ACTOR DEL MES

Tendencias | Operaciones | Noticias | APTs

Nota de la redacción

Se está convirtiendo en costumbre poner un pequeña nota de redacción y dedicaros unas palabras a tod@s nuestr@s lector@s.

Sin duda, estamos pasando unos momentos muy duros y difíciles, no solo a nivel nacional si no a nivel global. Por ello, desde la redacción esperamos que os encontréis tod@s bien dentro de lo que las circunstancias pueden permitir esto y animaros, que cada día que pasa es uno menos y ya queda poco.

En esta situación excepcional y única hasta la fecha, no todos los ciberdelincuentes descansan e incluso hay algunos que no dan tregua alguna. Por ello hemos querido hablar sobre este actor y hacer un análisis del mismo en la sección "El Actor del Mes".

Antes de comenzar:

¿Todos los ataques con la temática COVID son de este APT? No, es un tema de actualidad y encontraremos otros actores usando estas técnicas.

Novedad:

En este actor del mes, contamos con la ayuda de **Iván Portillo** de GINSEG que, sin duda, aporta una nueva visión y conocimientos a esta sección aportando una mayor calidad de contenido, por ello os pedimos que si os gusta lo compartáis por redes sociales, un gesto que os agradeceremos enormemente.

Y como siempre agradecimientos a **Julio San José**, por su inestimable ayuda y apoyo durante todos estos proyectos y los que vendrán.

Os compartimos nuestros canales oficiales en un acto de spam del sano :P

- Canal principal: https://t.me/DerechodelaRed
- Canal CTI: https://t.me/cti_espana
- Canal información COVID19: https://t.me/CORONAV1RU

Vicious Panda

Actor del 13 de Abril de 2020, Luis Diago e Ivan Portillo

Presentación

Vicious Panda es uno de esos actores que se aprovecha del entorno y el contexto para realizar ingeniería social.

Por ello y en los tiempos que corren, es un actor que utiliza como pretexto el COVID.

Este grupo, según la fuente, no es nuevo. Realizó campañas que se ajustan a este modo de actuación en 2016. Otros nombres con los que se les relaciona con:

- **Mustang Panda**
- **APT36** (realiza campañas usando el COVID-19)

Algunos de los países afectados hasta la fecha por Vicious Panda son:

- **Mongolia - Sector público**
- **Ucrania**
- **Rusia**
- **Bielorrusia**

En la última campaña utilizan ingeniería social para lanzar ataques contra el sector público mongol.

Este APT se considera que es de origen Chino.

Operaciones

Durante la realización de este artículo y cómo es habitual en este punto, hemos encontrado una serie de informes sobre las operaciones y que pueden aportar más información.

- **Campaña COVID-19**
  - https://research.checkpoint.com/2020/vicious-panda-the-covid-campaign/
  - https://www.forbes.com/sites/zakdoffman/2020/03/12/chinese-hackers-weaponized-coronavirus-data-to-launch-this-new-cyber-attack/#38e3db223861

- https://ko.com.ua/koronavirus_geotrekingi_i_rasprostranenie_vredonosnogo_po_132414
- https://www.recordedfuture.com/coronavirus-panic-exploit/
- https://www.anomali.com/blog/china-based-apt-mustang-panda-targets-minority-groups-public-and-private-sector-organizations
- https://greatgameindia.com/coronavirus-triggers-worldwide-cyberattacks/

Malware asociado

A este grupo se le atribuyen, entre otros, el uso de los siguientes **malwares**:

- **Hades Adware**
- **CoronaVirus Ransomware**
- **Emotet Botnet, Trollano Bancario**
- **Loki Mobile Malware**
- **REMCOS RAT**
- **AZORult Stealware**

IOCs

Ahora vamos a poner una lista de algunos de los indicadores de compromiso relacionados con este actor:

IPs:

199.247.25[.]102

95.179.156[.]97

95.179.210[.]61

95.179.242[.]27

95.179.242[.]6

45.128.134[.]14

104.24.103[.]192

95.179.142[.]217

Dominios:

windmilldrops[.]com

adyboh[.]com

esvnpe[.]com

hqoohoa[.]com

kkooppt[.]com

my03[.]com

vueleslie[.]com

Hashes:

8a6ddc8afdccef25166874388c642d1487c13113

0e0b006e85e905555c90dfc0c00b306bca062e7b

dde7dd81eb9527b7ef99ebeefa821b11581b98e0

fc9c38718e4d2c75a8ba894352fa2b3c9348c3d7

601a08e77ccb83ffcd4a3914286bb00e9b192cd6

27a029c864bb39910304d7ff2ca1396f22aa32a2

8b121bc5bd9382dfdf1431987a5131576321aefb

bf9ef96b9dc8bdbc6996491d8167a8e1e63283fe

fcf75e7cad45099bf977fe719a8a5fc245bd66b8

0bedd80bf62417760d25ce87dea0ce9a084c163c

5eee7a65ae5b5171bf29c329683aacc7eb99ee0c

3900054580bd4155b4b72ccf7144c6188987cd31

e7826f5d9a9b08e758224ef34e2212d7a8f1b728

a93ae61ce57db88be52593fc3f1565a442c34679

5ff9ecc1184c9952a16b9941b311d1a038fcab56

36e302e6751cc1a141d3a243ca19ec74bec9226a

080baf77c96ee71131b8ce4b057c126686c0c696

c945c9f4a56fd1057cac66fbc8b3e021974b1ec6

5560644578a6bcf1ba79f380ca8bdb2f9a4b40b7

207477076d069999533e0150be06a20ba74d5378

b942e1d1a0b5f0e66da3aa9bbd0fb46b8e16d71d

9ef97f90dcdfe123ccb7d9b45e6fa9eceb2446f0

cf5fb4017483cdf1d5eb659ebc9cd7d19588d935

92de0a807cfb1a332aa0d886a6981e7dee16d621

cde40c325fcf179242831a145fd918ca7288d9dc

2426f9db2d962a444391aa3ddf75882faad0b67c

9eda00aae384b2f9509fa48945ae820903912a90

2e50c075343ab20228a8c0c094722bbff71c4a2a

2f80f51188dc9aea697868864d88925d64c26abc

e9766b6129d9e1d59b92c4313d704e8cdc1a9b38905021efcac334cdd451e617

3c756d761e89a0ea1216e2b7e57250ac76a80d5fe4f072e3b4b372e609ece74e

238a1d2be44b684f5fe848081ba4c3e6ff821917

234a10e432e0939820b2f40bf612eda9229db720

751155c42e01837f0b17e3b8615be2a9189c997a

ae042ec91ac661fdc0230bdddaafdc386fb442a3

d7f69f7bd7fc96d842fcac054e8768fd1ecaa88a

dba2fa756263549948fac6935911c3e0d4d1fa1f

Grafos:

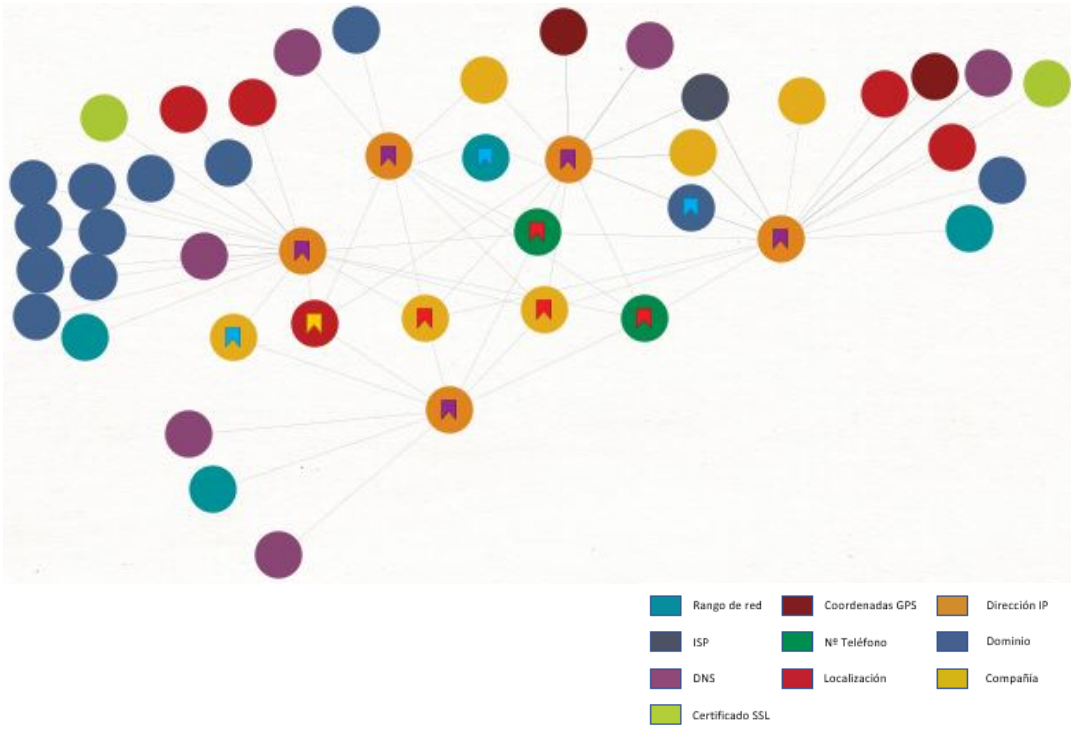
https://www.virustotal.com/graph/
g5c19f646300a4adabff44fe488d1917cbe30e398ea3f47e3807e7eb8cb99970b

Análisis: Investigación de la superficie de los IoCs

En el presente apartado vamos a realizar una breve investigación sobre las direcciones IP y los dominios detectados como IoCs de Vicious Panda y facilitados en la información básica sobre el actor.

Análisis de las direcciones IP

Comenzamos la investigación con las 5 direcciones IP detectadas en la información de partida y que tienen algún tipo de relación con el actor. Un primer vistazo de los datos recolectados pueden ser visualizados en la Imagen A001, en el cual son representadas las relaciones existentes entre los nodos detectados a alto nivel. Cada uno de los nodos simbolizan un tipo de dato concreto tal como puede verse en la leyenda del grafo.



Si se presta atención al grafo anterior, existen algunos nodos que disponen de una marca con un color determinado. Cada una de estas marcas representa el número de relaciones totales con otros nodos, los cuales son los siguientes:

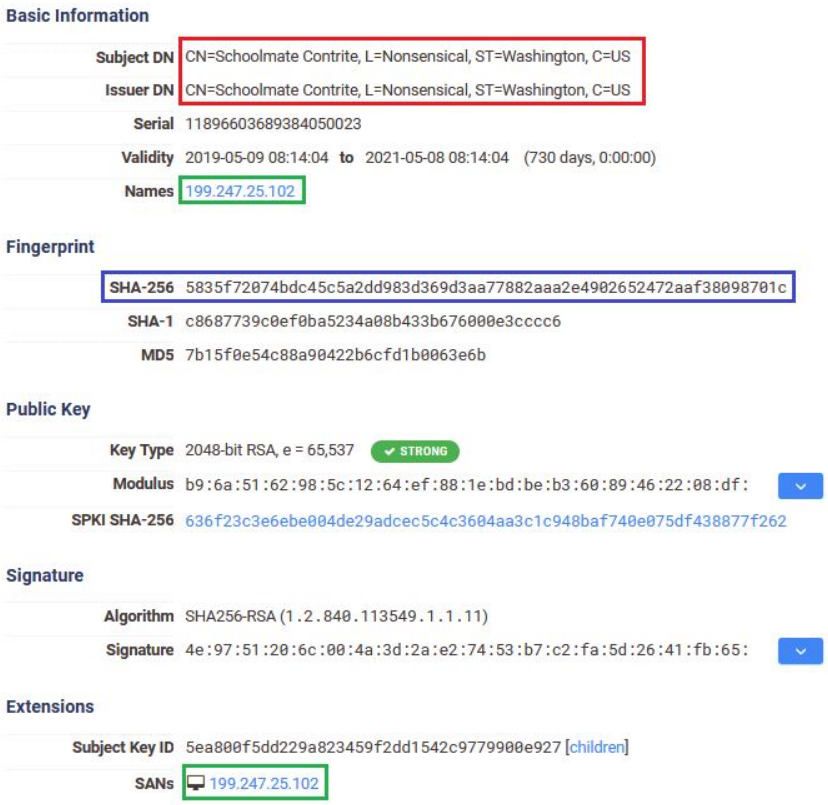
- Nodo con **marca roja** representa un total de **5 relaciones entre nodos**.
- Nodo con **marca amarilla** representa un total de **4 relaciones entre nodos**.
- Nodo con **marca azul** representa un total de **2 relaciones entre nodos**.
- Nodo con **marca morada** representa la **dirección IP investigada** con sus relaciones directas con el resto de nodos.

Si prestamos atención ahora a la siguiente imagen podemos observar el grafo desde la perspectiva del tipo de dato detectado.

Si analizamos la dirección IP **199.247.25.102** sacamos en claro lo siguiente:

- La dirección IP apunta a **Holanda** en concreto a **Haarlem**.
- Su **DNS Inverso** es **199.247.25.102.vultr.com**.
- Se detectan **9 dominios/subdominios (ampletrace.com, aalborgonfire.dk, primalact.art, main.seederv2.wgr.host, www.iamyenz.me, www.aalborgonfire.dk, www.ampletrace.com, iamyenz.me y six.iamyenz.me)** que apuntan a la propia dirección IP.
- La dirección IP está asociada al **rango IP 199.247.24.0-199.247.31.255**.

- Es detectado un **certificado SSL** asociado a la dirección IP con el hash **5835f72074bdc45c5a2dd983d369d3aa77882aaa2e4902652472aaf38098701c**. Analizando el propio hash descubrimos que el certificado ha sido creado con un algoritmo de cifrado **SHA256, el Common Name (CN)** asociado al certificado es **Schoolmate Contrite**, el estado o provincia asociado es **Washington** en **Estados Unidos** y dicho certificado es válido hasta el **8 de mayo de 2021**. En la siguiente imagen puede visualizarse la información del certificado extraído.



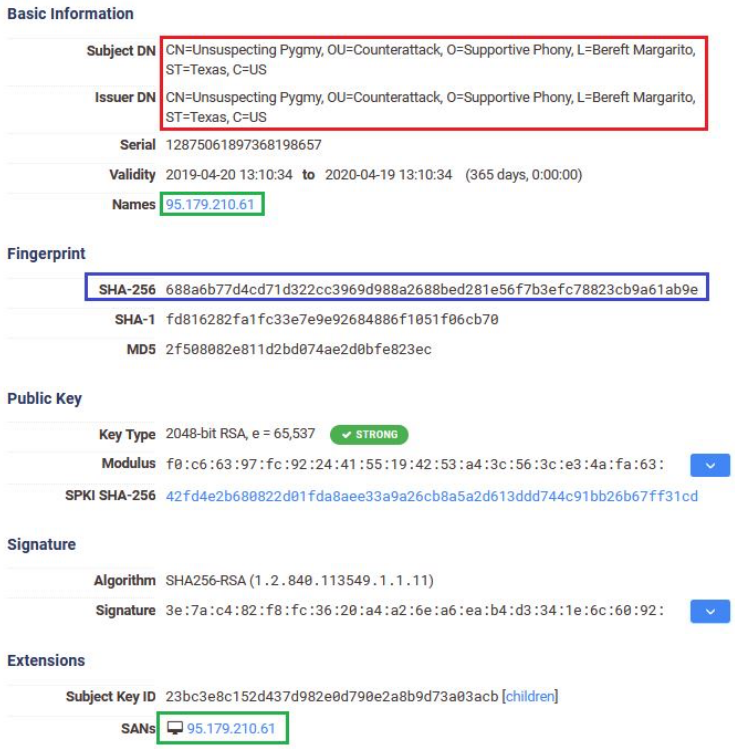
- Son detectados dos números de teléfono (**+1 973 849 0500 y +31 20 535 4444**).
- Son detectadas tres compañías relacionadas (**Vultr Holdings LLC Amsterdam, Vultr Holdings LLC y Network Coordination Centre**).

Analizando la dirección IP **95.179.156.97** sacamos en claro lo siguiente:

- La dirección IP apunta a **Holanda**.
- Su DNS Inverso es **95.179.156.97.vultr.com**.
- Se detecta **un dominio (adyboh.com)** que apuntan a la propia dirección IP.
- La dirección IP está asociada al **rango IP 95.179.144.0-95.179.159.255**.
- Son detectados dos números de teléfono (**+1 973 849 0500 y +31 20 535 4444**).
- Son detectadas tres compañías relacionadas (**Vultr Holdings LLC Amsterdam, Vultr Holdings LLC y Network Coordination Centre**).

Mirando la dirección IP **95.179.210.61** sacamos en claro lo siguiente:

- La dirección IP apunta a Francia en concreto a **Aubervilliers**.
- Su DNS Inverso es **95.179.210.61.vultr.com**.
- Se detectan **2 dominios/subdominios (ttk.alfjgh.com y vultr.com)** que apuntan a la propia dirección IP.
- La dirección IP está asociada al rango IP **95.179.210.0-95.179.211.255**.
- Es detectada unas **coordenadas GPS (latitud 48.917 y longitud 2.383)**.
- Es detectado un **certificado SSL asociado** a la dirección IP con el hash **688a6b77d4cd71d322cc3969d988a2688bed281e56f7b3efc78823cb9a61ab9e**. Analizando el propio hash descubrimos que el certificado ha sido creado con un algoritmo de cifrado **SHA256, el Common Name (CN)** asociado al certificado es **Unsuspecting Pygmy**, la **organización** es **Supportive Phony**, el nombre de la unidad de la organización es **Counterattack**, el estado o provincia asociado es **Texas** en **Estados Unidos** y dicho certificado es válido hasta el **19 de abril de 2020**. En la siguiente imagen puede visualizarse la información del certificado extraído.



- Son detectados dos números de teléfono (**+1 973 849 0500 y +31 20 535 4444**).
- Son detectadas cuatro compañías relacionadas (**Vultr Holdings LLC, AUBERVILLIERS Cedex, Choopa LLC y Network Coordination Centre**).
- Es detectado un ISP (**Choopa, LLC**).

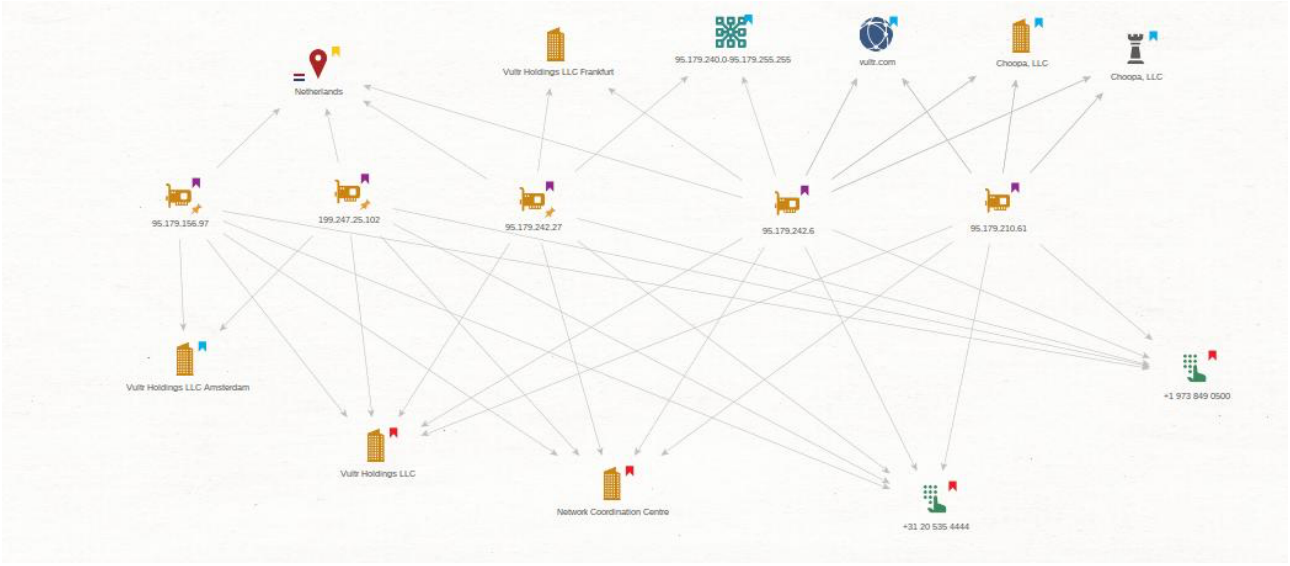
Si analizamos la dirección IP **95.179.242.6** sacamos en claro lo siguiente:

- La dirección IP apunta a **Holanda**.
- Su DNS Inverso es **95.179.242.6.vultr.com**.
- Se detecta un dominio (**vultr.com**) que apunta a la propia dirección IP.
- La dirección IP está asociada al rango IP **95.179.240.0-95.179.255.255**.
- Es detectada unas **coordenadas GPS (latitud 52.382 y longitud 4.899)**.
- Son detectados dos números de teléfono (**+1 973 849 0500 y +31 20 535 4444**).
- Son detectadas cuatro compañías relacionadas (**Vultr Holdings LLC, Choopa LLC, Vultr Holdings LLC Frankfurt y Network Coordination Centre**).
- Es detectado un ISP (**Choopa, LLC**).

Si analizamos la dirección IP **95.179.242.27** sacamos en claro lo siguiente:

- La dirección IP apunta a **Holanda**.
- Su DNS Inverso es **95.179.242.27.vultr.com**.
- Se detecta **un dominio (feb.kkooppt.com)** que apunta a la propia dirección IP.
- La dirección IP está asociada al rango **IP 95.179.240.0-95.179.255.255**.
- Son detectados dos números de teléfono (**+1 973 849 0500 y +31 20 535 4444**).
- Son detectadas tres compañías relacionadas (**Vultr Holdings LLC, Vultr Holdings LLC Frankfurt y Network Coordination Centre**).

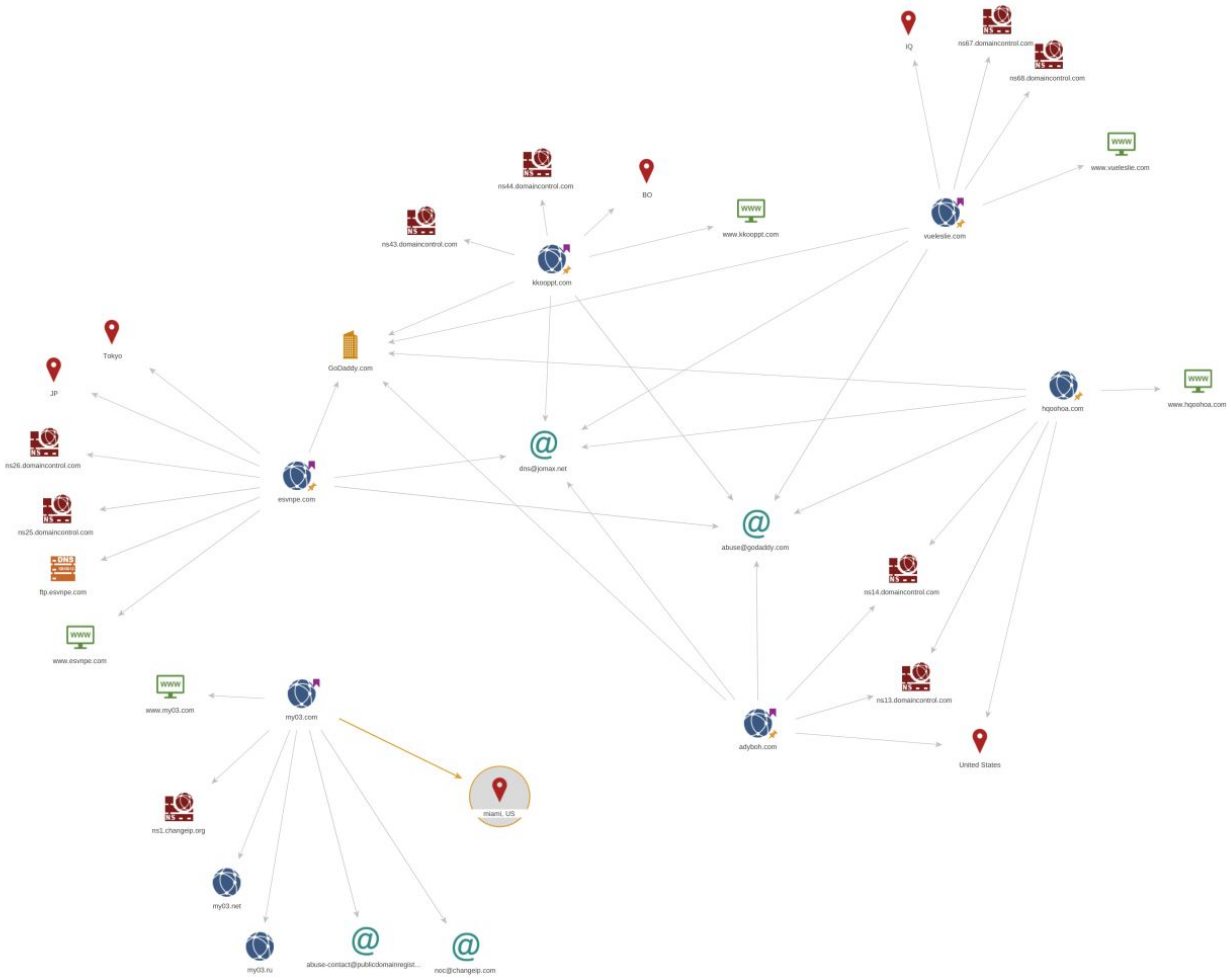
Por último, en la siguiente imagen pueden visualizarse las relaciones directas y ver qué dirección IP de ellas comparten conexiones.



Podemos concluir que todas las direcciones IP tienen algún tipo de relación con los dos números de teléfono detectados (**+1 973 849 0500 y +31 20 535 4444**), las 5 direcciones IPs comparten el mismo registrador (**Vultr Holdings LLC**), además de haber utilizado RIPE como Registro Regional de Internet (**Network Coordination Centre**). Es descubierto que cuatro direcciones IP (**95.179.156.97, 199.247.25.102, 95.179.242.27 y 95.179.242.6**) comparten la misma geolocalización (**Holanda**), el proveedor **Choopa** es utilizado como **ISP** en dos de las IPs (**95.179.242.6 y 95.179.210.61**) y un **rango IP (95.179.240.0-95.179.255.255)** es compartido entre las mismas direcciones IP mencionadas anteriormente.

Análisis de los dominios

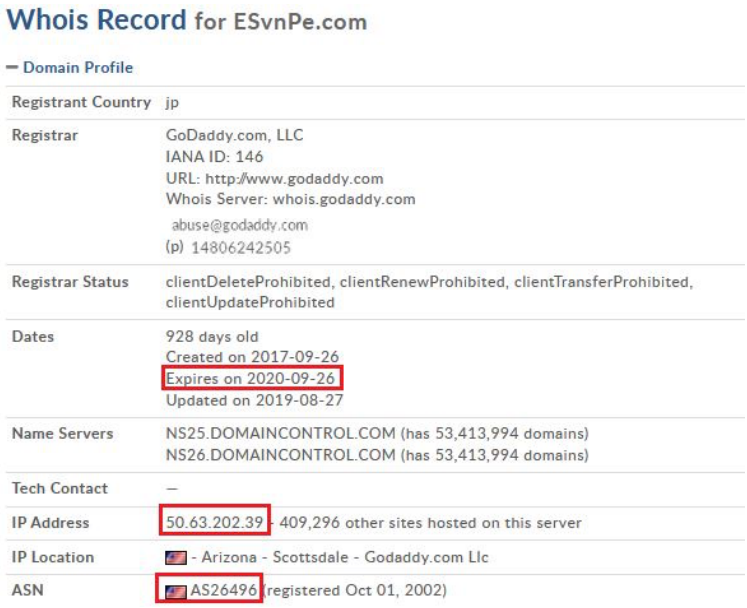
Comenzamos ahora la investigación sobre los dominios detectados en la información de partida y que tienen algún tipo de relación con el actor. Un primer vistazo de los datos recolectados pueden ser visualizados en la siguiente imagen a través de las relaciones existentes entre dichos dominios.



Si analizamos cada dominio podemos sacar en claro lo siguiente:

- **esvnpe.com**
  - El dominio está registrado en Japón en concreto en **Tokio**.
  - Dispone de dos registros NS (**ns25.domaincontrol.com y ns26.domaincontrol.com**).
  - Se detecta un servicio web (**www.esvnpe.com**) y un FTP (**ftp.esvnpe.com**).
  - Son detectados dos correos electrónicos, el primero a través del abuse especificado por el registrador **(abuse@godaddy.com**) y el segundo a través de una resolución DNS por medio del registro SOA (**dns@jomax.net**).
  - Es detectada una compañía registradora a través del Whois (**GoDaddy**).

- A través de otra herramienta (DomainTools) es detectada la **dirección IP** a la que apunta el dominio (**50.63.202.39**), su ASN asociado (**AS26496**) y que **su registro expira el 26 de septiembre de 2020**. Lo mencionado puede visualizarse en la siguiente imagen. Al realizarse varias pruebas de conexión es detectado que la propia IP va rotando, esto indica que el dominio puede tener un balanceador por medio que reparta una dirección IP nueva cada cierto tiempo.



Whois Record for ESvnPe.com

— Domain Profile

Registrant Country	jp
Registrar	GoDaddy.com, LLC IANA ID: 146 URL: http://www.godaddy.com Whois Server: whois.godaddy.com abuse@godaddy.com (p) 14806242505
Registrar Status	clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, clientUpdateProhibited
Dates	928 days old Created on 2017-09-26 Expires on 2020-09-26 Updated on 2019-08-27
Name Servers	NS25.DOMAINCONTROL.COM (has 53,413,994 domains) NS26.DOMAINCONTROL.COM (has 53,413,994 domains)
Tech Contact	—
IP Address	50.63.202.39 - 409,296 other sites hosted on this server
IP Location	- Arizona - Scottsdale - Godaddy.com Llc
ASN	AS26496 (registered Oct 01, 2002)

- **kkooppt.com**
  - El dominio está registrado en Bolivia detectado mediante el código de país BO.
  - Dispone de dos registros NS (**ns43.domaincontrol.com y ns44.domaincontrol.com**).
  - Se detecta un servicio web (**www.kkooppt.com**).
  - Son detectados dos correos electrónicos, el primero a través del abuse especificado por el registrador (**abuse@godaddy.com**) y el segundo a través de una resolución DNS por medio del registro SOA (**dns@jomax.net**).
  - Es detectada una compañía registradora a través del Whois (GoDaddy).
  - A través de otra herramienta (DomainTools) es detectada la dirección IP a la que apunta el dominio (**184.168.221.38**), su ASN asociado (**AS26496**) y que su registro expira el 4 de abril de 2021. Lo mencionado puede visualizarse en la siguiente imagen. Al realizarse varias pruebas de conexión es detectado que la propia IP va rotando, esto indica que el dominio puede tener un balanceador por medio que reparta una dirección IP nueva cada cierto tiempo.

Whois Record for kKoopPt.com

– Domain Profile

Registrant Country	bo
Registrar	GoDaddy.com, LLC IANA ID: 146 URL: http://www.godaddy.com Whois Server: whois.godaddy.com abuse@godaddy.com (p) 14806242505
Registrar Status	clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, clientUpdateProhibited
Dates	731 days old Created on 2018-04-11 Expires on 2021-04-11 Updated on 2020-03-08
Name Servers	NS43.DOMAINCONTROL.COM (has 53,425,169 domains) NS44.DOMAINCONTROL.COM (has 53,425,169 domains)
Tech Contact	–
IP Address	184.168.221.38 - 407,169 other sites hosted on this server
IP Location	- Arizona - Scottsdale - Godaddy.com Llc
ASN	AS26496 (registered Oct 01, 2002)
Domain Status	Registered And Active Website
IP History	28 changes on 28 unique IP addresses over 2 years

- **vueleslie.com**
  - El dominio está registrado en Iraq detectado mediante el código de país IQ.
  - Dispone de dos registros NS (**ns67.domaincontrol.com y ns68.domaincontrol.com**).
  - Se detecta un servicio web (**www.vueleslie.com**).
  - Son detectados dos correos electrónicos, el primero a través del abuse especificado por el registrador (**abuse@godaddy.com**) y el segundo a través de una resolución DNS por medio del registro SOA (**dns@jomax.net**).
  - Es detectada una compañía registradora a través del Whois (GoDaddy).
  - A través de otra herramienta (DomainTools) es detectada la dirección IP a la que apunta el dominio (**50.63.202.42**) y su ASN asociado (**AS26496**). Lo mencionado puede visualizarse en la siguiente imagen. Al realizarse varias pruebas de conexión es detectado que la propia IP va rotando, esto indica que el dominio puede tener un balanceador por medio que reparta una dirección IP nueva cada cierto tiempo.

Whois Record for VuelesLie.com

Domain Profile

IP Address	50.63.202.42 409,560 other sites hosted on this server
IP Location	- Arizona - Scottsdale - Godaddy.com Llc
ASN	AS26496 registered Oct 01, 2002)
Domain Status	Registered And Active Website
IP History	22 changes on 22 unique IP addresses over 2 years
Registrar History	1 registrar
Hosting History	1 change on 2 unique name servers over 2 years

- **hqoohoa.com**:
  - El dominio está registrado en Estados Unidos.
  - Dispone de dos registros NS (**ns13.domaincontrol.com y ns14.domaincontrol.com**).
  - Se detecta un servicio web (**www.hqoohoa.com**).
  - Son detectados dos correos electrónicos, el primero a través del abuse especificado por el registrador **(abuse@godaddy.com**) y el segundo a través de una resolución DNS por medio del registro SOA (**dns@jomax.net**).
  - Es detectada una compañía registradora a través del Whois (GoDaddy).
  - A través de otra herramienta (DomainTools) es detectada la dirección IP a la que apunta el dominio (**50.63.202.72**) y su ASN asociado (**AS26496**). Lo mencionado puede visualizarse en la siguiente imagen. Al realizarse varias pruebas de conexión es detectado que la propia IP va rotando, esto indica que el dominio puede tener un balanceador por medio que reparta una dirección IP nueva cada cierto tiempo.

Whois Record for HqOoHoA.com

Domain Profile

IP Address	50.63.202.72 - 29,917 other sites hosted on this server
IP Location	- Arizona - Scottsdale - Godaddy.com Llc
ASN	AS26496 registered Oct 01, 2002)
Domain Status	Registered And No Website
IP History	2 changes on 2 unique IP addresses over 1 years
Registrar History	1 registrar
Hosting History	1 change on 2 unique name servers over 1 year

- **adyboh.com**
  - El dominio está registrado en **Estados Unidos**.
  - Dispone de dos registros NS (**ns13.domaincontrol.com y ns14.domaincontrol.com**).
  - Son detectados dos correos electrónicos, el primero a través del abuse especificado por el registrador (**abuse@godaddy.com**) y el segundo a través de una resolución DNS por medio del registro SOA (**dns@jomax.net**).
  - Es detectada una compañía registradora a través del Whois (GoDaddy).
  - A través de otra herramienta (DomainTools) es detectada la dirección IP a la que apunta el dominio (**184.168.221.82**), su ASN asociado (**AS26496**) y que su registro expiró el 20 de marzo de 2020. Lo mencionado puede visualizarse en la siguiente imagen. Al realizarse varias pruebas de conexión es detectado que la propia IP va rotando, esto indica que el dominio puede tener un balanceador por medio que reparta una dirección IP nueva cada cierto tiempo.

Whois Record for AdyBoh.com

— Domain Profile

Registrant Country	us
Registrar	GoDaddy.com, LLC IANA ID: 146 URL: http://www.godaddy.com Whois Server: whois.godaddy.com abuse@godaddy.com (p) 14806242505
Registrar Status	clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, clientUpdateProhibited
Dates	388 days old Created on 2019-03-20 Expires on 2020-03-20 Updated on 2019-03-20
Name Servers	NS13.DOMAINCONTROL.COM (has 53,425,169 domains) NS14.DOMAINCONTROL.COM (has 53,425,169 domains)
Tech Contact	–
IP Address	184.168.221.82 - 29,942 other sites hosted on this server
IP Location	- Arizona - Scottsdale - Godaddy.com Llc
ASN	AS26496 (registered Oct 01, 2002)
Domain Status	Registered And No Website
IP History	6 changes on 6 unique IP addresses over 1 years
Registrar History	1 registrar
Hosting History	1 change on 2 unique name servers over 1 year

- **my03.com**
  - El dominio está registrado en Estados Unidos en concreto en **Miami**.
  - Dispone de un registro NS (**ns1.changeip.org**).
  - Es detectado un servicio web asociado (**www.my03.com**).
  - Son detectados dos correos electrónicos, el primero a través del abuse especificado por el registrador (**abuse-contact@publicdomainregistry.com**) y el segundo a través de una resolución DNS por medio del registro SOA (**noc@changeip.com**).
  - A través de otra herramienta (DomainTools) es detectada la dirección IP a la que apunta el dominio (**209.208.4.62**), su ASN asociado (**AS6364**) y que su registro expira el 20 de marzo de 2021. Lo mencionado puede visualizarse en la siguiente imagen. Al realizarse varias pruebas de conexión es detectado que la propia IP va rotando, esto indica que el dominio puede tener un balanceador por medio que reparta una dirección IP nueva cada cierto tiempo.

Whois Record for My03.com

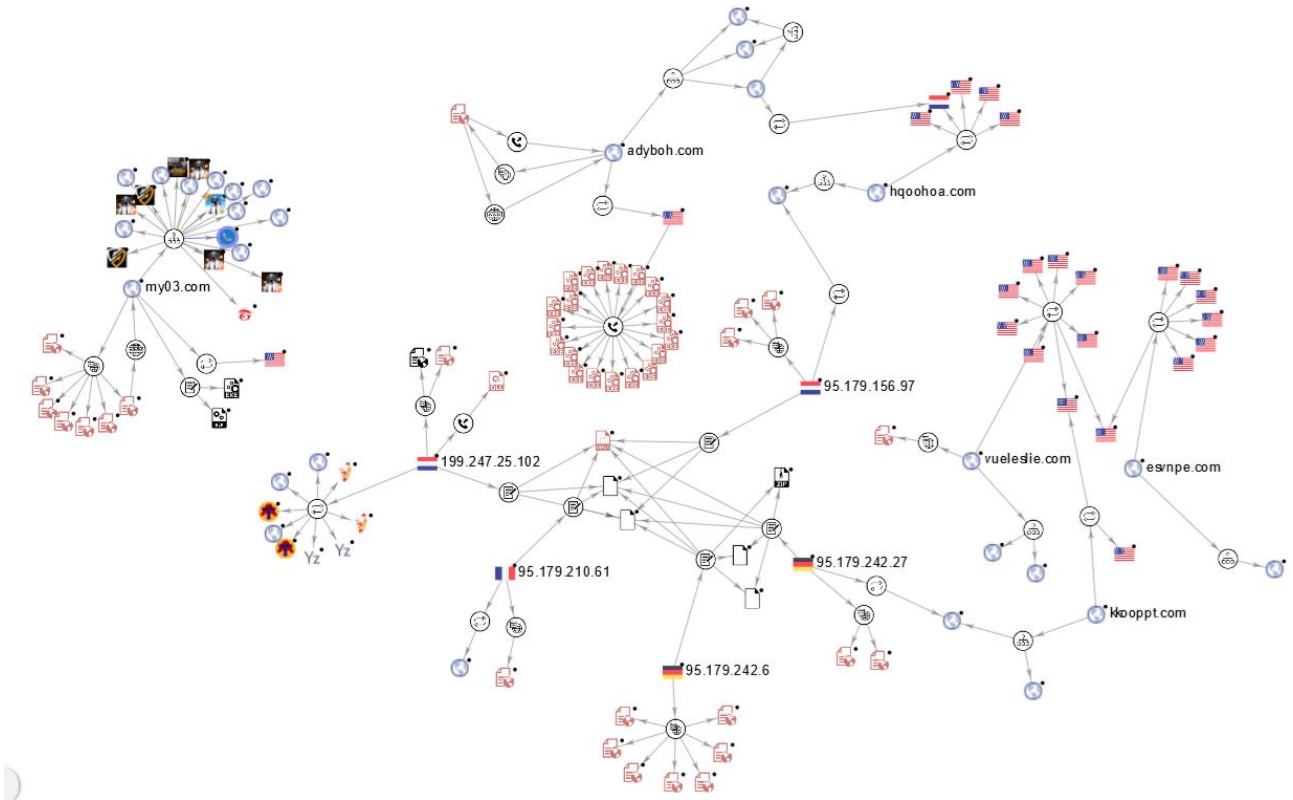
— Domain Profile

Registrant	changeip operations
Registrant Org	changeip.com
Registrant Country	us
Registrar	PDR Ltd. d/b/a PublicDomainRegistry.com IANA ID: 303 URL: www.publicdomainregistry.com,http://www.publicdomainregistry.com Whois Server: whois.publicdomainregistry.com abuse-contact@publicdomainregistry.com (p) 12013775952
Registrar Status	OK, ok
Dates	6,962 days old Created on 2001-03-20 Expires on 2021-03-20 Updated on 2020-01-15
Name Servers	NS1.CHANGEIP.COM (has 3,426 domains) NS2.CHANGEIP.COM (has 3,426 domains) NS3.CHANGEIP.COM (has 3,426 domains) NS4.CHANGEIP.COM (has 3,426 domains) NS5.CHANGEIP.COM (has 3,426 domains)
Tech Contact	changeip operations changeip.com 1200 brickell ave, miami, florida, 33131, us noc@changeip.com (p) 1800791337
IP Address	209.208.4.62 - 152 other sites hosted on this server
IP Location	- Florida - Orlando - Atlantic.net Inc.
ASN	AS6364 (registered Mar 20, 1996)
Domain Status	Registered And Active Website
IP History	7 changes on 7 unique IP addresses over 16 years
Registrar History	4 registrars with 2 drops
Hosting History	2 changes on 2 unique name servers over 12 years

Como conclusión del análisis podemos indicar que los dominios **esvnpe.com, kkooppt.com, vueleslie.com, hqoohoa.com y adyboh.com** están relacionados por medio del mismo registrador (**GoDaddy**) y ASN (**AS26496**), ambos correos electrónicos detectados y el mismo dominio utilizado en los registros NS (domaincontrol.com) lo que indica que están utilizando el mismo proveedor. En concreto, entre los dominios hqoohoa.com y adyboh.com existe algún tipo de relación más directa ya que comparten los mismo registros NS y la localización. Aparentemente el dominio my03.com no cuenta con ninguna relación con los otros dominios.

Análisis de relaciones entre los IoCs en VirusTotal

En esta sección procedemos a realizar una investigación de todos los IoCs analizados individualmente en las secciones anteriores para ver cómo están relacionados entre si dentro de una herramienta de inteligencia de amenazas como VirusTotal. En la siguiente imagen puede visualizarse el grafo de las relaciones entre los dominios y las direcciones IP detectados como IoCs.



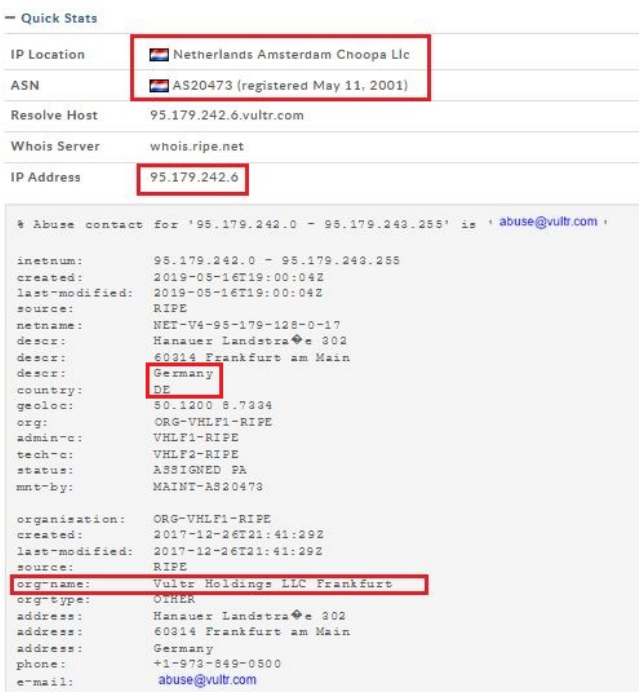
A continuación mostramos un breve resumen de las conexiones detectadas por cada uno de los IoCs analizados.

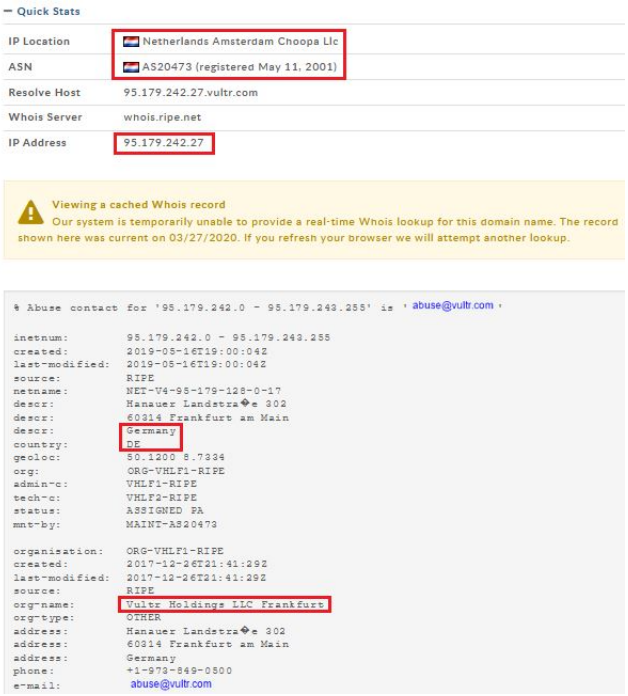
- **<u>IoC 1. Dirección IP 199.247.25.102</u>**:
    - La dirección IP apunta a **Holanda, su ASN es 20473 y su ASN Owner es Choopa, LLC**.
    - Se detectan **9 dominios/subdominios (ampletrace.com, aalborgonfire.dk, primalact.art, main.seederv2.wgr.host, www.iamyenz.me, www.aalborgonfire.dk, www.ampletrace.com, iamyenz.me** y **six.iamyenz.me)** que apuntan a la propia dirección IP.
    - Relación existente entre la dirección IP con dos URLs, una detectada como maliciosa por 4 motores antivirus (hxxp://199.247.25.102/).
    - Una librería DLL detectada como maliciosa por 51 motores antivirus (215c72df44fe8e564d24f4d9930c27409e7f76e2045c67940cdcecdbdbd3b04f), el cual establece comunicación con la dirección IP analizada.
    - **3 ficheros** que hacen referencia a la dirección IP, **un XML malicioso** y **dos ficheros de texto** que hacen referencia a IoCs utilizados en listados sobre **COVID-19**.
- **<u>IoC 2. Dirección IP 95.179.156.97</u>**:
    - La dirección IP apunta a **Holanda, su ASN es 20473 y su ASN Owner es Choopa, LLC**.
    - Relación existente entre la dirección IP con tres URLs catalogadas como maliciosas por varios motores antivirus, en concreto: 7 (hxxp://bmy.hqoohoa.com), 5 (hxxp://95.179.156.97) y uno (hxxps://bmy.hqoohoa.com).
    - Se detecta **un dominio (bmy.hqoohoa.com)** que apuntan a la propia dirección IP.
    - **3 ficheros** que hacen referencia a la dirección IP, **un XML malicioso** y **dos ficheros de texto** que hacen referencia a IoCs utilizados en listados sobre **COVID-19**.
- **<u>IoC 3. Dirección IP 95.179.210.61</u>**:
    - La dirección IP apunta a **Francia, su ASN es 20473 y su ASN Owner es Choopa, LLC**.
    - Se detecta **un dominio (ttk.alfjgh.com)** que apuntan a la propia dirección IP.
    - Relación existente entre la dirección IP con una URL catalogada como maliciosa por **6 motores antivirus** (**hxxp://95.179.210.61**) y que apunta a la propia dirección IP.
    - **3 ficheros** que hacen referencia a la dirección IP, **un XML malicioso** y **dos ficheros de texto** que hacen referencia a IoCs utilizados en listados sobre **COVID-19**.

- **<u>IoC 4. Dirección IP 95.179.242.6</u>**:
    - La dirección IP apunta a **Alemania, su ASN es 20473 y su ASN Owner es Choopa, LLC**.
    - Relación existente entre la dirección IP con siete URLs catalogadas como maliciosas por varios motores antivirus, en concreto: 8 (hxxp://95.179.242.6/), 8 (hxxp://95.179.242.6/img/0120/xnelzi), 7 (hxxp://95.179.242.6/img/0120), 4 (hxxp://95.179.242.6/img/0120/XNeLZI), 4 (hxxp://95.179.242.6/img/0115/MLntMQ), 4 (hxxp://95.179.242.6/img/0120/VIdALQ) y 3 (hxxp://95.179.242.6/img/0120/XNeLZI%20hxxp:/95.179.242.6/img/0115/MLntMQ%20xxtp:/95.179.242.6/img/0120/VIdALQ%2095.179.242.6).
    - **6 ficheros** que hacen referencia a la dirección IP, **un XML malicioso, un ZIP, un CSV** y **tres ficheros de texto** que hacen referencia a IoCs utilizados en listados sobre **COVID-19**.
- **<u>IoC 5. Dirección IP 95.179.242.27</u>**:
    - La dirección IP apunta a **Alemania, su ASN es 20473 y su ASN Owner es Choopa, LLC**.
    - Se detecta **un dominio (feb.kkooppt.com)** que apuntan a la propia dirección IP.
    - Relación existente entre la dirección IP con dos URLs catalogadas como maliciosas por varios motores antivirus, en concreto: 7 (hxxp://feb.kkooppt.com/) y 6 (hxxp://95.179.242.27/).
    - **6 ficheros** que hacen referencia a la dirección IP, **un XML malicioso, un ZIP, un CSV** y **tres ficheros de texto** que hacen referencia a IoCs utilizados en listados sobre **COVID-19**.
- **<u>IoC 6. Dominio esvnpe.com</u>:**
    - Se detecta **un subdominio (jocoly.esvnpe.com)** asociado al dominio.
    - Es detectado que el propio dominio resuelve a siete direcciones IP. Esto quiere decir que dicho dominio ha apuntado a lo largo del tiempo a cada una de las direcciones IP localizadas.
- **<u>IoC 7. Dominio kkooppt.com</u>:**
    - Se detectan **dos subdominios (www.kkooppt.com y feb.kkooppt.com)** asociados al dominio.
    - Es detectado que el propio dominio resuelve a dos direcciones IP (**50.63.202.50** y **50.63.202.42**). Esto quiere decir que dicho dominio ha apuntado a lo largo del tiempo a cada una de las direcciones IP localizadas.

- **IoC 8. Dominio vueleslie.com:**
    - Se detectan **dos subdominios (bur.vueleslie.com** y **nist.vueleslie.com)** asociados al dominio.
    - Relación existente entre el dominio con una URL catalogada como maliciosa por un motor antivirus (**hxxp://vueleslie.com**).
    - Es detectado que el propio dominio resuelve a nueve direcciones IP. Esto quiere decir que dicho dominio ha apuntado a lo largo del tiempo a cada una de las direcciones IP localizadas.
- **IoC 9. Dominio hqoohoa.com:**
    - Se detecta **un subdominio** (**bmy.hqoohoa.com**) asociados al dominio.
    - Es detectado que el propio dominio resuelve a cinco direcciones IP. Esto quiere decir que dicho dominio ha apuntado a lo largo del tiempo a cada una de las direcciones IP localizadas.
- **IoC 10. Dominio adyboh.com:**
    - Se detectan **tres subdominios** (**wy.adyboh.com, dw.adyboh.com** y **www.adyboh.com**) asociados al dominio.
    - Relación existente entre el dominio con una URL catalogada como maliciosa por un motor antivirus (**hxxp://adyboh.com**).
    - Es detectado que el propio dominio resuelve a la **dirección IP 184.168.221.86**.
- **IoC 11. Dominio my03.com:**
    - Se detectan **veinte subdominios** asociados al dominio.
    - Relación existente entre el dominio con siete URLs catalogadas como maliciosas por varios motores antivirus, en concreto: 6 (hxxp://my03.com/), 3 (hxxps://my03.com), 2 (hxxp://my03.com:112/), 2 (hxxp://my03.com:99), 2 (hxxp://my03.com:9090), 4 (hxxp://95.179.242.6/img/0120/VIdALQ), 2 (hxxp://my03.com:8080) y uno (hxxp://my03.com:6688).
    - Es detectado que el propio dominio resuelve a la **dirección IP 209.208.4.38**.
    - **2 ficheros** que hacen referencia al dominio, un **EXE** (**antispam.exe**) y un **ELF** (**ddns.cgi**).

Tanto la dirección IP 95.179.242.6 como la 95.179.242.27 parece que en un primer momento han sido registradas en Holanda pero las últimas evidencias obtenidas mediante VirusTotal indican que han sido registradas en Alemania. Si prestamos atención a sus Whoises podemos detectar que ambas IPs han sido registradas por medio de un proveedor de VPS con el nombre de "**Vultr Holdings LLC Frankfurt**" en Alemania, y que obtienen la geolocalización de Holanda por medio del **ISP Choopa** contratado en dicho país. En las siguientes imágenes pueden verse los respectivos Whoises de ambas direcciones IP.





En cuanto a las resoluciones de los dominios hacia diferentes direcciones IP, todo hace indicar que al estar alojado en un hosting como GoDaddy es normal que cada cierto tiempo resuelva a una dirección IP diferente ya que disponen de balanceadores que redireccionan a varias direcciones IP para proteger su infraestructura.

Como conclusiones tenemos lo siguiente:

- Las 5 direcciones IP están directamente relacionadas por medio de los 6 ficheros que mencionan a cada uno de estos, siendo los siguientes **un XML malicioso (testSI.docx"; filename*=UTF-8''testSI.docx), un ZIP (IOC_coronavirus.zip), un CSV (%225e787325c258765241f8b0fd.csv%22)** y **tres ficheros de texto** que hacen referencia a IoCs utilizados en listados sobre **COVID-19 (20032020_IOC_IP.txt, covid_ips_domains.txt** e **IOC_IP.txt)**.

- El dominio **kklooppt.com** está directamente conectado por medio de un subdominio suyo a la **dirección IP 95.179.242.27.**
- Los dominios **vueleslie.com** y **esvnpe.com** están relacionados con el dominio **kkplooppt.com** por medio de la misma infraestructura de red utilizada de GoDaddy.
- El dominio **hqoohoa.com** está directamente conectado por medio de un subdominio suyo a la **dirección IP 95.179.156.97.**
- El dominio **adyboh.com** está relacionado con el dominio **hqoohoa.com** por medio de la misma infraestructura de red utilizada de GoDaddy, además de una coincidencia de resolución hacia la **dirección IP 95.179.158.84**, que a lo largo del tiempo ambas han compartido.

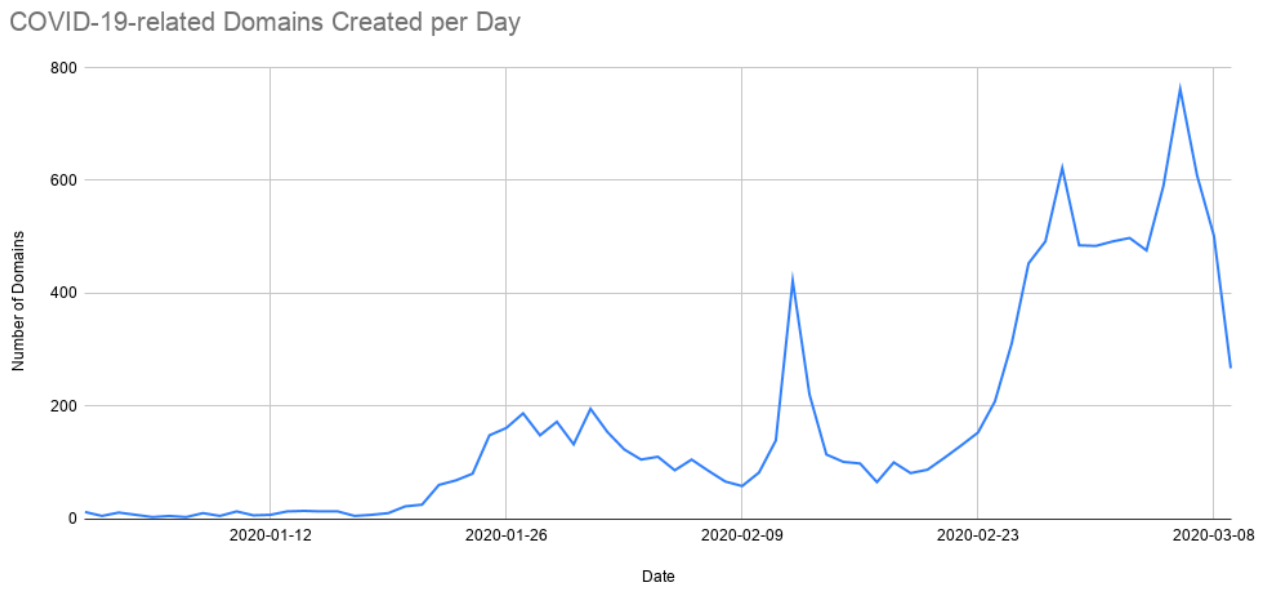
Os facilitamos el enlace del Graph de VirusTotal por si queréis seguir investigando:

https://www.virustotal.com/graph/gf5ee8b6780b347c5977ef431d9fab3711126888c011d4174b0fbc5f04f1801e9

Recursos extras

Vamos a añadir una serie de recursos extras como siempre, pero esta vez queremos que sea diferente.

Las campañas usando el Coronavirus son muchas, no se limitan solo a este actor, podemos ver esto en gráficos como los de Recorder Future:

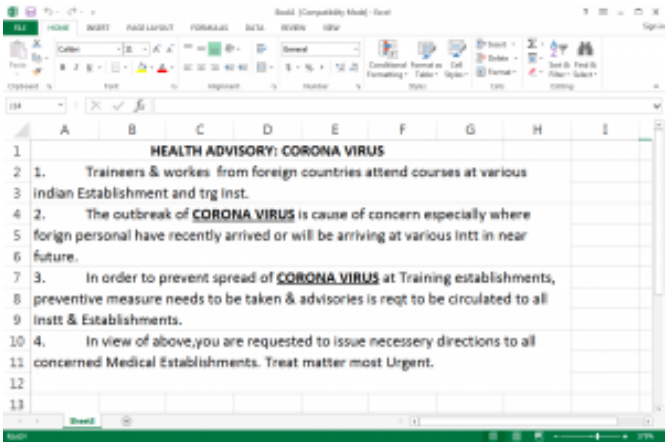


Aquí podemos ver el incremento de los dominios dados de alta cada día, llegando en su pico a casi 800 dominios.

Esto empezó en Enero, y la afectación se ha ido extendiendo a la vez que el virus a niveles impresionantes.

Las tácticas como ya hemos visto, no varían mucho con respecto a otras campañas, pero, sí que cambia el método de hacer llegar el malware y generar en el usuario la necesidad de descargarlo.

Ejemplo de macros maliciosas en un excel relativo al COVID-19:



Ejemplos de correos maliciosos usando el COVID-19:

Original

МОНГОЛ УЛСААС БНХАУ-Д СУУГАА
ЭЛЧИН САЙДЫН ЯАМ

ШУУРХАЙ МЭДЭЭ

2020 оны 1 дүгээр сарын 22-ны өдөр №ШМ072004 Бээжин хот

Шинэ коронавирусын халдварын тархалтын тухай

БНХАУ-ын Төрийн зөвлөлийн Хэвлэл мэдээллийн албанаас өнөөдрийн 10.00 цагт хийсэн хэвлэлийн бага хурлын үеэр Хятад улсад шинэ коронавирусын халдварт хатгалгаагаар өвчилсөн 440 хүн байгаа бөгөөд 9 нас барсан тохиолдол байгааг мэдээллэв.

Хятадын Үндэсний эрүүл мэндийн хорооноос гаргасан статистик мэдээллээр өнөөдрийн байдлаар Хятад улсын өмнөд болон зүүн өмнөд хэсгийн 14 муж, хот мөн АНУ, Япон, Өмнөд Солонгос, Австрали (түс бүр 1), Сингапур (7), Тайланд (2) зэрэг улсад тархсан байна. Вирусын тархалтын явц хурдан байгаа бөгөөд дээрх 440 өвчтөний ойрын хүрээний нийт 2197 хүнд тандалт хийж, 765 хүний халдваргүйг тогтоож, 1394 хүнийг үргэлжлүүлэн хянаж байна.

Шинэ коронавирусын халдварын талаарх шуурхай мэдээллийг үргэлжлүүлэн хүргэх болно.

Эх сурвалж: Хятадын Ардын өдрийн сонин цахим мэдээ

БОЛОВСРУУЛСАН: [redacted]

[redacted]

Translated (Automatically)

MONGOLIA FROM MONGOLIA TO CHINA
Ministry of Foreign Affairs

FAST NEWS

20 January 20 , 2004 No. SHM07 2004 Beijing

the 22nd day of the city

About the spread of new coronavirus infections

The State Council Media Service of the PRC informed at a press conference today at 10:00 a.m. that there are 440 people with the new coronary artery disease in China, and 9 have died.

According to statistics released by the National Health Committee of China, to date, it has spread to 14 provinces and cities in the southeast and southeast of China, as well as to the United States, Japan, South Korea, Australia (1), Singapore (7) and Thailand (2). The spread of the virus is rapid, with a total of 2197 surveys in the immediate vicinity of the 440 patients, 765 infected have been identified, and 1394 have been continuously monitored.

Instant updates on new coronavirus infections will continue to be provided.

Source: Chinese People's Day Newspaper

[redacted]

/ Temporary Provider /

[redacted]

Sacado del Informe de Check Point

Y así un sin fin de casos usando esta temática…