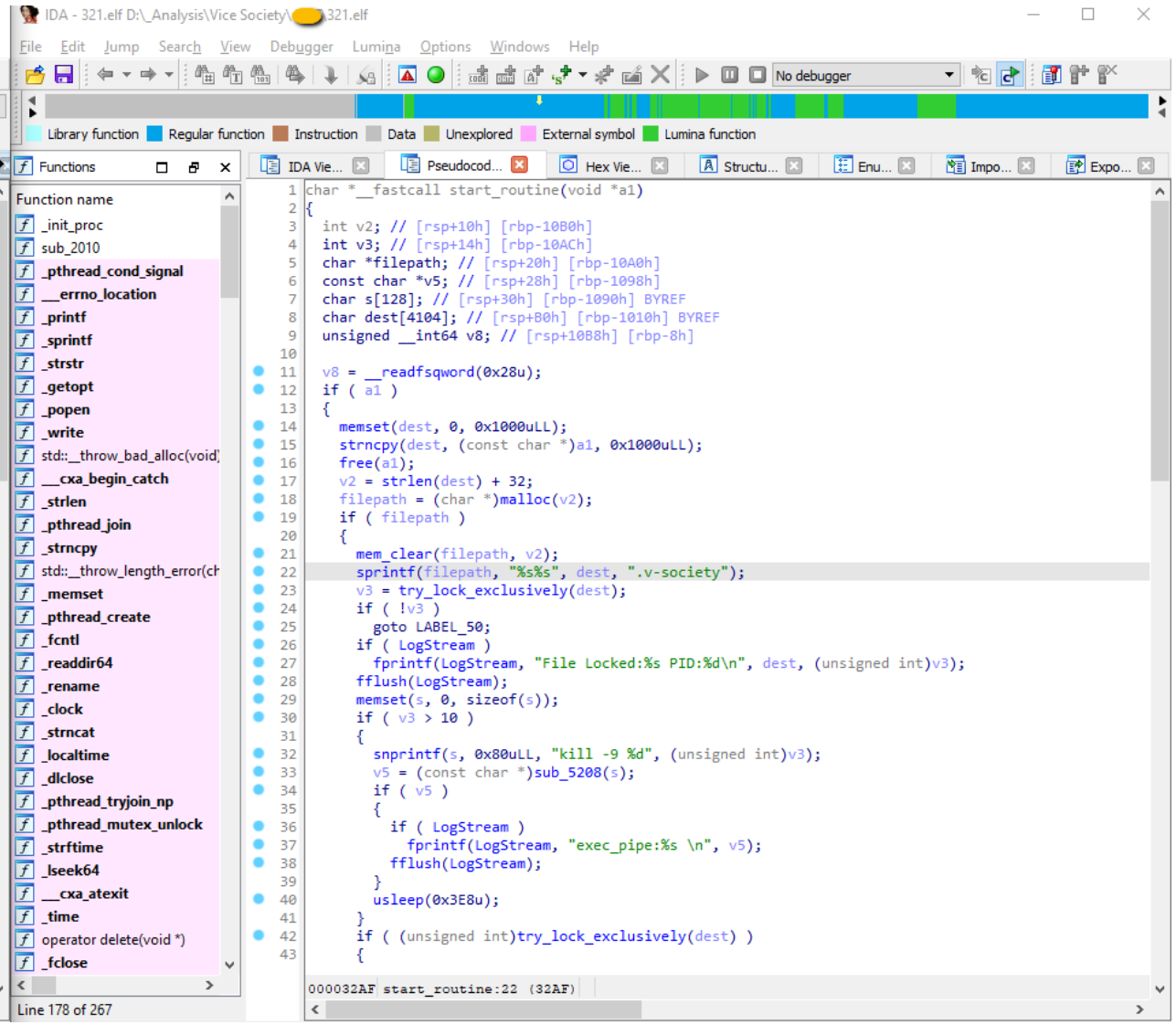
- Su lista de víctimas es bastante variada, pero esta es la segunda vez que listan una organización latinoamericana. ¿Cómo fue su experiencia? ¿Las organizaciones de LATAM suelen pagar o simplemente asumen la pérdida?

No es la segunda :), es la segunda que no pagó. Y sí, algunos de ellos pagan.

- ¿Qué planes futuros tiene Vice Society? ¿Planean continuar operando contra infraestructura argentina o latinoamericana en general?

¡Seguro! ¿Por qué no? Amamos lo que hacemos, y no lo hacemos solo por el dinero.


IDA - funny_36.elf.i64 (funny_36.elf) D:_Analysis\HelloKitty\tmp\funny_36.elf.i64
File Edit Jump Search View Debugger Lumina Options Windows Help
No debugger
Library function Regular function Instruction Data Unexplored External symbol Lumina function
Functions
Function name
_init_proc
sub_1EB0
_pthread_cond_signal
__errno_location
_printf
_sprintf
_strstr
_getopt
_popen
_write
std::__throw_bad_alloc(void)
__cxa_begin_catch
_strlen
_strncpy
std::__throw_length_error(ch
_memset
_pthread_create
_fcntl
_readdir64
_rename
_clock
_strncat
_localtime
_dlclose
_pthread_tryjoin_np
_pthread_mutex_unlock
_strftime
_lseek64
__cxa_atexit
_time
operator delete(void *)
_fclose
operator new(ulong)
Line 182 of 263
char *__fastcall start_routine(void *a1)
{
int v2; // [rsp+10h] [rbp-10B0h]
int v3; // [rsp+14h] [rbp-10ACh]
char *filepath; // [rsp+20h] [rbp-10A0h]
const char *v5; // [rsp+28h] [rbp-1098h]
char v6[128]; // [rsp+30h] [rbp-1090h] BYREF
char dest[4104]; // [rsp+B0h] [rbp-1010h] BYREF
unsigned __int64 v8; // [rsp+10B8h] [rbp-8h]
v8 = __readfsqword(0x28u);
if (a1)
{
memset(dest, 0, 0x1000uLL);
strncpy(dest, (const char *)a1, 0x1000uLL);
free(a1);
v2 = strlen(dest) + 32;
filepath = (char *)malloc(v2);
if (filepath)
{
mem_clear(filepath, v2);
sprintf(filepath, "%s%s", dest, ".crypt");
v3 = try_lock_exclusively(dest);
if (!v3)
goto LABEL_50;
if (log_stream)
fprintf(log_stream, "File Locked:%s PID:%d\n", dest, (unsigned int)v3);
fflush(log_stream);
memset(v6, 0, sizeof(v6));
if (v3 > 10)
{
snprintf(v6, 0x80uLL, "kill -9 %d", (unsigned int)v3);
v5 = (const char *)sub_50B4(v6);
if (v5)
{
if (log_stream)
fprintf(log_stream, "exec_pipe:%s \n", v5);
fflush(log_stream);
}
usleep(0x3E8u);
}
if ((unsigned int)try_lock_exclusively(dest))
{
0000315A start_routine:22 (315A)


IDA - 321.elf D:_Analysis\Vice Society\321.elf
File Edit Jump Search View Debugger Lumina Options Windows Help
No debugger
Library function Regular function Instruction Data Unexplored External symbol Lumina function
Functions
Function name
_init_proc
sub_2010
_pthread_cond_signal
__errno_location
_printf
_sprintf
_strstr
_getopt
_popen
_write
std::__throw_bad_alloc(void)
__cxa_begin_catch
_strlen
_pthread_join
_strncpy
std::__throw_length_error(ch
_memset
_pthread_create
_fcntl
_readdir64
_rename
_clock
_strncat
_localtime
_dlclose
_pthread_tryjoin_np
_pthread_mutex_unlock
_strftime
_lseek64
__cxa_atexit
_time
operator delete(void *)
_fclose
Line 178 of 267
char *__fastcall start_routine(void *a1)
{
int v2; // [rsp+10h] [rbp-10B0h]
int v3; // [rsp+14h] [rbp-10ACh]
char *filepath; // [rsp+20h] [rbp-10A0h]
const char *v5; // [rsp+28h] [rbp-1098h]
char s[128]; // [rsp+30h] [rbp-1090h] BYREF
char dest[4104]; // [rsp+B0h] [rbp-1010h] BYREF
unsigned __int64 v8; // [rsp+10B8h] [rbp-8h]
v8 = __readfsqword(0x28u);
if (a1)
{
memset(dest, 0, 0x1000uLL);
strncpy(dest, (const char *)a1, 0x1000uLL);
free(a1);
v2 = strlen(dest) + 32;
filepath = (char *)malloc(v2);
if (filepath)
{
mem_clear(filepath, v2);
sprintf(filepath, "%s%s", dest, ".v-society");
v3 = try_lock_exclusively(dest);
if (!v3)
goto LABEL_50;
if (LogStream)
fprintf(LogStream, "File Locked:%s PID:%d\n", dest, (unsigned int)v3);
fflush(LogStream);
memset(s, 0, sizeof(s));
if (v3 > 10)
{
snprintf(s, 0x80uLL, "kill -9 %d", (unsigned int)v3);
v5 = (const char *)sub_5208(s);
if (v5)
{
if (LogStream)
fprintf(LogStream, "exec_pipe:%s \n", v5);
fflush(LogStream);
}
usleep(0x3E8u);
}
if ((unsigned int)try_lock_exclusively(dest))
{
000032AF start_routine:22 (32AF)

Zeppelin code

Depending on the options set during the building process, it will either check the machine's default language and default country calling code or use an online service to obtain the victim's external IP address:

```
.text:0042D7D3 check_user_lang:                        ; CODE XREF: malware_main+404↑j
.text:0042D7D3                 call    GetUserDefaultLangID
.text:0042D7D8                 movzx   eax, ax
.text:0042D7DB                 mov     ds:default_lang, eax
.text:0042D7E0                 cmp     ds:default_lang, 422h ; LANG_UKRAINIAN
.text:0042D7EA                 jz      short exit
.text:0042D7EC                 cmp     ds:default_lang, 423h ; LANG_BELARUSIAN
.text:0042D7F6                 jz      short exit
.text:0042D7F8                 cmp     ds:default_lang, 419h ; LANG_RUSSIAN
.text:0042D802                 jz      short exit
.text:0042D804                 cmp     ds:default_lang, 43Fh ; LANG_KAZAK
.text:0042D80E                 jnz     short check_country_code
.text:0042D810
.text:0042D810 exit:                                   ; CODE XREF: malware_main+4B6↑j
.text:0042D810                                         ; malware_main+4C2↑j ...
.text:0042D810                 push    0               ; uExitCode
.text:0042D812                 call    ExitProcess_0
.text:0042D817 ; ---------------------------------------------------------------------------
.text:0042D817
.text:0042D817 check_country_code:                     ; CODE XREF: malware_main+4DA↑j
.text:0042D817                 lea     edx, [ebp+System::AnsiString]
.text:0042D81A                 mov     eax, LOCALE_ICOUNTRY ; LCType
.text:0042D81F                 call    get_locale_info
.text:0042D824                 mov     eax, [ebp+System::AnsiString] ; System::AnsiString
.text:0042D827                 call    @Sysutils@StrToInt$qqrx17System@AnsiString ; Sysutils::St
.text:0042D82C                 mov     ds:default_lang, eax
.text:0042D831                 cmp     ds:default_lang, 7 ; CTRY_RUSSIA || CTRY_KAZAKSTAN
.text:0042D838                 jz      short exit_
.text:0042D83A                 cmp     ds:default_lang, 375 ; CTRY_BELARUS
.text:0042D844                 jz      short exit_
.text:0042D846                 cmp     ds:default_lang, 380 ; CTRY_UKRAINE
.text:0042D850                 jnz     short continue
.text:0042D852
.text:0042D852 exit_:                                  ; CODE XREF: malware_main+504↑j
```

RESUMEN

1. **VICE SOCIETY** tiene un logotipo imitando a **Vice City**. Otros nombres que han usado también lo mencionan: **Vice Spider**
2. Encontramos documentos de CISA pero no lo relacionan al grupo con Rusia
3. En Hispasec hablan de que el origen es VEGA y este es el antecesor de Zeppelin
4. En un medio que ha entrevistado e investigado al grupo mencionan que tienen dos ramas: **Zeppelin y HelloKitty/FiveHands**
5. **BlackBerry** en un informe expone partes del código donde se puede ver que Zeppelin filtra por países y no actúa en Rusia, Ucrania, Bielorrusia y Kazakstan
6. El FBI tiene una intrusión por HelloKitty y el FBI los ubica en Ucrania
7. Encontramos muchos parecidos en las notas entre Zeppelin y Vice Society
8. En las entrevistas se les ve formas de hablar de personas norte americanas
9. Inicialmente ninguna prueba que indiquen que trabajen regularmente para el gobierno ruso

cias

El Confidencial

España Cotizalia Opinión Salud Internacional Cultura Teknautas Deportes ACyV Televisión Vanitatis

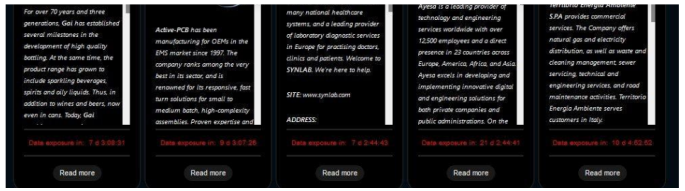
Tecnología

ABREN UNA INVESTIGACIÓN

Banco Santander sufre un ciberataque que afecta a datos de clientes en España

Además de a los clientes de España, Chile y Uruguay, el ataque también ha afectado a todos los empleados y a algunos exempleados del grupo

Logo del Banco Santander. (EFE/Luis Tejido)



Black Basta reivindica en la dark web el ataque a Ayesa y el robo de 4,5 TB en datos

El responsable de ciberseguridad de Ayesa ya confirmó en el Congreso Internacional de Cibercrimen que era esa organización la responsable

Conclusiones

¡GRACIAS!
¿PREGUNTAS?