4. CASO PRÁCTICO DE INVESTIGACIÓN DE UNA AMENAZA

4.1. INVESTIGACIÓN DEL GRUPO CRIMINAL SILVERTERRIER

Durante la pandemia del COVID-19 aparecieron multitud de amenazas queriendo aprovecharse de la situación de aquel momento, como por ejemplo las campañas Business Email Compromise (BEC) distribuidas por medio del grupo criminal SilverTerrier.

SilverTerrier es un grupo nigeriano que lleva activo desde 2014. Según UNIT42 de Palo Alto han sido identificadas 10 campañas de malware bajo la temática COVID-19, detectándose un total de 170 correos electrónicos de phishing y directamente relacionados hacia este grupo criminal. El artículo de UNIT42 referente a este tema puede encontrarse en el siguiente artículo: "SilverTerrier: New COVID-19 Themed Business Email Compromise Schemes"

Entre los sectores objetivos de SilverTerrier se encuentran:

- Agencias gubernamentales de salud
- Gobiernos locales y regionales
- Grandes universidades con programas o centros médicos
- Empresas de servicios públicos regionales
- Editoriales médicas
- Compañías de seguros

Algunos de los países afectados por esta amenaza son los siguientes:

- Estados Unidos
- Australia
- Canadá
- Italia
- Reino Unido

4.1.1. OPERACIONES DE SILVERTERRIER

Entre las operaciones han sido detectadas 10 campañas BEC, tal como comentamos anteriormente. Según UNIT42 dentro de estas campañas son identificados tres actores diferentes pertenecientes al mismo grupo de SilverTerrier.

Al primer actor se le atribuyen ocho campañas:

- Campaña 1. Correo electrónico con una muestra de **LokiBot** camuflada como archivo adjunto y simulando ser el **departamento de salud de indonesia.**

Date:	1/30/2020
Subjects:	Coronavirus in Indonesia: KNOW HOW TO PROTECT AND PREVENT YOURSELF. DONT GET INFECTED Coronavirus di Indonesia: TAHU CARA MELINDUNGI DAN MENCEGAH DIRI. JANGAN MENDAPAT INFEKSI
Attachment:	INDONESIAN HEALTH DEPARTMENT_PDF.gz [3335ebffd8…]

Imagen 157. Indicadores de la primera campaña (Fuente: UNIT42)

- Campaña 2. Correo electrónico con un documento Excel que explotaba la vulnerabilidad **CVE-2017-11882**, simulando un envío de la **ONU** y cuyo objetivo era un **proveedor de Estados Unidos.**

Original Content	Translated
MBC	MBC
BESONDERHEDE BESONDERHEDE VIR HIERDIE MAAND	DETAILS DETAILS FOR THIS MONTH
DRAENDE NR. HOEV	BEARING NO. HOW
30208 NBC DRAAG 30 STK	30208 NBC DRESS 30 PCS
30308 NBC DRAAG 6 STK	30308 NBC DRESS 6 PCS
32007X NBC DRAAG 74 STK	32007X NBC BEAR 74 pcs
33005 NBC wat 5 stelle dra	33005 NBC carrying 5 sets
52799 / 800U (25877/21) NBC wat 30 PCS dra	52799 / 800U (25877/21) NBC carrying 30 PCS

Imagen 158. Contenido traducido del documento Excel adjunto (Fuente: UNIT42)

Date:	3/10/2020
Sender:	d.william@accountant[.]com
Subject:	Fw:UN, Coronavirus Update attached
Attachment:	UPDATE!!!.xlsx [e365100468…]

Imagen 159. Indicadores de la segunda campaña

- Campaña 3. Varios correos electrónicos de Phishing enviados a un **proveedor de seguros de salud australiano**. Esta campaña vuelve a aprovechar la

vulnerabilidad **CVE-2017-11882** con un documento RTF adjunto en el correo. Se detecta **Agent Tesla** como malware utilizado.

Date:	3/23/2020
Sender:	handie@indo.net[.]id
Subject:	COVID:19 - FACIAL MASKS NEW ORDER
Attachment:	COVID 19 NEW ORDER FACE MASKS.doc [27d601ef1a…]

Imagen 160. Indicadores de la tercera campaña (Fuente: UNIT42)

- Campaña 4. Varios correos electrónicos de Phishing que simulaban estar relacionados con **suministros de COVID-19**. Dentro de esta campaña fueron detectados tres objetivos diferentes enviados desde tres correos distintos siendo los siguientes:

    - Entre el primer objetivo se encontraba una **universidad de los Estados Unidos con un reconocido programa médico**. El adjunto utilizado vuelve a aprovechar la vulnerabilidad **CVE-2017-11882.**

    - El segundo objetivo fue una **agencia de salud canadiense**. En esta ocasión utilizan una muestra de malware de **Agent Tesla** empaquetado como archivo adjunto.

    - Entre el tercer objetivo fue detectada una **compañía de energía australiana**. Como archivo adjunto vuelven a utilizar una muestra del malware **Agent Tesla**

Date:	3/24/2020-3/25/2020
Sender:	april@jetfacilities[.]com
Subject:	COVID-19 Supplies (Masks, Gloves, & other products)
Attachment:	Sample Products.xlsx [563b1c6252…]
Date:	3/29/2020
Sender:	rohan.jayawardena@multywaychem[.]com
Subject:	COVID-19 Supplies (Masks, Gloves, & other products)
Attachment	Product_Sample_List.r09 [0ae2aaeb29…]
File:	Product_Sample_List.exe [4b8b49bdfa…]
Date:	4/7/2020
Sender:	sales@mailgoesbulkworld[.]live
Subject:	COVID-19 Supplies (Masks, Gloves, & other products)
Attachment	Sample Product.r15 [589a1900b2…]
File:	Sample Product.exe [7f661c6f5e…]

Imagen 161. Indicadores de la cuarta campaña (Fuente: UNIT42)

- Campaña 5. Se detectan varios correos electrónicos con múltiples muestras de malware simulando ser una organización de investigación clínica de los Estados Unidos. Tal como ocurre con la campaña anterior son detectados tres objetivos diferentes:

    - En uno de los correos de phishing detectados es identificado un adjunto con el nombre de "Galaxy International Trading Limited" que vuelve a aprovechar la vulnerabilidad **CVE-2017-11882**

    - En una segunda operación dentro de esta campaña se identifica como objetivo una **agencia del gobierno de los Estados Unidos** utilizando el mismo asunto y nombre del fichero adjunto de la oleada de phishing mencionada anteriormente. La única diferencia es que esta vez es utilizada una muestra de **Agent Tesla** camuflada como fichero adjunto

    - La tercera operación tenía como objetivo a una **editorial médica en Europa** y una agencia del **gobierno de los Estados Unidos**. Como documento adjunto vuelve a utilizarse una muestra de **Agent Tesla**

Date:	3/26/2020
Sender:	info.mmd@medpace[.]com
Subject:	Purchase Order (PO For-COVID-19 Products)
Attachment:	PO For-COVID-19 ProductS.xlsx [f7183d3a99…]
Date:	3/29/2020
Sender:	roseline@reynoldsgh[.]com
Subject:	Purchase Order (PO For-COVID-19 Products)
Attachment	PO For-COVID-19 Products.exe [83457e2b8f…]
Date:	4/6/2020
Sender:	info.mmd@medpace[.]com
Subject:	Purchase Order (PO For-COVID-19 Products)
Attachment	PO For-COVID-19 Products.exe [b58e386928…]

Imagen 162. Indicadores de la quinta campaña (Fuente: UNIT42)

- Campaña 6. Correo electrónico de phishing simulando ser una carta de retraso de un barco perteneciente a una **compañía naviera de Singapur**. En dicho correo fue utilizado un documento **Word** adjunto que explotaba la vulnerabilidad **CVE 2017-11882** utilizando los **servicios de DNS dinámicos** ofrecidos por **DuckDNS**

Date:	3/30/2020
Sender:	tanc@richfield[.]com[.]sg
Subject:	VESSEL DELAY LETTER-COVID-19
Attachment	VESSEL DELAY LETTER.docx [c5c43b3409…]

Imagen 163. Indicadores de la sexta campaña (Fuente: UNIT42)

- Campaña 7. Simularon un correo electrónico relacionado con una **vacuna de COVID-19** utilizando dos muestras del **RAT NanoCore**. Los objetivos de esta campaña fueron una **agencia de salud del gobierno de los Estados Unidos**, dos **universidades con programas médicos** del mismo país y una **aseguradora de salud canadiense.**

Date:	4/7/2020
Sender:	berge@ladbible[.]com
Subject:	Latest vaccine release for Corona-virus(COVID-19)
Attachment	COVID-19 Vaccine Sample.rar [f7b9219f81…]
File	COVID-19 Vaccine Sample.exe [241f09feda…]
Date:	4/7/2020 – 4/8/2020
Sender:	berge@ladbible[.]com
Subject:	Latest vaccine release for Corona-virus(COVID-19)
Attachment	RFQ-0043232QQ.rar [31d2ef10ca…]
File	MS-RFQ.exe [7b2512d067…]

Imagen 164. Indicadores de la séptima campaña (Fuente: UNIT42)

- Campaña 8. Simularon un correo electrónico con el asunto de **materiales de ayuda de COVID-19** procedentes del **departamento médico de Tailandia** utilizando una muestra de **Lokibot** adjunta. Los objetivos de esta campaña fueron una **agencia de salud del gobierno de los Estados Unidos**, **una infraestructura del estado, una aseguradora de salud del mismo país, una universidad italiana, un gobierno regional italiano y varias instituciones gubernamentales australianas.**

Date:	4/8/2020
Sender:	enquiry@herrnessolar[.]com
Subject:	NEW ORDER 300879 - COVID-19 RELIEF MATERIALS
Attachment:	NEW ORDER 300879.exe [aff38fe42c…]
Attachment:	NEW ORDER 300879.exe [8f56fb41ee…]

Imagen 165. Indicadores de la octava campaña (Fuente: UNIT42)

Al **segundo actor** se le atribuye una campaña dirigida hacia una **agencia de salud del gobierno** de los **Estados Unidos** descubriéndose dos muestras de malware de LokiBot entre los adjuntos de los correos electrónicos enviados.

Date:	3/17/2020 – 3/18/2020
Sender:	sofian@cahayapack[.]com[.]my
Subject:	COVID-19 UPDATE // BUSINESS CONTINUITY PLAN ANNOUNCEMENT STARTING MARCH 2020.
Attachment:	AWARENESS NOTICE ON CORONAVIRUS COVID-19 DOCUMENT_pdf.exe [da26ba1e13…]
Date:	3/18/2020
Sender:	sofian@cahayapack[.]com[.]my
Subject:	CORONAVIRUS (COVID-19) UPDATE // BUSINESS CONTINUITY PLAN ANNOUNCEMENT STARTING MARCH 2020.
Attachment:	AWARENESS NOTICE ON CORONAVIRUS COVID-19 DOCUMENT_pdf.exe [1ee6646e0e…]

Imagen 166. Indicadores asociados a la campaña del segundo actor (Fuente: UNIT42)

Al **tercer actor** se le atribuye una campaña en la que camufla muestras de malware como adjuntos, los cuales, utilizan PowerShell para descargar archivos ejecutables maliciosos. Esta vez simulan ser correos electrónicos relacionados con información sobre COVID-19.

Date:	3/23/2020 - 3/24/2020
Sender:	info@welheadcontrol[.]com
Subject:	Information about Covid- 19 Actions
Attachment:	information.rtf [d80a440755…]
Attachment:	covid 19.rtf [d731fb3fcc…]
Attachment:	WxByN.xlsm [8037a8e12e…]

Imagen 167. Indicadores asociados a la campaña del tercer actor (Fuente: UNIT42)

4.1.2. INDICADORES DE COMPROMISO ASOCIADOS

En la propia investigación que se podrá ver en su sección correspondiente, nos centraremos en **SilverTerrier** y el malware **Agent Tesla**. A modo resumen han sido detectados un total de 90 IoCs divididos en los siguientes tipos:

- **2 direcciones IP**
- **17 dominios**
- **69 hashes (MD5, SHA1, SHA256)**
- **1 URL**
- **1 CVE**

4.1.3. MALWARE ASOCIADO

A este grupo criminal se le atribuye la utilización de los siguientes malware en sus campañas:

- Agent Tesla. Se trata de un troyano espía cuyo objetivo de ataque son las plataformas de Microsoft Windows. Sus primeras apariciones datan del 29 de enero de 2019 teniendo sus últimas apariciones este mismo mes de mayo
- NanoCore. Remote Access Tool (RAT) desarrollado en .NET y utilizado para espiar y robar información a las víctimas. Amenaza activa desde el año 2013
- DarkComet. Remote Access Tool (RAT) y backdoor utilizado de nuevo para espiar y robar información a sus víctimas utilizando múltiples técnicas para ello.
- NETWIRE. Remote Access Tool (RAT) de acceso público utilizada por diferentes grupos criminales y APT desde el año 2012 para espiar y robar información a sus víctimas

4.1.4. TTPs ASOCIADOS

La única técnica atribuida a SilverTerrier es la denominada como "*Standard Application Layer Protocol*". Esta técnica permite la comunicación de los adversarios a sus C2 a través de un protocolo de capa de aplicación común como pueden ser HTTP, HTTPS, SMTP o DNS.

La táctica asociada a la técnica mencionada es "*Command and Control*". Dicha táctica hace referencia al intento de conexión del adversario a los sistemas comprometidos de las víctimas y su control por medio de un panel de control conformando una botnet compuesto de múltiples servidores víctima infectados.

4.1.5. INVESTIGACIÓN DE LAS DIRECCIONES IP DETECTADAS

Comenzamos la investigación con las 2 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 puede ser visualizados en la Imagen 168, 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

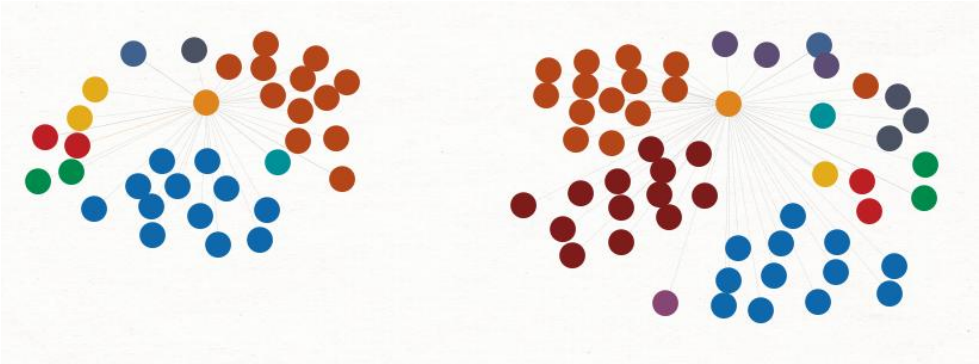


Imagen 168. Relación entre los diferentes IoCs asociados a SilverTerrier

Si prestamos atención en la Imagen 170 y 171 podemos observar el grafo desde la perspectiva del tipo de dato detectado, descubriendo que no existen relaciones entre ambas direcciones IP de manera directa.

Si hacemos foco ahora en la dirección IP 185.126.202[.]111 (Imagen 169) sacamos en claro lo siguiente:

- La dirección IP apunta a **Irán** en concreto a **Tehran.**
- Se detecta **un dominio** (dn-server.com) que apuntan a la propia dirección IP.
- Se detectan **9 subdominios** (tb.64-b.it, tbillboard.64-b.it, px834095.64-b.it, live.samanedu.ir, tbb.16-b.it, ll.n4t.co, test.msisoft.ir, git.msisoft.ir y parsonline.dn-server.com) que apuntan a la propia dirección IP.
- Se detectan **2 registros NS** (ns1.surfoption.com y ns2.surfoption.com) que apuntan a la misma dirección IP.
- La dirección IP está asociada al **rango IP** 185.126.202.0-185.126.202.255.

- Son detectadas **dos compañías relacionadas** (XZN Hosting y Network Coordination Centre).
- Son detectados **dos números de teléfono** (+98 2172308 y +31 20 535 4444).
- Son detectadas **12 URLs** que han dado positivo en algún motor antivirus por estar relacionada con actividad maliciosa.

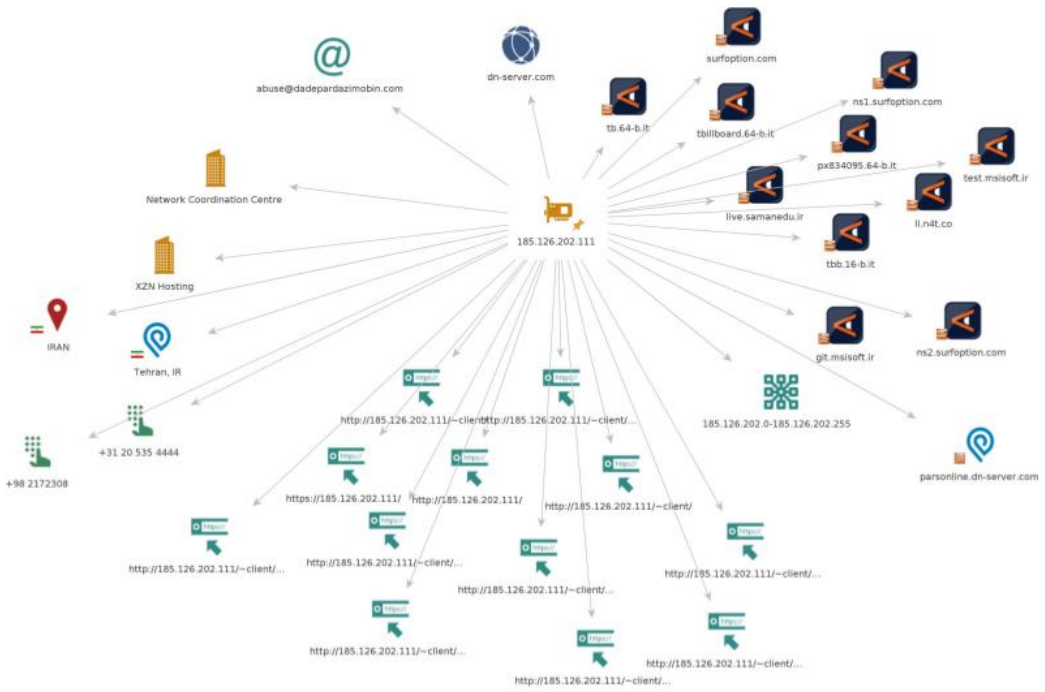


Imagen 169. Recolección de información del IoC 185.126.202[.]111

Ahora nos centramos en la dirección IP 23.95.132[.]48 (Imagen 170) sacando en claro lo siguiente:

- La dirección IP apunta a **Estados Unidos** en concreto a **Buffalo.**
- Se detectan **4 dominios** (slotsipedia.com, andyhindmarsh.com, colocrossing.com y ilivethedream2.com) que apuntan a la propia dirección IP.
- Se detectan **3 subdominios** (test.slotsipedia.com, 23-95-132-48-host.colocrossing.com y www.slotsipedia.com) que apuntan a la propia dirección IP.
- Se detectan **8 registros NS** (ns1.mbir.ir, ns2.mbir.ir, ns2.azarwebsite.com, ns1.andyhindmarsh.com, ns2.andyhindmarsh.com, ns2.ilivethedream2.com,

ns1.azarwebsite.com y ns1.ilivethedream2.com) que apuntan a la propia dirección IP.

- Se detectan **2 servidores de correo** (mail.andyhindmarsh.com y mail.slotsipedia.com) que apuntan a la propia dirección IP.
- La dirección IP está asociada al **rango IP** 23.95.128.0-23.95.159.255.
- Es detectada **una compañía relacionada** (Colocrossing).
- Son detectados **dos números de teléfono** (+1 800 518 9716 y 1-800-518-9716).
- Son detectadas **12 URLs** que han dado positivo en algún motor antivirus debido a actividad maliciosa.
- Son detectadas **13 muestras de malware.**
- Es detectado **un correo electrónico** (abuse@colocrossing.com).
- Son detectados perfiles creados en las siguientes redes sociales: LinkedIn, Facebook y Twitter
- Es detectado un **certificado SSL** asociado a la dirección IP con el hash 080a59a1609de3f55e23d9cb075d507f8c3694ecfc4802e9a5e0c7b5ab439043. 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 23.95.132.48, la organización asociada es AliReza y dicho certificado es válido hasta el 19 de mayo de 2028. En la Imagen 171 puede visualizarse la información del certificado extraído.

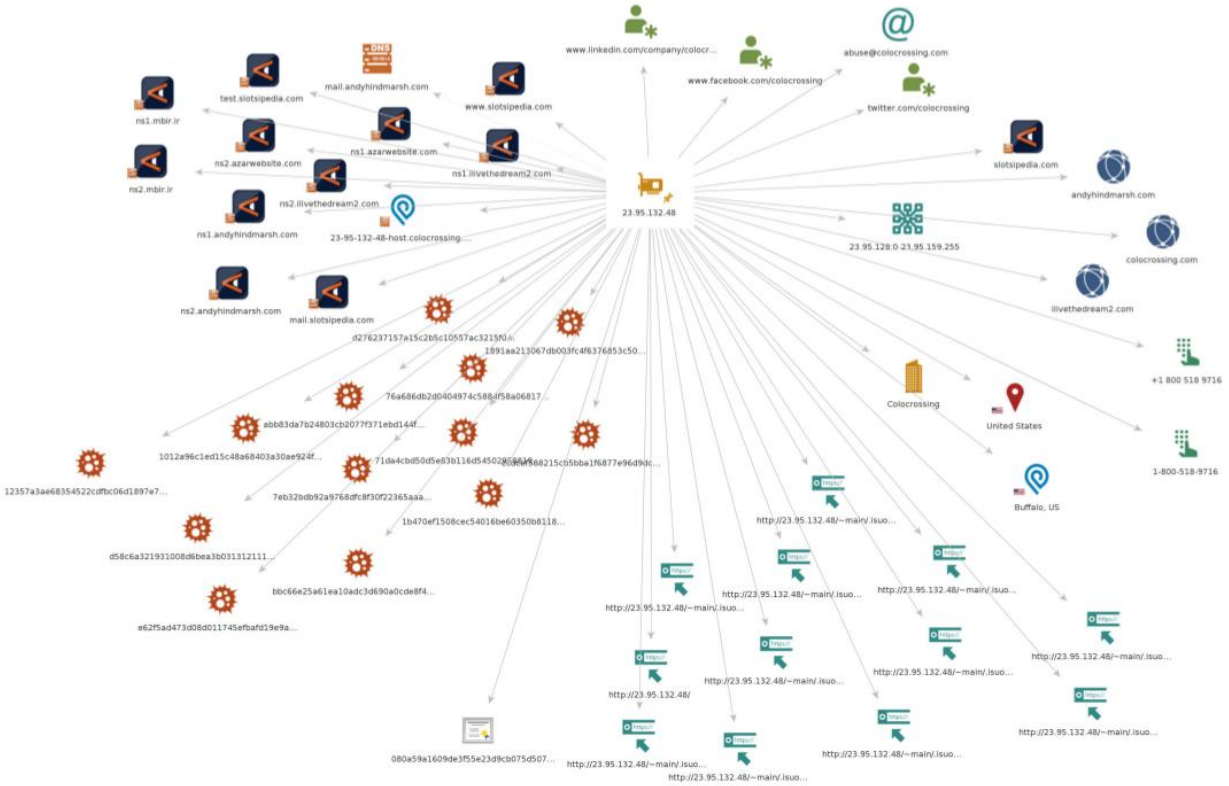


Imagen 170. Recolección de información del IoC 23-95-132[.]48

Imagen 171. Información del certificado SSL asociado al IoC 23.95.132[.]78

Podemos concluir que ambas direcciones IP no comparten ningún tipo de dato entre sí.

4.1.6. INVESTIGACIÓN DE LOS DOMINIOS DETECTADOS

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 puede ser visualizados en la Imagen 172 a través de las relaciones existentes entre dichos dominios.

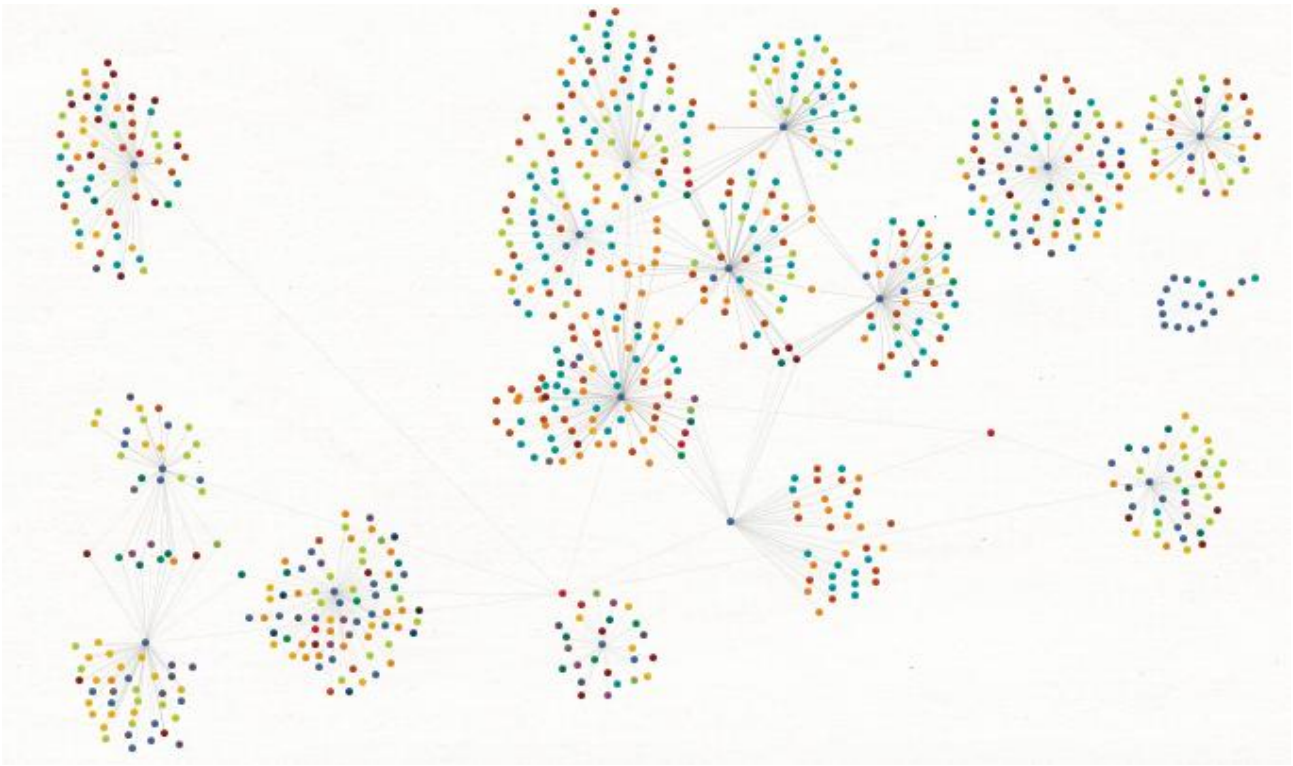


Imagen 172. Relaciones globales existentes entre los diferentes dominios asociados con SilverTerrier

Debido a la gran volumetría de datos obtenidos de los 17 dominios, tal como puede visualizarse en la imagen superior, vamos a centrarnos en las relaciones directas entre los diferentes dominios. El grafo resultante puede ser visualizado en la Imagen 173.

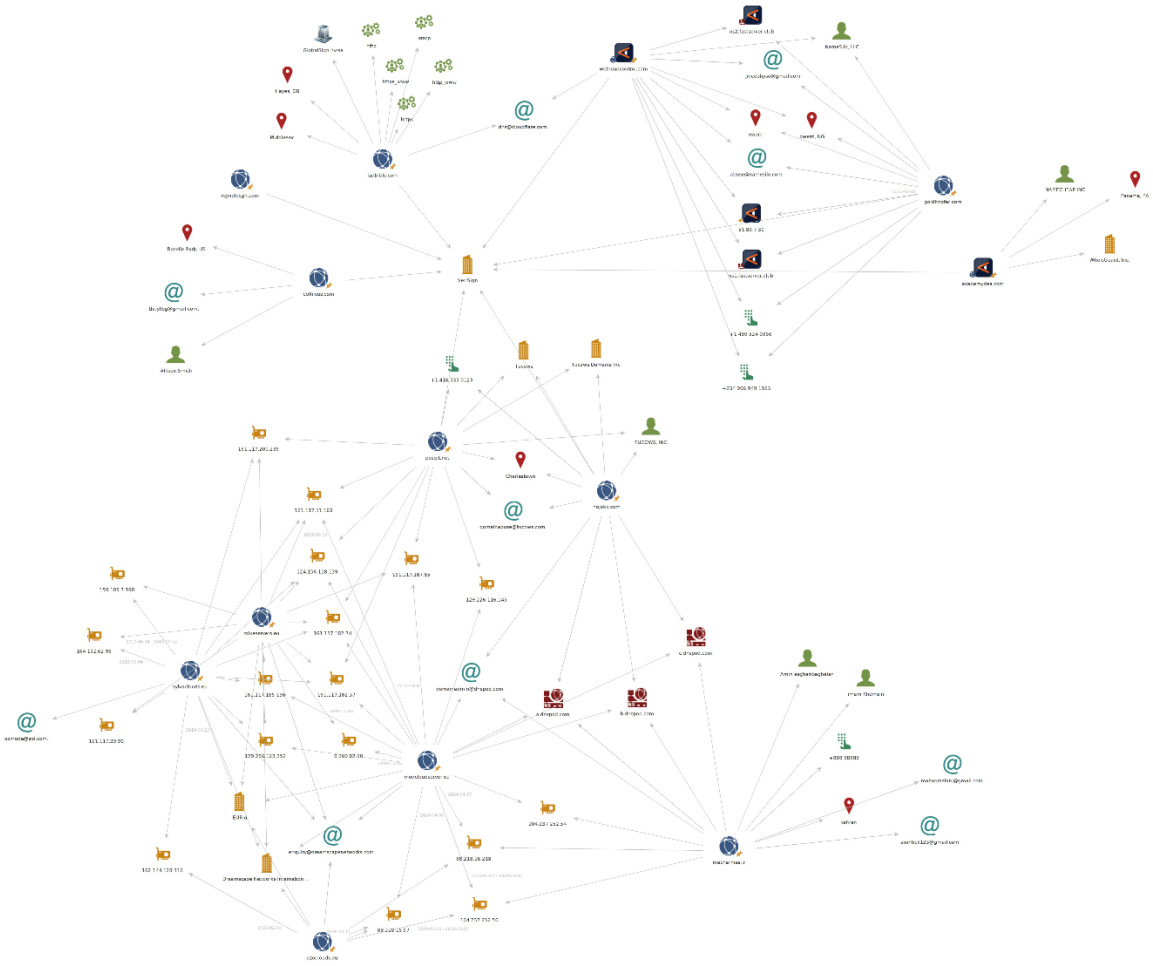
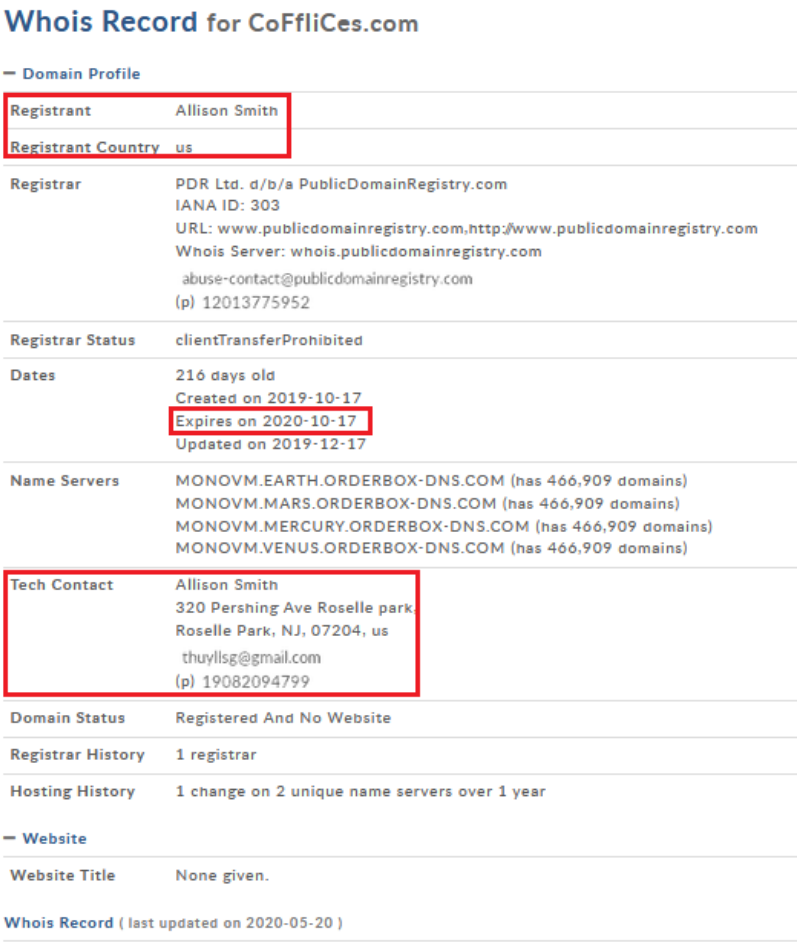


Imagen 173. Relaciones directas entre los dominios

Si analizamos en conjunto todo el grafo podemos sacar en claro las siguientes relaciones por cada uno de los dominios:

- coffiices.com:
    - El dominio comparte el proveedor de dominios **VeriSign** junto a otros **7 dominios** (reynoldsgh.com, ladbible.com, goldhhofer.com, academydea.com, hojokk.com, welheadcontrol.com y posqit.net).
    - A través de otra herramienta (DomainTools) se corrobora que el propio dominio está registrado en **Estados Unidos** por medio de Allison Smith,

además su **registro expira el 20 de octubre de 2020**. Lo mencionado puede visualizarse en la Imagen 174.



Whois Record for CoFfliCes.com

– Domain Profile

Registrant	Allison Smith
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	clientTransferProhibited
Dates	216 days old Created on 2019-10-17 Expires on 2020-10-17 Updated on 2019-12-17
Name Servers	MONOVM.EARTH.ORDERBOX-DNS.COM (has 466,909 domains) MONOVM.MARS.ORDERBOX-DNS.COM (has 466,909 domains) MONOVM.MERCURY.ORDERBOX-DNS.COM (has 466,909 domains) MONOVM.VENUS.ORDERBOX-DNS.COM (has 466,909 domains)
Tech Contact	Allison Smith 320 Pershing Ave Roselle park Roselle Park, NJ, 07204, us thuyllsg@gmail.com (p) 19082094799
Domain Status	Registered And No Website
Registrar History	1 registrar
Hosting History	1 change on 2 unique name servers over 1 year

– Website

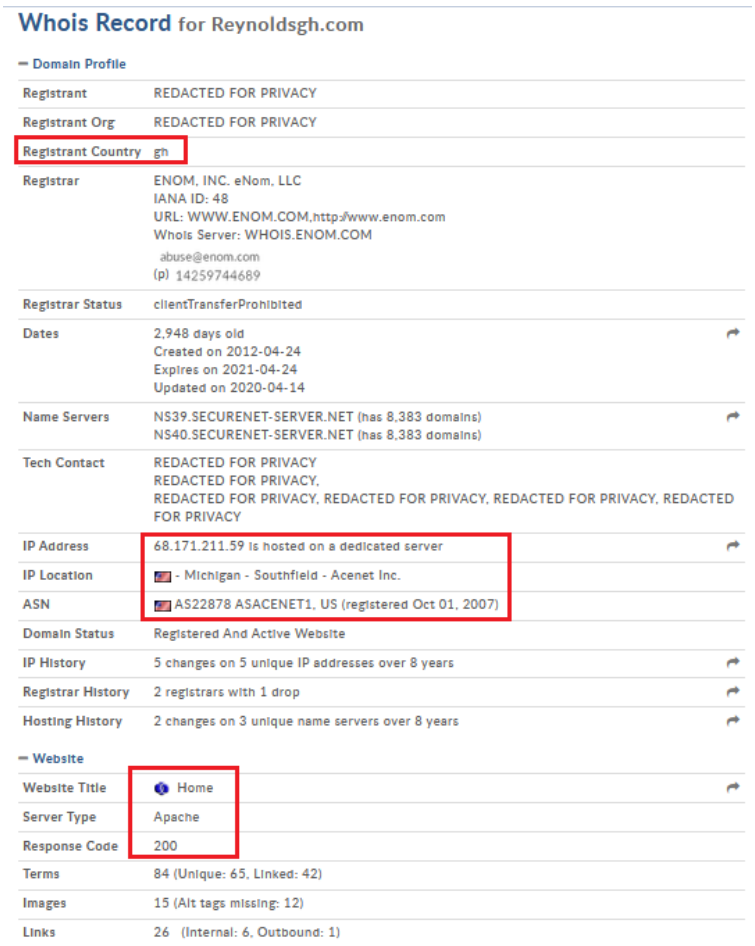
Website Title	None given.

Whois Record (last updated on 2020-05-20)

Imagen 174. Whois del dominio coffiices.com

- reynoldsgh.com
  - El dominio comparte el proveedor de dominios **VeriSign** junto a otros **7 dominios** analizados de partida (coffiices.com, ladbible.com, goldhhofer.com, academydea.com, hojokk.com, welheadcontrol.com y posqit.net).
  - A través de otra herramienta (DomainTools) es detectada la **dirección IP** a la que apunta el dominio actualmente (68.171.211.59), su **ASN asociado** (AS22878), **el país del registrante** (gh - Ghana), s**u geolocalización**

(Michigan – Southfield, Estados Unidos) y que su **registro expira el 24 de abril de 2021**. Lo mencionado puede visualizarse en la Imagen 175.



Whois Record for Reynoldsgh.com

Domain Profile

Registrant	REDACTED FOR PRIVACY
Registrant Org	REDACTED FOR PRIVACY
Registrant Country	gh
Registrar	ENOM, INC. eNom, LLC IANA ID: 48 URL: WWW.ENOM.COM,http://www.enom.com Whois Server: WHOIS.ENOM.COM abuse@enom.com (p) 14259744689
Registrar Status	clientTransferProhibited
Dates	2,948 days old Created on 2012-04-24 Expires on 2021-04-24 Updated on 2020-04-14
Name Servers	NS39.SECURENET-SERVER.NET (has 8,383 domains) NS40.SECURENET-SERVER.NET (has 8,383 domains)
Tech Contact	REDACTED FOR PRIVACY REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY
IP Address	68.171.211.59 is hosted on a dedicated server
IP Location	- Michigan - Southfield - Acenet Inc.
ASN	AS22878 ASACENET1, US (registered Oct 01, 2007)
Domain Status	Registered And Active Website
IP History	5 changes on 5 unique IP addresses over 8 years
Registrar History	2 registrars with 1 drop
Hosting History	2 changes on 3 unique name servers over 8 years

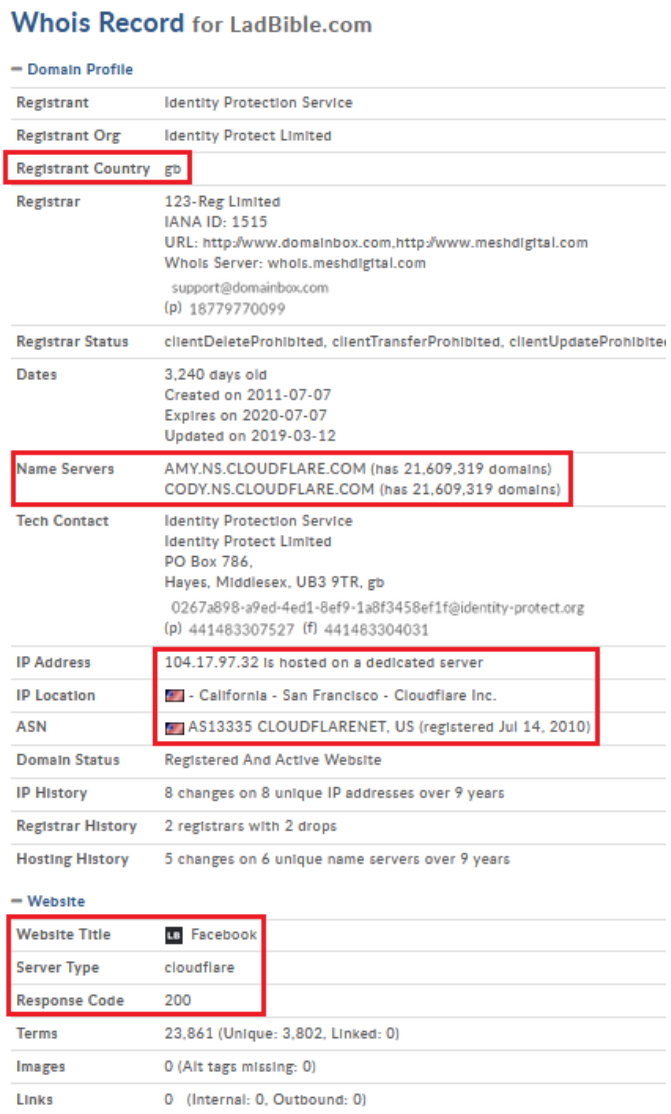
Website

Website Title	Home
Server Type	Apache
Response Code	200
Terms	84 (Unique: 65, Linked: 42)
Images	15 (Alt tags missing: 12)
Links	26 (Internal: 6, Outbound: 1)

Imagen 175. Whois del dominio reynoldsgh.com

- ladbible.com
  - El dominio comparte el proveedor de dominios **VeriSign** junto a otros **7 dominios** analizados de partida (coffiices.com, reynoldsgh.com, goldhhofer.com, academydea.com, hojokk.com, welheadcontrol.com y posqit.net).

- El dominio tiene asociado un **correo electrónico** (dns@cloudflare.com) que comparte con **welheadcontrol.com**. Esto indica que existe alguna vinculación con el proveedor de Cloudflare por parte de ambos dominios.
- Son detectados 3 servicios expuestos a Internet (HTTP, HTTPS y SMTP).
- A través de otra herramienta (DomainTools) es detectada la **dirección IP** a la que apunta el dominio actualmente (104.17.97.32), su **ASN asociado** (AS13335), un **CDN** (Cloudflare), **el país del registrante** (gb – Reino Unido), **su geolocalización** (California, Estados Unidos) y la **expiración del registro el 07 de julio de 2020**. Lo mencionado puede visualizarse en la Imagen 176.



Whois Record for LadBible.com

Domain Profile

Registrant	Identity Protection Service
Registrant Org	Identity Protect Limited
Registrant Country	gb
Registrar	123-Reg Limited IANA ID: 1515 URL: http://www.domainbox.com,http://www.meshdigital.com Whois Server: whois.meshdigital.com support@domainbox.com (p) 18779770099
Registrar Status	clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibite
Dates	3,240 days old Created on 2011-07-07 Expires on 2020-07-07 Updated on 2019-03-12
Name Servers	AMY.NS.CLOUDFLARE.COM (has 21,609,319 domains) CODY.NS.CLOUDFLARE.COM (has 21,609,319 domains)
Tech Contact	Identity Protection Service Identity Protect Limited PO Box 786, Hayes, Middlesex, UB3 9TR, gb 0267a898-a9ed-4ed1-8ef9-1a8f3458ef1f@identity-protect.org (p) 441483307527 (f) 441483304031
IP Address	104.17.97.32 is hosted on a dedicated server
IP Location	- California - San Francisco - Cloudflare Inc.
ASN	AS13335 CLOUDFLARENET, US (registered Jul 14, 2010)
Domain Status	Registered And Active Website
IP History	8 changes on 8 unique IP addresses over 9 years
Registrar History	2 registrars with 2 drops
Hosting History	5 changes on 6 unique name servers over 9 years

Website

Website Title	Facebook
Server Type	cloudflare
Response Code	200
Terms	23,861 (Unique: 3,802, Linked: 0)
Images	0 (Alt tags missing: 0)
Links	0 (Internal: 0, Outbound: 0)

Imagen 176. Whois del dominio ladbible.com

- welheadcontrol.com
  - El dominio comparte el proveedor de dominios VeriSign junto a otros **7 dominios** analizados de partida (coffiices.com, reynoldsgh.com, goldhhofer.com, academydea.com, hojokk.com, ladbible.com y posqit.net). Además, este dominio comparte **proveedor de dominios** (NameSilo) con el dominio **goldhhofer.com**, junto a otro **correo electrónico relacionado con dicho proveedor** (abuse@namesilo.com).

- El dominio tiene asociado **un correo electrónico** (dns@cloudflare.com) que comparte con **ladbible.com**. Esto indica que existe alguna vinculación con un CDN (Cloudflare) por parte de ambos dominios. Este dominio dispone de otra relación por medio de un **correo electrónico** (jincephyso@gmail.com) con el dominio **goldhhofer.com.**

- Comparte **dos números de teléfono** con el dominio **goldhhofer.com**, uno asociado al proveedor de dominios NameSilo y otro al contacto técnico, en este caso Black Emeka.

- Es detectada una **relación con el dominio goldhhofer.com** por medio de dos **servidores NS** y una **dirección IP**. Analizando el histórico de las direcciones IP asociadas al dominio podemos ver que en un instante de tiempo en el pasado apuntó a la **dirección IP** (51.89.7.30) detectada en Maltego. En la Imagen 177 puede verse lo mencionado.

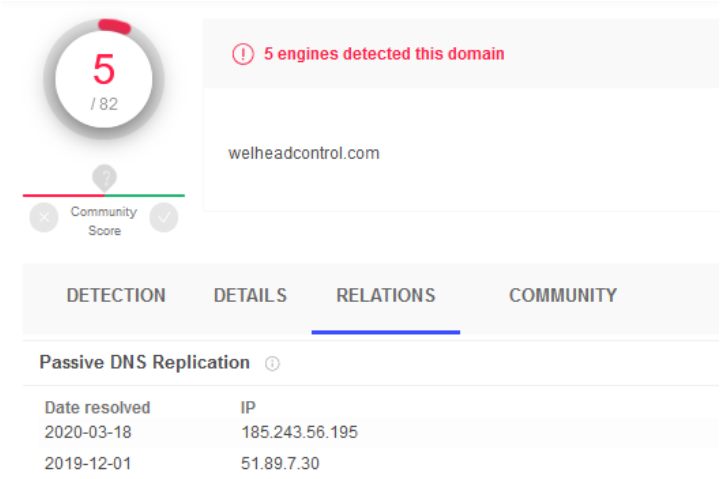
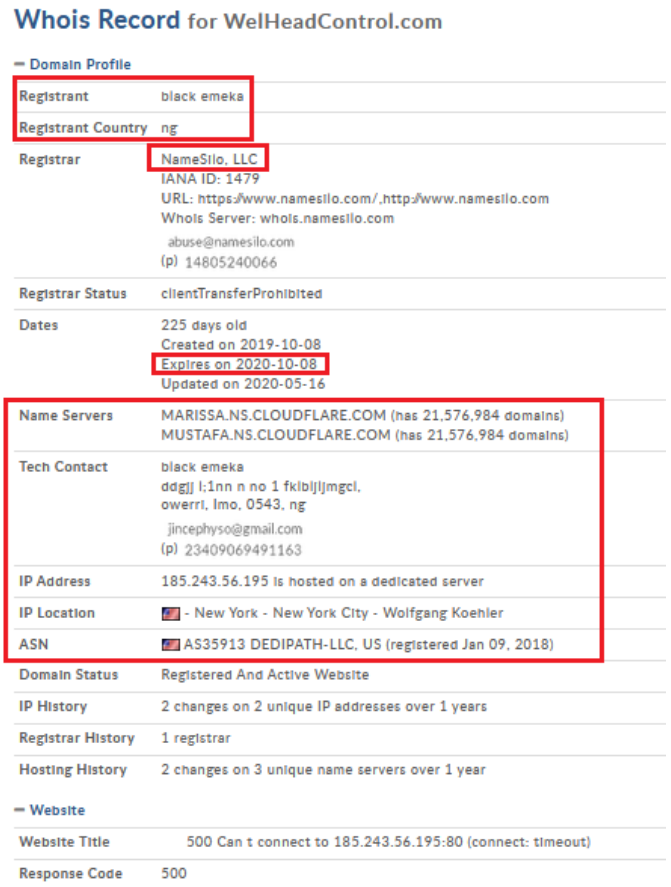


Imagen 177. Dirección IP obtenida mediante el histórico del dominio con VirusTotal

- A través de otra herramienta (DomainTools) es detectada la **dirección IP a la que apunta el dominio actualmente** (185.243.56.195), su **ASN asociado** (AS35913), el **CDN utilizado** (Cloudflare), **su registrante** (Black

Emeka), **el país del registrante** (ng – Nigeria), **su geolocalización** (Nueva York, Estados Unidos) y **la expiración del registro el 08 de octubre de 2020**. Lo mencionado puede visualizarse en la Imagen 178.



Whois Record for WelHeadControl.com

– Domain Profile

Registrant	black emeka
Registrant Country	ng
Registrar	NameSilo, LLC IANA ID: 1479 URL: https://www.namesilo.com/,http://www.namesilo.com Whois Server: whois.namesilo.com abuse@namesilo.com (p) 14805240066
Registrar Status	clientTransferProhibited
Dates	225 days old Created on 2019-10-08 Expires on 2020-10-08 Updated on 2020-05-16
Name Servers	MARISSA.NS.CLOUDFLARE.COM (has 21,576,984 domains) MUSTAFA.NS.CLOUDFLARE.COM (has 21,576,984 domains)
Tech Contact	black emeka ddgjj l;1nn n no 1 fkibijjmgcl, owerri, imo, 0543, ng jincephyso@gmail.com (p) 23409069491163
IP Address	185.243.56.195 is hosted on a dedicated server
IP Location	- New York - New York City - Wolfgang Koehler
ASN	AS35913 DEDIPATH-LLC, US (registered Jan 09, 2018)
Domain Status	Registered And Active Website
IP History	2 changes on 2 unique IP addresses over 1 years
Registrar History	1 registrar
Hosting History	2 changes on 3 unique name servers over 1 year

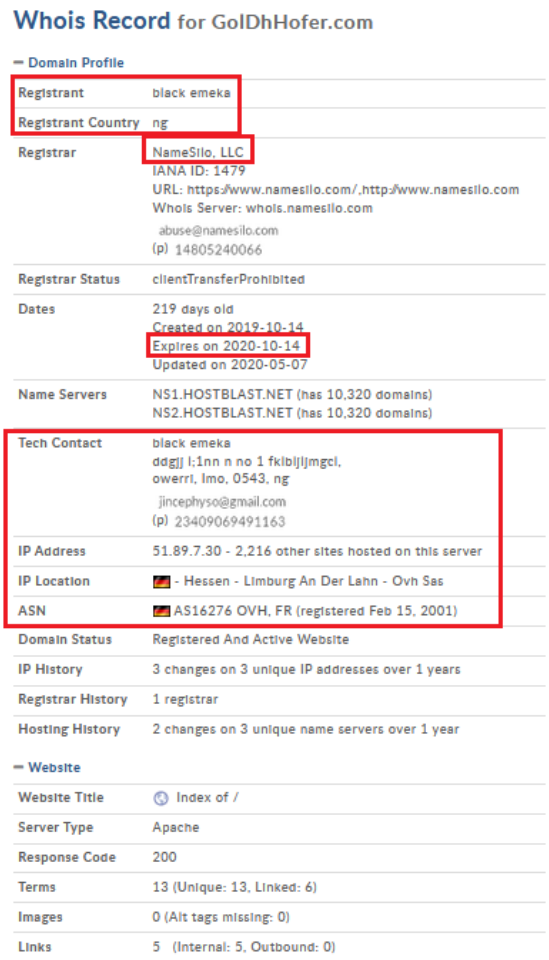
– Website

Website Title	500 Can t connect to 185.243.56.195:80 (connect: timeout)
Response Code	500

Imagen 178. Whois del dominio welheadcontrol.com

- goldhhofer.com
    - El dominio comparte el proveedor de dominios **VeriSign** junto a otros **7 dominios** analizados de partida (coffiices.com, reynoldsgh.com, welheadcontrol.com, academydea.com, hojokk.com, ladbible.com y posqit.net). Además, este dominio comparte proveedor de dominios (NameSilo) con el dominio **welheadcontrol.com**, junto a otro **correo relacionado con dicho proveedor** (abuse@namesilo.com).

- El dominio tiene asociado **un correo electrónico** (jincephyso@gmail.com) que comparte con el dominio **welheadcontrol.com.**
- Comparte dos números de teléfono con el dominio welheadcontrol.com, uno asociado al proveedor de dominios NameSilo y otro al contacto técnico, en este caso Black Emeka.
- Es detectada una **relación con el dominio welheadcontrol.com** por medio de dos **servidores NS** y una **dirección IP.**
- A través de otra herramienta (DomainTools) es detectada la **dirección IP** a la que apunta el dominio actualmente (51.89.7.30), **su ASN asociado** (AS16276), **su registrante** (Black Emeka), **el país del registrante** (ng – Nigeria), **su geolocalización** (Hessen - Limburg An Der Lahn, Alemania) y que **su registro expira el 14 de octubre de 2020**. Lo mencionado puede visualizarse en la Imagen 179.



Whois Record for GolDhHofer.com

Domain Profile

Registrant	black emeka
Registrant Country	ng
Registrar	NameSilo, LLC IANA ID: 1479 URL: https://www.namesilo.com/,http://www.namesilo.com Whois Server: whois.namesilo.com abuse@namesilo.com (p) 14805240066
Registrar Status	clientTransferProhibited
Dates	219 days old Created on 2019-10-14 Expires on 2020-10-14 Updated on 2020-05-07
Name Servers	NS1.HOSTBLAST.NET (has 10,320 domains) NS2.HOSTBLAST.NET (has 10,320 domains)
Tech Contact	black emeka ddgjj l;1nn n no 1 fkibijjmgcl, owerri, Imo, 0543, ng jincephyso@gmail.com (p) 23409069491163
IP Address	51.89.7.30 - 2,216 other sites hosted on this server
IP Location	- Hessen - Limburg An Der Lahn - Ovh Sas
ASN	AS16276 OVH, FR (registered Feb 15, 2001)
Domain Status	Registered And Active Website
IP History	3 changes on 3 unique IP addresses over 1 years
Registrar History	1 registrar
Hosting History	2 changes on 3 unique name servers over 1 year

Website

Website Title	Index of /
Server Type	Apache
Response Code	200
Terms	13 (Unique: 13, Linked: 6)
Images	0 (Alt tags missing: 0)
Links	5 (Internal: 5, Outbound: 0)

Imagen 179. Whois del dominio goldhhofer.com

- academydea.com
    - El dominio comparte el proveedor de dominios **VeriSign** junto a otros **7 dominios** analizados de partida (coffiices.com, reynoldsgh.com, welheadcontrol.com, goldhhofer.com, hojokk.com, ladbible.com y posqit.net).

- A través de otra herramienta (DomainTools) es detectada la **dirección IP** a la que apunta el dominio actualmente (165.227.16.98), **su ASN asociado** (AS14061), **su registrante** (WhoisGuard Protected), **el país del registrante** (pa - Panama), **su geolocalización** (Nueva York, Estados Unidos) y **la expiración del registro el 25 de agosto de 2020**. Lo mencionado puede visualizarse en la Imagen 180.

Whois Record for AcademyDea.com

– Domain Profile

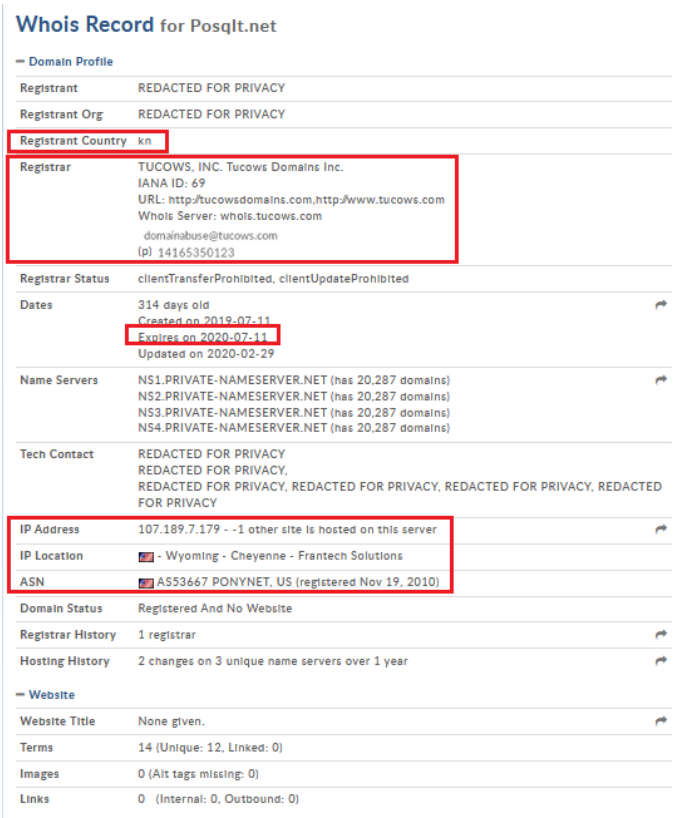
Registrant	WhoisGuard Protected
Registrant Org	WhoisGuard, Inc.
Registrant Country	pa
Registrar	NAMECHEAP INC NameCheap, Inc. IANA ID: 1068 URL: http://www.namecheap.com Whois Server: whois.namecheap.com abuse@namecheap.com (p) 16613102107
Registrar Status	clientTransferProhibited
Dates	269 days old Created on 2019-08-25 Expires on 2020-08-25 Updated on 0000-12-31
Name Servers	NS1.MOGULBOUND.IO (has 33 domains) NS2.MOGULBOUND.IO (has 33 domains) NS3.MOGULBOUND.IO (has 33 domains)
Tech Contact	WhoisGuard Protected WhoisGuard, Inc. P.O. Box 0823-03411, Panama, Panama, pa f749919287204eeab27693ae97780808.protect@whoisguard.com (p) 5078365503 (f) 5117057182
IP Address	165.227.16.98 - 25 other sites hosted on this server
IP Location	- New York - New York City - Digitalocean Llc
ASN	AS14061 DIGITALOCEAN-ASN, US (registered Sep 25, 2012)
Domain Status	Registered And Active Website
IP History	17 changes on 17 unique IP addresses over 12 years
Registrar History	5 registrars with 4 drops
Hosting History	13 changes on 9 unique name servers over 15 years

– Website

Website Title	500 SSL negotiation failed:
Response Code	500

Imagen 180. Whois del dominio academydea.com

- posqit.net
    - El dominio comparte el proveedor de dominios **VeriSign** junto a otros **7 dominios** analizados de partida (coffiices.com, reynoldsgh.com, welheadcontrol.com, goldhhofer.com, hojokk.com, ladbible.com y academydea.com).
    - El dominio tiene **diferentes tipos de relaciones con hojokk.com**, son los siguientes:
        - **Una empresa** (TUCOWS, INC) y **un correo electrónico** (domainabuse@tucows.com) asociado a dicha empresa
        - **Un número de teléfono**
        - **Una geolocalización** (Charlestown)
    - El dominio está relacionado con mikeservers.eu, sylvaclouds.eu y modcloudserver.eu por medio de **7 direcciones IP.**
    - A través de otra herramienta (DomainTools) es detectada la **dirección IP** a la que apunta el dominio actualmente (107.189.7.179), **su ASN asociado** (AS53667), **el país del registrante** (kn – Corea del Norte), **su geolocalización** (Wyoming - Cheyenne, Estados Unidos) y que **su registro expira el 11 de julio de 2020**. Lo mencionado puede visualizarse en la Imagen 181.



Whois Record for Posqlt.net

Domain Profile

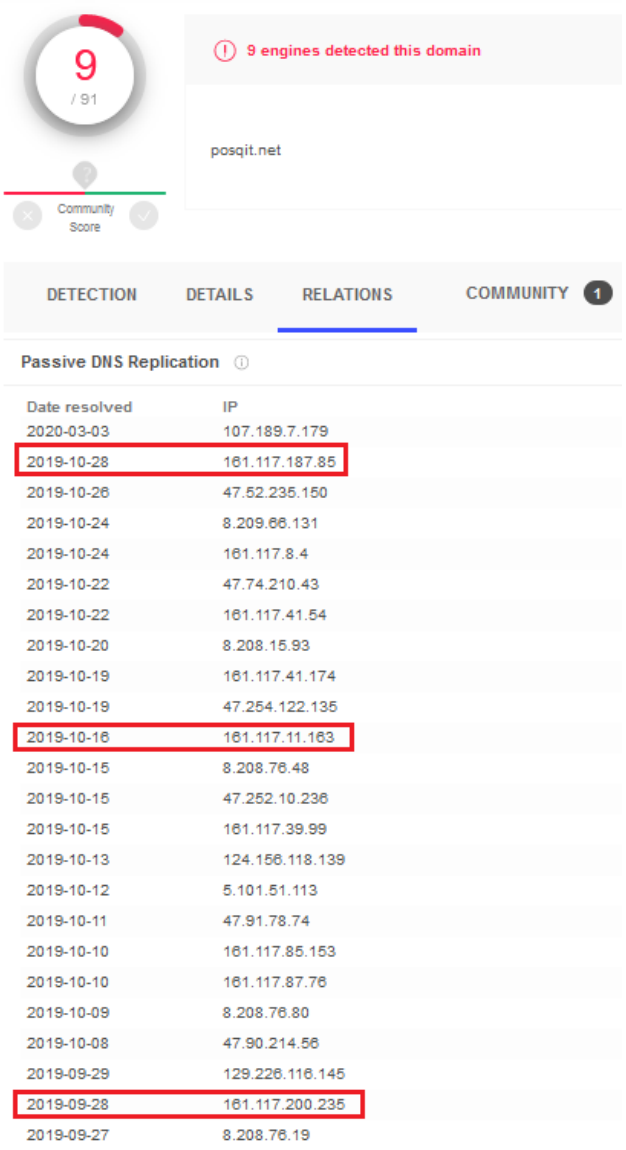
Registrant	REDACTED FOR PRIVACY
Registrant Org	REDACTED FOR PRIVACY
Registrant Country	kn
Registrar	TUCOWS, INC. Tucows Domains Inc. IANA ID: 69 URL: http://tucowsdomains.com,http://www.tucows.com Whois Server: whois.tucows.com domainabuse@tucows.com (p) 14165350123
Registrar Status	clientTransferProhibited, clientUpdateProhibited
Dates	314 days old Created on 2019-07-11 Expires on 2020-07-11 Updated on 2020-02-29
Name Servers	NS1.PRIVATE-NAMESERVER.NET (has 20,287 domains) NS2.PRIVATE-NAMESERVER.NET (has 20,287 domains) NS3.PRIVATE-NAMESERVER.NET (has 20,287 domains) NS4.PRIVATE-NAMESERVER.NET (has 20,287 domains)
Tech Contact	REDACTED FOR PRIVACY REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY
IP Address	107.189.7.179 - -1 other site is hosted on this server
IP Location	- Wyoming - Cheyenne - Frantech Solutions
ASN	AS53667 PONYNET, US (registered Nov 19, 2010)
Domain Status	Registered And No Website
Registrar History	1 registrar
Hosting History	2 changes on 3 unique name servers over 1 year

Website

Website Title	None given.
Terms	14 (Unique: 12, Linked: 0)
Images	0 (Alt tags missing: 0)
Links	0 (Internal: 0, Outbound: 0)

Imagen 181. Whois del dominio posqit.net

- Analizando el histórico de las direcciones IP asociadas al dominio podemos ver que en un instante de tiempo en el pasado apuntó a las **7 direcciones IP** detectadas en Maltego. En la Imagen 182 pueden visualizarse algunas de las coincidencias.



Date resolved	IP
2020-03-03	107.189.7.179
2019-10-28	161.117.187.85
2019-10-26	47.52.235.150
2019-10-24	8.209.66.131
2019-10-24	161.117.8.4
2019-10-22	47.74.210.43
2019-10-22	161.117.41.54
2019-10-20	8.208.15.93
2019-10-19	161.117.41.174
2019-10-19	47.254.122.135
2019-10-16	161.117.11.163
2019-10-15	8.208.76.48
2019-10-15	47.252.10.236
2019-10-15	161.117.39.99
2019-10-13	124.156.118.139
2019-10-12	5.101.51.113
2019-10-11	47.91.78.74
2019-10-10	161.117.85.153
2019-10-10	161.117.87.76
2019-10-09	8.208.76.80
2019-10-08	47.90.214.56
2019-09-29	129.226.116.145
2019-09-28	161.117.200.235
2019-09-27	8.208.76.19

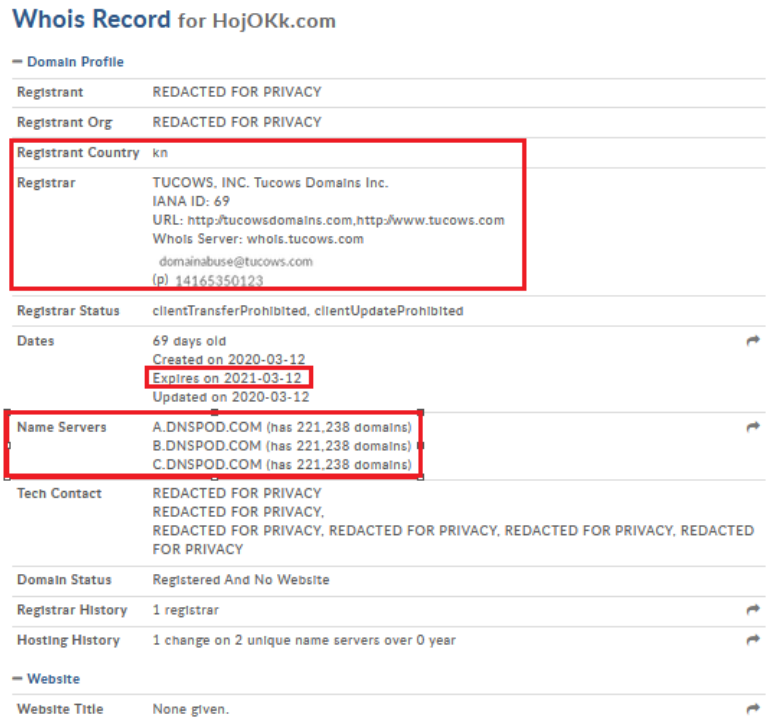
Imagen 182. Histórico de direcciones IP asociadas al dominio posqit.net

- hojokk.com
    - El dominio comparte el proveedor de dominios **VeriSign** junto a otros **7 dominios** analizados de partida (coffiices.com, reynoldsgh.com, welheadcontrol.com, goldhhofer.com, posqit.net, ladbible.com y academydea.com).
    - El dominio tiene **diferentes tipos de relaciones con posqit.net** siendo los siguientes:

- **Una empresa** (TUCOWS, INC) y **un correo electrónico** (domainabuse@tucows.com) asociado a dicha empresa.
- **Un número de teléfono.**
- **Una geolocalización** (Charlestown).

- Relacionado con los dominios modcloudserver.eu y mecharnise.ir por medio de un correo (domainadmin@dnspod.com) y tres registros NS (a.dnspod.com, b.dnspod.com y c.dnspod.com).

- A través de otra herramienta (DomainTools) es detectado el **país del registrante** (kn – Corea del Norte) y **la expiración del registro el 12 de marzo de 2021**. Lo mencionado puede visualizarse en la Imagen 183.



Whois Record for HojOKk.com

Domain Profile

Registrant	REDACTED FOR PRIVACY
Registrant Org	REDACTED FOR PRIVACY
Registrant Country	kn
Registrar	TUCOWS, INC. Tucows Domains Inc. IANA ID: 69 URL: http://tucowsdomains.com,http://www.tucows.com Whois Server: whois.tucows.com domainabuse@tucows.com (p) 14165350123
Registrar Status	clientTransferProhibited, clientUpdateProhibited
Dates	69 days old Created on 2020-03-12 Expires on 2021-03-12 Updated on 2020-03-12
Name Servers	A.DNSPOD.COM (has 221,238 domains) B.DNSPOD.COM (has 221,238 domains) C.DNSPOD.COM (has 221,238 domains)
Tech Contact	REDACTED FOR PRIVACY REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY
Domain Status	Registered And No Website
Registrar History	1 registrar
Hosting History	1 change on 2 unique name servers over 0 year

Website

Website Title	None given.

Imagen 183. Whois del dominio hojokk.com

- mikeservers.eu
    - El dominio comparte relación con EURid y el proveedor Singapur Dreamscape Networks International Pte Ltd junto a otros tres dominios analizados de partida (sylvaclouds.eu, uzoclouds.eu y modcloudserver.eu).
    - El dominio está relacionado con posqit.net, sylvaclouds.eu y modcloudserver.eu por medio de 11 direcciones IP en total.
    - El dominio tiene asociado un correo electrónico (enquiry@dreamscapenetworks.com) que comparte con tres dominios (sylvaclouds.eu, modcloudserver.eu y uzoclouds.eu).
    - A través de otra herramienta (DomainTools) es detectado únicamente el registrante (Dreamscape Networks International Pte Ltd) y los registros NS. Lo mencionado puede visualizarse en la Imagen 184.

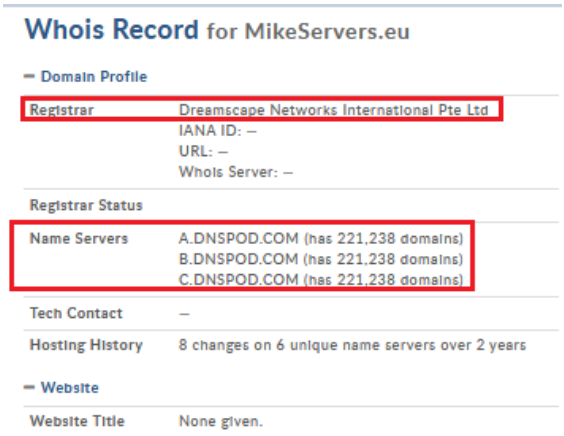


Imagen 184. Whois del dominio mikeservers.eu

- sylvaclouds.eu
    - El dominio comparte relación con EURid y el proveedor Singapur Dreamscape Networks International Pte Ltd junto a otros tres dominios analizados de partida (mikeservers.eu, uzoclouds.eu y modcloudserver.eu).

- El dominio está relacionado con posqit.net, mikeservers.eu y modcloudserver.eu por medio de 11 direcciones IP en total.
- El dominio tiene asociado un correo electrónico (enquiry@dreamscapenetworks.com) que comparte con tres dominios (mikeservers.eu, modcloudserver.eu y uzoclouds.eu).
- A través de otra herramienta (DomainTools) es detectada la dirección IP a la que apunta el dominio actualmente (162.214.75.129), su ASN asociado (AS46606) y su geolocalización (Utah, Estados Unidos). Lo mencionado puede visualizarse en la Imagen 185.

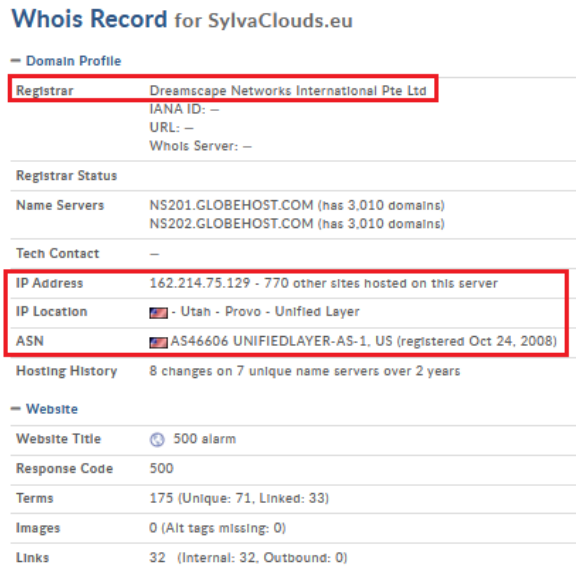


Imagen 185. Whois del dominio sylvaclouds.eu

- modcloudserver.eu
  - El dominio comparte relación con EURid y el proveedor Singapur Dreamscape Networks International Pte Ltd junto a otros tres dominios analizados de partida (mikeservers.eu, uzoclouds.eu y sylvaclouds.eu).

- Dispone de relación con los dominios posqit.net, sylvaclouds.eu, uzoclouds.eu, mikeservers.eu y mecharnise.ir por medio de 13 direcciones IP en total.
- El dominio tiene asociado un correo electrónico (enquiry@dreamscapenetworks.com) que comparte con tres dominios (sylvaclouds.eu, modcloudserver.eu y uzoclouds.eu).
- Relacionado con los dominios hojokk.com y mecharnise.ir por medio de un correo (domainadmin@dnspod.com) y tres registros NS (a.dnspod.com, b.dnspod.com y c.dnspod.com).
- A través de otra herramienta (DomainTools) es detectada la dirección IP a la que apunta el dominio actualmente (88.218.16.57), su ASN asociado (AS50673), su registrante (Dreamscape Networks International Pte Ltd) y su geolocalización (Flevoland – Dronten, Holanda). Lo mencionado puede visualizarse en la Imagen 186.

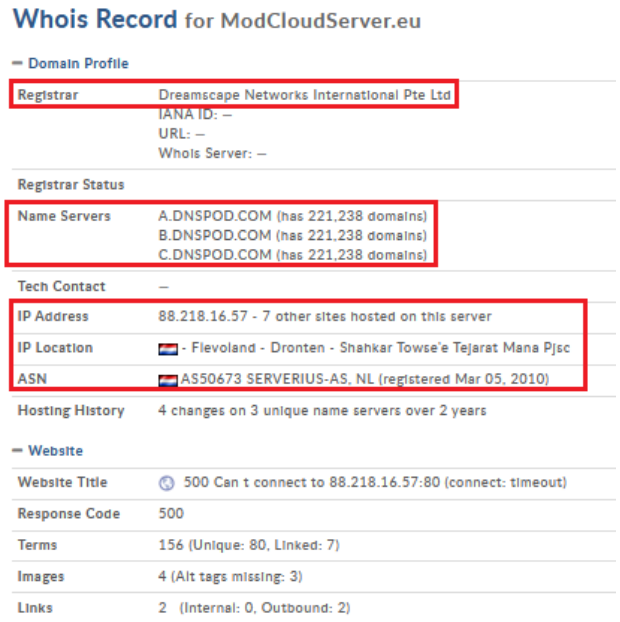
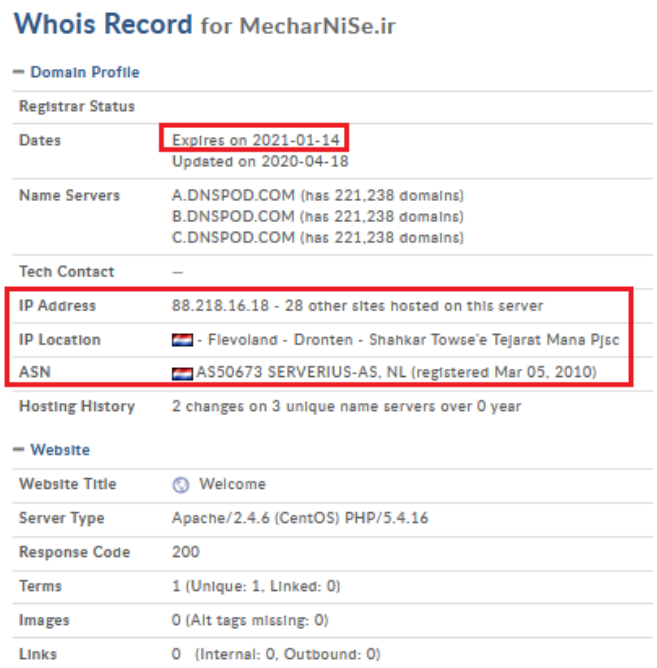


Imagen 186. Whois del dominio modcloudserver.eu

- mecharnise.ir
    - Dispone de relación con los dominios modcloudserver.eu y uzoclouds.eu por medio de cuatro direcciones IP en total.
    - Relacionado con los dominios hojokk.com y modcloudserver.eu por medio de un correo (domainadmin@dnspod.com) y tres registros NS (a.dnspod.com, b.dnspod.com y c.dnspod.com).
    - A través de otra herramienta (DomainTools) es detectada la dirección IP a la que apunta el dominio actualmente (88.218.16.18), su ASN asociado (AS50673), su geolocalización (Flevoland – Dronten, Holanda) y la expiración del registro el 14 de enero de 2021. Lo mencionado puede visualizarse en la Imagen 187.



Whois Record for MecharNiSe.ir

Domain Profile	
Registrar Status	
Dates	Expires on 2021-01-14 Updated on 2020-04-18
Name Servers	A.DNSPOD.COM (has 221,238 domains) B.DNSPOD.COM (has 221,238 domains) C.DNSPOD.COM (has 221,238 domains)
Tech Contact	–
IP Address	88.218.16.18 - 28 other sites hosted on this server
IP Location	- Flevoland - Dronten - Shahkar Towse'e Tejarat Mana Pjsc
ASN	AS50673 SERVERIUS-AS, NL (registered Mar 05, 2010)
Hosting History	2 changes on 3 unique name servers over 0 year
Website	
Website Title	Welcome
Server Type	Apache/2.4.6 (CentOS) PHP/5.4.16
Response Code	200
Terms	1 (Unique: 1, Linked: 0)
Images	0 (Alt tags missing: 0)
Links	0 (Internal: 0, Outbound: 0)

Imagen 187. Whois del dominio mecharnise.ir

- uzoclouds.eu
    - El dominio comparte relación con EURid y el proveedor Singapur Dreamscape Networks International Pte Ltd junto a otros tres dominios analizados de partida (mikeservers.eu, modcloudserver.eu y sylvaclouds.eu).
    - Dispone de relación con los dominios sylvaclouds.eu, modcloudserver.eu, mikeservers.eu y mecharnise.ir por medio de cuatro direcciones IP en total.
    - El dominio tiene asociado un correo electrónico (enquiry@dreamscapenetworks.com) que comparte con tres dominios (sylvaclouds.eu, modcloudserver.eu y modcloudserver.eu).
    - A través de otra herramienta (DomainTools) es detectada únicamente su registrante (Dreamscape Networks International Pte Ltd). Lo mencionado puede visualizarse en la Imagen 188.


Whois Record for UzoClouds.eu

Domain Profile

Registrar	Dreamscape Networks International Pte Ltd IANA ID: – URL: – Whois Server: –
Registrar Status	
Name Servers	NS1.CRAZYDOMAINS.COM (has 546,742 domains) NS2.CRAZYDOMAINS.COM (has 546,742 domains)
Tech Contact	–
Hosting History	3 changes on 3 unique name servers over 1 year

Website

Website Title	None given.

Whois Record (last updated on 2020-05-20)

Imagen 188. Whois del dominio uzoclouds.eu

Como conclusión del análisis podemos indicar lo siguiente:

- Los dominios mikeservers.eu, modcloudserver.eu y sylvaclouds.eu y uzoclouds.eu están relacionados por medio del mismo proveedor de servicios de Internet (Dreamscape Networks International Pte Ltd), el cual es originario de Singapur.

- Los dominios hojokk.com, modcloudserver.eu y mecharnise.ir comparten los mismos registros NS, lo que indica que están relacionados con la misma empresa proveedora de DNS.
- Los dominios hojokk.com y posqit.net a su vez comparten la misma empresa proveedora (TUCOWS, INC) relacionada con un portal de descarga de software. Además, el país registrante de ambos es Corea del Norte.
- Los dominios welheadcontrol.com y goldhhofer.com comparten el mismo proveedor de servicios (NameSilo), dos números de teléfono y el contacto Black Emeka que apunta a Nigeria.
- Los dominios ladbible.com y welheadcontrol.com comparten el mismo correo electrónico (dns@cloudflare.com), lo que indica que ambos disponen de CloudFlare como proveedor.
- Ocho dominios (hojokk.com, coffiices.com, reynoldsgh.com, welheadcontrol.com, goldhhofer.com, posqit.net, ladbible.com y academydea.com) comparten el mismo proveedor de servicios (VeriSign).
- En resumen, los países registrantes de los dominios detectados apuntan a Nigeria, Corea del Norte, Panamá, Ghana, Reino Unido y Estados Unidos.