PARA HACER BIEN EL AMOR CON UN **RAMSOMWARE** HAY QUE IR AL SU

JORGE CORONADO

QUANTIKA 14

C N FORENSE

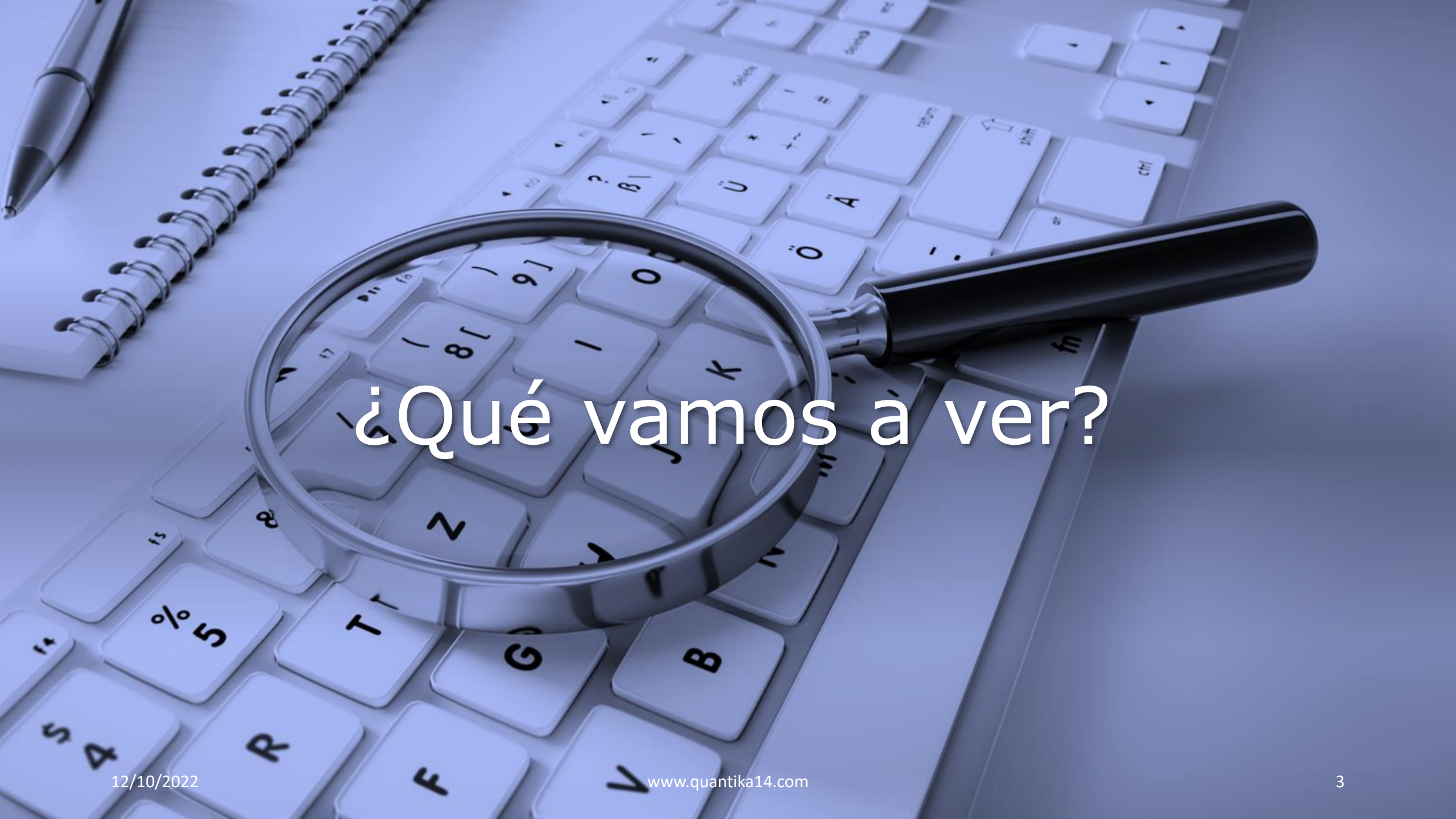
Sobre el autor

Sígueme: @jorgewebsec
https://www.linkedin.com/in/jorge-coronado-quantika14/

- CEO de QuantiKa14
- Director de ciberinteligencia
- Profesor de cosas
- Vocal de APTAN
- Coordinador de la secretaría de investigación de criptomonedas y hacking en AIVC
- Creador de Dante's Gates, Guasap Forensic, Twiana, etc (https://github.com/Quantika14/)

APTAN

ASOCIACIÓN INTERNACIONAL VÍCTIMAS DEL FRAUDE DIGITAL Y CIBERESTAFA



¿Qué vamos a ver?

2022

- **Costa Rica** paralizada por el grupo Conti
- **LAPSUS$** ataca a Nvidea, Ubisoft, Samsung y Microsft. Son detenidos y en septiembre vuelven a atacar a Uber y Rockstar Game
- Guerra de **Ucrania y Rusia**
- **Conti** apoya a Rusia y publican los chats (ContiLeaks)
- **CSIC** y otras grandes entidades españolas atacadas

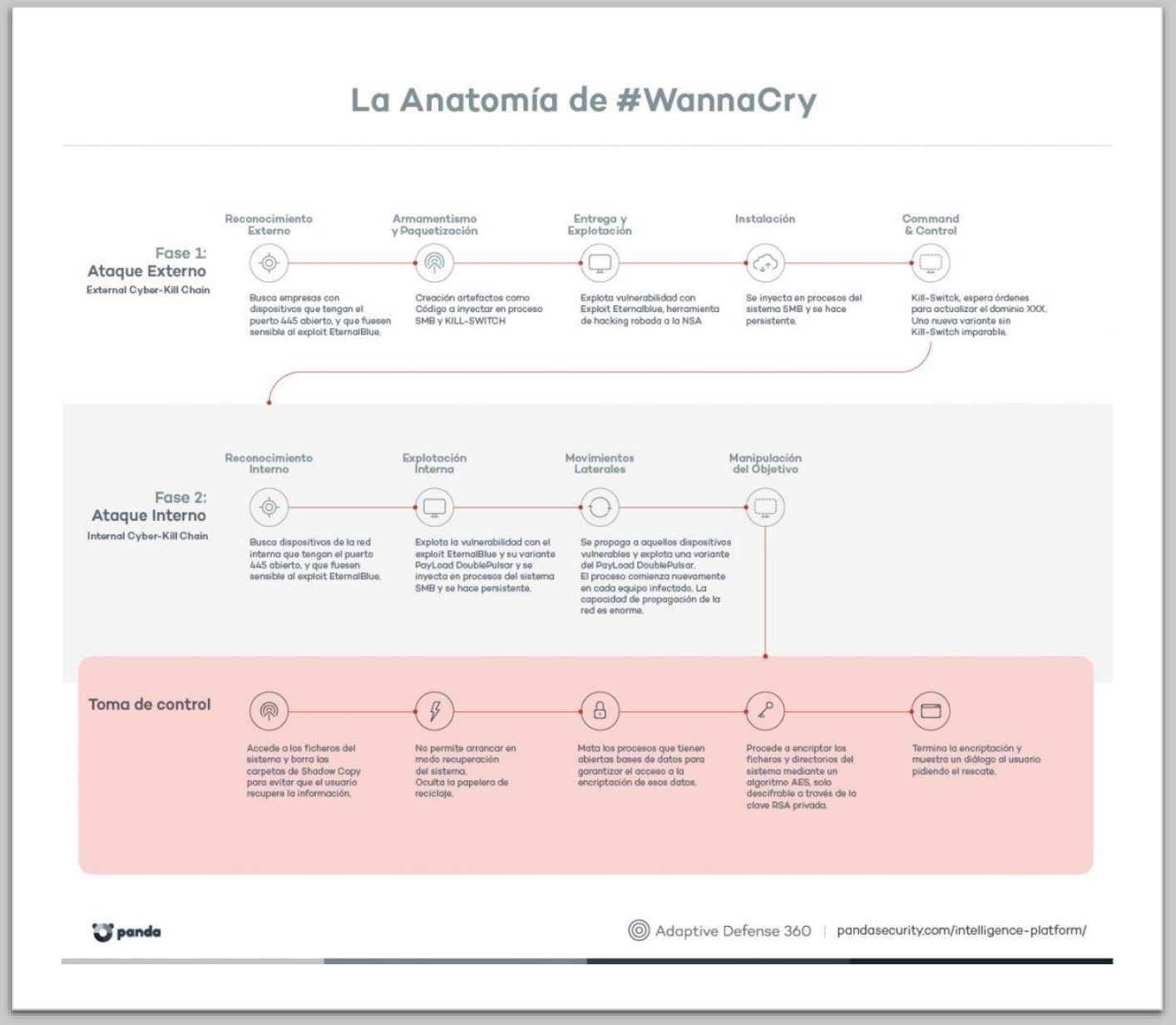
¿En qué puede ayudar una investigación OSINT contra el ransomware?

Forensic + OSINT

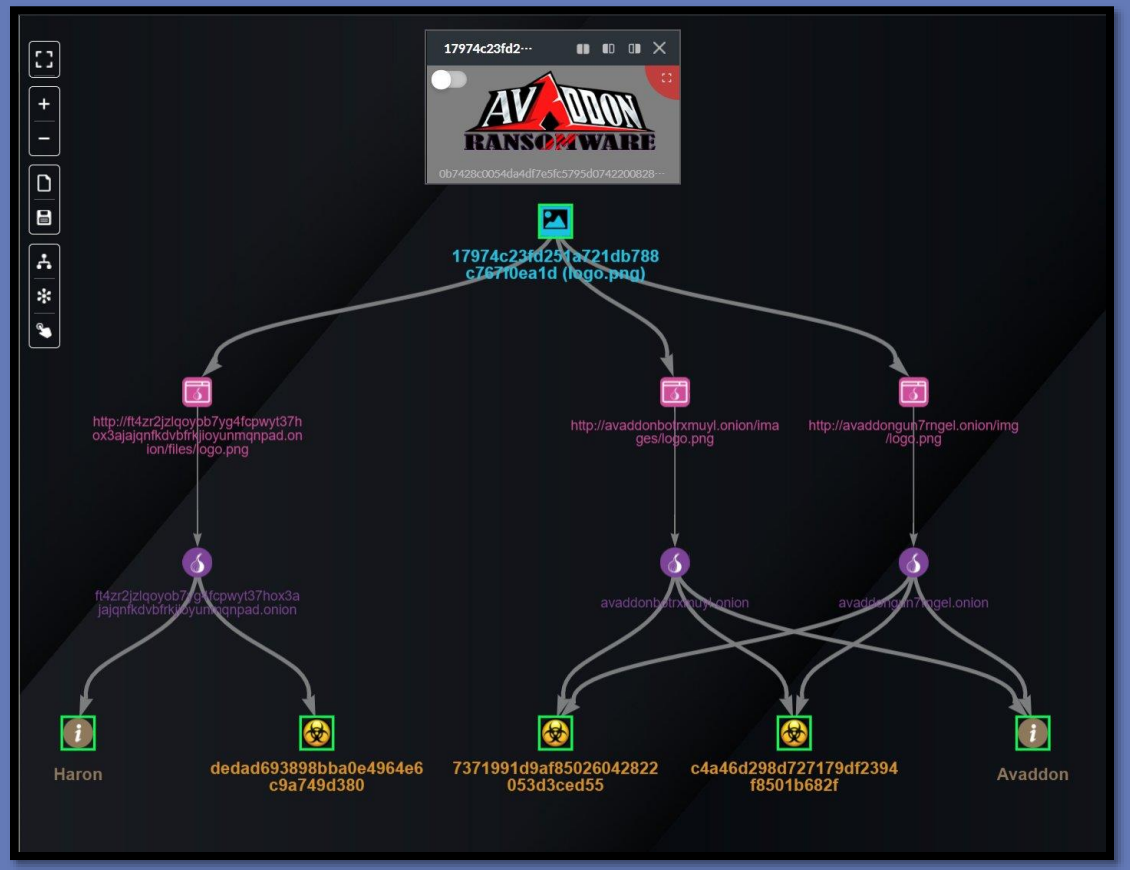
1.1 Conceptos.: Cyber Kill Chain

- La cadena de asesinato cibernético (CKC) es una forma de exponer las etapas que realizan los ataques informáticos con el objetivo de saber qué medidas implementar a nivel de ciberseguridad.

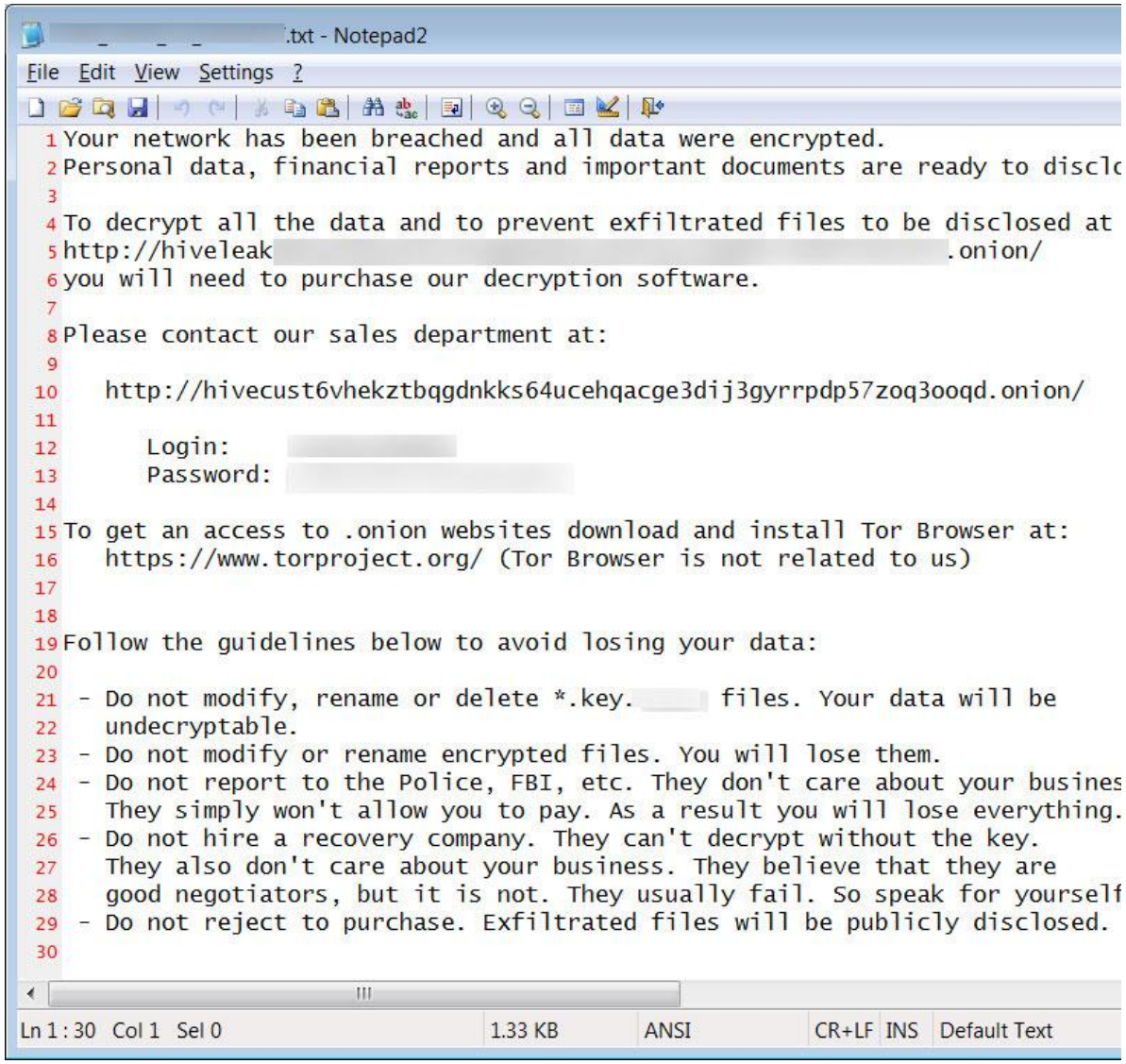
- Podemos decir que CKC es un modelo que está compuesto por diferentes Técnicas, Tácticas y Procedimientos (TTPs).



1.2 Indicadores de compromiso (IOCs)



- IPs de CCs
- Nota
  - Urls
  - Wallets
  - TOX
- URLs
- Aplicaciones
  - Netscan
  - Mimikatz
  - etc
- Emails y adjuntos
- Extensiones
- Ficheros que crea
- Claves de registros

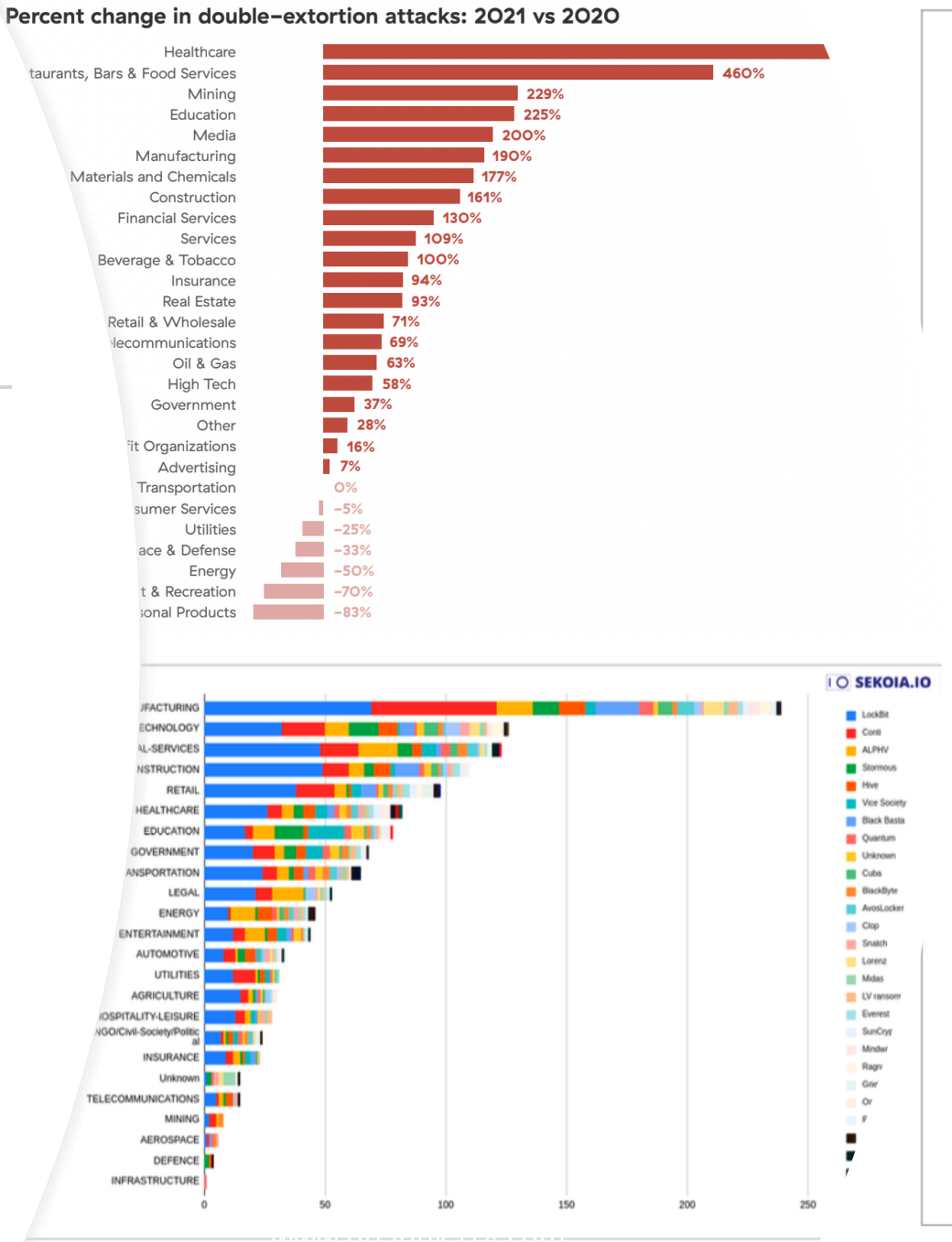


1.3 Atención a la víctima (cliente)

- **TOX:** es un protocolo p2p de mensajería instantánea y videollamadas con cifrado de extremo a extremo
- **EMAIL:** protonmail, onion, etc
- **Login + contact form**

1.4 Sus víctimas

- Tipos de víctimas
- La ubicación de las víctimas



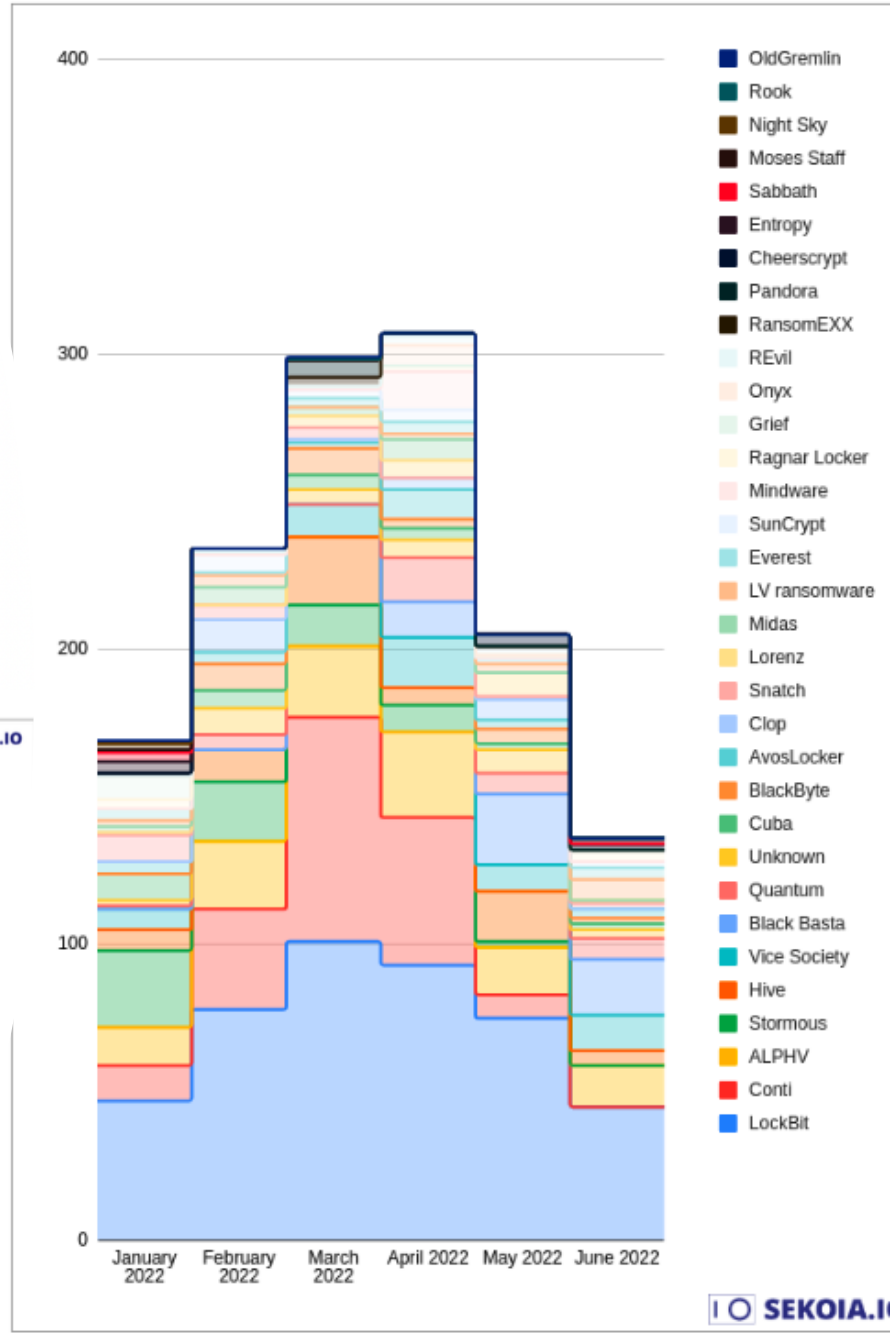
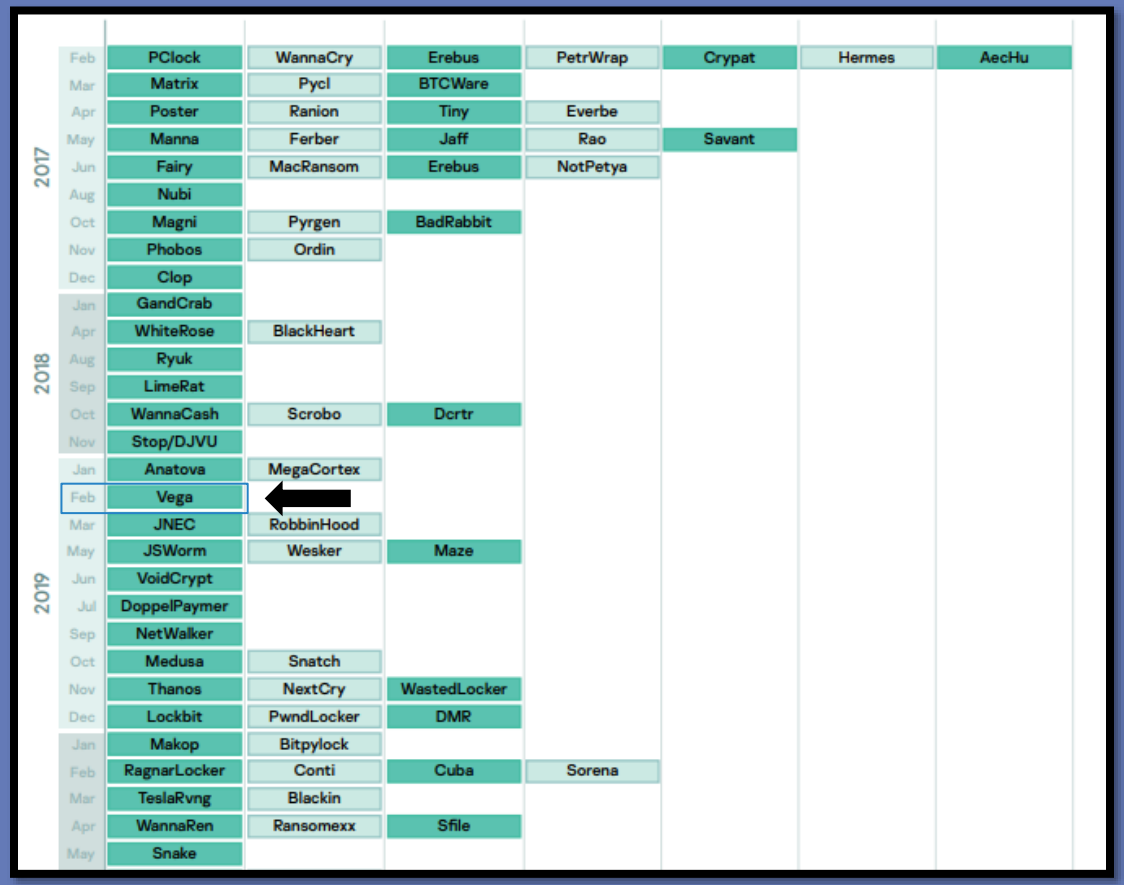
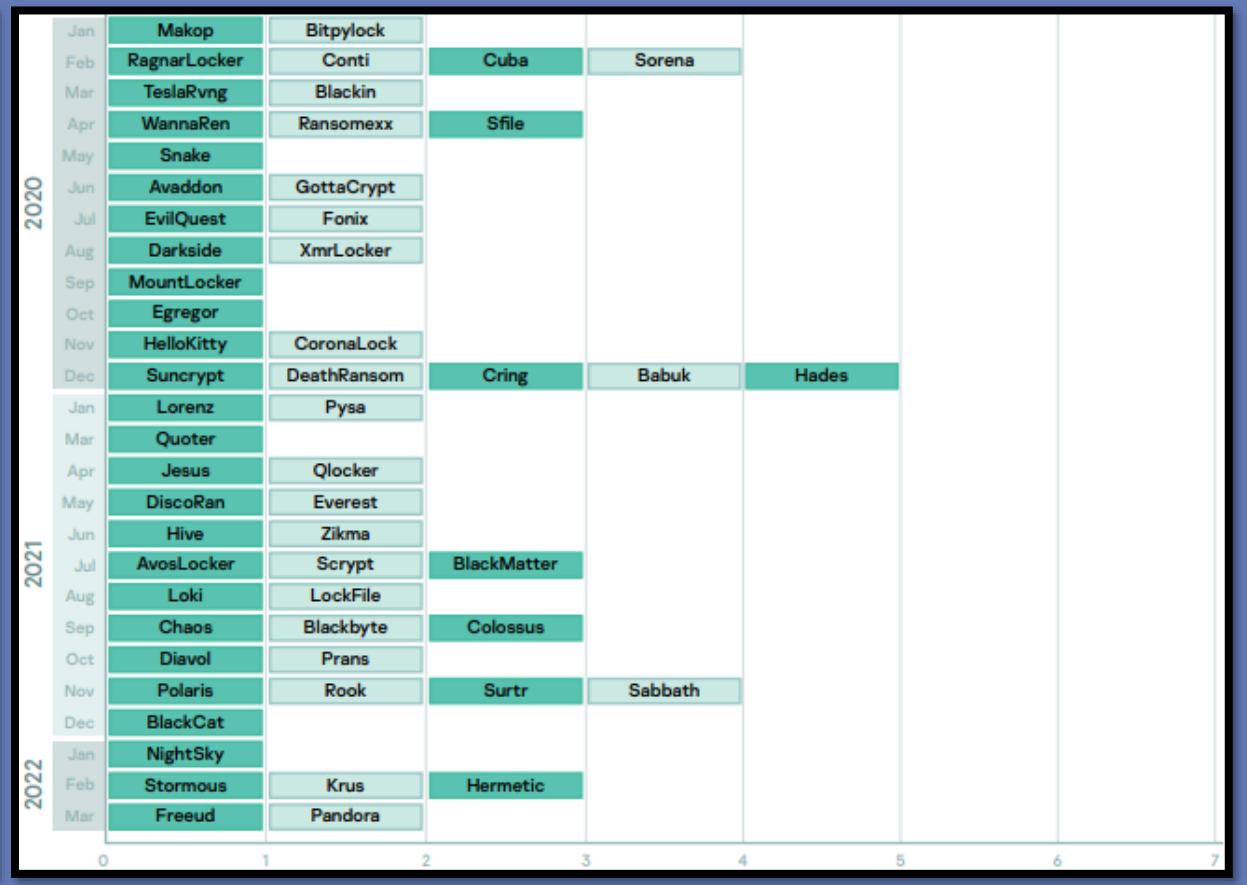


Figure 3. Industries most impacted by ransomware groups in S1 20 igure 2. Publicly disclosed ransomware attacks by threat group in

1.5. Familias y grupos





Fuente: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/06/23093553/Common-TTPs-of-the-modern-ransomware_low-res.pdf

¿Cómo podemos estar actualizados?

2. Monitorización

- https://github.com/fastfire/deepdarkCTI/blob/main/ransomware_gang.md
- https://ransomwatch.telemetry.ltd/#/INDEX
- https://www.ransomlook.io/
- https://raw.githubusercontent.com/fastfire/deepdarkCTI/main/ransomware_gang.md
- https://twitter.com/RansomwareNews

Group Name	Onion V.	Link
Arvin Club	v3	Open
Babuk	v3	Open
Black Basta	v3	Open
AlphaVM/BlackCat	v3	Open
BlackByte	v3	Open
Bl4ckt0r	v3	Open
CL0P	v3	Open
CONTI	v3	Open
CRYP70N1C0D3	v3	Open
Cuba	v3	Open
Everest	v3	Open
Grief	v3	Open
Hive	v3	Open
HolyGhost	v3	Open
Karakurt	v3	Open | DEEP-WEB
KelvinSecurity		DEEP-WEB
LockBit 2.0	v3	Open
LockData Auction	v3	Open
Lorenz	v3	Open
LV BLOG	v3	Open | Open
Medusa	v3	Open
Midas	v3	Open
Moses Staff	v2	Open | DEEP-WEB
Pandora	v3	Open
Pay2Key	v3	Open
Quantum	v3	Open
Ragnar_Locker	v3	Open
RAMP	v3	Open
Ransom Cartel	v3	Open
Ransom House	v3	Open
RansomEXX	v3	Open
REvil	v3	Open
Snatch	v3	Open
Stormous	v3	Open
Onyx	v3	Open
Vice Society	v3	Open
x001xs	v3	Open

2.1 Crear tu propio data set

- https://github.com/Quantika14/osint-suite-tools

	Target	Onion 1	Onion 2	TOX	Email 1	Email 2	XMPP	Web	Telegram	Víctimas	V-Spain	Twitter	Idioma	País
2	AvosLocker	http://avosqxh72b5ia23dl5fgwcpndkctuzqvh2iefk5imp3pi5gfhel5klad.onion	None	9A751AC90A5F020	avos@onionmail.org	None	avos@strong	None	None	41	1	None	Inglés	None
3	Babuk	http://nq4zyac4ukl4tykmidbzgdlvaboqeqsemkp4t35bzvjeve6zm2lqcjid.onion	None	None	None	None	None	None	None	6	0	None	Inglés	None
4	BI@cktor	http://bl4cktorpms2gybrcyt52aakcxt6yn37byb65uama5cimhifcscnqkid.onion	None	None	None	None	None	None	None	5	0	None	Inglés	None
5	Clop Leaks	http://santat7kpllt6iyvqbr7q4amdv6dzrh6paatvyrzl7ry3zm72zigf4ad.onion	ekbgzchl6x2ias37.onion	None	unlock@support-mult.com	unlock@rsv-b	None	None	None	70	0	None	Inglés	Rusia
6	HiveLeak	http://hiveleakdbtnp76ulyhi52eag6c6tyc3xw7ez7iqy6wc34gd2nekazyd.onion	hivecust6vhekztbqgdnkks64ucehqacge3dij3gyrrpdp57zoq3ooqd.onion	None	Web form	None	None	None	None	166	0	None	Inglés	None
7	Lockbit 3.0	http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion	http://lockbitapt2d73krlbewgv27tquljgxr33xbwwsp6rkyieto7u4ncead.onion/	3085B89A0C515D2	None	None	None	None	None	260	3	None	Inglés	Rusia
8	Lorenz	http://lorenzmlwpzgxq736jzseuterytjueszsvznuibanxomlpkyxk6ksoyd.onion	woe2suafeg6ehxivgvvn4nh6ectbdhdqgc4vzph27mmyn7rjf2c52jid.onion/index.	None	Web form	None	None	None	None	45	1	None	Inglés	None
9	Quantum	http://quantum445bh3gzuyilxdzs5xdepf3b7lkcupswvkryf3n7hgzpxebid.onion	22rnyep2aa2exx3fdm26p4onwjfmhciodb55v5l3w4iny7e5bxpg3yad.onion	None	None	None	None	None	None	53	0	None	Inglés	None
10	Ragnar_Locker	http://rgleaktxuey67yrgspmhvtnrqtgogur35lwdrup4d3igtbm3pupc4lyd.onion	None	None	None	None	None	None	None	81	None	None	None	None
11	Ransomexx	http://rnsm777cdsjrsdlbs4v5qoeppu3px6sb2igmh53jzrx7ipcrbjz5b2ad.onion	None	None	None	None	None	None	None	60	None	None	Inglés	None
12	Suncrypt	http://x2miyuiwpib2imjr5ykyjngdu7v6vprkkhiltrk4qafymtawey4qzwid.onion	None	None	None	None	None	None	None	20	None	None	Inglés	None
13	Vice Society	http://ssq4zimieeaanazkzc5ld4y5hdibi2nzwzdibfh5n5w4pw5mcik76lzyd.onion/	None	None	v-society.official@onionma	ViceSociety@	None	None	None	152	12	None	Inglés	None
14	Moses	http://mosesstaffm7hptp.onion/	None	None	contact@moses-staff.se	None	None	https://mose	@moses_sta	None	None	https://tw	Inglés	Israel
15	ARVIN CLUB	3kp6j22pz3zkv76yutctosa6djpj4yib2icvdqxucdaxxedumhqicpad.onion	None	D6164C90642CD9	None	None	None	None	https://t.me/	None	None	None	None	None
16	Stormous	http://ahb6hjhe4nomgfwxequu52hazigh4ty4gdcnrf3r7z5tiyhour5py2id.onion	None	None	stormouss@onionmail.org	None	None	None	https://t.me/	None	None	None	None	None
17	RansomHouse	http://zohlm7ahjwegcedoz7lrdrti7bvpofymcayotp744qhx6gjmxbuo2yid.onion/	None	None	None	None	None	None	https://t.me/	None	None	None	Inglés	None
18	Conti	None	None	None	None	None	None	None	None	None	None	None	None	Rusia

2.2 Analizamos con Dante’s Gates

- /buscar
- /buscaremail
- /buscarusername
- /buscarip
- /analizardominio

https://quantika14.com/dantes-gates-all-in-one-osint-telegram-bot/

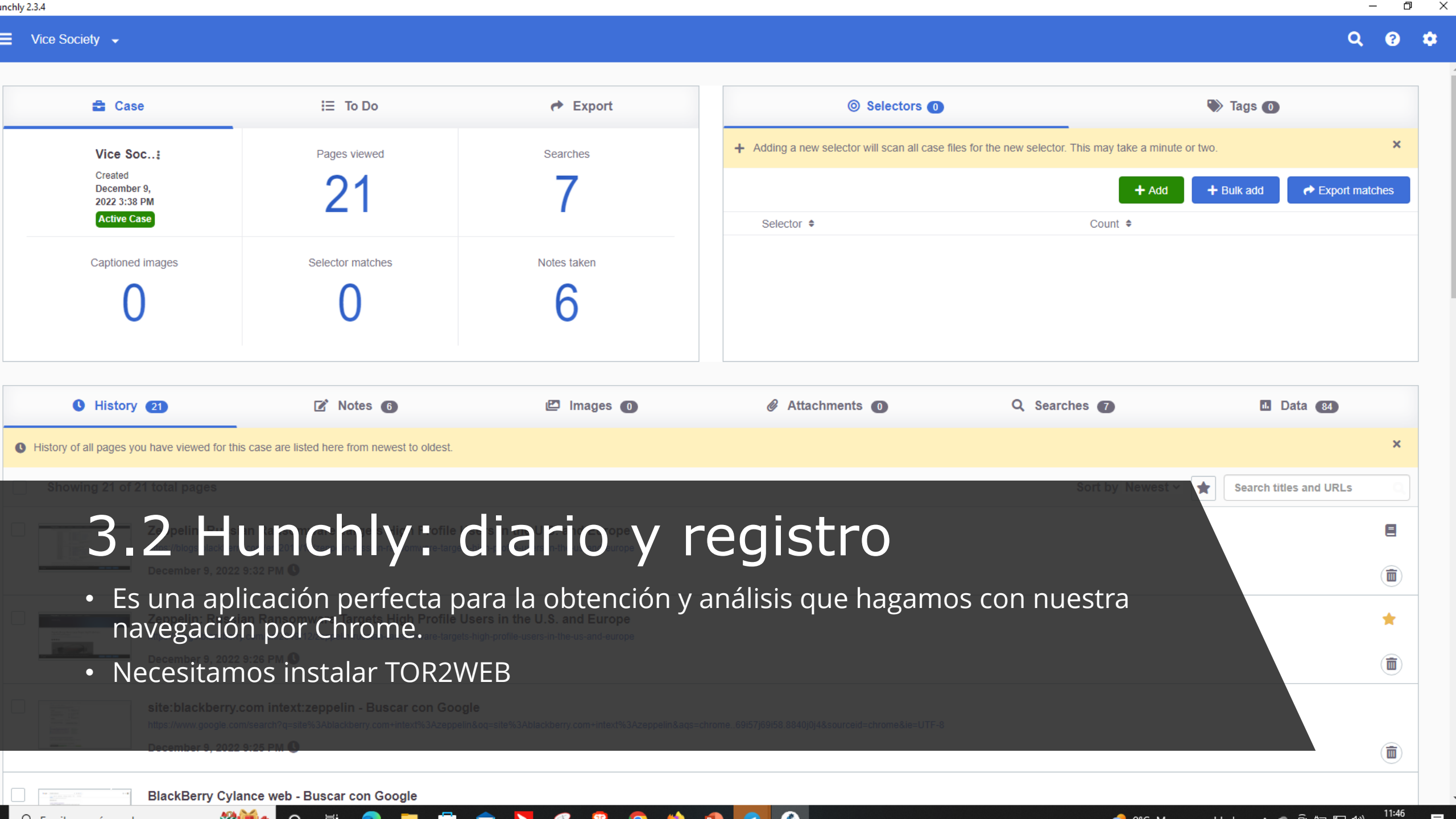
DANTE’S GATES

OSINT MADE IN SPAIN

WWW.QUANTIKA14.COM

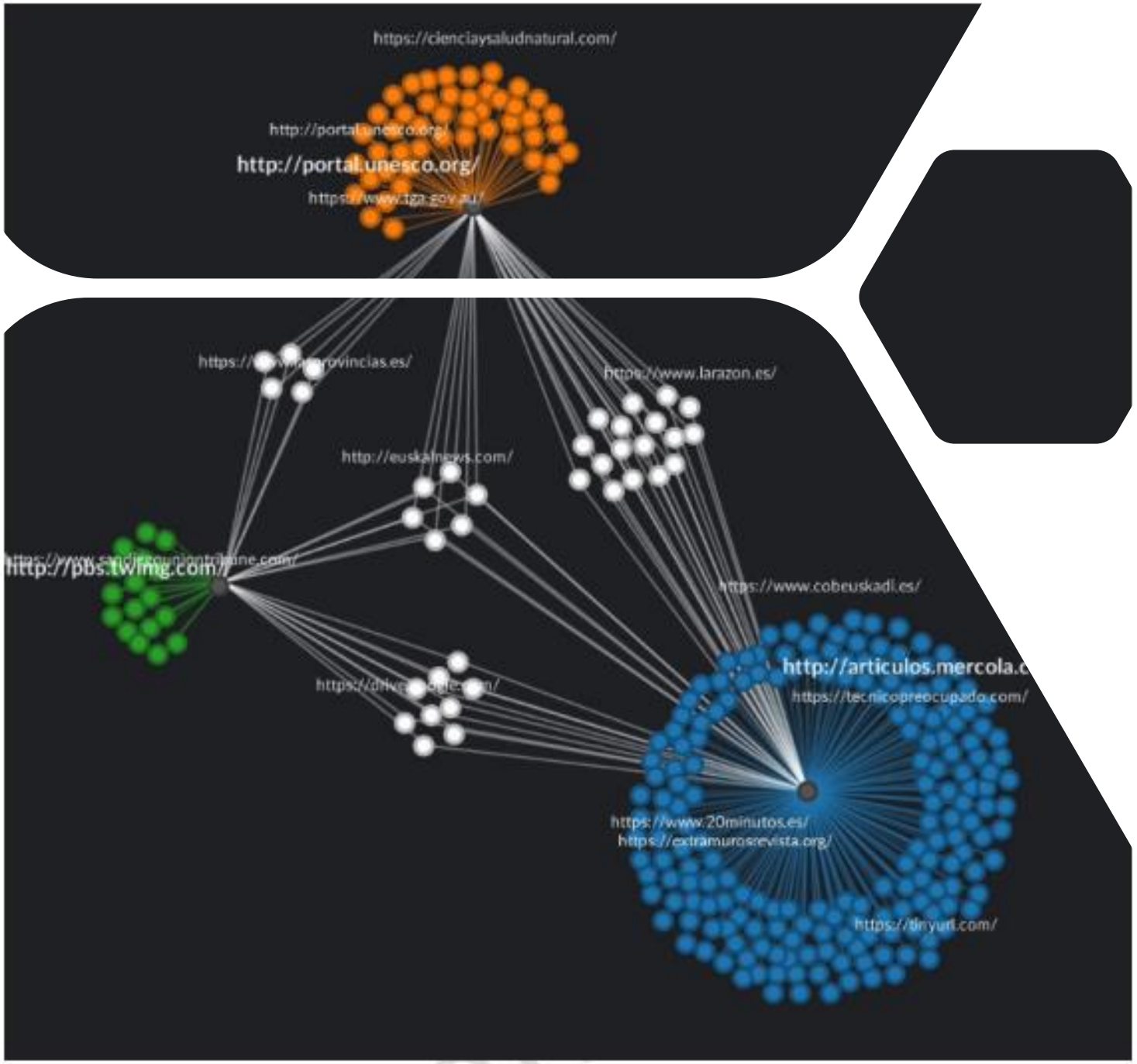
3.1 ¿Qué es NINT?

- Es una disciplina de inteligencia a través de la prensa online y escrita.
- A través de diferentes metodologías se obtiene, analiza y se evalua la información de la prensa con un objetivo concreto



3.2 Hunchly: diario y registro

- Es una aplicación perfecta para la obtención y análisis que hagamos con nuestra navegación por Chrome.
- Necesitamos instalar TOR2WEB



3.2 Análisis de Telegram

- JupyterLab
- Tableu
- Graphext
- Comando /buscar de Dante's Gates
- Descarga gratis el estudio:

https://quantika14.com/estudios-de-investigacion

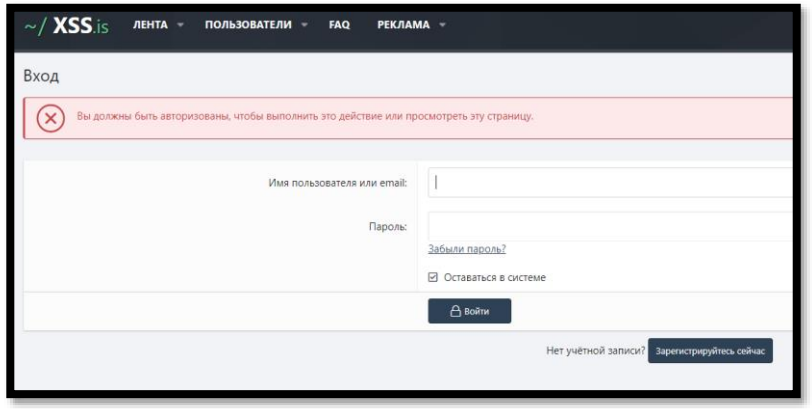
12/10/2022

3.3 Fallos (de ellos)

- Rastros de marcas o familias antiguas (emails, leaks, dominios, logs, etc)
- Redes sociales
- IoCs
  - Sobre todos las Ips a CCs
- Entrevistas
- Comunicaciones internas (https://github.com/ThePar mak/conti-leaks-englished)

4. Vice Society

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



4.1 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.**"

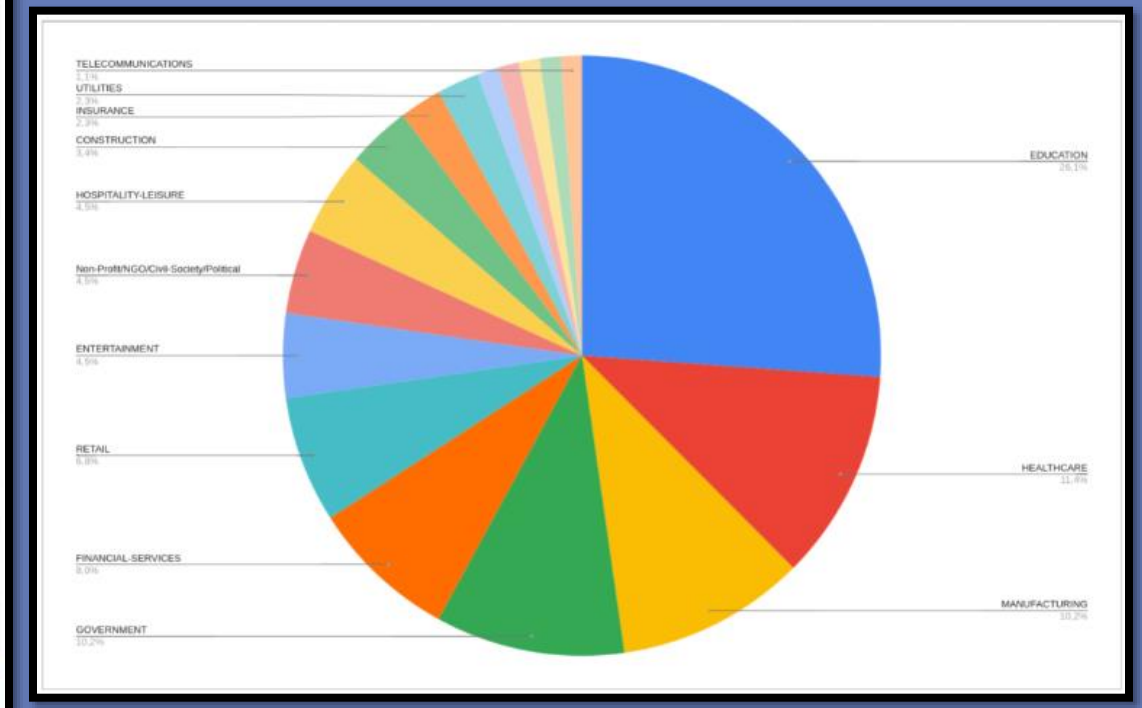
https://therecord.media/the-fbi-believes-the-hellokitty-ransomware-gang-operates-out-of-ukraine

4.2 Analizamos el logo

4.3 Analizamos sus víctimas

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



4.4 IoCs

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}

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*.*

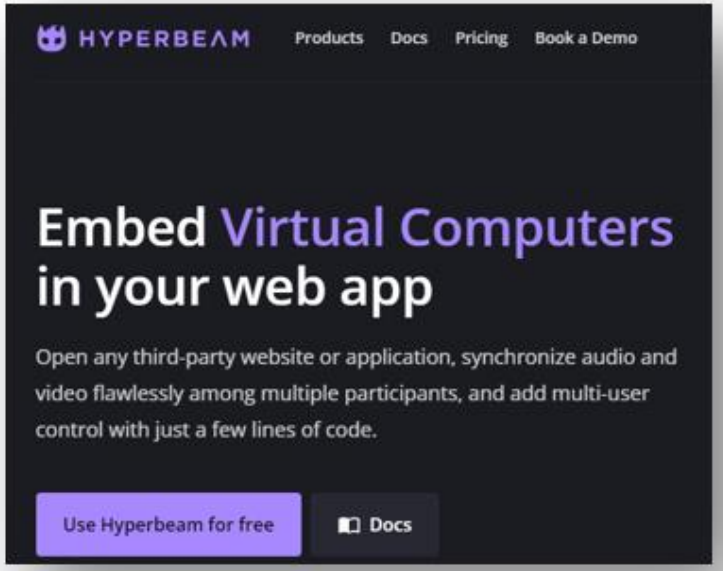
Fuente: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6690-ccn-cert-id-09-22-vice-society-neshta-1/file.html

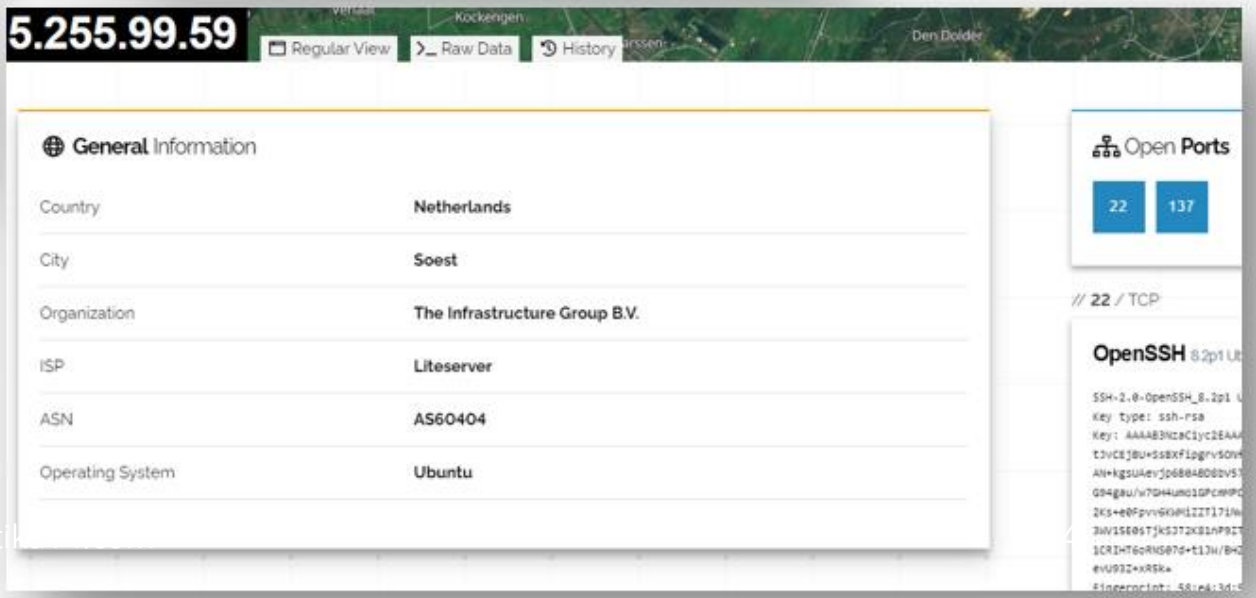
IOCs

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

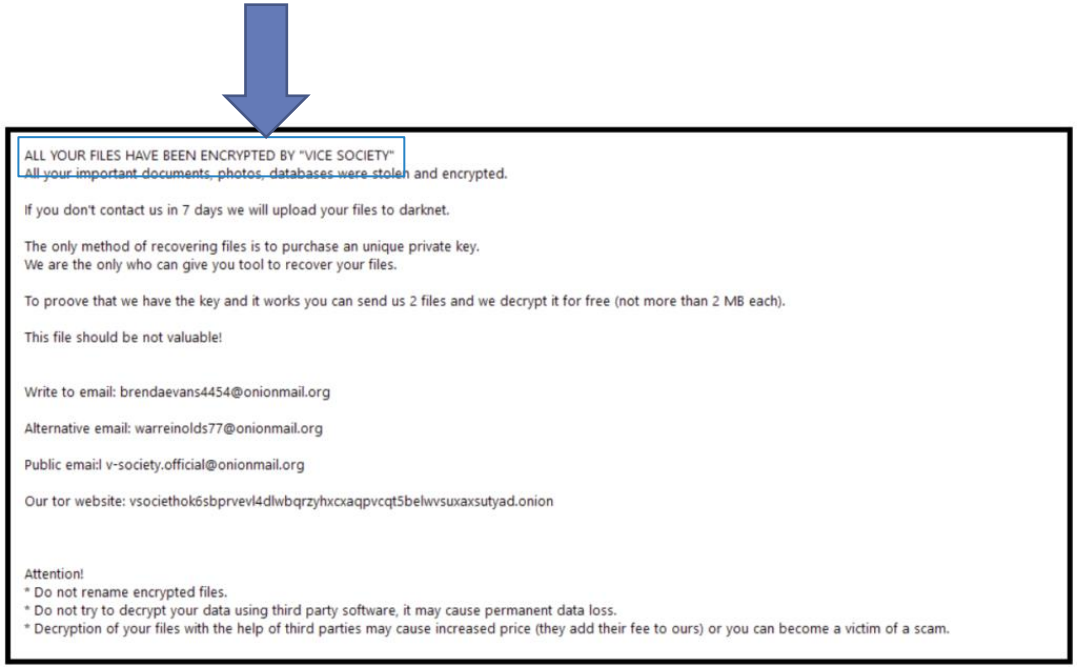
5.161.136.176





¿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!

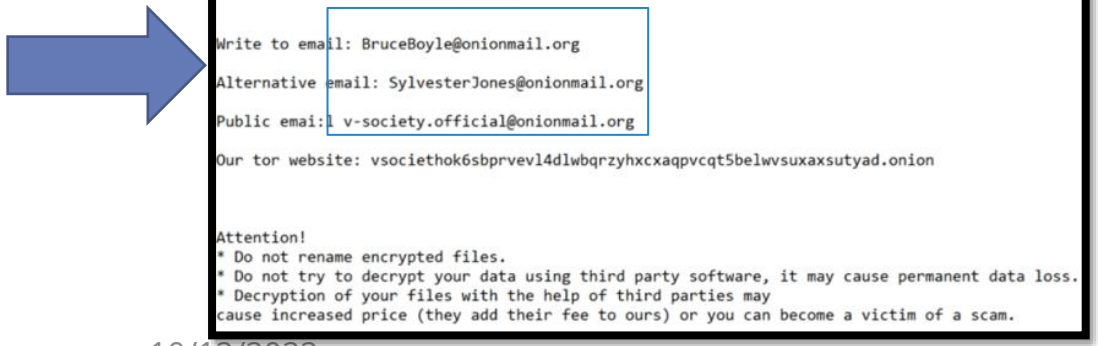
Write to email: brendaevans4454@onionmail.org

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!

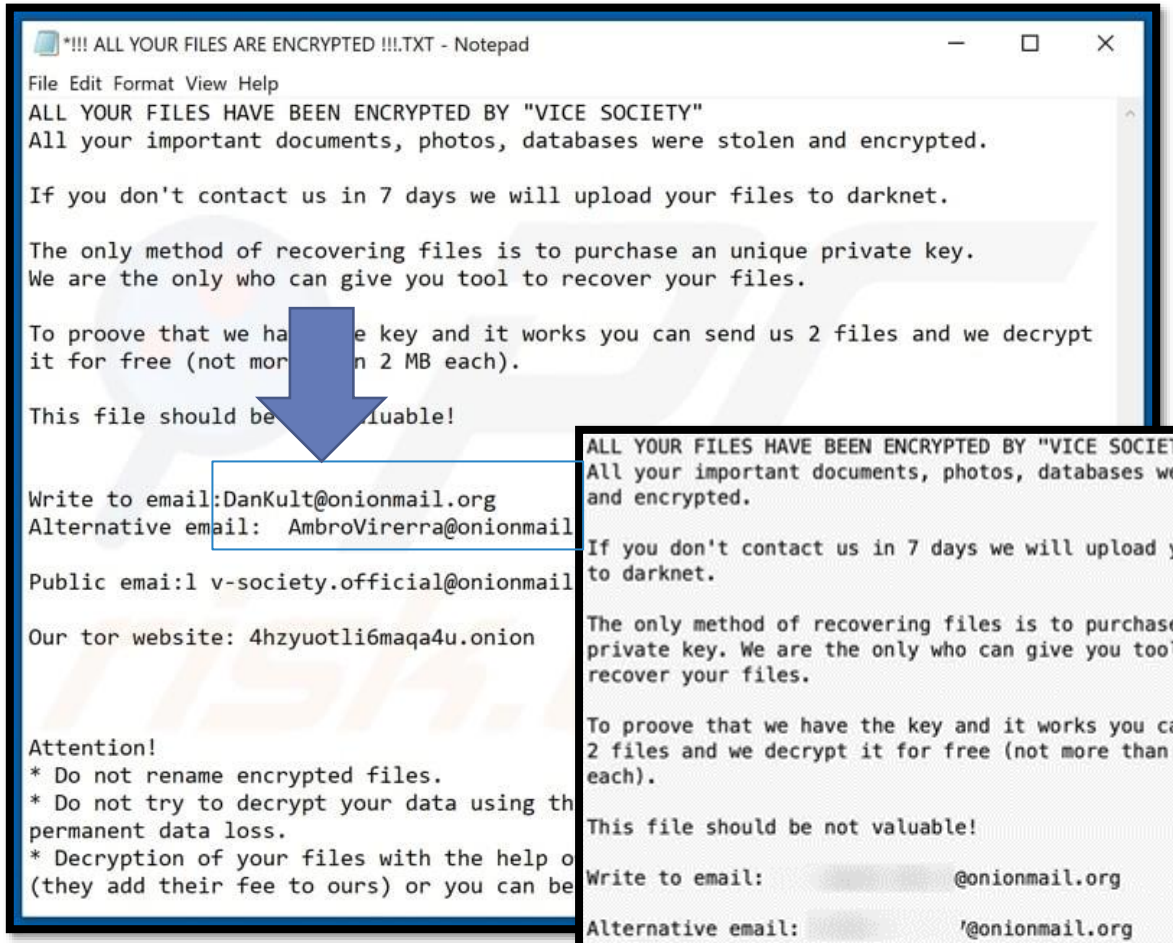
Write to email: BruceBoyle@onionmail.org

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).

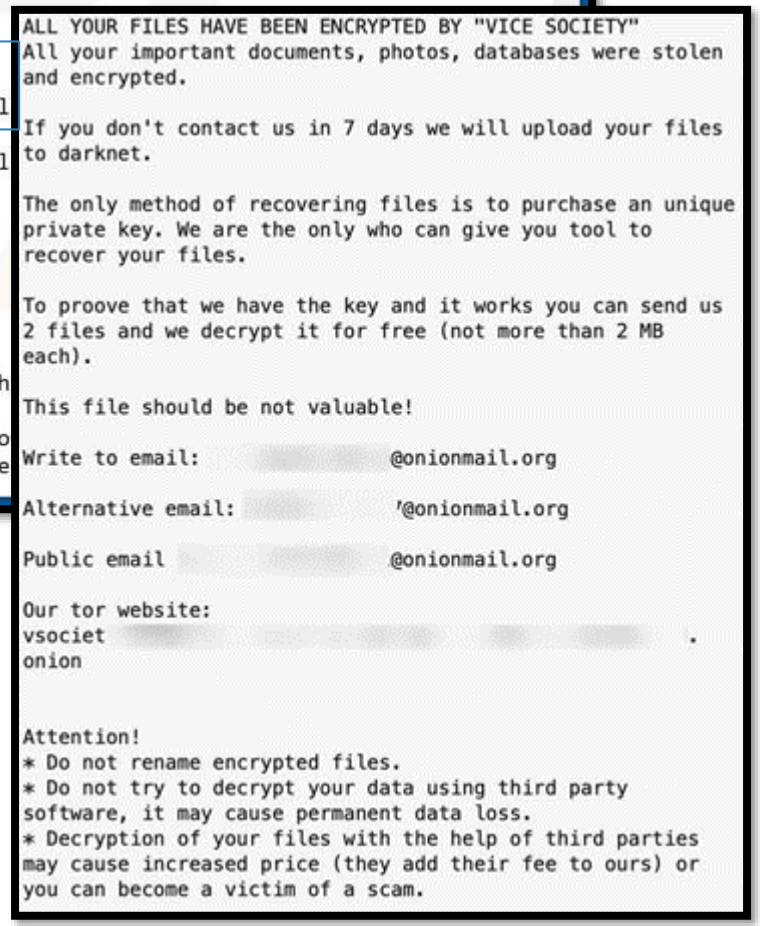
This file should be uable!

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!

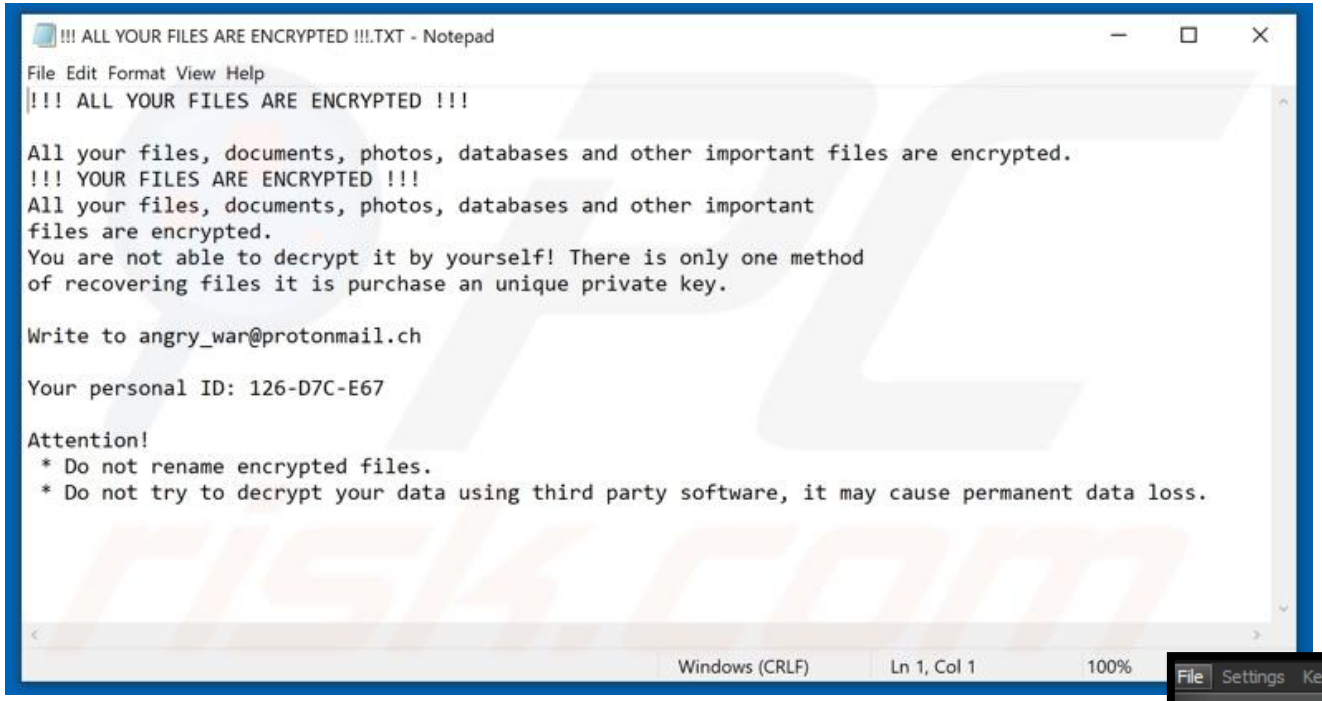
Write to email: @onionmail.org

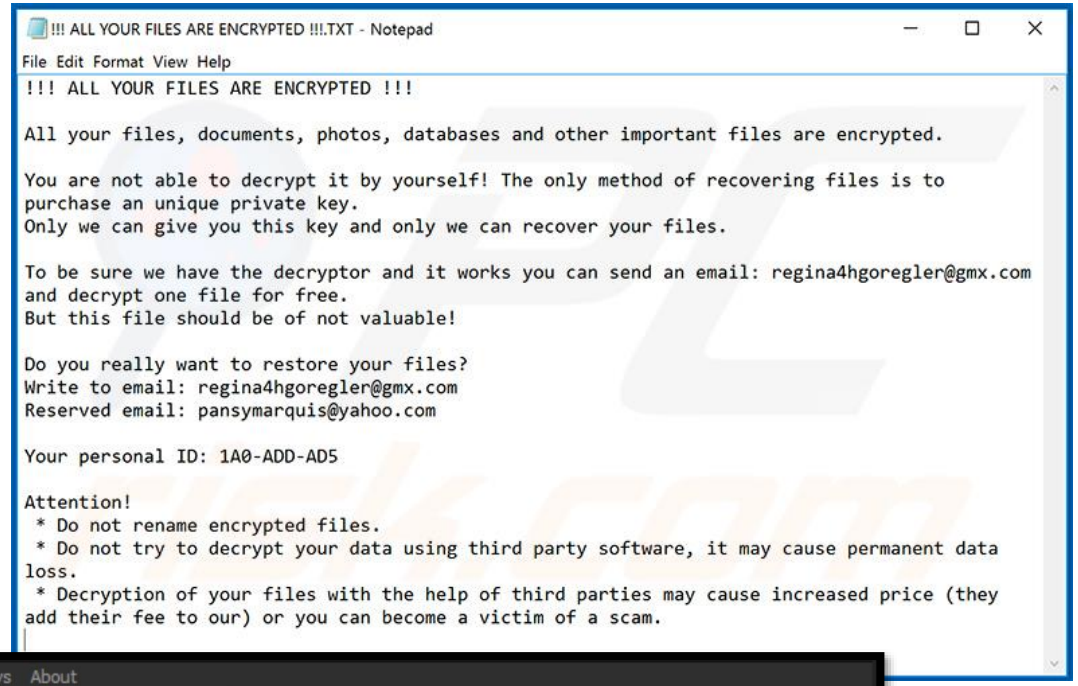
Alternative email: '@onionmail.org

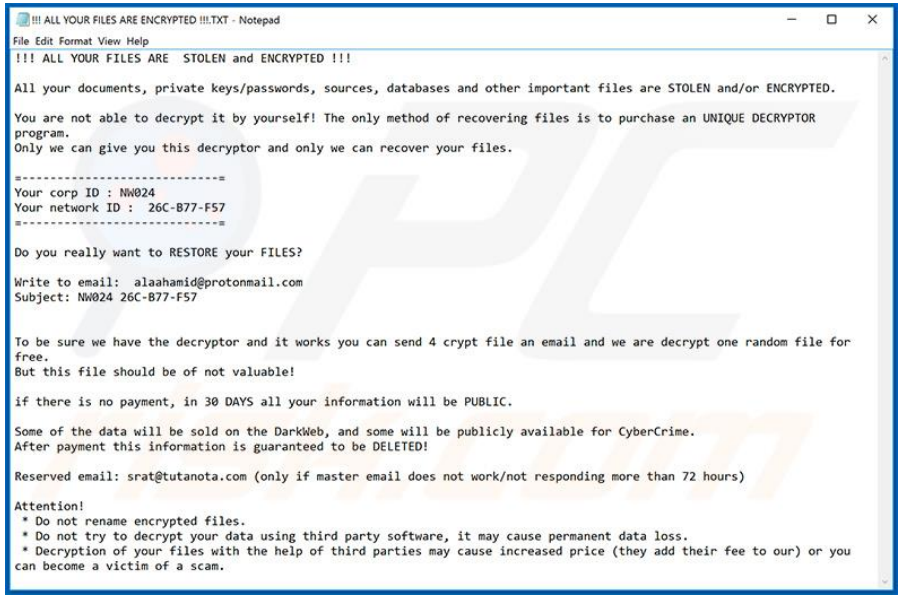
Public email @onionmail.org

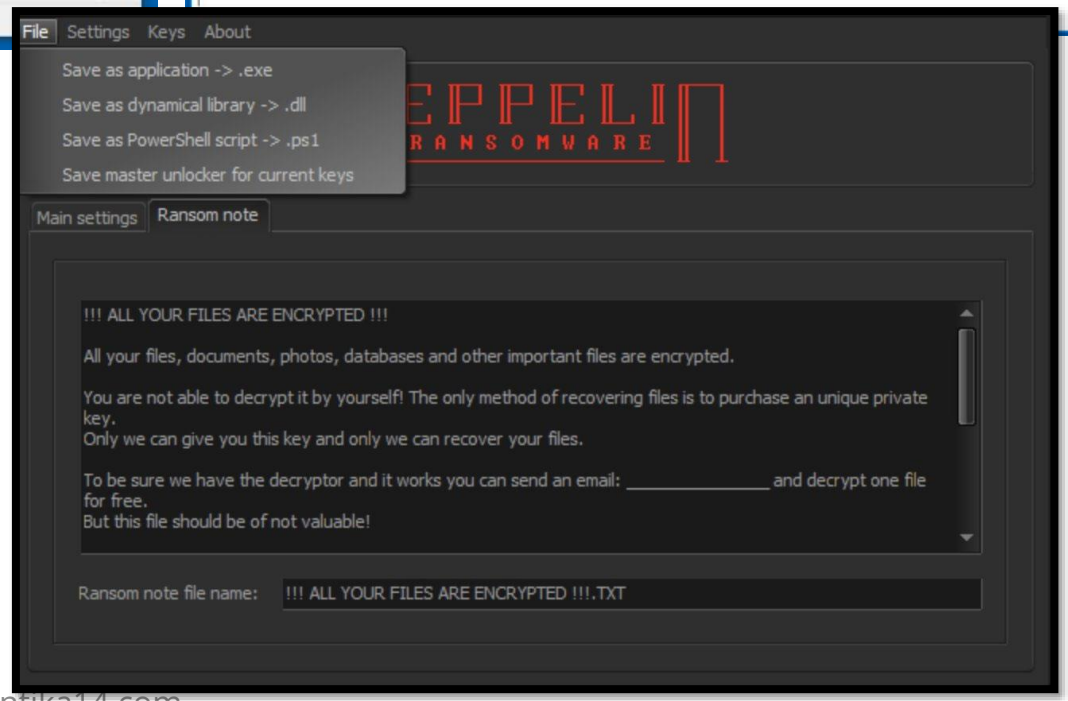
Our tor website:
vsociet .
onion

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

4.5 Entrevistas

Sergiu Gatlan

Lawrence Abrams

Bill Toulas

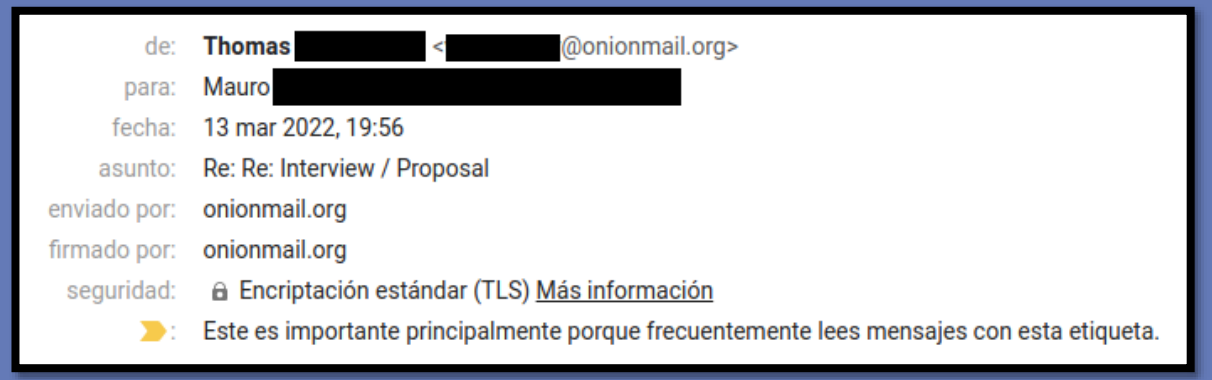
Fuente: https://www.bleepingcomputer.com/tag/vice-society/

"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?

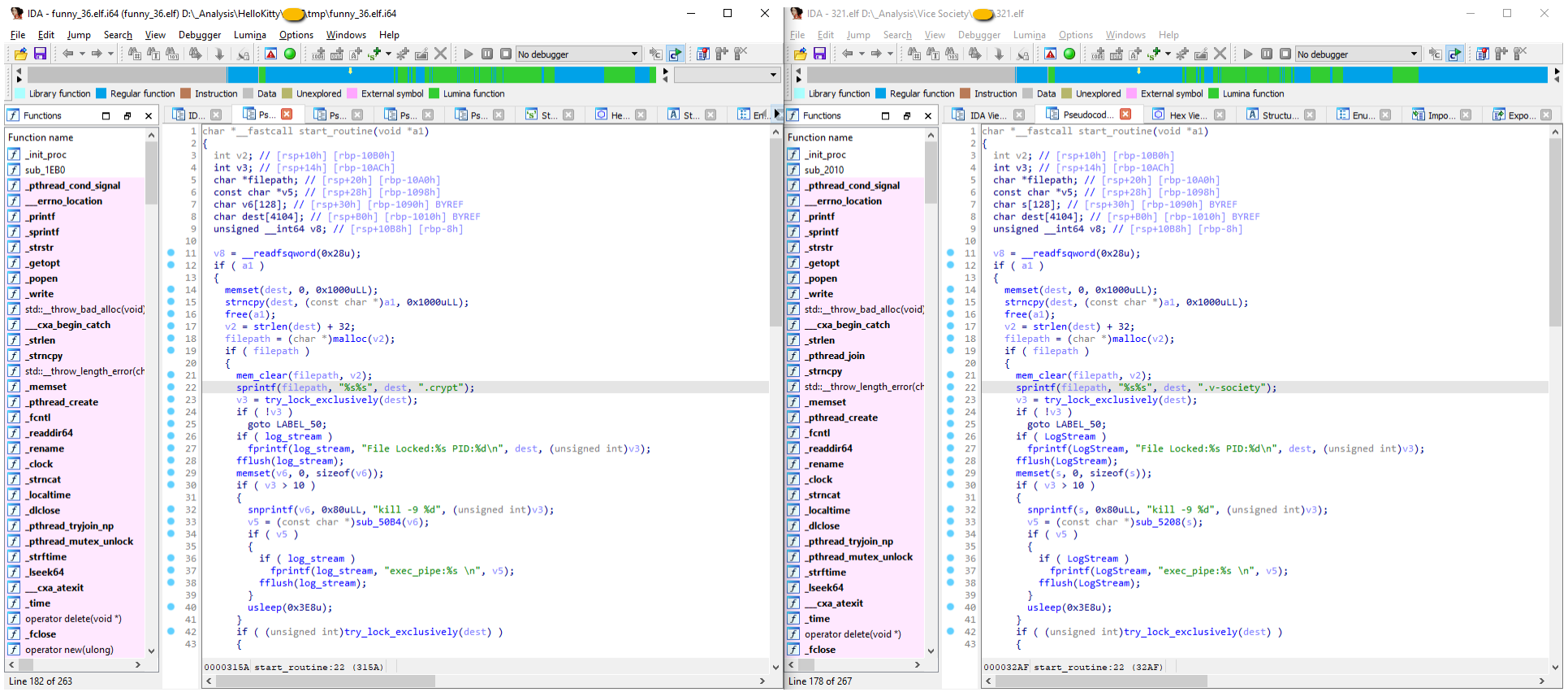
No es la segunda :), es la segunda que no pagó. Y sí, algunos de ellos pagan.

- ¿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.

https://github.com/MauroEldritch/vicesociety

4.6 Análisis del código



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
```

5. Conclusiones

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

¡GRACIAS!