Boletín Mensual Comunidades 05/2020

Dedicado a tod@s los que quieren investigar, cacharrear, aprender y colaborar. De la comunidad, para la comunidad.

Contenido

Nota de redacción

Como se puede ver en la portada del boletín, en esta ocasión participamos varias comunidades. La idea principal de esta colaboración es traer un contenido de mayor calidad para tod@s. Por ello, cada comunidad aporta su granito de arena, siendo el producto final, el conjunto de los aportes de todas las comunidades presentes.

Esta vez, hemos decidido introducir nuevos contenidos, aptos para un público mayor y no tan especializado, pero sin olvidarnos del público técnico.

Para conocer más sobre las comunidades que somos, podéis pinchar en nuestros logotipos de la portada o en el enlace al comienzo de cada sección.

Animaros como siempre a comentar si os gusta y a compartirlo en vuestras redes sociales.

Un saludo y al lio 😉

Entrevista Casimiro Nevado y Daniel Mery

Luis Diago de Aguilar – Derecho de la Red

Son las 8 de la tarde, acabamos de entrevistar a Casimiro Nevado (@pedaguitu) y Daniel Mery (@dmery), dos personas increíbles, amables y simpáticas muy comprometidas con la comunidad hacker.

Casimiro Nevado inspector de la Policía Nacional, profesor de la escuela de Ávila y coordinador del congreso de ciberseguridad C1b3rWall.

Daniel Mery, co-fundador de HackMadrid %27, Co-organizador de Madrid Haskell User Group y Project Manajer de Epsilon Hack.

Antes de hacer esta entrevista **C1b3rWallAcademy** no había sido anunciado. Pero, ahora que se ha hecho público, podemos hablar un poco más sobre ella y publicar esta primera entrevista (atent@s a futuras publicaciones y RRSS, porque habrá más 😉).

Ambos entrevistados han coincidido en muchos de los puntos a lo largo de la entrevista, y es que sí, las comunidades nos unen, nos enseñan, ayudan y evolucionan. Porque el pensamiento colaborativo, en materias como la informática o la ciberseguridad es, sin lugar a dudas, imprescindible.

Sin mayor tardanza os dejamos con la entrevista, no sin antes aclarar que está transcrita literalmente, sin interpretaciones de ningún tipo, ha sido escrita tal cual, sobre el papel, en su estricto orden, contando con las propias interacciones entre ambos entrevistados.

DDR: ***Desde el año pasado que pudimos asistir a C1b3rWall, llevamos con una pregunta, fue un evento que no nos dejó indiferentes y queremos saber, ¿qué fue lo que os motivó y lo que os hizo organizar este evento?***

Casimiro: El espíritu de C1b3rWall es sobre todo el poder aunar fuerzas con todos los actores principales en la seguridad digital y juntarnos todos en un sitio, conocernos, comenzar a trabajar juntos, plantear ideas, proyectos... Por nuestra parte como actor público, institución y cuerpo de seguridad invitar a expertos de las empresas, sector privado, asociaciones o que trabajan por libre. Interesaba juntarnos todos en un mismo lugar, compartir esas experiencias y empezar a plantear proyectos juntos. En la ciberseguridad está más que claro que o trabajamos juntos o no hacemos nada. Cualquier actor que pretenda trabajar de forma individual, no va a conseguir sus objetivos, más allá.

Esa era la idea, todos los actores que juegan un papel en esta materia, juntos y trabajando unidos.

DDR: ***¿Por qué es tan importante el unir fuerzas y colaborar juntos?***

Daniel: Empresas, comunidades, instituciones civiles o de otra índole, todos, se enfocan en un problema de distintas perspectivas, la forma de enriquecerlas es poder nutrirse unos de otros, si no, corres el riesgo de escuchar tu misma voz todo el tiempo. Precisamente el enriquecimiento consiste en ver que detrás de la ciberseguridad hay un montón de condiciones técnicas, sociales, de todo tipo que enriquece la propuesta para todos.

Casimiro: Y que es una materia tan compleja y tan difícil de abarcar por un solo actor que necesariamente hay que contar con el punto de vista de otras personas, la carencia que vas a tener tú, que es inevitable tener carencias, te la va a suplir otro experto de una asociación, de una empresa y te va a ayudar a solucionar el problema. Esa es la idea, trabajar juntos conocernos, compartir experiencias, compartir ideas e intentar ayudar al otro en las carencias que pueda tener.

DDR: ***Networking también claro.***

Casimiro: Totalmente, totalmente. El año pasado lo vimos en C1b3rWall, como empresas contactaban con estudiantes de los grados de la Universidad Autónoma o de las distintas universidades que estaban allí, como se hacían entrevistas, como nosotros conocíamos a personas que nos interesaba mucho conocer su punto de vista y luego los hemos integrado en grupos de trabajo como experto externo, en la propia escuela o en otros proyectos más operativos de las distintas unidades. Se trata de eso al final.

DDR: ***Estamos viendo la importancia de colaborar juntos y el por qué, pero, ¿de qué más formas podríamos disponer para colaborar juntos? A parte de este tipo de eventos.***

Casimiro: Pues, por ejemplo, dentro del proyecto C1b3rWall, que no es solamente el congreso que conocemos, estamos intentando abordar distintas iniciativas. Una de ellas que la vamos a presentar dentro de muy poquito que es el C1b3rWallAcademy, La escuela del CNP es una de las partes que están dentro de ese proyecto. Aquí tenemos a Daniel que es representante de otra parte, también tenemos a la parte académica de las universidades y la parte del sector privado de las empresas que van a entrar en el proyecto de la C1b3rWallAcademy.

Este es un ejemplo que va más allá del congreso, ¿otros ejemplos? Como comentaba antes, expertos que han entrado como asesores en distintos proyectos que estamos planteando nosotros dentro del cuerpo, desarrollo de herramientas, formación, etc. que están colaborando con nosotros, empresas que también quieren colaborar con nosotros en el desarrollo de herramientas, que evidentemente es muy atractivo el poder contar con un experto en investigación policial dentro de tu equipo de desarrollo de una herramienta

porque te va a dar esa perspectiva, hace falta esa perspectiva de todos los actores para poder tener un producto bueno, una herramienta, un curso formativo, cualquier cosa. Eso es lo que se ha generado tras C1b3rWall y era el objetivo de C1b3rWall.

DDR: ***Y Daniel, ¿por el lado de las comunidades?***

Daniel: Por el lado de las comunidades, sin tener intención obviamente de menospreciar nada, las comunidades tienen una gran ventaja, que es la libertad de la que gozan para plantearse sus objetivos. Nosotros no tenemos que rendir cuentas económicas, no estamos acuciados por un objetivo económico de ganancia, no pertenecemos a ninguna institución que de algún modo u otro depende de distintos factores de aprobación. Eso genera un campo muy abierto y muy descontracturado para plantear proyectos, iniciativas y de paso se pueda entender que mucha gente que participa, de cuerpos de seguridad o de empresas, pueden formar parte perfectamente, no es contradictorio.

Las comunidades quizás son el espectro más amplio que hay, porque en la empresa, tú participas si eres parte de la estructura de la empresa, por relaciones económicas, etc. Los Cuerpos del Estado también tienen determinadas relaciones y obligaciones. En cambio, las comunidades, en ese aspecto, ofrecen plena libertad, que participe gente que trabaja en corporaciones, empresas, organismos del estado, cuerpos de seguridad, en las comunidades encuentran su espacio sin ningún problema.

Casimiro: ¿Y de esa libertad? De esa libertad salen proyectos impresionantes, porque, precisamente, al no tener ataduras, te permite plantearte cualquier opción, cualquier posibilidad y eso, eso es una de las cosas que nos gusta integrar en C1b3rWall. Esa perspectiva de alguien que pertenece a una comunidad y que no tiene ningún límite en plantearse una opción, un escenario o un desarrollo, entonces, nos interesa mucho esa perspectiva más libre como dice Daniel.

DDR: ***Es un poco entonces como recuperar aquellos congresos en los que uno traía todo lo que había estado estudiando durante el año y lo presentaba allí a todo el mundo para que todos pudieran compartir y apoyar y decir a pues a mí se me ha ocurrido esto o se me ha ocurrido lo otro, o he estado trabajando en aquello y creo que podría ayudarte.***

Casimiro: Sí, una de las cosas que surgió y que fue curioso el año pasado en C1b3rWall fue que personas que estaban dentro del público, en un determinado taller, ofrecieron al ponente que estaba exponiendo una herramienta o un desarrollo en concreto, una posible solución a un problema que le había surgido en ese desarrollo. En la misma aula, durante el taller, surgía esa colaboración, y eso es lo bueno del C1b3rWall, que no es, vamos a juntarnos en un auditorio de 5000 personas y alguien te va a lanzar su "speech" y vamos a verlo y vamos a aplaudir todos. No. Teníamos unos talleres que son una formación muy especializada, que estás en contacto con

el ponente, que bueno, aquí las instalaciones son enormes, puedes ir a cualquier sitio, y te surge esa idea y, en ese mismo momento, se plantea la opción de iniciar un proyecto, y eso es lo que surgió en C1b3rWall y lo que más nos gusta del proyecto.

DDR: ***Sí, además recuerdo que la gente levantaba la mano, comentaba en directo, sobre la marcha salían nuevas ideas, completamente, ese es uno de los puntos clave, además.***

Casimiro: Ibas a la cafetería, te sentabas allí y venga y comenzabas. Esa era la idea y nosotros habilitábamos espacio cuando alguien nos lo pedía, cuando venía alguien y decía: oye necesito un espacio para reunirme tal. Buscábamos un espacio y una sala de reuniones y allí se reunían y salieron cosas magníficas.

Daniel: En la experiencia de C1b3rWall y la que plantean permanentemente las comunidades es como ir construyendo una inteligencia colectiva, con el aporte de todos ¿Qué es lo difícil de hacer? Lo fácil, y lo difícil también, es precisamente tener ese espíritu libre de nutrirse de muchas fuentes diversas, pero a sui vez también es muy difícil porque hay intereses muy concretos que te dice, no, yo tengo que ir por aquí por determinados motivos, y eso es precisamente ofertan comunidades y congresos como C1b3rWall en los que sus raíces son comunitarias. Integrar toda una experiencia de diferentes colectivos que terminan formando una inteligencia colectiva.

Es muy importante nutrirse de esas experiencias porque la complejidad del mundo tecnológico, de todo el conjunto, no ya solo de la ciberseguridad, es enorme. Tremendamente complejo. Y la única manera es la de trabajar de forma mancomunada, con distintas perspectivas, para poder abordar problemas y desafíos que tengan la posibilidad superarlo. Es muy importante contar con experiencias como la de C1b3rWall y otras experiencias y otros congresos.

DDR: ***De hecho, justo enlazamos con la siguiente pregunta, porque tenemos congresos en distintas provincias, incluso, podríamos decir que se puede hacer un tour por España y hacer turismo de interior asistiendo a eventos ¿Podría llegar a ser posible eso en un futuro? ¿Qué podamos incluso hacer un tour completo con su comunidad (hacker) en cada provincia y cada una compartiendo ideas allí?***

Casimiro: Piensa local para actuar en global ¿no? Yo creo que tendríamos que cuidar todas esas comunidades, cada una en su provincia, en su localidad, eso habría que cuidarlo, lo que no quita que haya ciertas fechas en las que no nos podamos reunir todos ¡Qué envidia tener un congreso como el que pueda desarrollarse en las Vegas y que no tenga que ser tan comercial! Estamos viendo que hay congresos magníficos, pero con un trasfondo muy muy comercial.

¿Por qué nosotros no potenciamos cada uno de esos congresos, cada una de esas comunidades, en su localidad, su provincia y luego nos juntamos en ciertas fechas como comunidades, como instituciones, universidades, sector privado, pero sin ser algo tan teledirigido por una empresa por ejemplo? Eso sería ideal, tener ese músculo como país de tener un gran evento un gran congreso que recoja todas esas sinergias de todos esos congresos y comunidades.

Daniel: Una de las visiones y los proyectos con los que surge HackMadrid es precisamente intentar crear en España una federación de comunidades de hackers, pero, dentro de esta temática, que todas tengan una libertad de poder plantearse sus propias peculiaridades. Y, que si hay un evento con un ponente, que ese ponente pueda recorrer todas esas comunidades, Sevilla, Galicia, Barcelona, Madrid, Valencia. Un ejemplo sería un ponente internacional, que pueda hacer el recorrido, en lugar de pedir a toda la gente de las provincias que tenga que venir a Madrid, porque podrán venir una vez por un congreso, pero no podrán venir siempre.

Creo que eso es importante, que haya congresos, como C1b3rWall, que no estén dominados precisamente por espíritu comercial, porque entonces termina siendo la venta de algo, de un producto o un servicio y tiene que ser, compartir conocimiento, poder experimentar juntos, crear proyectos.

Casimiro: Claro, yo creo que una de las claves con respecto al sector privado, de las empresas, fue eso claro, que desde el primer momento vieron que esto no se trataba de una posición de algo comercial, de una herramienta suya, sino que, vamos a formar a la gente, vamos a hablar sobre los temas que nos preocupan y aparte, bueno, podemos hablar de cualquier desarrollo o producto comercial cuando salgamos del aula. Pero se vio muy claro que las empresas quisieron participar de esa confluencia de ideas, de, como empresa, vamos a aportar esta idea, pero voy a escuchar la perspectiva de la policía del CCN, de Incibe, de determinada comunidad, de determinado profesor de la universidad y eso quedó muy patente el año pasado, en ningún momento hubo ningún espíritu comercial, sino más bien un espíritu formativo y común.

Nosotros siempre lo hemos dicho, C1b3rWall no es el congreso de la policía nacional, policía nacional es una parte de C1b3rWall, siempre escuchamos a todo el mundo que se pone en contacto con nosotros, el que nos r emite una propuesta, si nosotros no podemos darle salida a esa propuesta, buscamos a alguien dentro de la institución o de la universidad que pueda tener un interés en esa propuesta y siempre todo es bienvenido.

DDR: ***Estamos hablando de que C1b3rWall fue un congreso que unió a investigadores, hackers, sector privado y Fuerzas y Cuerpos de Seguridad. Creemos que este evento sirvió para acercar vuestra labor en la policía en materia de ciberseguridad, al final, es muy parecido a lo que se hace, por ejemplo, en una empresa privada.***

Casimiro: Al final, si nos paramos en detalle, y miramos a las personas que trabajan en estas funciones, ¿dónde se han formado? Pues se han formado dónde todo el mundo ¿no? Y todos coincidimos en todas las CON, en todas las reuniones y bueno, ahora a lo mejor, al venir a nuestra casa nos habéis visto de uniforme. Yo en las últimas que hemos asistido en Madrid, he cambiado un poco y he ido por "La Nave" (Madrid) de uniforme y ha llamado mucho la atención. Nos tenemos que acostumbrar a eso, al final todos tenemos la misma base prácticamente y nos hemos especializado en algo y tenemos que aportar cada uno nuestra visión para llegar a ese trabajo.

DDR: Ósea ¿Podríamos decir que en la Policía también se pueden encontrar hackers?

Casimiro: Sí sí, por supuesto, hay muchísimos. Así más conocidos, por ejemplo, tenemos a Manu, a Carlos Loureiro, pero tenemos auténticos cracks que trabajan fenomenal dentro de la policía y muchos están en todas esas convenciones, lo que pasa que no todo el mundo sabe que son policías.

DDR: ***Y ahora, debido a la situación actual estos últimos meses, tanto comunidades, como C1b3rawall, se han tenido que adaptar a la situación ¿no? ¿Qué tipo de cambios se han tenido que tomar para poder continuar con esta actividad?***

Casimiro: Respecto al C1b3rwall, congreso físico, seguimos planeándolo y diseñándolo, pero, evidentemente, no lo vamos a poder hacer en junio. Nosotros como institución de seguridad tenemos que ofrecer una seguridad a todas las personas que viniesen al congreso. Vamos a seguir diseñándolo, estudiando todas las propuestas y lo haremos cuando las autoridades correspondientes nos den autorización y sepamos, con total seguridad, que nadie absolutamente nadie corre ningún riesgo.

Mientras tanto, estamos llevando a cabo distintas acciones, porque C1b3rwall no es solo el congreso y estamos intentando apoyar todas las acciones que se están viendo últimamente como C0r0naCON u otros diversos congresos online que estamos apoyando podemos, con algún experto nuestro, con difusión mediática para que se sepa, nosotros lo comunicamos internamente para que toda la gente interesada se conecte y también diseñando una acción nueva que es el C1b3rwallAcademy.

C1b3rwallAcademy es parecido al congreso, pero lo vamos a empaquetar en formato curso, un "mooc", para que sea más fácil a cualquier persona acceder cuando quiera, sin tener que depender de conectarse a una hora concreta al directo porque si no se lo pierde y no puede. Vamos a intentar hacer ese C1b3rawallAcademy, ese curso en el que participan Cuerpo Nacional de Policía, las comunidades, expertos individuales, los ponentes clásicos de C1b3rwall y en el que está invitado todo el mundo a participar.

Hasta que podamos hacer el congreso físico, vamos a intentar seguir dando servicio público, que para eso somos nosotros la Policía y creemos que

estamos en la misma onda con las comunidades, con la universidad y con las empresas de dar ese servicio público, esa formación, que es fundamental para que todo el mundo esté concienciado y tenga una labor importante dentro del tema de la seguridad digital, dentro de la ciberseguridad.

DDR: ***Las comunidades como dices van a colaborar y ahora durante este periodo siguen también con su labor, como, por ejemplo, HackMadrid desde Twitch que continua con los congresos y las charlas.***

Daniel: HackMadrid nació como una experiencia presencial con nuestros objetivos de compartir el conocimiento, el hacking inteligente, experimentar, trabajar, proyectos… y bueno, si es presencial, fue presencial, y hoy, la única opción que tenemos es online, por razones obvias. Cuando se pueda, volverá a ser presencial de nuevo, lo que pasa que no es una decisión que depende de nosotros. Depende de autoridades nacionales, regionales, locales y hasta de los dueños de los espacios o los que administran los espacios, habrá que esperar a que las condiciones estén dadas y creo que, cuando estén dadas, pasaremos a un proceso híbrido. Mantener la parte online, por ejemplo, permite traer ponentes del exterior que es muy difícil pagarles un avión para que vengan a Madrid y volverse. La idea es también apoyar el C1b3rwall, habrá ponentes de HackMadrid que van a dar talleres, y apoyar una experiencia como esta tan importante para nosotros, nuestro crecimiento, nuestro aporte y sobre todo porque vemos que en los últimos tiempos se está pasando de lo competitivo a lo colaborativo. Todos entendieron que más que competir, hay que colaborar, porque colaborando ganamos todos… compitiendo… a veces no ganamos todos. Se torna eso en un ocultar cosas… y no, al contrario, hay que colaborar. La tecnología está planteando lo colaborativo de forma inmediata, es la manera en la que crecieron la ciencia y el conocimiento a través de la historia, de forma colaborativa y en eso las comunidades tienen mucho que aportar, porque tienen una rica experiencia en ese sentido.

DDR: ***Completamente, completamente, además que se está acelerando todo debido a la situación claro (COVID-19).***

Casimiro: Es que no se puede hacer de otra manera, estamos hablando de seguridad digital, en un mundo muy digital, pues tendremos que hacerlo ¿no? Abordarlo definitivamente. Estamos viendo que el teletrabajo funciona. Hay empresas que se han dado cuenta que creían que iba a ser muy problemático y bueno, pues has salido bien el experimento. Ha salido bien, claro, siempre que integremos todas las visiones dentro de ese experimento, no dejemos de lado la seguridad, vamos a diseñar todas esas aplicaciones integrando la visión de la seguridad.

Daniel: Si, a parte, todo ese proceso sirve para acelerar migraciones hacia nuevas formas que están mostrando virtudes, por otro lado, todo eso hace que el enfoque acerca de que la seguridad en cuanto a intromisiones,

malware, todo el tema de la privacidad, los datos, etc, etc. También necesita una respuesta. Ya nuestra vida era digital, pero ahora también el trabajo es digital, está circulando por internet, ceros y unos, que llevan datos y que hay que protegerlos.

Por otro lado, ayuda a que no solo las empresas, las grandes corporaciones que tienen pulmones financieros y de talento como para poder dar ese paso y muchas de ellas han sido pioneras en eso, sino para un montón de empresas que les costaba entender este proceso, que eran renuentes, y que hay que ayudarlos a que puedan ver las ventajas que tiene esto, el trabajo en remoto. Sobre todo, porque a lo mejor hay que trabajar mucho más en remoto y las amenazas de las pandemias no van a cesar con el coronavirus, luego podrán venir otras, ya no sabemos… pero hay que estar preparados.

Antes de la entrevista lo estábamos comentando, Twitter permitirá el teletrabajo permanente, no van a volver a oficinas, algunos pasarán una etapa híbrida o lo que sea, pero este fenómeno no se puede desconocer y creo que hay que ayudar a eso. Ver cuáles son las plataformas adecuadas, la seguridad con esas plataformas, los métodos adecuados… nosotros como comunidades lo hemos tenido que hacer, hacer cursos de OVS, de Jitsi, de plataformas de transmisión, de preguntas… en fin, hay que adaptarse, y puede ser, se pueden dar respuestas y han sido buenas.

Casimiro: Y muy importante el tema de la educación, lo estamos viendo, como los niños no pueden ir al colegio y tienen que habituarse a ese entorno digital, a saber, desenvolverse en ese entorno con unas determinadas herramientas, o buscar otras opciones que no sea una herramienta en concreto. Entonces tenemos que formar a nuestros niños también en ese hábito de saber manejarse en ese entorno digital, de saber los riesgos que pueden encontrarse y esta es una oportunidad que estamos viendo que se tiene que aprovechar. No seamos el país del péndulo, pasamos de todo presencial a todo en remoto, no, tampoco, vamos a buscar algo híbrido y no nos olvidemos nunca de las dos vertientes. Hagamos presencial lo que tengamos que hacer presencial porque nos beneficia, y hagamos online, lo que tengamos que hacer online porque nos beneficia también al conjunto de todos. Vamos a intentar integrar en este entrono digital a todas las personas a las que las afecta, que prácticamente es el cien por cien de la población.

Daniel: Si, en el campo de la educación, tanto primario, como secundario, como terciario, universidades, una vieja idea que surgió, la educación a distancia, hay que volverla a plantear, ¿Por qué? Porque soluciona muchos problemas, cuantas materias pueden darse en forma digital, y que es mejor que presenciales ¿no? Yo he ido por ejemplo a cátedras, estoy dando análisis matemático que éramos cuatrocientos en un anfiteatro y se veía la pizarrita chiquita y si te perdías algo, te lo perdías. Ni se te ocurra preguntar al de al lado porque te decía… ¡Cállate! Y ahora, si eso está bien grabado tu lo puedes ver veinte veces en tu casa, en el horario que te conviene, consultar en internet cosas… yo creo que cómo decía Casemiro, la parte presencial tiene

que ver con las experiencias sociales, a lo mejor hay que hacer "hub" dónde haya que reunirse, discutir, intercambiar opiniones… pero por ejemplo, lo que es el estudio de determinadas materias… se hacen mejor desde casa, mejor más tranquilo. La parte presencial tiene que estar para todo lo que es la relación, la experimentación, adquirir "skills", habilidades sociales, como relacionarse, que son muy importantes.

Casimiro: Y que tenemos dispositivos que son tremendamente buenos, que luego al final no los aprovechamos, los utilizamos para colgar una foto en Instagram, vamos a utilizar todos esos dispositivos que nos ofrecen muchas posibilidades para… grabar una clase… ofrecerla para que el alumno pueda verla cuando quiera, que pueda colgar unas preguntas, unas dudas, que pueda incorporar al temario ciertas opciones… que disponemos de muchas opciones, que un móvil, un ordenador, no solo sirve para almacenar las fotografías de las vacaciones, o para subirlas a Instagram, ¿no?

Daniel: Yo le contaba a Luis, antes de empezar la entrevista una experiencia. El sábado hicimos una reunión de organizadores de HackMadrid, que participaron 14 personas. Empezó a las 7PM y terminó a las 8:30PM y fue una hora y media dedicada a tratar temas organizativos. Si esa reunión hubiera sido presencial, primero habría que haber coincidido todos… a las 7 para mi es muy tarde, a La Nave, como voy como vengo… y por ejemplo en mi caso si… a las 7 nos reunimos, yo tengo que salir a las 6 y luego cuando acabamos a las 9 de la noche llego a mi casa a las 10, es decir que, para 1 hora de reunión, tengo que invertir, 4h de mi vida, y la parte online soluciona cosas. Ahora, si queremos reunirnos para compartir socialmente algo, me parece que sí, que lo que vale es reunirnos con algún objetivo. Entender lo que es la necesidad del mundo presencial cuando sea posible para todas las relaciones, la experiencia social, y que hay cosas que se hacen mejor online, muchísimo más rápido. Son experiencias que tenemos que ir sacando de lo que nos sucede.

DDR: ***Como última pregunta, así un poco más atrevida, queríamos preguntaros sobre este revuelo que hay últimamente con la privacidad, la geolocalización (sobre todo ahora con el COVID)… ¿creéis realmente es por qué quieren saber dónde estamos continuamente? O ¿se hace más por ver el conjunto de la población y sacar estadísticas que puedan aportar algo de valor?***

Casimiro: Yo creo que es un tema muy importante, muchísimo, que todas las personas deberían preguntarse, que datos están generando, y que datos están obteniendo ciertas entidades de ellos. Creo que para ello es fundamental la educación, y tener una ciudadanía adulta, no podemos tratar a los ciudadanos como si fuesen niños, todos tienen que tener una formación y todos tienen que ser conscientes de los riesgos, y de lo que está generando su vida en ese ciberespacio, dentro de la red.

Creo que desde las instituciones y sobre todo Policía Nacional, defendemos esa posición de implicar al ciudadano, para que sepa en todo momento lo que se está haciendo, y él, con esa conciencia, pueda tomar sus propias decisiones. El problema de esto, que haya ciertas zonas oscuras en las que al ciudadano no le quede claro lo que está sucediendo ¿Qué solución veo yo, aparte de tener esa educación? Cualquier proyecto que se quiera implementar y que quiera contar con esos datos, debe contar, desde su propio inicio en el desarrollo y diseño, con la opinión de los ciudadanos y ellos mismo formar parte de este proyecto.

Luego, es cierto, que este tema genera y puede alentar… eso, que interesa el morbo. Me hace mucha gracia cuando leo artículos de… "La policía podrá saber", "La policía te podrá detectar" y claro, yo, como se cómo es por dentro mi institución me hace gracia, la policía no tiene ningún interés en eso ¿Para que le va a servir eso a la policía? O, si tuviese interés, la Policía, tiene que cumplir unos requisitos y solicitarlo a un juez, que es el que tiene que autorizar el acceso a esos datos.

Cuando conoces el procedimiento, te das cuenta de que eso no es real. Toda esa prensa que con esos titulares… ahí tan especulativos… de la Policía tal, no sé qué… pues eso no es real, porque los procedimientos son muy distintos, muy claros, legalmente establecidos y tú necesitas una autorización judicial y eso no se lo salta absolutamente nadie. Todos somos ciudadanos al final, la policía está compuesta de ciudadanos, igual que yo puedo investigar, otros compañeros de la Policía o de otro cuerpo de las Fuerzas de Seguridad, me puede investigar a mí. Somos todos ciudadanos, no somos una parte ajena a la sociedad.

Creo que es eso, fundamental, dar mucha información, implicar al ciudadano en cualquier desarrollo y cualquier herramienta que sepa cómo se están utilizando sus datos, que sea él el que de dé el consentimiento de esos datos porque le da un beneficio individual o social, son evidentes los beneficios, y creo que esa es la cuestión. La policía tendrá acceso a los datos que, los ciudadanos, a través de los legisladores y a través de la ley, quieran que tengamos acceso, ha sido siempre así, y será así.

Daniel: Yo creo que siempre hay dos cosas. Cuando se plantean determinadas aplicaciones que tienden a subsanar un problema, es como un cuchillo de doble filo, por un lado, subsanan un problema, pero, por otro lado, no podemos ignorar que hay un negocio con los datos, en el cual la Policía no participa, eso estamos seguros, ese negocio está ubicado en otras esferas… que son los que aprovechan esos datos con objetivos comerciales, políticos, etc. Y se capturan muchos datos fuera del control de los ciudadanos, pero para que exista ese control, tiene que haber educación. Porque de que vale hacer eso si un tío se toma una cerveza y se saca un "selfie" y está todo el tiempo diciendo por dónde anda. Eso es falta precisamente de educación y de ver los problemas.

A los datos hay que quitarles el objetivo económico que tienen y que es tremendo, que eso sí que saca colmillos para afuera, pero no precisamente los cuerpos policiales son los que van a sacar beneficio de eso, son otras instancias. Para eso tiene que haber una educación y un control de la ciudadanía y que exista el derecho a que tu puedas hacerlo o no. Para eso hay que educar a los ciudadanos de que cada decisión que tomemos tiene sus consecuencias. Si la gente no entiende que hay consecuencias no tiene una actitud adulta, tiene una actitud infantil, hago las cosas y después… eh y ¿esto? Bueno, lo hubieras pensado antes, eso tiene consecuencias y tú tienes que saber cómo enfrentar esas consecuencias luego.

Es un problema de educación, nosotros decimos que lo que hay que evitar en el mundo del Software y del Hardware son las cajas negras. Las cajas negras alientan a todo ese tráfico, porque tú no sabes que hay en esa caja negra, a dónde están derivando los datos, a dónde los envía y por eso todo el software y hardware tiene que ser auditable. No tiene que ver con su esfera comercial, eso de que tiene que ser secreto para que ellos lo vendan es mentira, tiene que ser auditable por el conjunto de la sociedad. Inclusive por la misma policía. Al fin y al cabo, cuantas cajas negras hay funcionando en nuestra sociedad, que ni la misma policía puede auditarlas. El factor de la educación es muy importante para que la ciudadanía pueda tomar decisiones inteligentes.

Casimiro: Llegar a esa responsabilidad requiere mucho trabajo y mucho esfuerzo, Mucha de esta gente que protesta… no es que mis datos… hacen negocio con mis datos… no se esfuerza en aprender y en tener una estrategia correcta de conservar esos datos y no regalarlos, entonces, si, efectivamente, vamos a ponernos a trabajar, vamos trazar una estrategia correcta para que los datos, sepamos como se tratan, dónde van, etc. Pero que seamos conscientes como bien dice Daniel, que eso requiere un esfuerzo por parte de todos. Aquí somos todos adultos, y si quiero un resultado, tengo que plantear mi esfuerzo, y aportar ese esfuerzo, no puedo pretender que me lo den todo hecho porque, cualquier cosa que te den hecha, tu no conoces que hay detrás. Ese es el problema.

Daniel: Uno tiene que sospechar cosas, porque, si algo te lo dan gratis, ¿Qué hay detrás de eso? Que te lo de gratis un grupo de franciscanos bueno, es parte de su espiritualidad, pero que te lo den gratis otros… tu dices, oye aquí hay algo raro en todo esto… Y la gente no se hace esas preguntas… y es renuente a pagar cosas o a hacer esfuerzos… yo voy a aprender a ver como funciona un sistema operativo, como lo puedo instalar, como puedo entenderlo… porque en eso precisamente consiste tu libertad, tu capacidad de decidir. Si tu todo te lo dan gratis y toda caja negra y no entiendes de nada, pues luego no te quejes. Van a hacer contigo lo que quieran. Está claro.

La tarea de difusión y de educación, es muy importante, y enseñar a la gente que también hay que hacer esfuerzos, a nivel de estado, de sociedad y de instituciones. Desarrollar software, sistemas operativos que sean

controlados, que sepas lo que hacen, que puedas auditarlos… y vemos que eso no pasa. Y luego no te quejes, de que los datos van a dónde no debían.

Casemiro: Yo por ejemplo participo en muchas reuniones dónde se habla de cosas como esta, de soluciones de comprar herramientas, etc, etc y somos muchos los que defendemos la opción de, ¿Por qué lo vamos a comprar, si lo podemos desarrollar? Si hay herramientas que son gratuitas, que son de acceso libre a cualquier persona, partamos de ellas, aprovechamos ese conocimiento, que ya está en la sociedad, que han puesto a nuestra disposición… desarrollemos herramientas nuevas y luego a su vez, pongámoslas a disposición de otros que puedan hacer nuevos desarrollos. Esa corriente la defendemos mucho dentro de mi casa, y creo que sería muy beneficiosa.

Es una de las cosas que queremos incentivar en C1b3rwall, vamos a desarrollar entre todos herramientas que necesitemos.

Daniel: Y eso genera un escenario de conocimiento, porque si no, tu eres un consumidor pasivo. Estás consumiendo cosas que las hacen en otro país… y tú te estas negando la posibilidad de tener conocimiento, autonomía y soberanía tecnológica y eso, eso luego se paga. Se paga económicamente, políticamente… eso tiene un precio altísimo.

Casimiro: Y estamos viviendo lo importante que es tener un tejido empresarial, industrial y productivo dentro del país. Que no tengas que depender de una cadena de suministros que es completamente incierta y está en el aire. No sabes si te va a llegar o no, para cualquier cosa tan básica como una mascarilla.

Daniel: Claro, si no, pasa cualquier cosa y tú te quedas sin nada, eso es muy importante, por ejemplo… tener la soberanía de que muchos servidores de datos importantes están en el país. Porque, si tú, pones un servidor con tus datos, en otro país, bueno, luego no te quejes porque ese servidor se va a regir por las leyes de ese país.

Casimiro: A nivel institucional yo creo que eso sí que está quedando cada vez más claro, lo vimos el año pasado con el Real Decreto, el 14/2019, en el que todos los datos especialmente sensibles de los ciudadanos españoles que se tengan que conocerse en una administración, tienen que estar en servidores nacionales. Los muy sensibles. Luego los datos personales tienen que estar alojados necesariamente, en servidores de la Unión Europea. Creo que está calando ese mensaje y acciones como las de C1b3rwall y todas las CONs de las comunidades, etc. Es lo que están transmitiendo, y parece que cala.

Daniel: Poco a poco hay que ir pensando en un mundo distribuido dónde nadie maneje el enchufe que desconecte a todos. Que todo esté descentralizado y distribuido. Esa es la única forma de evitar tentaciones, de gobernar o de hacer cosas que no se deban. C1b3rwall está haciendo la faceta

educativa, de difusión, de crear comunidades, y muchas comunidades. No solo HackMadrid, también HackBarcelona, Interferencias, BitUp, HackingSevilla y otros muchos más que hay, que también se apuntan, que es muy importante, sobre todo llegar al ciudadano de a pie.

Una de las cosas que decimos y que queremos evitar es vendernos la moto entre los que ya la compramos, porque eso si que no tiene sentido. No vas a conocer a Carlos Loureiro de cosas que ya sabe. Lo importante es hablar con otro tipo de personas e ir a plantear este problema. Carlos Loureiro, Manu, Chema Alonso, ellos esto ya lo saben, irles a vender a ellos, ¿Qué les vas a vender, lo que ya saben? No tiene sentido. Por eso hay que hacer esfuerzo en llegar a sectores que desconocen este problema.

Comentario final DDR

Finalmente, dejamos la entrevista por aquí tras un buen rato hablando y comentando, incluso, podría decirse que filosofando. Sin duda una entrevista muy enriquecedora y que esperamos, os enseñe esta visión de dos expertos como Casimiro y Daniel, además de avanzaros algo de nuevo contenido sobre la C1b3rWallAcademy.

Desde Derecho de la Red, apoyaremos este tipo de prácticas, pues pensamos que es la forma correcta de abordar esta situación, tod@s unid@s junt@s aportando conocimiento, valor, trabajo, confianza, soluciones y mejoras tod@s junt@s haciendo comunidad.

Análisis de la Amenaza SilverTerrier

Iván Portillo – GINSEG

Presentación

En los últimos meses, debido en parte a la pandemia, están apareciendo multitud de amenazas que quieren aprovecharse de la situación actual. Algunas de estas amenazas son las campañas Business Email Compromise (BEC) distribuidas por medio del grupo malicioso **SilverTerrier.**

SilverTerrier es un grupo malicioso nigeriano que lleva activo desde 2014. Según una fuente han sido identificadas 10 campañas de malware bajo la temática COVID-19, detectándose un total de 170 correos electrónicos de phishing y directamente relacionado a este grupo criminal.

Entre los objetivos de SilverTerrier nos encontramos con los siguientes:

- **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 hasta la fecha por esta amenaza son los siguientes:

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

Operaciones

Entre las operaciones han sido detectadas 10 campañas BEC, tal como comentamos anteriormente. Según la fuente, 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**.

- 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**.

- 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.

- 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**.

- 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 objetivos 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**.

- 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**.

- 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**.

- 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**.

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.

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.

Durante la realización del presente boletín han sido detectadas una serie de informes o artículos en los que son mencionadas operaciones llevadas a cabo por el grupo SilverTerrier relacionadas con campañas sobre COVID-19, siendo los siguientes:

- https://unit42.paloaltonetworks.com/silverterrier-covid-19-themed-business-email-compromise/
- https://www.zdnet.com/article/phishing-alert-hacking-gang-turns-to-new-tactics-in-malware-campaign/
- https://www.zdnet.com/article/phishing-alert-hacking-gang-turns-to-new-tactics-in-malware-campaign/
- https://securityaffairs.co/wordpress/102949/cyber-crime/silverterrier-gang-bec-covid-19.html
- https://www.cyren.com/blog/articles/covid-agenttesla-3481

IoCs

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**

En el Anexo 1 tenéis disponibles dichos IoCs.

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.

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 central conformando una botnet compuesto de múltiples servidores víctima infectados.

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 **Agent Tesla** y el grupo malicioso **SilverTerrier**.

Análisis de las direcciones IP

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 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.

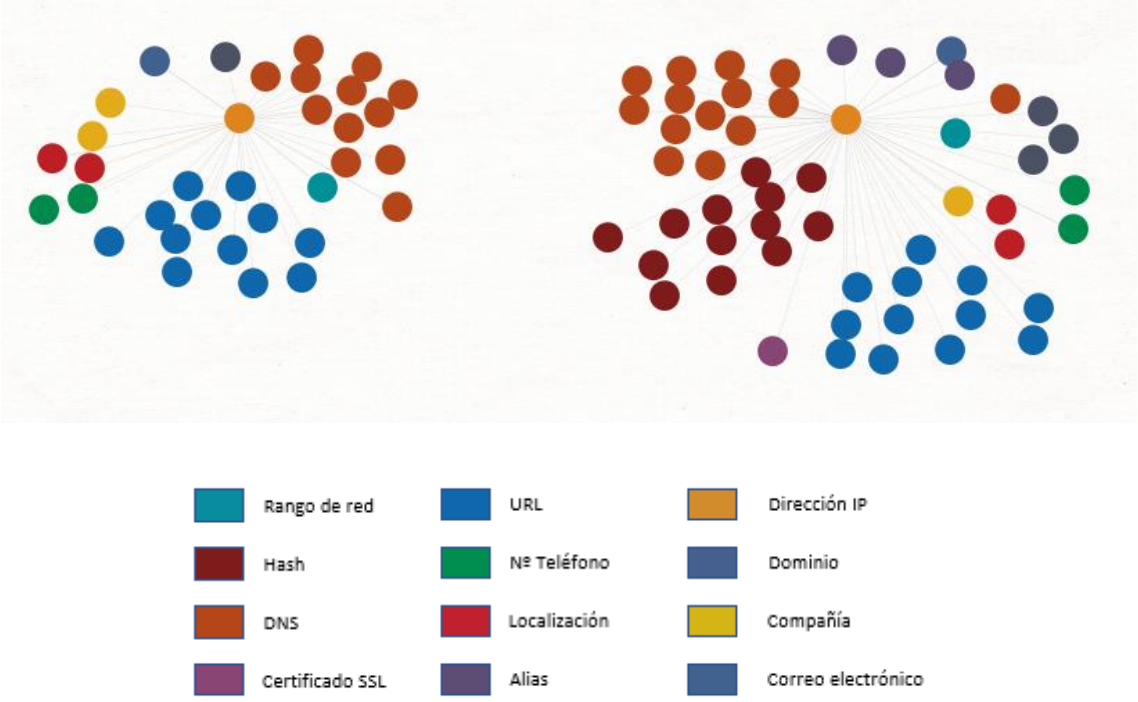


Imagen A001 e Imagen A002 (Leyenda)

Si prestamos atención ahora en la Imagen A003 y A004 podemos observar el grafo desde la perspectiva del tipo de dato detectado descubriendo que no existen relaciones entre ambas direcciones IP de manera directa.

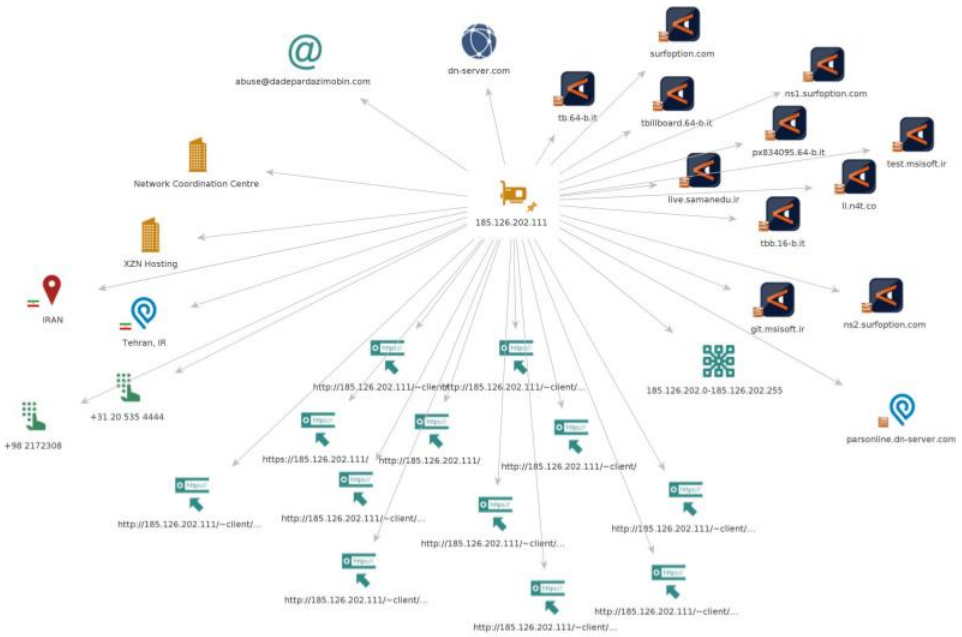


Imagen A003

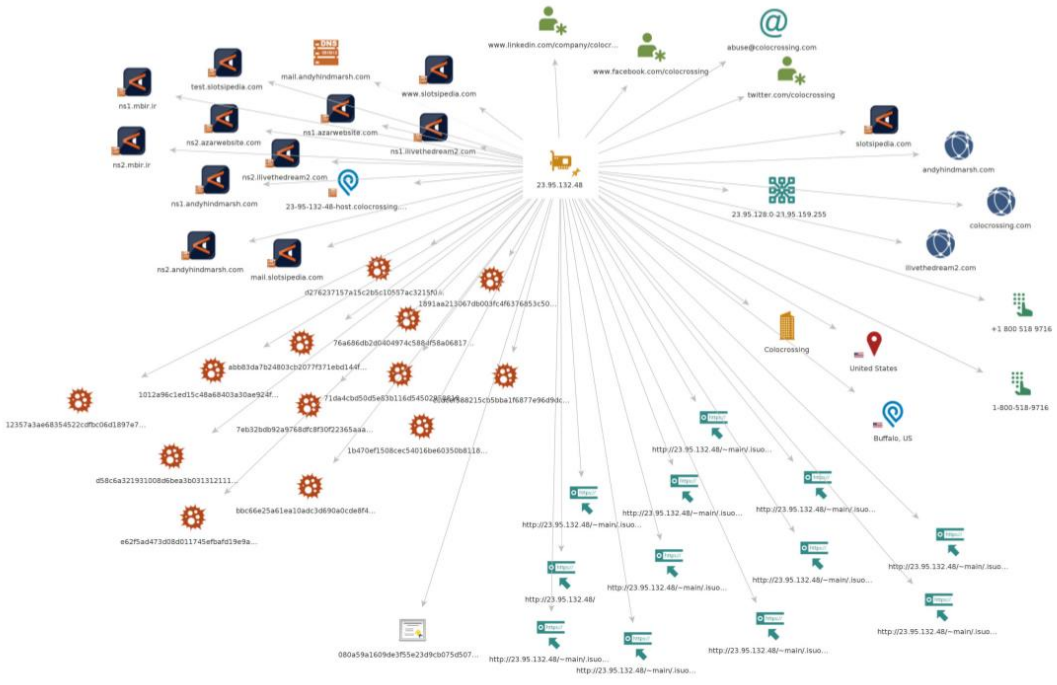


Imagen A004

Si analizamos la dirección IP 185.126.202.111 sacamos en claro lo siguiente:

- La dirección IP apunta a **Irán** en concreto a **Tehran**
- Se detectan **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 propia 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 URL que han dado positivo en algún motor antivirus.

Si analizamos la dirección IP 23.95.132.48 sacamos 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 URL que han dado positivo en algún motor antivirus.
- 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 A005 puede visualizarse la información del certificado extraído.

Imagen A005

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

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 puede ser visualizados en la Imagen A006 a través de las relaciones existentes entre dichos dominios.

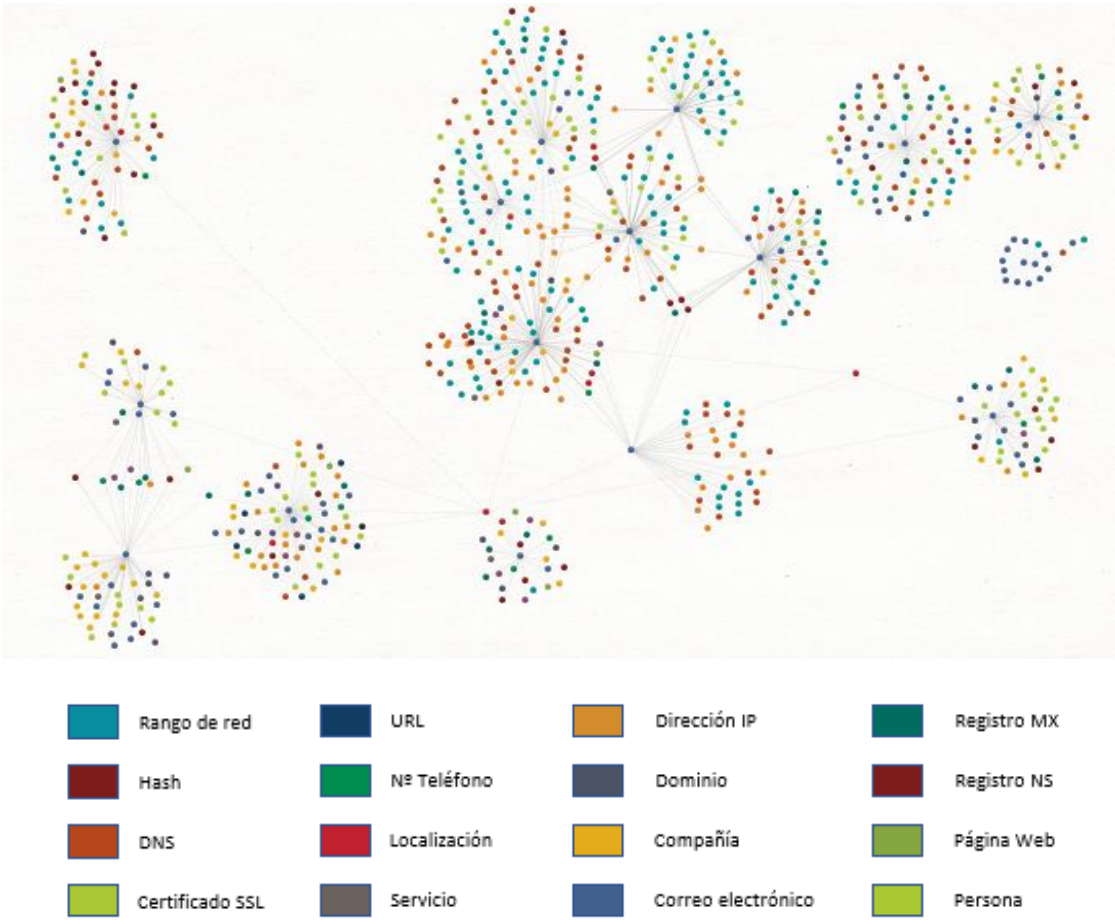


Imagen A006 *e Imagen A007*

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 A008.

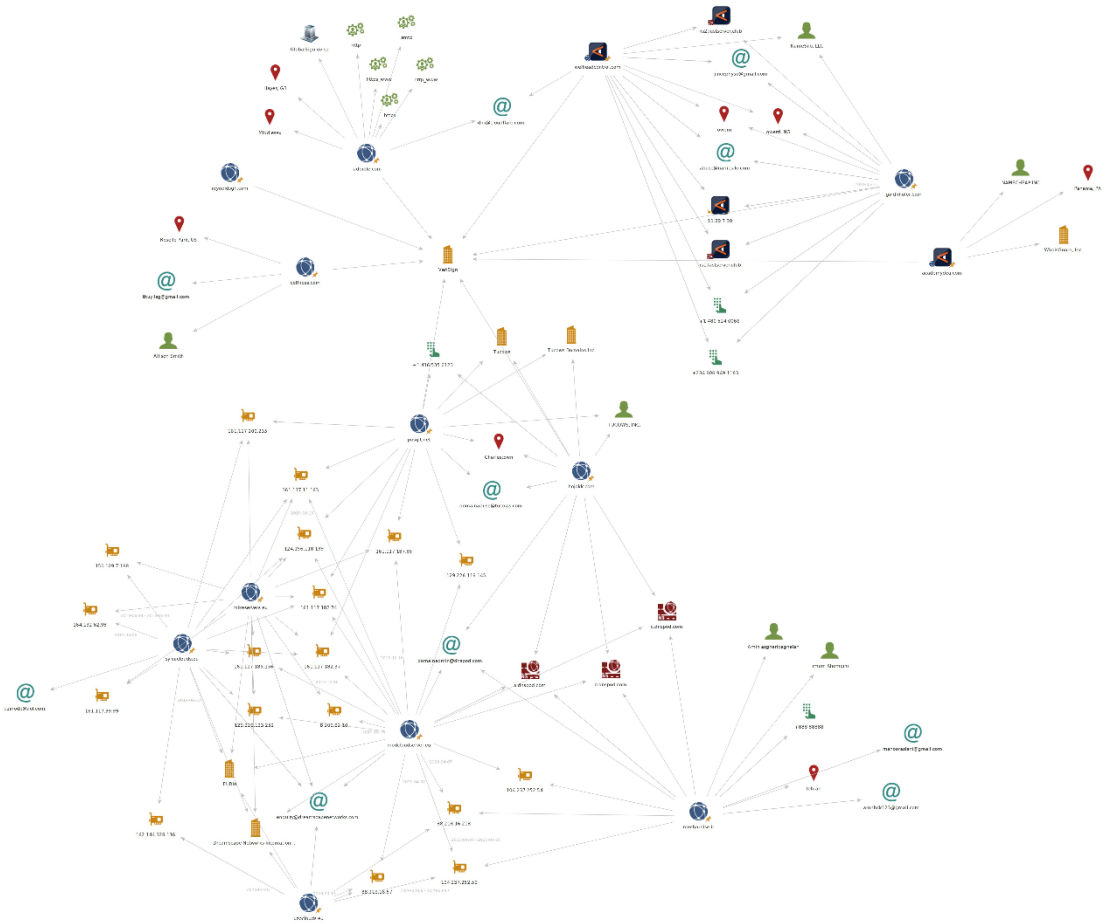
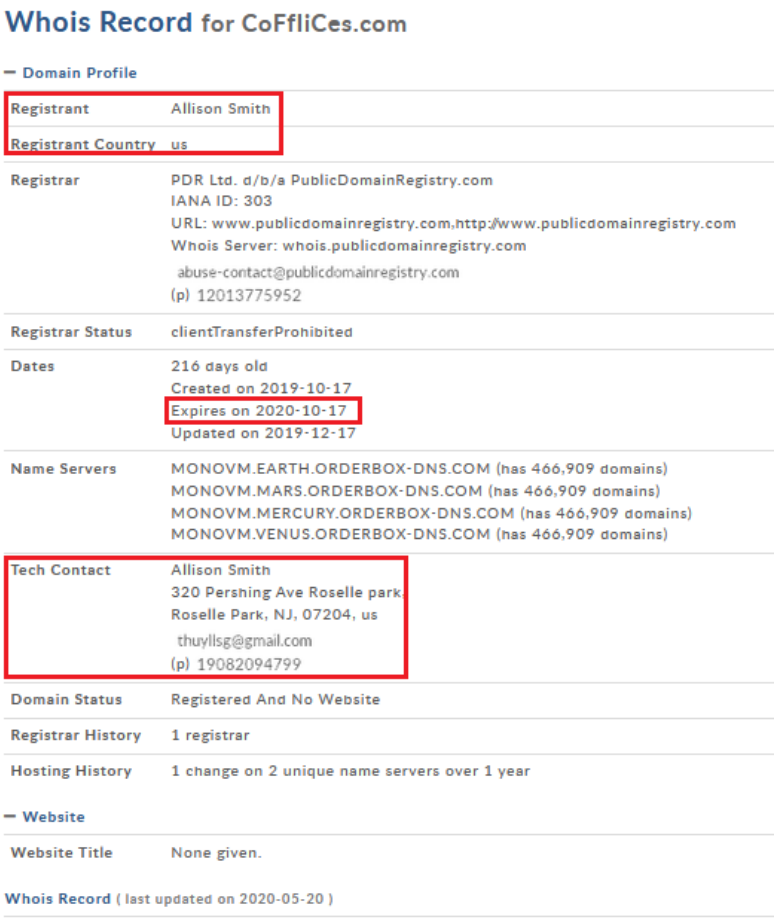


Imagen A008

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 servicio **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 A009.



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

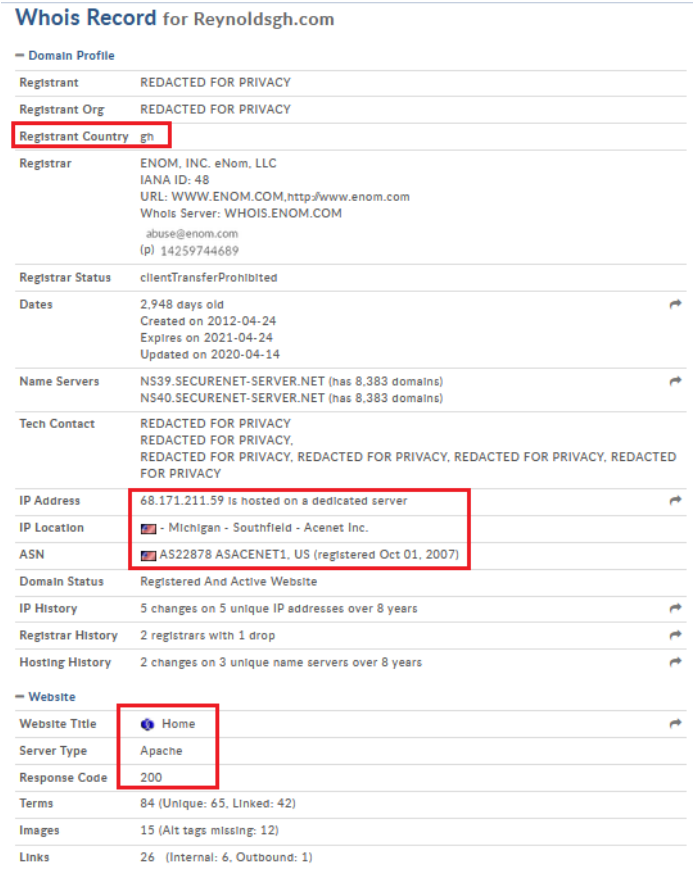
Website

Website Title	None given.

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

Imagen A009

- **reynoldsgh.com**
  - El dominio comparte el proveedor de servicio **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), su geolocalización (Michigan – Southfield, Estados Unidos) y que su registro expira el 24 de abril de 2021. Lo mencionado puede visualizarse en la Imagen A010.



Whois Record for Reynoldsgh.com

Domain Profile

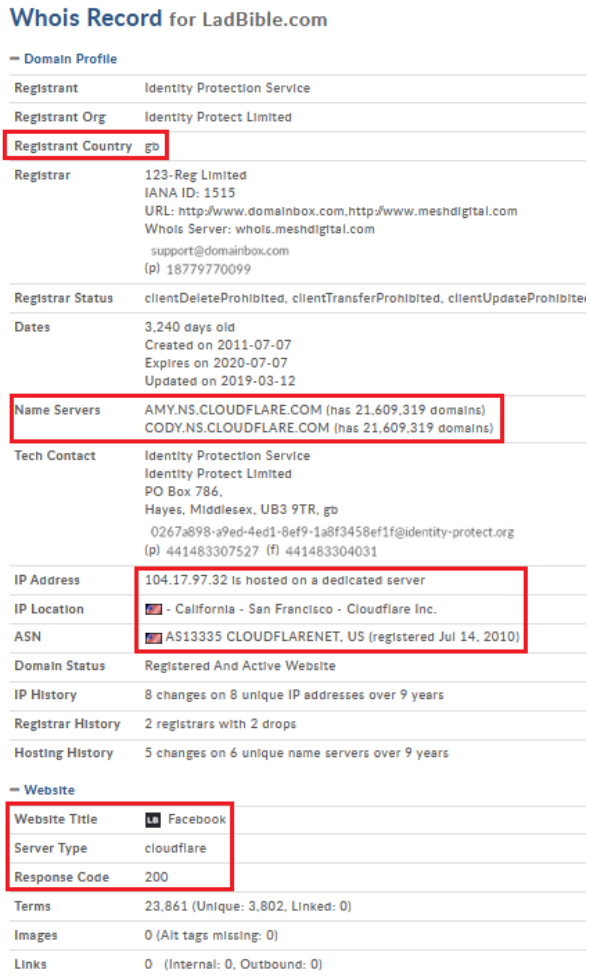
Registrant	REDACTED FOR PRIVACY
Registrant Org	REDACTED FOR PRIVACY
Registrant Country	gh
Registrar	ENOM, INC. eNom, LLC IANA ID: 48 URL: WWW.ENOM.COM,http://www.enom.com Whois Server: WHOIS.ENOM.COM abuse@enom.com (p) 14259744689
Registrar Status	clientTransferProhibited
Dates	2,948 days old Created 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 A010

- **ladbible.com**
  - El dominio comparte el proveedor de servicio **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), proveedor de servicios utilizado (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 A011



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 A011

- **welheadcontrol.com**

  - El dominio comparte el proveedor de servicio **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 servicios (NameSilo) con el dominio **goldhhofer.com**, junto a otro correo 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 el proveedor de 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 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 A012 puede verse lo mencionado.

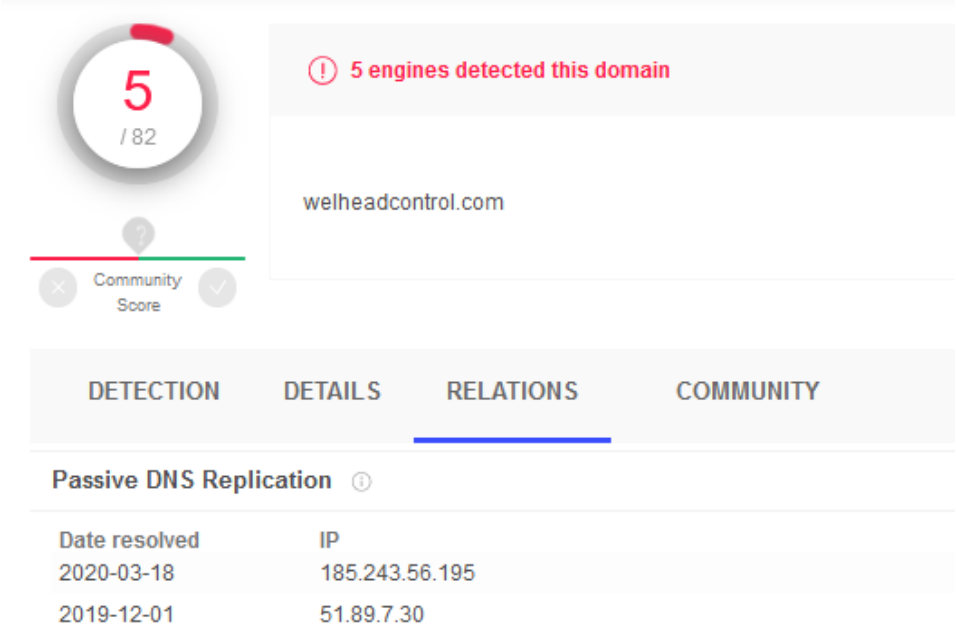
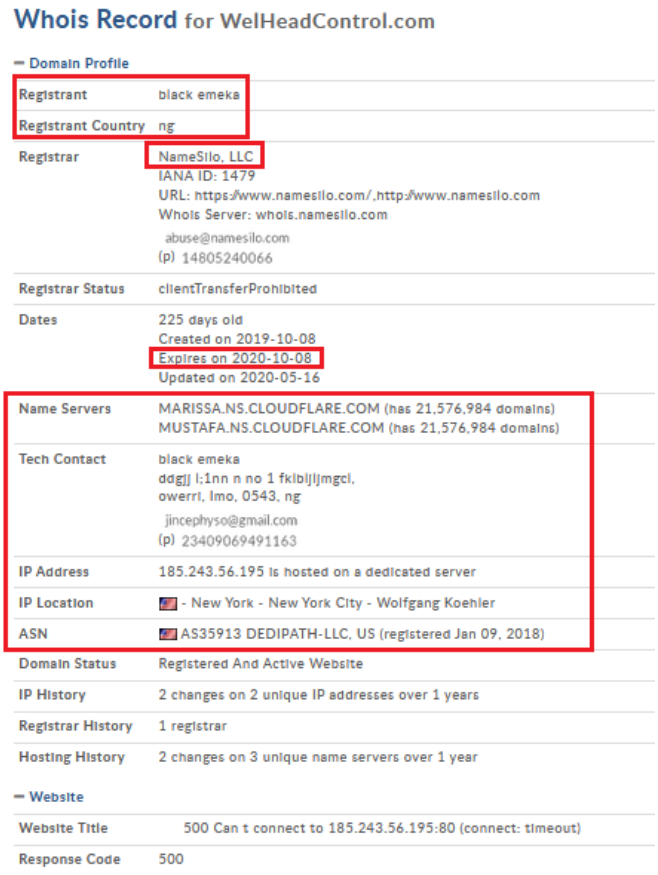


Imagen A012

- 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), proveedor de servicios 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 A013.



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 fklbljljmgcl, 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

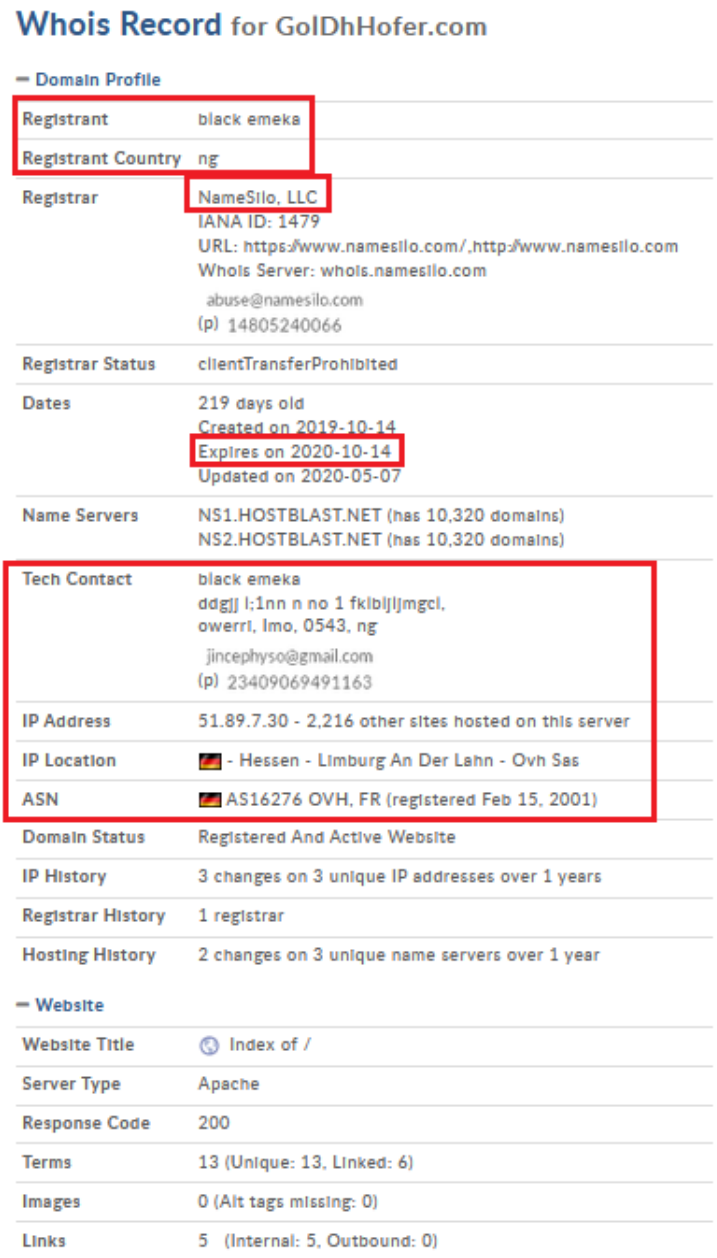
Website Title	500 Can t connect to 185.243.56.195:80 (connect: timeout)
Response Code	500

Imagen A013

- **goldhhofer.com**

  - El dominio comparte el proveedor de servicio **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 servicios (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 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 A014.



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 A014

- **academydea.com**

  - El dominio comparte el proveedor de servicio **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 A015.

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 A015

- **posqit.net**

  - El dominio comparte el proveedor de servicio **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 A016.

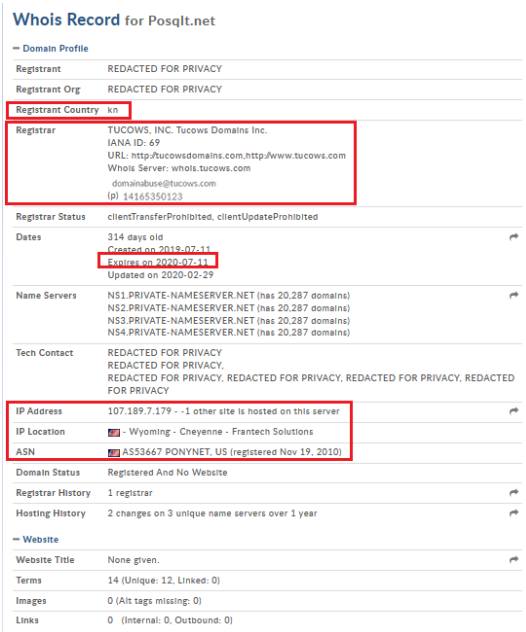


Imagen A016

- 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 A017 pueden visualizarse algunas de las coincidencias.

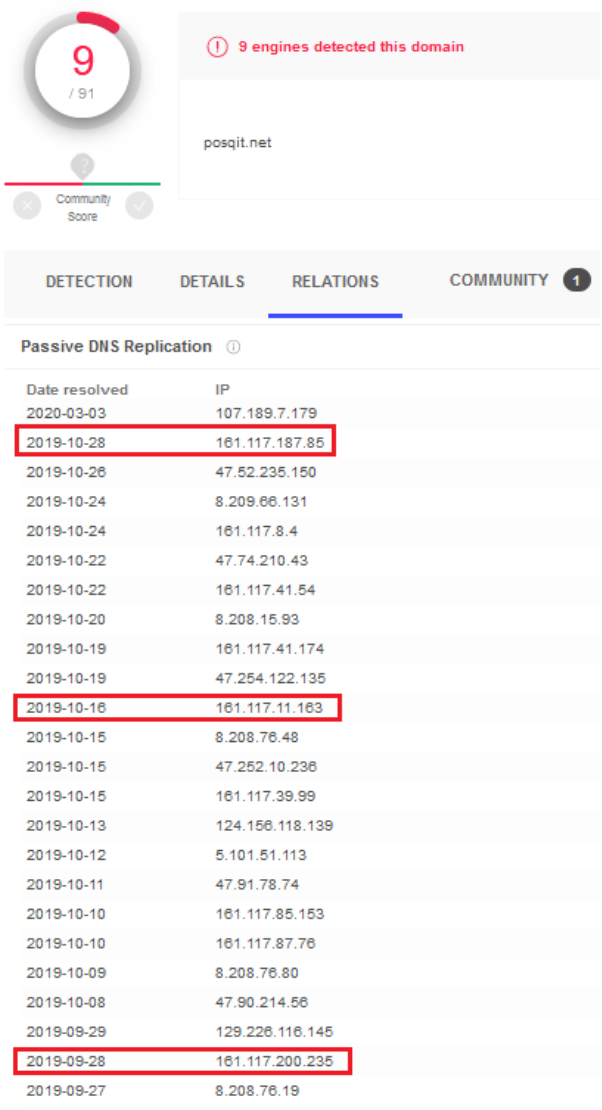
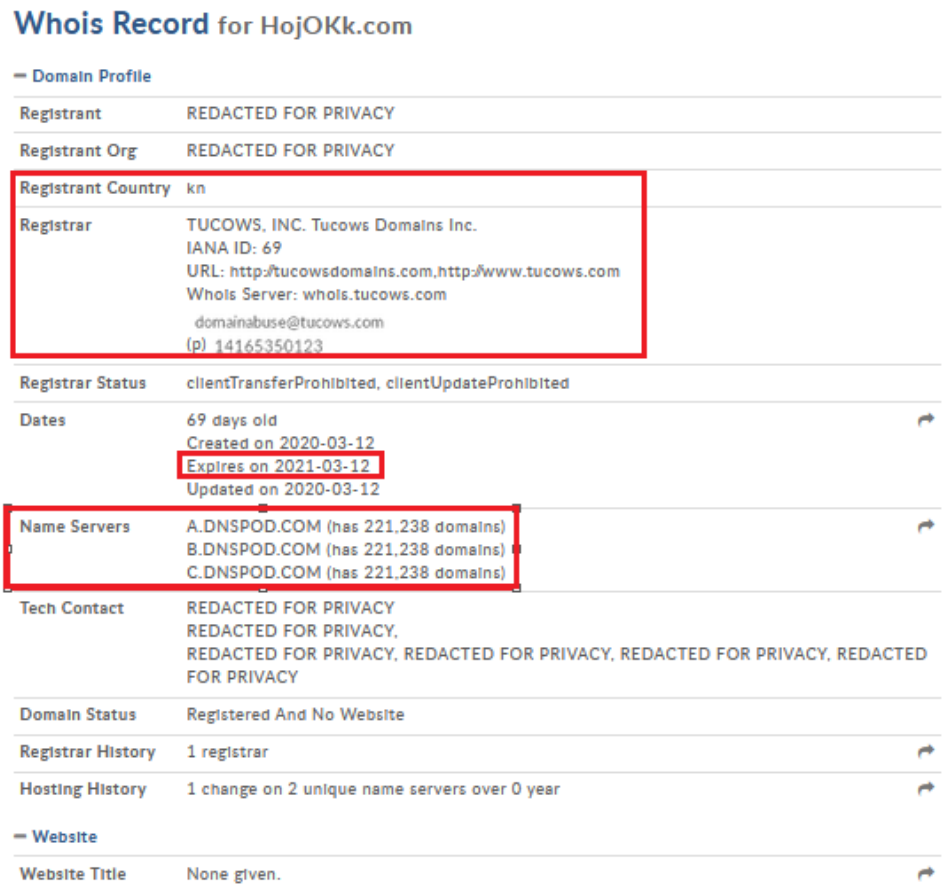


Imagen A017

- **hojokk.com**
    - El dominio comparte el proveedor de servicio **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 A018.



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 A018

- **mikeservers.eu**
    - El dominio comparte relación con **EURid** y el proveedor de servicios de Internet de 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 A019.

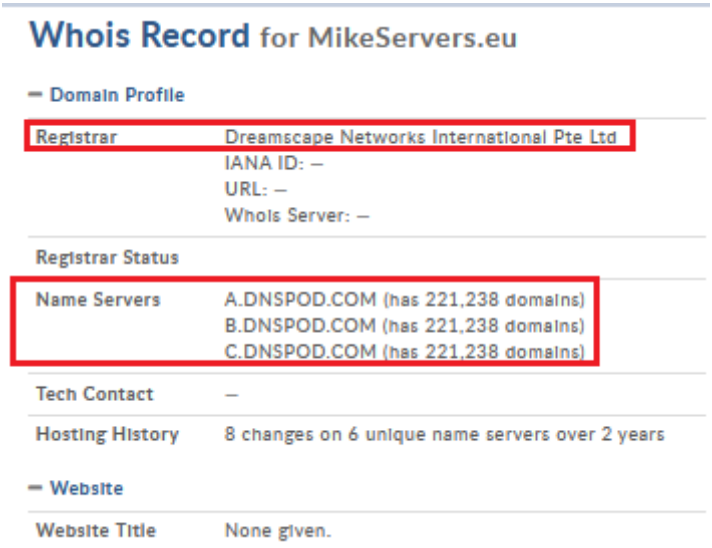
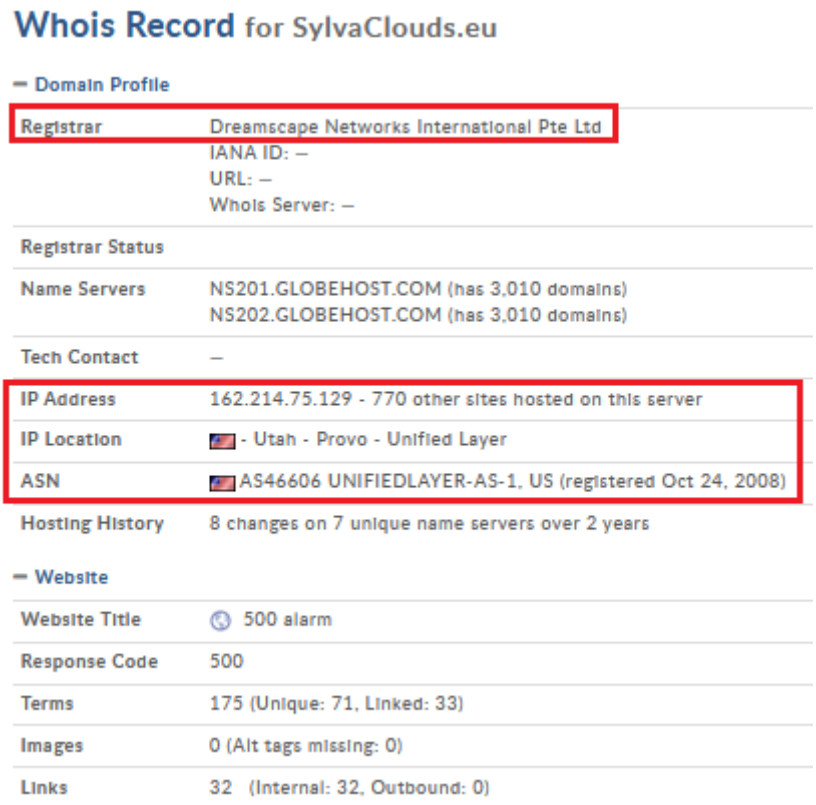


Imagen A019

- **sylvaclouds.eu**
    - El dominio comparte relación con **EURid** y el proveedor de servicios de Internet de 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 A020.



Whois Record for SylvaClouds.eu

— Domain Profile

Registrar	Dreamscape Networks International Pte Ltd IANA ID: – URL: – Whois Server: –
Registrar Status	
Name Servers	NS201.GLOBEHOST.COM (has 3,010 domains) NS202.GLOBEHOST.COM (has 3,010 domains)
Tech Contact	–
IP Address	162.214.75.129 - 770 other sites hosted on this server
IP Location	- Utah - Provo - Unified Layer
ASN	AS46606 UNIFIEDLAYER-AS-1, US (registered Oct 24, 2008)
Hosting History	8 changes on 7 unique name servers over 2 years

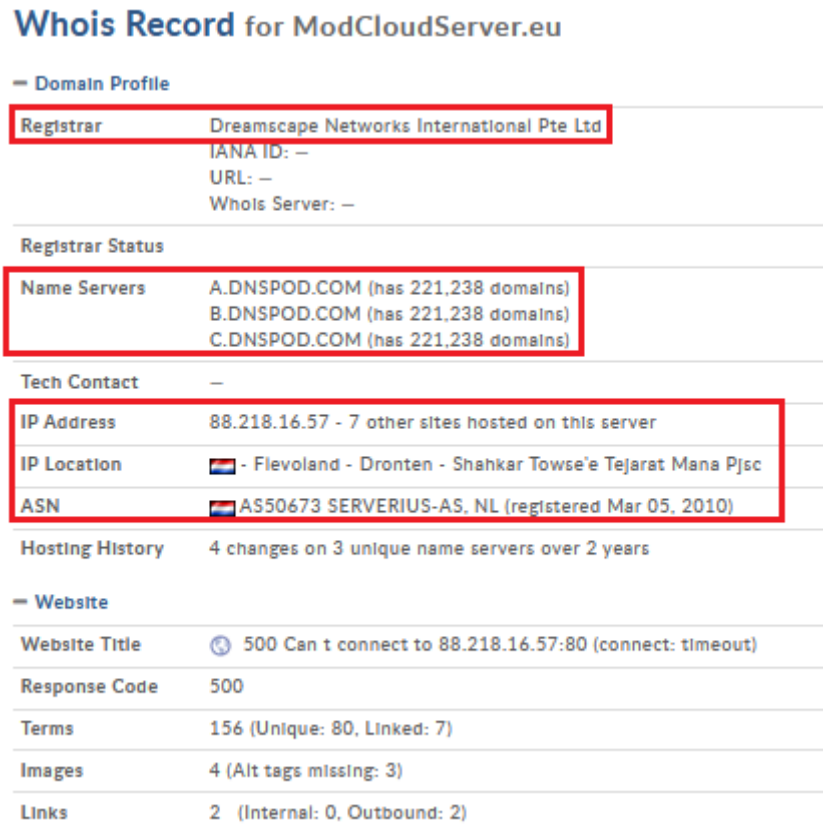
— Website

Website Title	500 alarm
Response Code	500
Terms	175 (Unique: 71, Linked: 33)
Images	0 (Alt tags missing: 0)
Links	32 (Internal: 32, Outbound: 0)

Imagen A020

- **<u>modcloudserver.eu</u>**
  - El dominio comparte relación con **EURid** y el proveedor de servicios de Internet de 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 A021.



Whois Record for ModCloudServer.eu

Domain Profile

Registrar	Dreamscape Networks International Pte Ltd IANA ID: – URL: – Whois Server: –
Registrar Status	
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	88.218.16.57 - 7 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	4 changes on 3 unique name servers over 2 years

Website

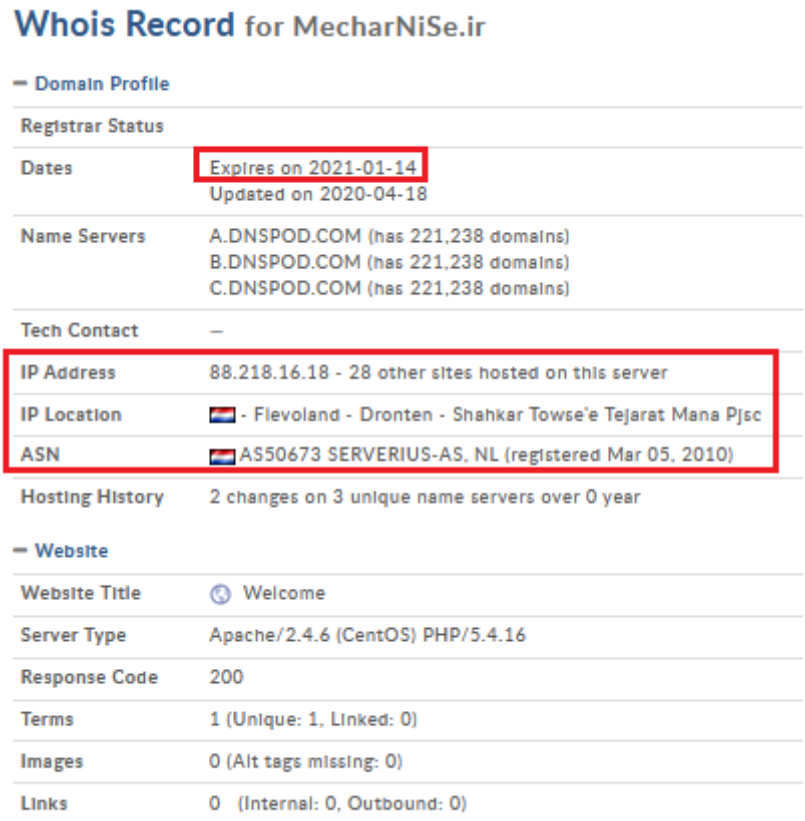
Website Title	500 Can t connect to 88.218.16.57:80 (connect: timeout)
Response Code	500
Terms	156 (Unique: 80, Linked: 7)
Images	4 (Alt tags missing: 3)
Links	2 (Internal: 0, Outbound: 2)

Imagen A021

- **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 A022.



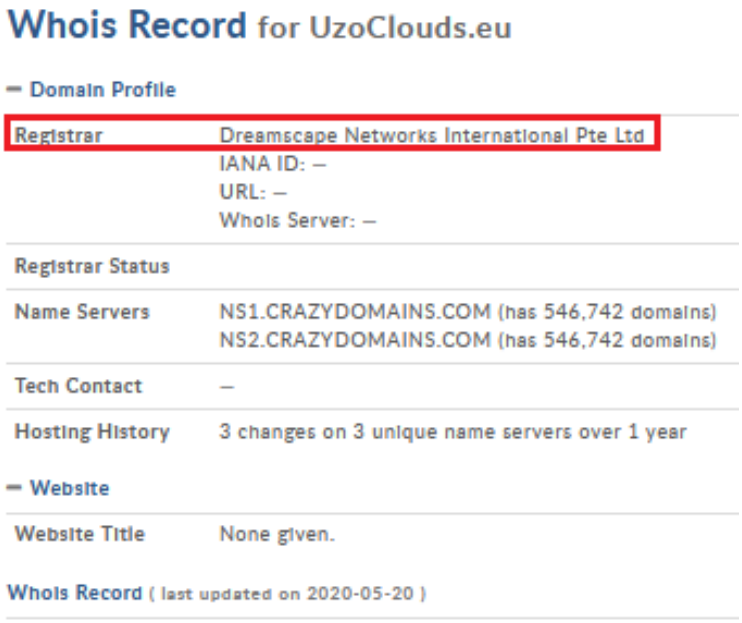
Whois Record for MecharNiSe.ir

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 A022

- **<u>uzoclouds.eu</u>**
  - El dominio comparte relación con **EURid** y el proveedor de servicios de Internet de 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 A023.



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 A023

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, Panama, Ghana, Reino Unido y Estados Unidos.

Nuevas estafas vinculadas a la inversión en Bitcoin: tiempos de COVID

Ariel Hakimi - Flu Project

Antecedentes

Hace más de un año, distintos medios de comunicación se hacían eco de la noticia de una estafa digital, que empleaba campañas de publicidad en Facebook y la imagen de numerosos famosos; entre ellos, Florentino Pérez, Amancio Ortega o Pablo Motos.

Noticias sobre la estafa digital analizada

La estafa, como tal, consistía en promocionar una plataforma ficticia que permitía invertir en productos financieros vinculados a Bitcoin; de este modo, el único requisito para poder empezar a operar en ella era realizar un primer ingreso de unos 200/250€. Obviamente, tras el depósito en dicha plataforma, la víctima perdía su dinero y no volvía a verlo nunca más.

Tal fue la expansión de la estafa, que hasta el propio Pablo Motos terminó denunciándolo en su programa El Hormiguero: "*está saliendo una publicidad con mi imagen, sin mi consentimiento, con una supuesta forma de ganar dinero que es un fraude*".

Capturas de distintas campañas fraudulentas en Facebook

De Facebook a Twitter

El 15 abril de 2020, en medio de la cuarentena por Covid-19, Ariel Hakimi detectó un extraño *tweet promocionado* de la cuenta @GreatBusiness7; dicho tweet, contaba con un enlace a *greatbusiness.club* y un breve vídeo, creado con imágenes y textos, en el que se hacía mención a una milagrosa forma de ganar dinero.

Tweet promocionado

Tal enlace a *greatbusiness.club* realmente era un enlace acortado que redirigía a una noticia del periódico "El Mondo", en la cual se mencionaba el secreto oculto del El Gran Wyoming, descubierto gracias a una supuesta entrevista realizada por Pablo Motos.

Noticia de El Mondo, sobre la última inversión de El Gran Wyoming

Curiosamente, días más tarde, el enlace acortado del tweet redirigía a un artículo en inglés del dominio *greatbusiness.club*, que nada tenía que ver ni con el tweet, ni con la noticia de la última inversión de *El Gran Wyoming.*

Además, en la URL de destino se añadían parámetros que hacían una clara referencia al tweet promocionado en Twitter: "*?campaign=ES&adgroup=25-UP&ad=3video*". Esto es, anuncio referido al vídeo 3 (ad), dentro del grupo de anuncios 25 (adgroup) y a la campaña dirigida a España (ES).

Artículo del dominio greatbusiness.club

Como por arte de magia, el artículo había sido creado, al día siguiente de la publicación del tweet promocionado: el 16 de abril de 2020; además, llamaba la atención que los títulos de la web estaban escritos en ucraniano, algo que destacaba sobre todo lo demás y no parecía ir en concordancia con el resto de la página.

A su vez, la cuenta de Twitter @GreatBusiness7 se había creado en marzo de 2020 y presentaba escasa actividad: 8 seguidores, 15 perfiles a los que seguía y únicamente 38 tweets.

Cuenta de Twitter @GreatBusiness7

En relación a estos últimos, la mayoría se repetían constantemente, una y otra vez, en su objetivo de difundir el mismo mensaje.

- *> 6 8 9 usuarios de Spain en el último mes. Ha oído hablar sobre su alternativa demostrada!!!!!*

- *Esta alternativa nos ha permitido vivir una vida independiente y protegida. Proteja su futuro, porque la verdadera crisis viene después!!!!!*

- *Reinvéntese e !nvierta en su familia. Sus seres queridos merecen el estilo de vida que usted deseaba para ellos!!!!!*

Gracias al contenido de estos tweets fue posible identificar cuentas que empleaban los mismos y seguían un patrón similar, así como nuevos tweets que permitieron llegar posteriormente a otras cuentas.

Tweet que presentaba el mismo contenido y un nuevo enlace acortado

Entre los nuevos tweets identificados aparecía uno realmente interesante. Alguien había cometido un error tipográfico al escribir la palabra "jamás" y se le había colado una letra del alfabeto cirílico, similar en forma a nuestro número seis: "б".

Otro tweet con enlace acortado

La distribución del alfabeto cirílico en el mundo resulta ser la siguiente: Rusia, Bielorrusia, Ucrania, Bulgaria y Macedonia, así como algunas zonas de Bosnia, Montenegro, Serbia y Kosovo; de este modo, la nacionalidad del posible creador del tweet, o la del traductor del mismo al castellano, se acotaba bastante.

Por otro lado, el enlace acortado del primer tweet mencionado, de la cuenta @fineemarketsb, añadía a la URL de destino los siguientes parámetros: "*?ad=1&adgroup=25-UP&amp=&amp=&campaign=ES*", mientras que, el segundo añadía estos otros: "?ad=2&adgroup=25-UP&campaign=ES".

Estos tweets parecían estar asociados a la misma campaña, señalada con anterioridad, dirigida a España.

El error tipográfico mencionado no era el único cometido por este tipo de cuentas, ya que también se apreciaban descuidos a la hora de añadir los respectivos emoticonos en los tweets.

Tweet con error de maquetación

Esto indicaba que el contenido de los tweets era redactado en inglés, para posteriormente ser traducido y maquetado; por ello, de forma probable, en el proceso estaban comprometidas distintas personas, de nacionalidades diferentes.

Además, el enlace acortado del tweet señalaba que este también pertenecía a la misma campaña: "*?ad=8&adgroup=25-UP&campaign=ES*".

El total de los perfiles identificados en Twitter alcanzaba los 14; todos ellos, con el mismo patrón:

- Imagen de perfil e imagen de portada; ambas en sintonía.
- Aspecto de perfil, asociado a un supuesto portal web o empresa.
- Nombre de usuario (@...) y nombre visible de perfil, con características similares.
- Vinculados a un correo electrónico de Gmail y a un teléfono.
- Dominio asociado, visible en el perfil.
- Pocos seguidores. Ninguno superaba los 55.
- Pocos perfiles seguidos. Ninguno superaba los 100.

No obstante, tres de los perfiles detectados se presentaban como cuentas asociadas a una identidad personal: @PereleshinaY, @BelagoY y @AdrianKachalov.

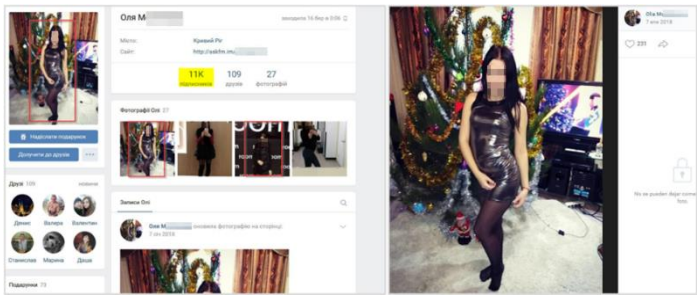
Perfil de Twitter, asociado a "Yana Pereleshina"

El perfil de Yana Pereleshina contaba con una biografía en ruso y con imágenes de lo que parecía ser una chica joven.

Tweet que contenía una imagen de la supuesta Yana Pereleshina

Sin embargo, tras realizar la correspondiente ingeniería inversa sobre las imágenes, se lograba identificar a la persona real ligada a estas.

La cuenta de Yana Pereleshina estaba empleando de forma fraudulenta las imágenes de Olya M., una joven de 26 años residente en Kriviy Rig (Ucrania). Olya M. resultaba ser así una persona completamente anónima, que tenía una cuenta en la red social VK con 11.000 seguidores.

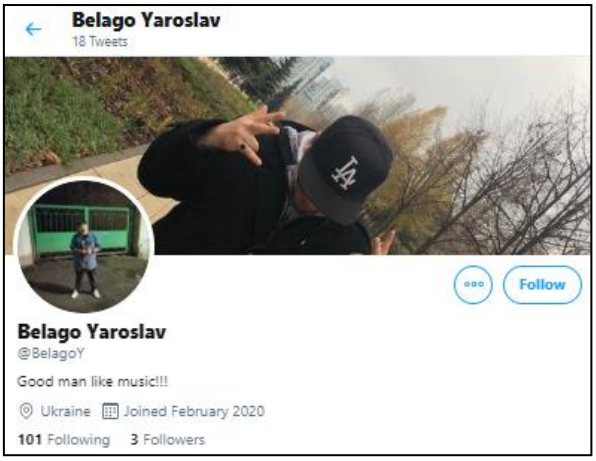


Perfil en VK de Olya M.

Entre los seguidores de la cuenta de Yana Pereleshina, aparecía otra de características similares que parecía estar orquestada del mismo modo: @BelagoY.

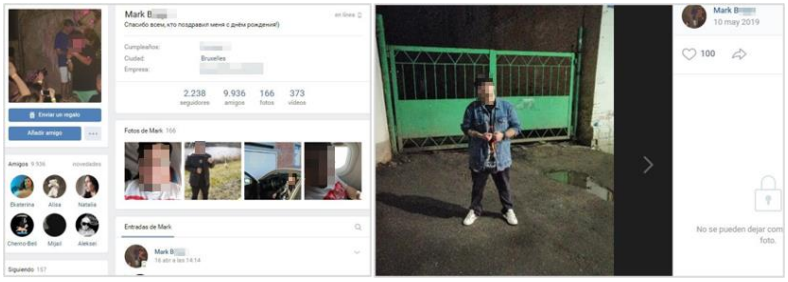
Las cuentas @PereleshinaY y @BelagoY, presentaban el mismo patrón de comportamiento

De este modo, la cuenta @BelagoY parecía estar vinculada a una supuesta identidad personal de Ucrania, que se hacía llamar Yaroslav Belago.



Perfil de Twitter, asociado a "Yaroslav Belago"

De nuevo, otra vez se lograba identificar a la persona que realmente estaba ligada a las imágenes. La cuenta de Twitter de Yaroslav Belago estaba empleando las imágenes de Mark B., un joven de origen ruso que actualmente se encontraba afincado en Bruselas.



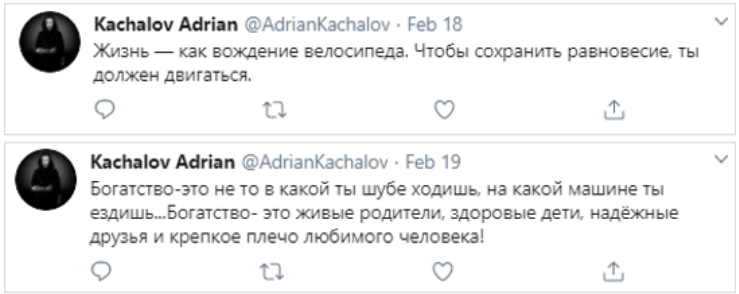
Perfil en VK de Mark B.

La cuenta @BelagoY parecía ser una posible cuenta latente, lista para operar, que todavía no había publicado ningún tweet relativo a la estafa fraudulenta.

Por otro lado, el último de los perfiles vinculados a supuestas identidades personales, la cuenta @AdrianKachalov, aparecía asociada a una persona que se hacía llamar Adrian Kachalov.

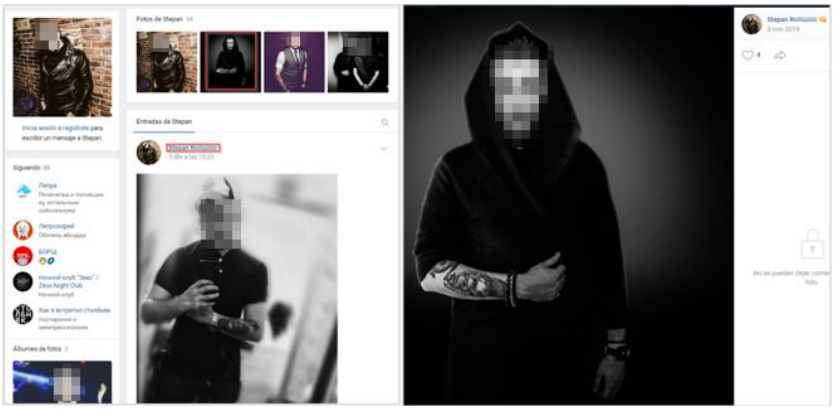
Perfil de Twitter, asociado a "Adrian Kachalov"

La cuenta @AdrianKachalov presentaba una biografía de perfil y tweets, escritos en ruso.



Tweets en ruso, publicados por "Adrian Kachalov"

Otra vez se conseguía identificar a la persona que realmente estaba ligada a las imágenes, que el perfil de Adrian Kachalov estaba empleando; de este modo, las imágenes pertenecían a Stepan R., un ciudadano ruso de la ciudad de Volgograd.



Perfil en VK de Stepan R.

De igual modo, los tweets de la cuenta @AdrianKachalov presentaban enlaces acortados, que mantenían el mismo patrón seguido por las otras cuentas identificadas con anterioridad.

Tweet que presentaba un enlace acortado

Sin embargo, esta vez, el enlace acortado incorporaba en la URL de destino los siguientes parámetros: "*?ad=2&adgroup=25-UP%28bitcoin%29&amp=&amp=&campaign=CL-11.03.20*", lo que permitía identificar que el tweet presentaba vinculación con una campaña dirigida a Chile, que había sido lanzada previamente a la de España.

Con ello se lograban identificar así otras cuentas, que directamente empleaban la imagen de personajes públicos, en función del país al que se dirigiera la campaña, e incluso, que se reutilizaban para diferentes campañas

dirigidas a países distintos, tal como había sido el caso de la cuenta de Twitter @GeekqU.

A principios de diciembre de 2019, la cuenta @GeekqU empleaba la imagen del presentador de televisión chileno Rafael Arenda en sus tweets.

Tweet de @GeekqU, que empleaba la imagen de Rafael Arenda

Estos presentaban enlaces acortados con los siguientes parámetros "*?ad=8&adgroup=1&campaign=CL-04.12.19*", que apuntaban a una campaña dirigida a Chile.

Semanas más tarde, la misma cuenta de Twitter empleaba la imagen del personaje público italiano Christian De Sica.

Tweet de @GeekqU, que empleaba la imagen de Christian De Sica

En los enlaces acortados de tales tweets, a través de los parámetros empleados: "*?ad=V1-11&adgroup=1&campaign=IT-18.12.19*", se apreciaba el rastro de una campaña dirigida, esta vez, a Italia.

Esto indicaba que se estaba ante una estafa internacional de gran magnitud, con recursos suficientes como para ir pivotando de país en país, que generaba así campañas adaptadas y específicas para cada uno de ellos.

Diferentes nombres, una misma estafa

Tal como se ha mencionado al principio, en los antecedentes, el funcionamiento de la estafa resulta ser el mismo en todos los casos: el objetivo final a perseguir por todas estas campañas promocionadas, es seducir a la víctima para que acabe depositando la cantidad de 200/250€ en una supuesta plataforma de inversión.

En España, las estafas digitales en las que la cuantía no supera los 400€, tal como refleja la Ley Orgánica 1/2015 del Código penal, son consideradas un delito leve de hurto que lleva ligado una multa económica de 1 a 3 meses; de este modo, la cifra requerida por la estafa no parece ser casual, teniendo en cuenta que si superase los 400€ estaríamos hablando ya de penas de prisión de entre 6 a 18 meses.

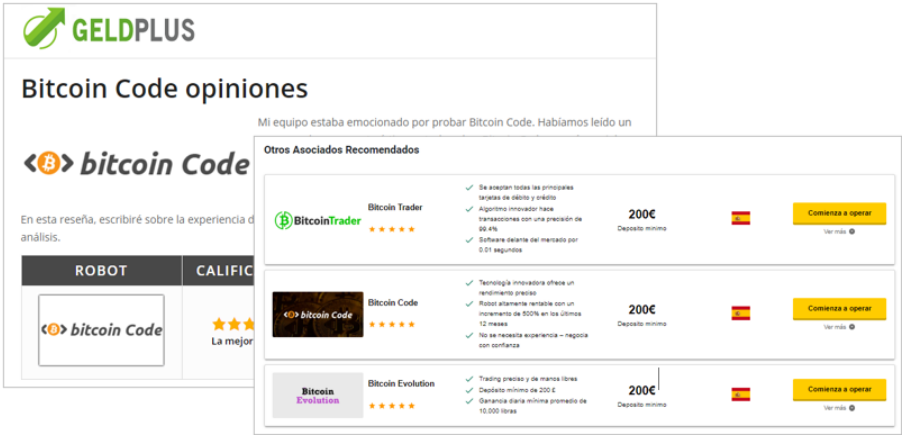
Entre las características más reseñables de esta estafa, hay que destacar así su capacidad de adaptación, cambiando constantemente de forma para que el engaño siga teniendo éxito a lo largo del tiempo.

Hasta ahora, se tiene constancia de que, al menos, la estafa ha empleado los siguientes nombres: *Bitcoin Era*, *Bitcoin Evolution*, *Bitcoin Revolution*, *Bitcoin Profit*, *Bitcoin Future*, *Bitcoin Trader*, *Bitcoin System, CryptoBoom*, *CryptoSoft*, *The Ethereum Code*, Bitcoin Code.

Logotipos de las plataformas fraudulentas, asociadas a la estafa

Sin embargo, no se descarta que esta haya empleado y siga empleando otros nombres, no identificados todavía con tal fraude.

De igual modo, como complemento a las plataformas fraudulentas, también se emplea gran cantidad de dominios y portales genéricos que buscan dar credibilidad a las mismas.



Portales empleados, para promocionar las distintas plataformas fraudulentas

Tal cosa no acaba ahí, ya que al buscar en Google cada uno de los términos referidos a las plataformas implicadas, se puede apreciar que dichas búsquedas están inundadas de anuncios que buscan generar confianza respecto a la estafa.

Anuncios promocionados en Google, al buscar cada uno de los términos

Incluso, con tal de generar mayor confianza en la víctima, se llega a indicar que el creador de tal software es un talentoso desarrollador que se hace llamar Steve Mckay.

Steve Mckay, el supuesto desarrollador de las milagrosas plataformas

Gracias a la imagen que se aporta sobre Steve Mckay, es posible encontrar un artículo en noruego escrito por Av Maja *** *** *****, alojado en la caché de Google, que ya en abril de 2016 habla de la aparición de este tipo de estafas.

Articulo publicado en abril de 2016, que ya refiere a este tipo de estafas

Según comenta el autor del artículo, en un primer momento la estafa presenta el nombre de "Binære opsjoner" (opciones binarias) o "método noruego". Esta consistía en una especie de juego de azar que estaba vinculado a un software/plataforma; sin embargo, para poder participar en dicho juego de azar era necesario ingresar previamente 250€ en una cuenta creada. Al ingresar el dinero, la víctima lo perdía directamente.

En relación a las "opciones binarias", hay dos artículos del diario digital *The Times of Israel* que profundizan en la cuestión y permiten entender bien todo el entramado que hay detrás de ello: https://www.timesofisrael.com/the-wolves-of-tel-aviv-israels-vast-amoral-binary-options-scam-exposed/ y https://www.timesofisrael.com/fbi-says-its-investigating-binary-options-fraud-worldwide-invites-victims-to-come-forward/

En línea con esto, decir que en julio de 2018 la *Autoridad Europea de Valores y Mercados* prohibió la comercialización, distribución y venta de "opciones binarias" en la UE.

A fecha de septiembre de 2017, Av Maja *** *** **** actualizó su artículo e indicó la aparición de una misma estafa, esta vez bajo los nombres de *Bitcoin Code*, *CopyTrader* o *Ethereum Code*.

En este punto, el autor del artículo también adjuntó la mención al supuesto creador de tales plataformas; con ello, se comprueba que, a lo largo del tiempo, se le ha ido cambiando el nombre al supuesto desarrollador.

"Steve Mckay" fue previamente Steffen Madsen

Conclusiones

En síntesis, hay que dejar claro que tal estafa, vinculada a la inversión en Bitcoin, responde a una red internacional bien articulada, con recursos y capacidad operativa suficiente, como para ir adaptándose a nuevos retos y a los requisitos necesarios para abordar campañas orientadas a distintos países.

A su vez, no hay duda de que la cuantía económica empleada en las campañas de publicidad, a través de las distintas redes sociales, así como por medio de las plataformas de anunciantes, redes de afiliados y buscadores, alcanza cifras altamente elevadas, que puede que incluso lleguen a ser superiores a las 7 cifras.

Por otro lado, a día de hoy, Twitter únicamente ha suspendido un par de cuentas (@greatbusiness7 y @SydneyGreaves), de las 14 identificadas en el análisis llevado a cabo, por lo que parece evidente que la red social tiene problemas para detectar correctamente a aquellas cuentas que presentan una actividad anómala y/o sospechosa.

Por último, hay que señalar que este tipo de estafas seguirán dándose, hasta que no haya un esfuerzo claro y decidido por parte de todas aquellas redes sociales y redes de anunciantes implicadas, en las que, a día de hoy, los anuncios relativos a la estafa, operan libremente sin control alguno.

MAZE Flash Note

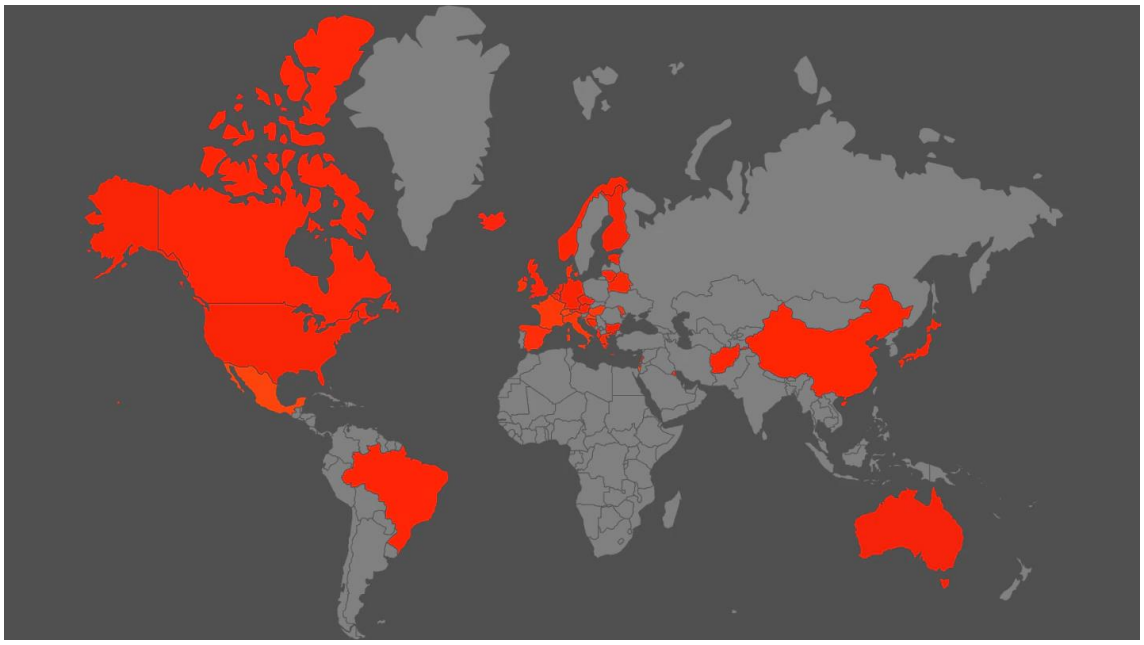
Luis Diago de Aguilar – Derecho de la Red

En el boletín de este mes creemos que no puede faltar **Maze**. Durante el último periodo de tiempo ha sido uno de los protagonistas en diferentes ocasiones y vamos por tanto a analizarlo un poco más en profundidad. Veremos sus tácticas, técnicas y procedimientos (TTPs) resumidos, adjuntaremos todos los enlaces usados para su posterior consulta de forma más técnica.

Nota: no pretendemos hacer un informe técnico al 100%, si no un informe para que todos los usuarios de todos los niveles comprendan la amenaza y puedan aprender sobre inteligencia.

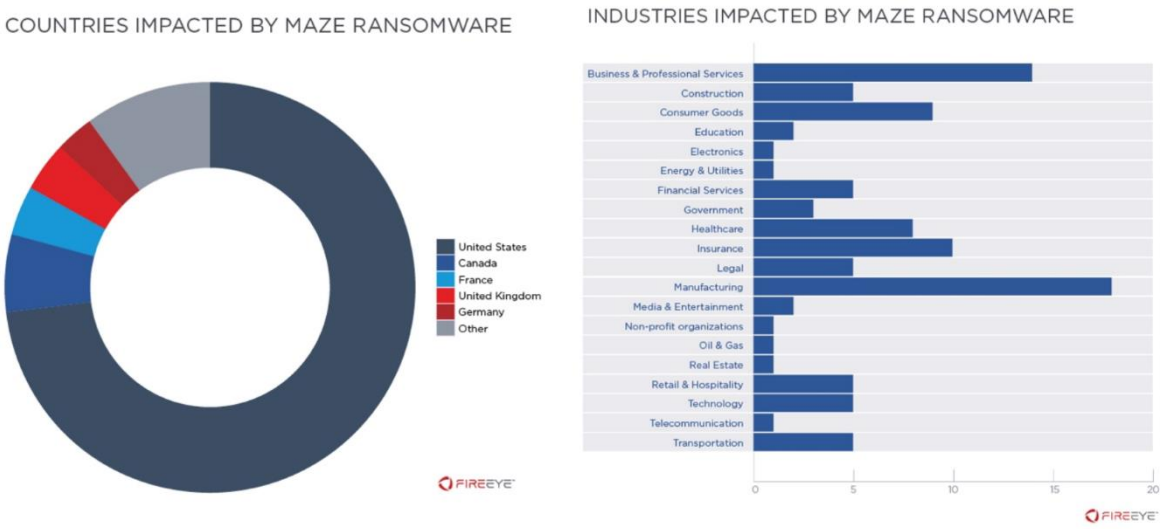
Zonas de actuación

Este grupo adopta como zonas de actuación países de casi todos los continentes, **McAfee** en un reporte sobre esta amenaza adjuntaba el siguiente mapa:



En el mapa podemos ver que se centra sobre todo en las zonas más avanzadas en lo que a tecnología se refiere.

FireEye también nos mostraba hace unos días datos sobre esta amenaza, que, como puede verse afecta sobre todo a EEUU a fecha del informe:

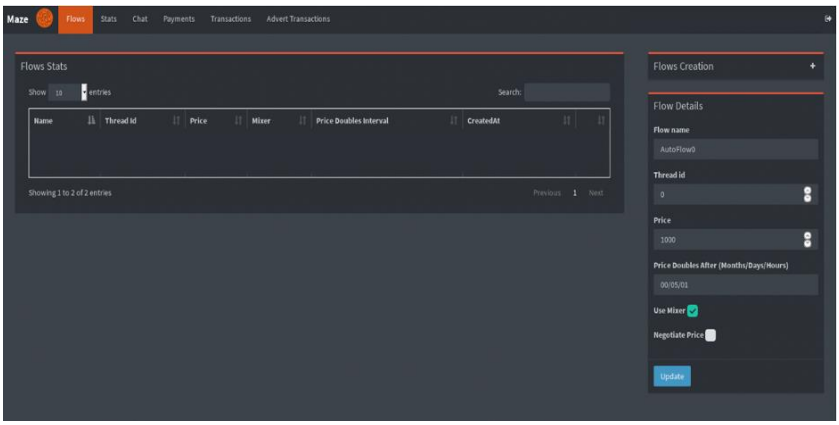


En la imagen podemos ver a las industrias más afectadas por el ransomware de Maze.

Características

Si analizamos las campañas de este Actor encontramos que pueden identificarse diferentes técnicas para obtener acceso, principalmente utilizando kits de exploits, conexiones de escritorio remoto o suplantaciones de correo electrónico con adjuntos que incluyen macros para ejecutar el malware.

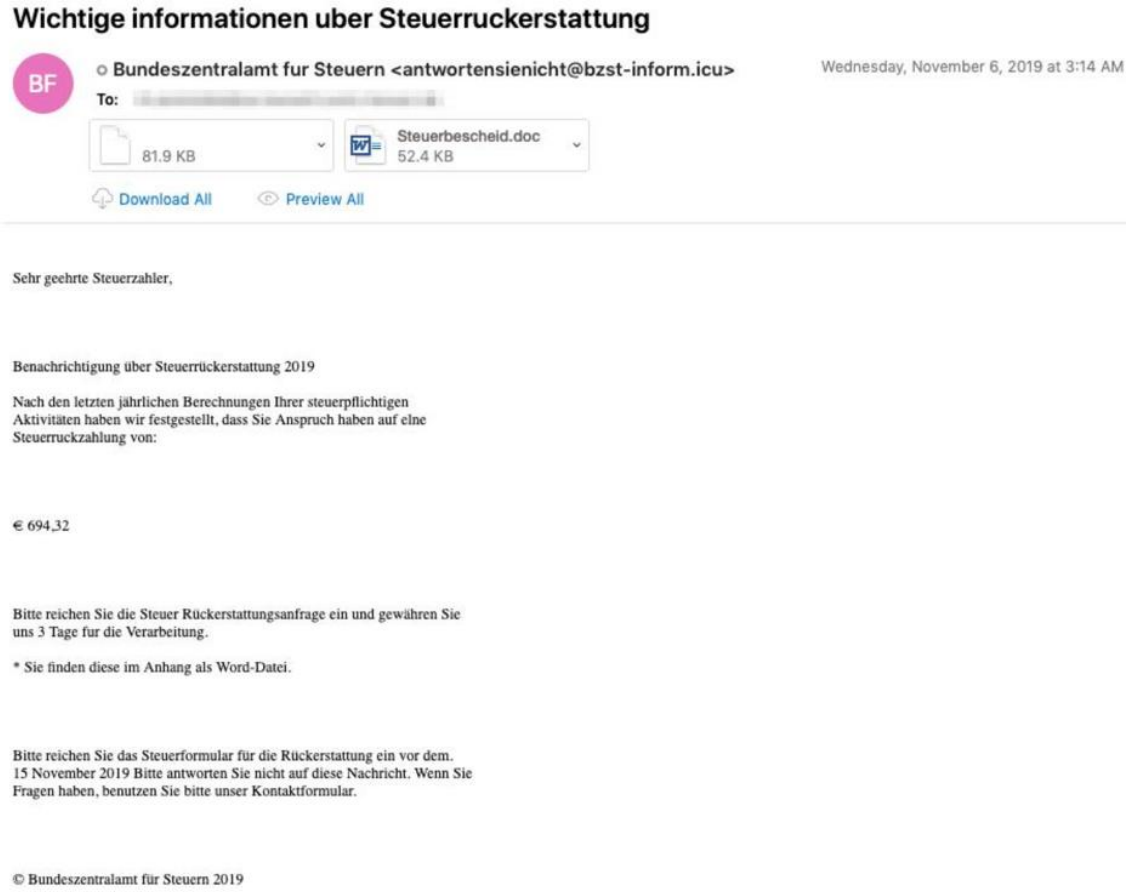
Algunos de estos kits son: Fallout o Spelvo.



En la foto anterior podemos ver un panel de control del ransomware Maze. Desde estos paneles los atacantes pueden interactuar con los equipos infectados y lanzar comandos a los mismos.

Campañas de Malspam

Las campañas de spam malicioso son el principal vector de entrada y la mayor vía de propagación. En el informe de FireEye podemos encontrar capturas de mensajes que cumplen esta tipología.



Wichtige informationen uber Steuerruckerstattung

BF ○ Bundeszentralamt fur Steuern <antwortensienicht@bzst-inform.icu> Wednesday, November 6, 2019 at 3:14 AM

To:

81.9 KB | Steuerbescheid.doc 52.4 KB

Download All | Preview All

Sehr geehrte Steuerzahler,

Benachrichtigung über Steuerrückerstattung 2019

Nach den letzten jährlichen Berechnungen Ihrer steuerpflichtigen Aktivitäten haben wir festgestellt, dass Sie Anspruch haben auf eine Steuerruckzahlung von:

€ 694,32

Bitte reichen Sie die Steuer Rückerstattungsanfrage ein und gewähren Sie uns 3 Tage fur die Verarbeitung.

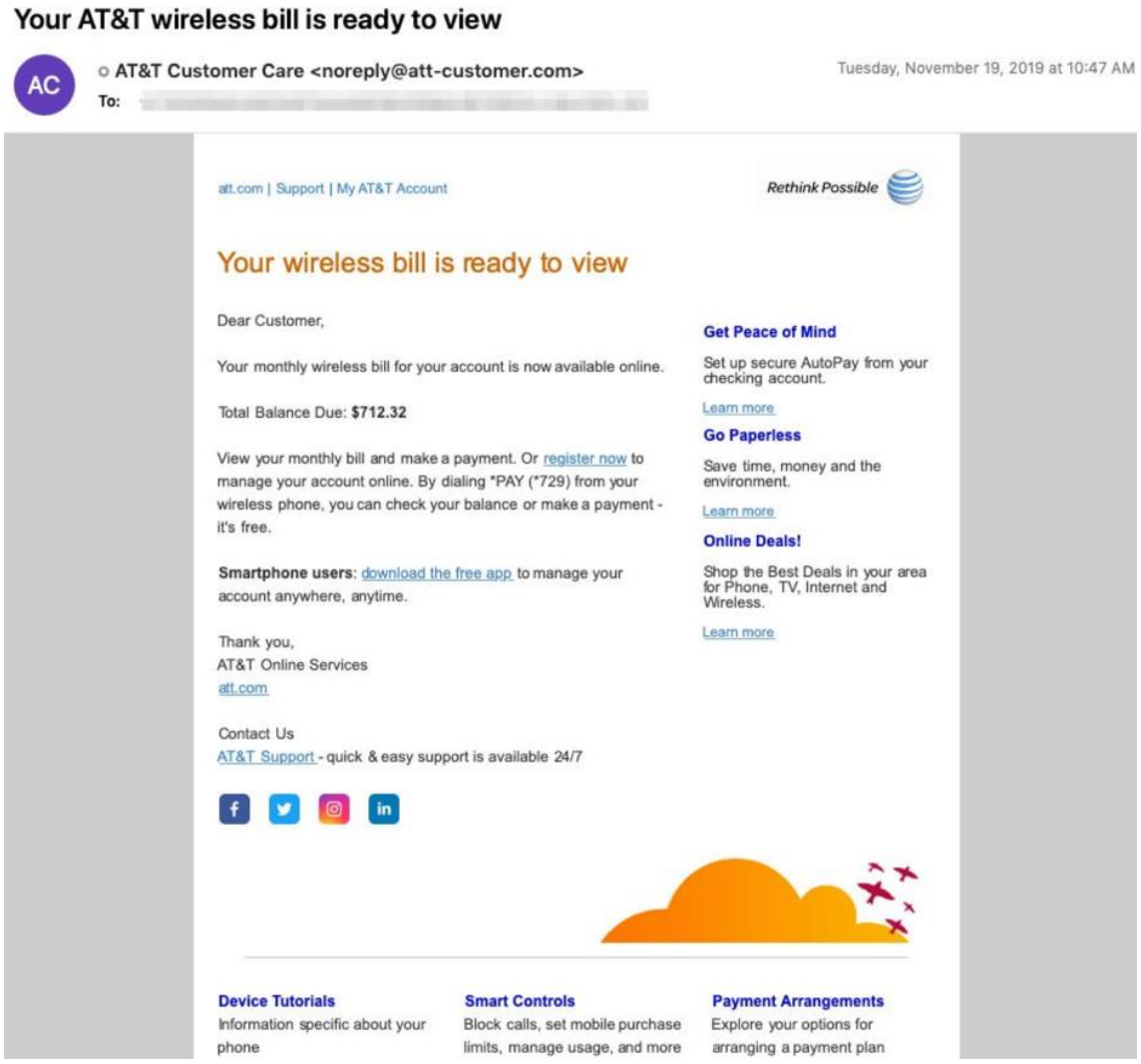
* Sie finden diese im Anhang als Word-Datei.

Bitte reichen Sie das Steuerformular für die Rückerstattung ein vor dem. 15 November 2019 Bitte antworten Sie nicht auf diese Nachricht. Wenn Sie Fragen haben, benutzen Sie bitte unser Kontaktformular.

© Bundeszentralamt für Steuern 2019

En la siguiente imagen podemos ver como se suplanta a una entidad conocida para intentar que parezca que se trata de un mensaje legítimo.

En este caso la entidad afectada por la suplantación es AT&T.



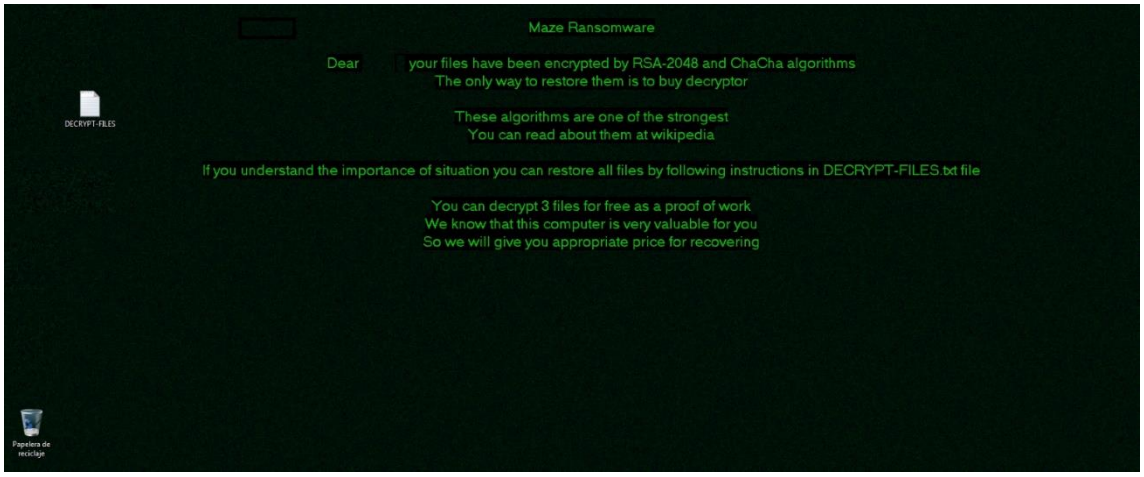
Rescates

Una vez el usuario ha bajado el malware incluido en el malspam y se ha propagado el ransomware, Maze, aprovecha para pedir un rescate, si este no se cumple, aprovecharán para exfiltrar datos privados de la empresa.

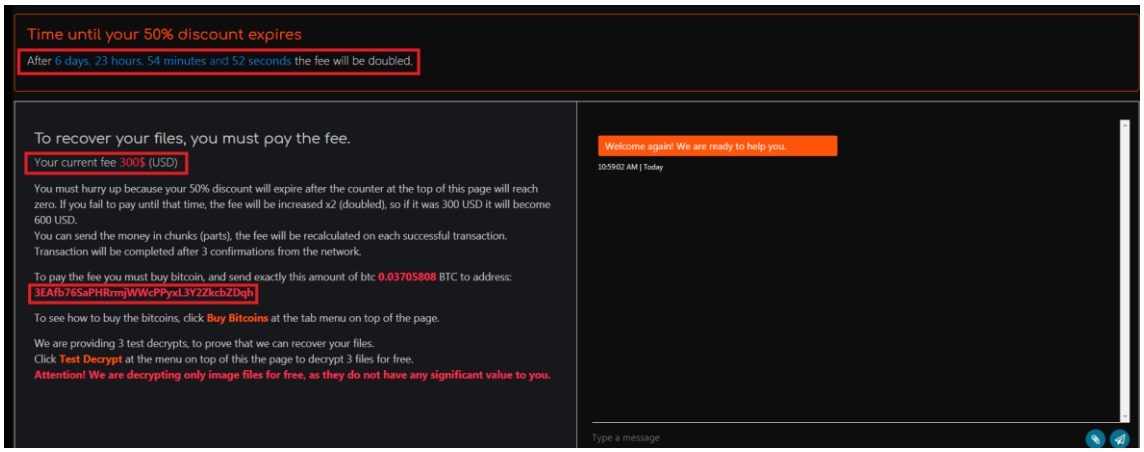
Esto supone una presión adicional contra las empresas que se verán coaccionadas y chantajeadas.

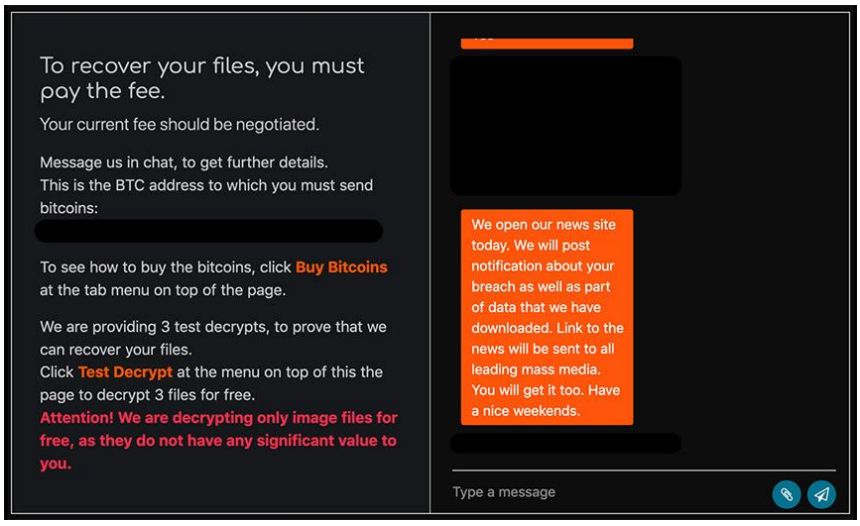
Se han detectado patrones diferentes según el actor que esté tras la infección mediante este malware.

Cuando nuestro equipo se infecta con Maze, en nuestro escritorio nos aparece un mensaje como el siguiente:



También os adjuntamos una imagen de la página de pago que aparece durante una infección de este tipo. Contiene incluso su propio chat para interactuar con los atacantes.





IoCs

Adjuntamos a continuación una pequeña lista de IoCs en el Anexo 2.

Fuentes para consulta

Os proporcionamos una lista de los enlaces usados durante este reporte y de otros enlaces que pueden servir para consultas a aquellas personas que quieran profundizar más en la amenaza.

- https://www.fireeye.com/blog/threat-research/2020/05/tactics-techniques-procedures-associated-with-maze-ransomware-incidents.html
- https://www.mcafee.com/blogs/other-blogs/mcafee-labs/ransomware-maze/
- https://success.trendmicro.com/solution/000250200-Maze-Ransomware-Attack-on-a-US-IT-Firm
- https://blog.redteam.pl/2020/05/sodinokibi-revil-ransomware.html
- https://labs.sentinelone.com/maze-ransomware-update-extorting-and-exposing-victims/
- https://www.crowdstrike.com/blog/maze-ransomware-deobfuscation/
- https://cyberflorida.org/2020/04/24/maze-ransomware/
- https://www.theregister.co.uk/2020/04/21/cognizant_maze_malware
- https://es.cointelegraph.com/news/maze-hacker-group-claims-infecting-insurance-giant-chubb-with-ransomware

Anexo 1. IoCs de SilverTerrier y Agent Tesla

IPs:

185.126.202.111

23.95.132.48

Dominios:

academydea[.]com

coffiices[.]com

goldenlion[.]sg

goldhhofer[.]com

goldlion[.]sg

hojokk[.]com

hokokk[.]com

ladbible[.]com

mecharnise[.]ir

mikeservers[.]eu

modcloudserver[.]eu

petroindonesia[.]co[.]id

posqit[.]net

reynoldsgh[.]com

sylvaclouds[.]eu

uzoclouds[.]eu

welheadcontrol[.]com

Hashes:

00a9db70a41ca50aa6a99345ca63e63af0c9a4d9

092391846c8553da1a40d3586945a5df

0ae2aaeb2938cf4c777be4aa192e4994020609f5640add8e7296de9ff34eb227

1155701d076bdb7859aee4469d7031b16ca4f0e7

14394063d006546430a86a885417fe2463d2594a

16b35e258a234b05c9034410faf5ff2464ebdb48

1772e753961265b36a41fcc9ee32044d

1ee6646e0ea9ceb6fa1721f809bd3cdaeb38c6b2bdd7171b340097c237527568

241f09feda09dc33b86e23d317bc2425f4d43b91221815caa5eb055a9a97be74

27d601ef1a2b340b6b644493a627064f60ad8a95271248e00f7bb54a59abb069

27ffbd2ba9216b1c3476d4b465d5721a

28da69231488771a16f666e982a3353a8bb054a4

313e99e54ca50189908d9b59f27e30eb572e815e

31d2ef10cad7d68a8627d7cbc8e85f1b118848cefc27f866fcd43b23f8b9cff3

3335ebffd8b4ab739db99f68cd6d79caa39c1210c274bbe4166194cc26de4123

39419cf0c4a2aec86db7e87aaecf2972ed7cddb6

3ac570ece5e73d5e4e48df28de2ab28bed53436f

421df0bf9a7e850108055593ca47ea24

442e4f13bc586440d05b5736a8a40516

47efa008c600b2b0394ce3230345a901

4972fac34f773668a523ef51b4898387

4a84e57f0b3e7868cea1904cce9c1c7e

4b8b49bdfa435d0faba2e3964b04e20bbfc86aa4ffc3c3b8e1449894892f125b

4ccf34a84fb8b857f1ded666c93fdcf062d26c47

5185871926a3d76d90ded3754cf80e87

563b1c6252612d06b714bf29b9f53f7aade4c7ac6658b2d0c774a7e244ea83da

589a1900b210826e97ec8da3c5c40f707963146e934393eb15e1b07a1398912c

58ad7eae8866af7a058a9eb4034a2557

5f3e254e5431866f3827e8b49b7d1435

6041fc3d78207e31cb053276c2b2873ee573ac5c

62523aaf31e6d489bdca6d74d19a1927

6b52e6e93ec0774bc275e3f82ddd0d15

6bbf26ad27f7848810e259cac35f1188f54cddaa

715605d64b12a3a961183e4f0b3912fc75827ee4

7b2512d06723cc29f80ae8c8d6df141f27bc9d962ae76b5651b84d7be4379bba

7f661c6f5ebba3eca82e1dbf1a96e27f2503da405093464538d90dc113a7b439

8037a8e12e8cacdaca24b993ffdbd8cdc63ec29dd78eee136083fa09049dbf0c

80b86324201ddecd36225a1c29f3cdc5

83457e2b8f9209ec1c987b1a0bee65140cc41d1d59ed38f1d1ad160ea0d1d13c

8d75fa4fa19262fbb90b272016e8fb11

8f2ccd9692400fd2a012de48de931940092351ff

8f56fb41ee706673c706985b70ad46f7563d9aee4ca50795d069ebf9dc55e365

9498ba71b33e9e9e19c352579e0d1b0a

950131767229dfc275cadc8b86832859

99ec42d89a369a63e6059d7eb805cd7c7fe81d00

9f5814aa51e0e28c230cb93b0cb7f1f3dd66e374

a234e562b665a53385e205996231a355

aff38fe42c8bdafcd74702d6e9dfeb00fb50dba4193519cc6a152ae714b3b20c

b421129407ec3238fa3092c30d3d80d4

b4aec5b451708ddb0d6abefa698d65b70eb0817b

b58e386928543a807cb5ad69daca31bf5140d8311768a518a824139edde0176f

bbfa96c5ae64d9ed61c0c6bad5fc4185

c1b04a9474ca64466ad4327546c20efc

c5c43b340957830f5d7484ce06f9de0ef593d88f3d48c09cd2150e670661f672

c7396711136f5436f944fa966a53b64c7bb32eb2

c81f446422337416cedb324fcc678015983fdb4c

ce43ba757dcc353a9bf1df0a60ad756f81ac83e4

d731fb3fcc6ecd266251408a282ef4409eac94ce25cecadbfcb2df08e7ca7693

d80a440755dc15803db459b15b991d1abe81054f0942d054d965a578b92917b7

d80cc7eb66e11a56e71745fae8e66da096fae6e4

d91568e23ae0ece0181f4cc021c975cb758f9c87

da26ba1e13ce4702bd5154789ce1a699ba206c12021d9823380febd795f5b002

dd0802b2a4c476917099862193e7ab08

e0e03f5dcf68b47cae8f3cf2466275c4

e365100468e9472518d1875796932a8085ab29f6bbfe3357928fa9cc6187628b

e822943f7a8f47ef1da431af917a70f42ec3a0de

ef111eb4c0f4089e1a042b2f210ee13e5a56349e

f7183d3a992ead2bf194ac46b1f6f70ad9e30bfd5b6065ffbd96a3529c311725

f7b9219f81772e928ab0fbd0becbcf10ca3792ce211bb4a7fa68b41050bdb220

URL:

http://academydea[.]com/alhaji/Panel/five/fre.php

CVE:

CVE-2017-11882

Anexo 2. IoCs MAZE

91514e6be3f581a77daa79e2a4905dcbdf6bdcc32ee0f713599a94d453a26fc1	**Ransom.Win32.MAZE.THKBIAI**
e8a091a84dd2ea7ee429135ff48e9f48f7787637ccb79f6c3eb42f34588bc684	**Ransom.Win32.MAZE.H**
04e22ab46a8d5dc5fea6c41ea6fdc913b793a4e33df8f0bc1868b72b180c0e6e	**Ransom.Win32.MAZE.THKBIAI**
067f1b8f1e0b2bfe286f5169e17834e8cf7f4266b8d97f28ea78995dc81b0e7b	**Ransom.Win32.MAZE.THKBIAI**
1161b030293e58d15b6a6a814a61a6432cf2c98ce9d156986157b432f3ebcf78	**Ransom_Gen.R011C0PKA19**
153defee225de889d2ac66605f391f4aeaa8b867b4093c686941e64d0d245a57	**Ransom.Win32.MAZE.THKBIAI**
195ef8cfabc2e877ebb1a60a19850c714fb0a477592b0a8d61d88f0f96be5de9	**Ransom.Win32.MAZE.THKBIAI**
30b72e83d66cbe9e724c8e2b21179aecd4bcf68b2ec7895616807df380afab54	**Ransom.Win32.MAZE.THKBIAI**
33afa2f1d53d5279b6fc87ce6834193fdd7e16e4b44e895aae4b9da00be0c502	**Ransom_Maze.R002C0DC720**
4080402553e9a86e954c1d9b7d0bb059786f52aba4a179a5d00e219500c8f43d	**Ransom.Win32.MAZE.THKBIAI**
5603a16cbf81d183d3ff4ffea5477af1a4be01321865f0978c0e128051ec0a82	**Ransom.Win32.MAZE.THKBIAI**
58fe9776f33628fd965d1bcc442ec8dc5bfae0c648dcaec400f6090633484806	**Ransom.Win32.MAZE.THKBIAI**
5c9b7224ffd2029b6ce7b82ea40d63b9d4e4f502169bc91de88b4ea577f52353	**Ransom.Win32.MAZE.THJBBAI**
6878f7bd90434ac5a76ac2208a5198ce1a60ae20e8505fc110bd8e42b3657d13	**Ransom_Instructions.R002C0PCK20**
6a22220c0fe5f578da11ce22945b63d93172b75452996defdc2ff48756bde6af	**Ransom.Win32.MAZE.THJBBAI**
822a264191230f753546407a823c6993e1a83a83a75fa36071a874318893afb8	**Ransom.Win32.MAZE.THKBIAI**
83f8ce81f71d6f0b1ddc6b4f3add7a5deef8367a29f59b564c9539d6653d1279	**Ransom_Maze.R002C0DCK20**
877c439da147bab8e2c32f03814e3973c22cbcd112d35bc2735b803ac9113da1	**Ransom.Win32.MAZE.SMDA**
91514e6be3f581a77daa79e2a4905dcbdf6bdcc32ee0f713599a94d453a26fc1	**Ransom.Win32.MAZE.THKBIAI**
9751ae55b105ad8ffe6fc5dc7aea60ad723b6df67a959aa2ea6f4fa640d20a71	**TROJ_GEN.USMGAHAL**
9ad15385f04a6d8dd58b4390e32d876070e339eee6b8da586852d7467514d1b1	**Ransom.Win32.MAZE.G**
9be70b7fe15cd64aed5b1adc88c2d5270bce534d167c4a42d143ae0059c3da1c	**Ransom.Win32.MAZE.C**
b30bb0f35a904f67d3ac0082c59770836cc415dc5b7225be04e8d7c79bde73be	**Ransom.Win32.MAZE.THKBIAI**
c040defb9c90074b489857f328d3e0040ac0ddab26cde132f17cccae7f1309cc	**Ransom_Mazedec.R002C0DDE20**
c11b964916457579a268a36e825857866680baf1830cd6e2d26d4e1e24dec91b	**Trojan.Win32.SMOKELOAD.SMD2.hp**
ea19736c8e89e871974aabdc0d52ad0f0948159d4cf41d2889f49448cbe5e705	**TROJ_GEN.R002C0DDE20**
ecd04ebbb3df053ce4efa2b73912fd4d086d1720f9b410235ee9c1e529ea52a2	**Ransom.Win32.MAZE.SMDA**
F491fb72f106e879021b0bb1149c4678fb380c255d2ef11ac4e0897378793f49	**TROJ_GEN.USMGAHAL**
c84b2c7ec20dd835ece13d5ae42b30e02a9e67cc13c831ae81d85b49518387b9	**Ransom.Win32.MAZE.SMDA**
042273f30363405ee416ca4dae6f0279668dfc5ea742c0e265b9553798a90ae5	**Ransom_Maze.R03FC0DAI20**
0f1cbf09b19fc9963742e3f60def1434fa86ac760790fb974a6b5fcd81b4881f	**Ransom.Win32.MAZE.SMDA**
4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a	**Ransom.Win32.MAZE.AC**
9845f553ae868cd3f8d8c3f8684d18f226de005ee6b52ad88b353228b788cf73	**Ransom.Win32.MAZE.AD**
5470f0644589685000154cb7d3f60280acb16e39ca961cce2c016078b303bc1b	NORMAL