Boletín Mensual Comunidades 07/2020

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

Contenido

Nota de redacción

Ya es habitual escribir unas palabras en los boletines, y como no, en este no iba a ser diferente.

Ante todo, disculpadnos por la tardanza, una serie de impedimentos personales nos han surgido a lo largo de la realización del mismo y esto no hizo retrasar la salida de éste.

Agradecer a las comunidades su participación y sus aportes para poder seguir manteniendo estos boletines de libre distribución.

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 😉

Finalmente ¿qué sucederá?...

Daniel Mery – HackMadrid %27

Las tecnologías con mayor empuje en el siglo XXI –robótica, ingeniería genética y nanotecnología– amenazan con convertir a los seres humanos en una especie en peligro de extinción.
Bill Joy

Las diferentes tecnologías presentes en la actualidad han impactado de modo muy pronunciado procesos, económicos, sociales y finalmente culturales. Lo que comenzó siendo un método de automatización y facilitador de la producción abarcó la totalidad de la vivencia cultural, las experiencias educativas, científicas, industriales, sociales, el mundo del entretenimiento, fue alojandose en las relaciones interpersonales. Resumiendo, logró establecer un verdadero cambio "copernicano", que se expresa en el día a día de cualquier persona. Los computadores personales iniciaron esta travesía, que continúo con el "móvil", rodeado de Internet, la transmisión satelital, la fibra óptica y el mundo web marcó un hito en los finales de los 90. Los gigantescos "Data Centers", la inteligencia artificial, el machine learning gestionaron la "trillonaria" cantidad de petabytes de datos producidos por dispositivos y aplicaciones, nació una sociedad basados en los datos, cuya utilidad es transformarlos finalmente en información. Una línea de tiempo de pocas décadas en las que pasamos del "reino" del PC a la WEB, la sociedad de los datos y el actual mundo digital, ahora deberemos observar la influencia que nos depare, la realidad virtual, la computación cuántica y las tecnologías 5G, una base fundamental para la robótica y la inteligencia artificial.

Pero aún hoy, en este futurista escenario del actual presente, el ser humano sigue siendo el origen y el principal protagonista de la historia, o sea de las decisiones. La pregunta que todos tenemos en nuestra intimidad es ¿ por

cuánto tiempo ? Un terreno lleno de especulaciones, teorías, sueños y esperanzas.

Frente a este fenómeno en curso hay varias opiniones formadas, entre el blanco y el negro, hay una variedad de grises, pero solamente valoraremos las posiciones mas extremas y opuestas. Muchas personas, en general la parte más vieja de la población, suele demonizar la tecnología como la creadora y gestora de todos los males que nos rodean, aunque realmente estos "males" están anidados en los ciudadanos y las culturas que formaron en entornos sociales concretos. Este sector sufre una suerte de añoranza, en el que todo tiempo pasado fue mejor. Los videojuegos, las redes sociales, el blockchain y otras tecnologías son las culpables de la violencia, del narcotráfico y otras malas "yerbas". Como si la guerras Púnicas, o la batalla de las Termópilas hubieran sido engendradas por un antiguo "Call of Duty", o quizá, el narcotráfico y el lavado de dinero nunca existieron antes del 2009, fecha del nacimiento del Bitcoin. Obviamente, intentar diseñar un futuro basado en estos preceptos nos conducen a una práctica "Amish" <que por cierto no son los únicos>, pero sin lugar a dudas este sistema o estilo de vida basado en tales supuestos, es totalmente inviable para un mundo con más de 7000 millones de terrícolas.

En el otro extremo del "arco iris" residen los ingenuos, me refiero a aquellos que creen que no hay problema humano o material que no lo pueda resolver una aplicación WEB o para el móvil. La magia de la inteligencia artificial y el machine learning, algo como héroes de un cómic virtual, resuelven todo tipo de problemas humanos y materiales. La reciente pandemia ha dejado una evidencia interesante, un simple microorganismo, microscópico y sin habilidades para reproducirse así mismo, puso de "rodillas" a una sociedad presuntuosa de poseer una tecnología sin precedentes en toda nuestra historia. Los ciberdelitos, entre los cuales debemos incluir el uso indebido de los datos por parte de corporaciones e instituciones, que "azotan" a Internet con todo tipo de ataques a infraestructuras, tarjetas de crédito, extorsiones, ransomware, phishing, ddos, ingeniería social, etc, son "modelos de negocio" permanentes. Muchos años atrás decidimos subir toda nuestra vida (personal, social y económica) a Internet, y ahora un "monstruo" nos devora implacablemente, programas inseguros e ineficientes, infraestructuras con la mismas características, y como única solución posible, seguimos haciendo todo como hasta ahora, el gran negocio consiste en administrar el desastre cometido por la ausencia diseño y métodos científicos en el desarrollo. Concluyendo, en lugar de I+D aplicamos P+P (parche más parche). El deseo de "mano de obra barata", una formación inconsistente y parcial, son las verdaderas responsable de las vulnerabilidades encontradas cada día. Urge que los actores vinculados al mundo tecnológico comiencen a valorar el

"conocimiento" y establezcan una nueva relación con la enseñanza, que vaya más allá de emitir certificados de dudosa calidad en cuanto a conocimiento y habilidades.

Ahora bien, retomando el origen de esta reflexión, al comienzo de la nota hay una cita a un pensamiento de Bill Joy (William Joy), es un abordaje de gran perspectiva a la tecnología y sus consecuencias en términos estratégicos. Bill Joy es uno de los grandes "genios" en el nacimiento del software libre y uno de los responsables del mundo tecnológico en el que vivimos. Construyó su conocimiento desde las raíces del mundo físico -llamado hardware-, es Ingeniero Electrónico, además de Doctor en ciencias de la computación -llamado software-, contemporáneo y profesor de una camada de "hackers" de la Escuela de Berkeley… ¿os suena BSD? Berkeley Software Distribution. Creador y desarrollador del legendario VI (editor), además de reescribir todo el código Unix (privativo) en BSD (software libre), increíblemente realizó esta tarea en un fin de semana, cosas de una mente privilegiada. Fue cofundador de Sun Microsystem (Stanford University Network) y principal inspirador de NFS (Network File System), de los microprocesadores SPARC, de Java programming language, Jini (Apache River) / JavaSpaces (Tuple space), y JXTA (Juxtpoxe). Precedió a Richard Stallman y Linus Torvalds en casi 8 años, un verdadero "Padre Fundador" del software libre. A partir de los años 2000 se dedicó a reflexionar sobre el futuro de la tecnología, de la cual es uno de sus principales artífices. Escribió un memorable artículo "**Por qué el futuro no nos necesita"**, que ofrece su visión sobre este fenómeno tecnológico, una visión crítica y honesta intelectualmente, claro que leerlo es solo para "nutrirse", informarse, pensar y reflexionar, no porque lo haya escrito Bill Joy debe ir sin más a "misa".

"Allá en aquel bar de hotel, Ray Kurzweil me remitió a una serie de pruebas extraídas de su libro La Era de las Máquinas Espirituales, entonces a punto de aparecer. En esta obra, trazaba las grandes líneas de una utopía visionaria: una utopía según la cual, uniéndose a la tecnología robótica, el ser humano se convertiría en una criatura inmortal. Al hilo de las páginas, mi sentimiento de malestar fue creciendo: no sólo Ray, con toda seguridad, minimizaba los peligros de una vía como aquella, sino que reducía del mismo modo la importancia de sus potenciales efectos devastadores".

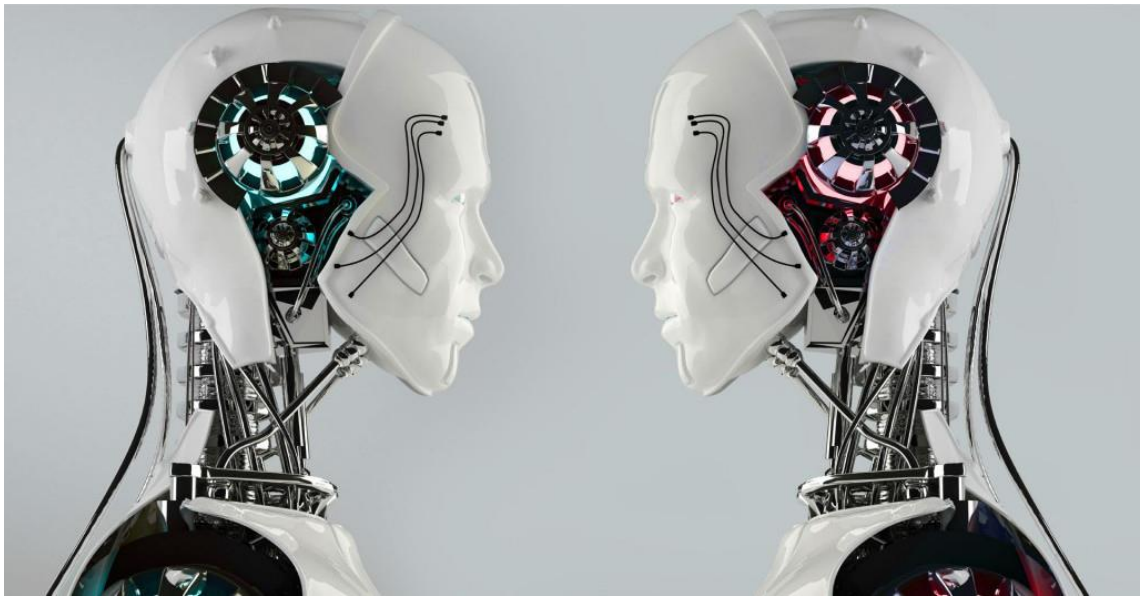
La anterior cita del artículo de Bill Joy plantea una utopía, no exenta de consecuencias peligrosas, la cual podría generar una reacción distópica, algo así como un nuevo desafío para los Ludditas -movimiento surgido en Inglaterra en el siglo XIX, que destruyó las máquinas por considerarlas perjudiciales para los artesanos-. Los investigadores informáticos logran

crear máquinas inteligentes, muy rápidas y eficaces que vuelven superfluo cualquier esfuerzo humano, frente a lo cual son posibles dos opciones: dejar a estas máquinas absolutamente dueñas de sus decisiones, sin supervisión humana, o bien, mantener la supervisión humana -algo que sucede actualmente-. La primera opción nos conduce a una posible respuesta dada por Bill Joy.

"***A medida que la sociedad y sus problemas se van haciendo más complejos, y las máquinas más inteligentes, la gente irá dejando sus decisiones en manos de las máquinas, simplemente porque las decisiones tomadas por máquinas obtendrán mejores resultados que las tomadas por humanos. Con el tiempo podría llegarse a una fase en la cual las decisiones necesarias para mantener el sistema en funcionamiento sean tan complejas que los seres humanos no puedan tomarlas de forma inteligente. En esta fase, las máquinas tendrán de hecho el control. La gente no podrá apagar las máquinas porque dependerán tanto de ellas que apagarlas equivaldría a un suicidio".***

Una opción alternativa a la anterior distopía es el futuro planteado por visionarios de la talla de George Orwell, Aldous Huxley, Ray Bradbury, Isaac Asimov y Yevgueni Zamiatin. Veamos que plantea Bill Joy….

"La opción alternativa sería servirse de las máquinas para controlar al hombre. Si en una tal hipótesis, el individuo lambda conserva la dirección de ciertos aparatos personales tales como su coche o su ordenador, el de los sistemas de gran envergadura serían monopolio de una élite restringida, como ocurre de hecho hoy en día, pero mayor. Con la evolución de las técnicas, esta elite ejercerá sobre las masas un control reforzado. Y, puesto que en este estadio la mano de obra humana no será necesaria, las masas mismas serán superfluas. No serán más que un fardo inútil entorpeciendo al sistema".



Continúa Bill Joy valorando posibles soluciones ofrecidas en esta consideración distópica, aquí es necesario aclarar que la anterior cita y la dos a continuación, son en realidad citas que realiza Bill Joy de Theodore Kaczynski aka Unabomber……

"Si la elite en cuestión es cruel, puede decidirse simplemente a exterminar a la humanidad. Si la elite se comporta humanamente, puede recurrir a la propaganda y a otras técnicas psicosociales o biológicas para provocar una caída de las tasas de natalidad de tal magnitud que el grueso de la humanidad acabará por extinguirse. La élite podrá entonces imponer sus puntos de vista al resto del mundo. Estando, la élite, constituida por demócratas de corazón tierno, pueden tomar el papel de granjeros, criando con benevolencia al resto de la humanidad".

Finalmente la última cita sobre esta posibilidad distópica…

"Sus pastores velarán que todas las necesidades materiales sean satisfechas, a que una educación sea garantizada a todos los niños en un clima psicológicamente sano, a que cada uno se ocupe con pasatiempos higiénicos, si alguien está descontento que siga el "tratamiento" destinado a "arreglar" su problema. Bien entendida, la vida estará tan vacía de sentido que será conveniente someter a los individuos a manipulaciones biológicas o psicológicas, ya sean destinadas a erradicar toda veleidad de poder, sean destinadas a sublimar esta sed de poder en algún pasatiempo inofensivo. En una sociedad como esa, estos seres humanos manipulados vivirán quizás felices; pero la libertad les será totalmente extraña. Les habrán

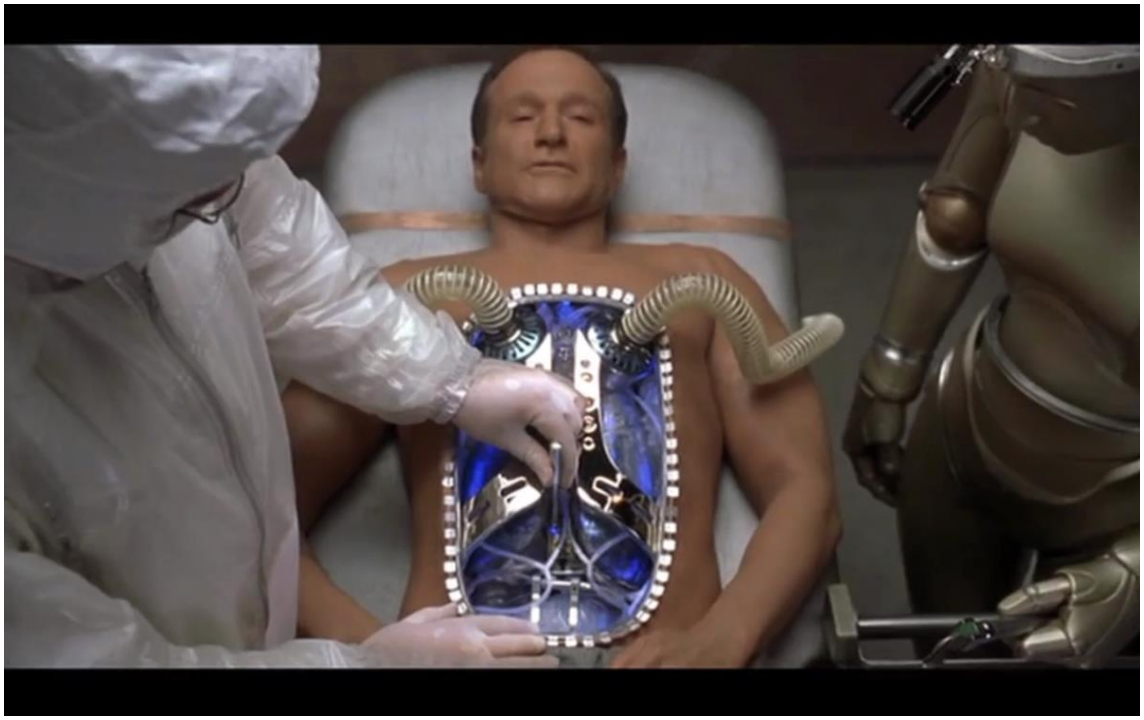
reducido al rango de animales domésticos".

Creo que es honesto citar textualmente a Bill Joy, para que no haya "falsas o malas interpretaciones sobre los pensamiento de Unabomber…

"Los actos de Kaczynski son criminales y, a mis ojos, la marca de una locura asesina. Estamos claramente en presencia de un "luddita". Sin embargo esta simple constatación no invalida su argumentación. Me cuesta, pero he de admitirlo: en este pasaje preciso, su razonamiento es digno de atención. He sentido la necesidad imperiosa de tomar al toro por los cuernos".

Bill Joy se apoya en el libro **"Robot: Madre Máquina o la Mente"** de Hans Moravec -experto en robótica, miembro de la Universidad de Carnegie Mellon-. Cuyas citas aportan luz a esta reflexión…..

"En un contexto de liberalismo sin freno, robots que presentaron un grado de evolución superior no dejarían de modificar al hombre del mismo modo que los placentados de América del norte modificaron a los marsupiales del sur (igual como el hombre a afectado a multitud de especies). Las industrias de la robótica librarán una feroz competición en la carrera por la materia, la energía y el espacio, aumentando de paso sus beneficios para situarse a un nivel inalcanzable a los hombres. Desde este momento, incapaz de cubrir sus necesidades, el hombre biológico se verá situado fuera de la existencia".



En otras de sus citas, realiza una severa advertencia, de las cuales hay infinitas evidencias que la corroboran…..

"¿Qué diferencia hay con el siglo XX? Ciertamente, las tecnologías ligadas a las armas de destrucción masiva (NBQ) –-nuclear, biológica y química– eran pujantes, y el arsenal hacía pesar sobre nosotros una amenaza extrema. Sin embargo la fabricación de ingenios atómicos suponía, al menos durante un tiempo, el acceso a materiales raros –-incluso inaccesibles– así como a información altamente confidencial. Además los programas de armamento biológico y químico exigían a menudo actividades a gran escala.

Las tecnologías del siglo XXI (GNR) –-genética, nanotecnología y robótica– son portadoras de un poder tal que tienen la capacidad de engendrar variedades diferentes de accidentes y abusos totalmente inéditos. Circunstancia agravante es que estos accidente y abusos están al alcance de individuos aislados o de grupos restringidos. En efecto estas tecnologías no precisan ni el acceso a instalaciones de gran envergadura, ni a materiales raros; la única condición para poder recurrir a ellos es la posesión del saber requerido".

El gran aporte e importancia del artículo de Bill Joy, por sí solo amerita una lectura y debate en torno al mismo, una tarea que debe ser acometida sin dilaciones por las comunidades tecnológicas y sociales. Entender que definitivamente realizar valoraciones de "corto plazo", como ser, perspectivas laborales, profesionales u oportunidades de negocio, no visualiza las importantes consecuencias del desarrollo tecnológico. Finalmente para todos

"los ingenuos" que creen cambiar la historia con una aplicación web o móvil…..

"He llegado a la conclusión que no es ni en el trabajo de los investigadores en informática, ni en el de los diseñadores de ordenadores o de los ingenieros a los que se debe el avance significativo en las tecnologías de la información, sino al de los investigadores en física. Al principio de los años 80, los físicos Stephen Wolfram y Brosl Hasslacher me iniciaron en la teoría del caos y de los sistemas no lineales. En el curso de los años 90, conversaciones con Danny Hillis, el biólogo Stuart Kauffman, el premio Nobel de física Murray Gell-Mann, y otros me han permitido descubrir los sistemas complejos. Más recientemente, Hasslacher y Mark Reed, ingeniero y físico, me han iluminado sobre las posibilidades extraordinarias de la electrónica molecular".

Mi conclusión final es que todas las comunidades tecnológicas, en especial las que giran entorno a la cultura hacker deben propiciar y estimular un enriquecedor debate sobre este "espinoso" tema, de un modo abierto, sin prejuicios, aprender a utilizar el debate para crecer y no para discutir. Si decidimos ser "aprendices de brujos" debemos valorar las consecuencias de ese accionar, no hacerlo es abrir las puertas a la tragedia.

Daniel Mery
CoFundador de HackMadrid %27
Fundador de Planet Linux Caffe

InvisiMole

Iván Portillo y Pablo Bentanachs – GINSEG

Presentación del grupo

InvisiMole es un grupo de cibercriminales especializados en el ciberespionaje de instituciones gubernamentales. El grupo ha sido detectado en dos operaciones; una en 2013 y otra en 2019 - ambas relacionadas con el espionaje a países de Europa del Este.

El grupo InvisiMole ha estado operativo por lo menos desde 2013 cuando llevó a cabo diversas campañas de ciberespionaje en Rusia y Ucrania según como indica la empresa de seguridad ESET.

Desde 2013 no se habían observado grandes movimientos de este grupo hasta que un nuevo informe publicado por ESET en junio de 2020 ha desvelado que dicho grupo ha resurgido con un nuevo arsenal de TTPs y contando con la cooperación de otro grupo criminal muy activo, **Gamaredon**. La sofisticación de sus malwares así como sus objetivos conocidos, invitan a pensar que el grupo puede ser respaldado por otro gobierno.

En el informe publicado por ESET recientemente, fue mencionado una nueva campaña de InvisiMole en 2019 (y que posiblemente siga en activo) contra instituciones militares y diplomáticas en el Este de Europa.

Dada la naturaleza de los ataques conocidos llevados a cabo por este actor o grupo criminal, se puede asumir que su objetivo es la obtención de inteligencia extranjera al contrario que muchos otros atacantes que buscan el beneficio económico, la disrupción de servicios y/o la notoriedad.

Motivaciones

Se deduce por las campañas en las que este actor ha sido detectado, que sus ataques están motivados por el robo de información clasificada existente en ámbitos militares y diplomáticos. La información manejada por ese tipo de instituciones puede ser muy confidencial y con potencial de ser

extremadamente peligrosa si cae en las manos erróneas. Dada la naturaleza de sus ataques, el grupo se caracteriza por ser muy sigiloso en sus operaciones intentando ocultar su rastro sin dejar huella.

Aunque no exista ninguna atribución al grupo InvisiMole de manera pública, los ataques de ciberespionaje por los que este actor se caracteriza suelen ser asociados a un gobierno extranjero.

Dicho esto, el grupo con el que está colaborando últimamente, Gamaredon, parece tener lazos con el gobierno ruso, lo cual puede dar alguna pista sobre su atribución.

Aunque la atribución no está clara, lo que parece certero después de analizar el informe de ESET, es que InvisiMole es un grupo muy cauteloso, el cual dispone de unos malwares bastante sofisticados y desarrollados con la meta de extraer información sensible.

Operaciones actuales

La última campaña identificada y atribuida a InvisiMole ha sido en colaboración con el grupo Gamaredon para atacar a instituciones gubernamentales en el Este de Europa. Esta campaña empezó a finales de 2019 y puede que siga existiendo a la hora de escribir esta publicación.

A pesar de no conocer los detalles de esta operación la telemetría nos da varios detalles como son:

- El grupo desarrolla su malware activamente según los obstáculos y condiciones encontradas durante la campaña
- La campaña se caracteriza por largas cadenas de ejecución con múltiples capas de cifrado por víctima, lo que dificulta la reconstrucción del ataque
- Utilizan aplicaciones legítimas para ejecutar su propio código, establecer persistencia

- Realizan movimientos laterales y otras operaciones con el objetivo de evitar listas blancas de aplicaciones y ser detectados

- El ataque a las instituciones ha sido muy sofisticado y específico a no más de 12 ordenadores afectados para evitar su detección

- Uno de sus modus operandi conocido es el de infectar una cámara de vídeo del ordenador, permitiendo que los atacantes vean y escuchen lo que sucede en la oficina de la víctima o donde sea que esté su dispositivo

En esta investigación se han encontrado varios TTPs que explican cómo han colaborado los dos grupos:

InvisiMole primero obtiene acceso inicial a los sistemas de las víctimas a través de un **downloader de .NET** llamado "**MSIL / Pteredo**", que se utiliza como un **mecanismo de entrega utilizado por el grupo Gamaredon**.

Acto seguido, los .NET downloaders entregan un archivo **ZIP troyanizado**, que extrae una herramienta legítima llamada "**winapiexec**", el cual permite ejecutar las funciones de la API de Windows a través de parámetros de línea de comandos.

Una vez infiltrados, InvisiMole busca mantener persistencia utilizando dos métodos para moverse lateralmente en el sistema infectado:

- El primer método explota las vulnerabilidades en los protocolos de red mediante la vulnerabilidad "**CVE-2019-0708**", también conocido como **BlueKeep**, y para su difusión dentro de la propia red aprovecha la vulnerabilidad "**CVE-2017-0144**".

- El segundo método es mediante el uso de documentos troyanizados e instaladores de software creados con archivos benignos robados de la organización comprometida.

A pesar de la aparente colaboración entre InvisiMole y Gamaredon, ESET los considera distintos grupos ya que tienen TTPs diferentes.

IoCs

En la propia investigación que se podrá ver en su sección correspondiente, nos centraremos en InvisiMole.

A modo resumen han sido detectados un total de **125 indicadores de compromiso (IoC)** divididos en cuatro tipos, tal como puede apreciarse en la Imagen 1.

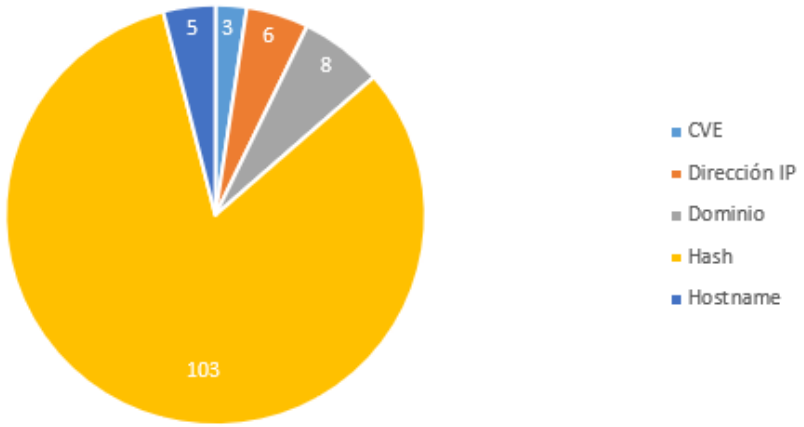


Imagen 1. Tipos de IoCs detectados

Analizando los **103 IoCs de tipo hash**, podemos subdividirlo en subtipos, tal como puede verse en la Imagen 2.

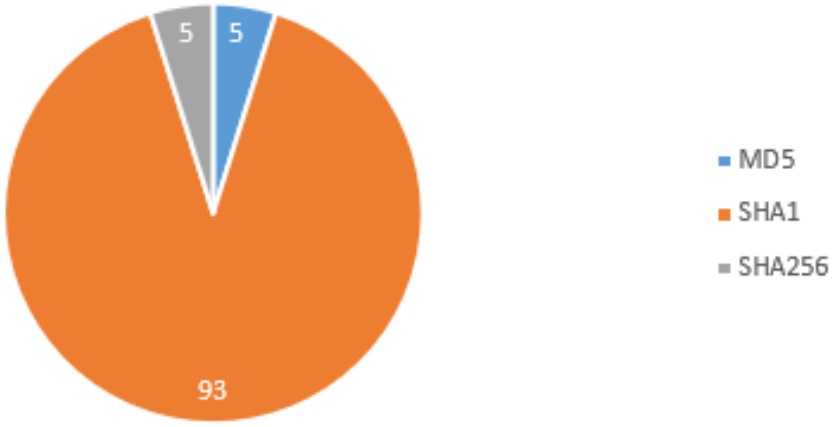


Imagen 2. Tipos de hashes detectados

Malware asociado

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

- **InvisiMole**. Se trata de un software espía cuyo objetivo de ataque son plataformas de Microsoft Windows, teniendo como fin la recopilación de cualquier tipo de información del equipo de la víctima por medio de una vigilancia de todas sus actividades. InvisiMole dispone de una arquitectura que cuenta con dos módulos que funcionan como backdoor, RC2FM y RC2CL (ambos serán descritos posteriormente) para la ejecución de actividades de post-explotación.

  El presente malware lleva activo desde 2018, al menos según datos públicos de ESET, volviéndose a reactivar a lo largo del mes de junio.

- **RC2FM**. Según informaciones facilitadas por ESET, este backdoor soporta hasta un total de 19 comandos, dependiendo de la versión utilizada. Algunos de estos disponen de capacidades de recopilación, extracción de documentos alojados en carpetas específicas y/o unidades mapeadas, o exfiltración de imágenes en formato JPEG de dispositivos directamente conectados y que estén utilizando la interfaz **WPD** (Windows Presentation Foundation). RC2FM dispone de otras funcionalidades bastante importantes como keylogging, descubrimiento de procesos, bypass del UAC y la capacidad de generar y ejecutar shell inversas.

- **RC2CL**. El presente backdoor soporta un mayor número de comandos que el anterior, en este caso un total de 87. Algunas de las capacidades disponibles son las siguientes:

    - Activar micrófono y webcam para capturar imágenes, grabar sonido y video
    - Ejecución de capturas de pantalla del escritorio
    - Recopilar información sobre la configuración de la red del dispositivo u obtener un listado del software y servicios instalado en este
    - Histórico de documentos visualizados recientemente

Análisis de TTPs

El grupo InvisiMole no dispone de ningún TTP directamente asociado, por ello procedemos a investigar los TTPs relacionados con los malwares vistos en la sección anterior.

Comenzamos comprobando qué tipo de información conoce **MITRE ATT&CK** sobre InvisiMole. El resultado puede visualizarse en la Imagen 3.

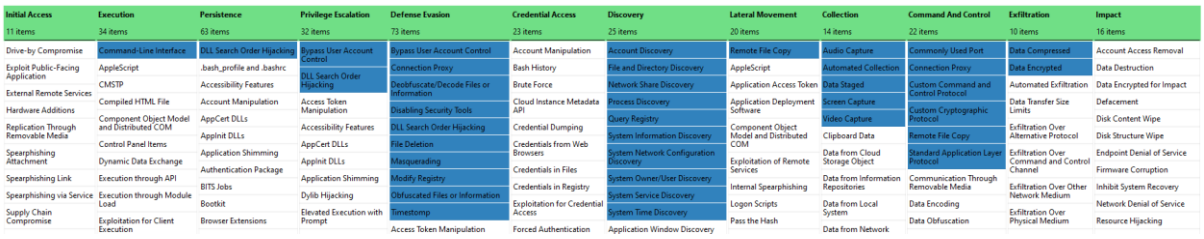


Imagen 3. TTPs detectados sobre InvisiMole en MITRE ATT&CK

En un primer vistazo podemos detectar la presencia de **9 tácticas y 38 técnicas empleadas**. Si añadimos otras técnicas detectadas por ESET (técnicas con fondo rojo), la matriz de TTPs del malware InvisiMole quedaría tal como puede verse en la Imagen 4.

Imagen 4. Combinatoria de TTPs final

A grandes rasgos, los TTPs asociados al malware InvisiMole disponen de **70 técnicas englobadas a lo largo de 9 tácticas**, siendo un resumen lo siguiente:

- Táctica de ejecución. Han sido detectadas un total de **9 técnicas**, entre las que se encuentran la ejecución de comandos por línea de consola, ejecución de cualquier acción por parte de los usuarios del sistema, y la ejecución de scripts, servicios o tareas programadas, entre otros.

- Táctica de persistencia. Dentro de este bloque han sido detectadas un total de **6 técnicas**, como son el caso de modificación de accesos directos, tareas programadas, creación de nuevos servicios, creación de nuevas entradas en el registro como claves de ejecución o en la carpeta de inicio del sistema, entre otros.

- Táctica de elevación de privilegios. Nos encontramos con **5 técnicas** en total, como la explotación para la elevación de privilegios, bypass del Windows User Account Control (UAC) y DLL Hijacking.

- Táctica de evasión defensiva. Dentro de este bloque han sido detectadas un total de **17 técnicas**, como pueden ser el uso de elementos del Panel de Control, utilización de ventanas ocultas para esconder las actividades maliciosas, desactivación de herramientas de seguridad u ofuscar información de cualquier índole.

- Táctica de descubrimiento. En total han sido descubiertas **12 técnicas** como pueden ser escaneos de servicios de red o el descubrimiento de

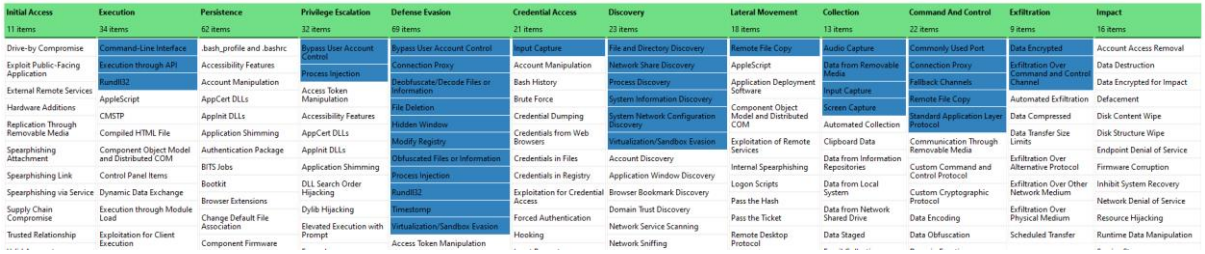
software, cuentas de usuarios, procesos ejecutados en el sistema o carpetas de red compartidas, entre otros.

- Táctica de movimiento lateral. Disponemos de un total de **3 técnicas** detectadas, como son la explotación de servicios remotos, transferencia de archivos remotamente y contenido compartido alterado.

- Táctica de colección. Han sido detectadas **5 técnicas** asociadas a esta táctica, algunas de ellas son la captura de audio, video o pantallazo del escritorio.

- Táctica de comando y control. Dentro de este bloque han sido detectadas un total de **10 técnicas**, como pueden ser la codificación de datos, utilización de canales de comunicación alternativos o de puertos no comunes, entre otros.

- Táctica de exfiltración. Dentro de esta táctica hemos detectado **2 técnicas**, siendo la compresión y el cifrado de los datos.



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	34 items	62 items	32 items	69 items	21 items	23 items	18 items	13 items	22 items	9 items	16 items
Drive-by Compromise	Command-Line Interface	.bash_profile and .bashrc	Bypass User Account Control	Bypass User Account Control	Input Capture	File and Directory Discovery	Remote File Copy	Audio Capture	Commonly Used Port	Data Encrypted	Account Access Removal
Exploit Public-Facing Application	Execution through API	Accessibility Features	Process Injection	Connection Proxy	Account Manipulation	Network Share Discovery	AppleScript	Data from Removable Media	Connection Proxy	Exfiltration Over Command and Control Channel	Data Destruction
External Remote Services	Rundll32	Account Manipulation	Access Token Manipulation	Deobfuscate/Decode Files or Information	Bash History	Process Discovery	Application Deployment Software	Input Capture	Fallback Channels	Data Encrypted for Impact	
Hardware Additions	AppleScript	AppCert DLLs	Accessibility Features	File Deletion	Brute Force	System Information Discovery	Component Object Model and Distributed COM	Screen Capture	Remote File Copy	Automated Exfiltration	Defacement
Replication Through Removable Media	CMSTP	AppInit DLLs	AppCert DLLs	Hidden Window	Credential Dumping	System Network Configuration Discovery	Exploitation of Remote Services	Automated Collection	Standard Application Layer Protocol	Data Compressed	Disk Content Wipe
Spearphishing Attachment	Compiled HTML File	Application Shimming	AppInit DLLs	Modify Registry	Credentials from Web Browsers	Virtualization/Sandbox Evasion	Internal Spearphishing	Clipboard Data	Communication Through Removable Media	Data Transfer Size Limits	Disk Structure Wipe
Spearphishing Link	Component Object Model and Distributed COM	Authentication Package	Application Shimming	Obfuscated Files or Information	Credentials in Files	Account Discovery	Logon Scripts	Data from Information Repositories	Custom Command and Control Protocol	Exfiltration Over Alternative Protocol	Endpoint Denial of Service
Spearphishing via Service	Control Panel Items	BITS Jobs	DLL Search Order Hijacking	Process Injection	Credentials in Registry	Application Window Discovery	Pass the Hash	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Other Network Medium	Firmware Corruption
Supply Chain Compromise	Dynamic Data Exchange	Bootkit	Dylib Hijacking	Rundll32	Exploitation for Credential Access	Browser Bookmark Discovery	Pass the Ticket	Data from Network Shared Drive	Data Encoding	Exfiltration Over Physical Medium	Inhibit System Recovery
Trusted Relationship	Execution through Module Load	Browser Extensions	Elevated Execution with Prompt	Timestomp	Forced Authentication	Domain Trust Discovery	Remote Desktop Protocol	Data Staged	Data Obfuscation	Scheduled Transfer	Network Denial of Service
	Exploitation for Client Execution	Change Default File Association		Virtualization/Sandbox Evasion	Hooking	Network Service Scanning					Resource Hijacking
		Component Firmware		Access Token Manipulation		Network Sniffing					Runtime Data Manipulation

Imagen 5. TTPs RC2FM

Si analizamos los TTPs asociados a **RC2FM** en la Imagen 5, podemos detectar la presencia de **9 tácticas** y **35 técnicas empleadas**. A modo resumen disponemos de los siguientes TTPs:

- Táctica de ejecución. Han sido detectadas **3 técnicas**, entre los que se encuentran la ejecución de comandos por línea de consola, ejecución a través de API, y la utilización del proceso Rundll32.

- Táctica de elevación de privilegios. Han sido detectadas **2 técnicas,** siendo el bypass del Windows User Account Control (UAC) y la inyección de código en procesos.

- Táctica de evasión defensiva. Dentro de este bloque han sido detectadas un total de **11 técnicas**, como puede ser la utilización de ventanas ocultas para esconder las actividades maliciosas, la detección y evasión de máquinas virtuales o sandbox u ofuscar información de cualquier índole, entre otros.

- Táctica de acceso a las credenciales. Ha sido detectada **una única técnica**, siendo la captura de datos de los usuarios por medio de cualquier dispositivo de entrada a la máquina, como el registro de teclas pulsadas a través de teclado.

- Táctica de descubrimiento. En total han sido descubiertas **6 técnicas** como pueden ser el descubrimiento de procesos ejecutados en el sistema o carpetas de red compartidas, entre otros.

- Táctica de movimiento lateral. Disponemos de **una única técnica** detectada, siendo la transferencia de archivos de manera remota.

- Táctica de colección. Han sido detectadas **4 técnicas** asociadas a esta táctica, siendo la captura de audio, pantallazo del escritorio, captura de datos de dispositivos de entrada de los usuarios y datos de medios extraíbles.

- Táctica de comando y control. Dentro de este bloque han sido detectadas un total de **5 técnicas**, como pueden ser la utilización de canales de comunicación alternativos o de puertos no comunes y la utilización de protocolos de capa de aplicación estandarizados, entre otros.

- Táctica de exfiltración. Dentro de esta táctica hemos detectado **2 técnicas**, siendo el cifrado de los datos y exfiltración de información utilizando canales de comando y control.

Si analizamos los TTPs asociados a **RC2CL** en la Imagen 6, podemos detectar la presencia de **8 tácticas** y **38 técnicas empleadas**. A modo resumen disponemos de los siguientes TTPs:

- Táctica de ejecución. Han sido detectadas **2 técnicas**, entre los que se encuentran la ejecución de comandos por línea de consola y la ejecución a través de API.

- Táctica de elevación de privilegios. Han sido detectadas **2 técnicas,** siendo el bypass del Windows User Account Control (UAC) y la manipulación de tokens de acceso.

- Táctica de evasión defensiva. Dentro de este bloque han sido detectadas un total de **10 técnicas**, como pueden ser la detección y evasión de máquinas virtuales o sandbox, eliminación de archivos, modificación del registro, u ofuscar información de cualquier índole, entre otros.

- Táctica de descubrimiento. En total han sido descubiertas **11 técnicas** como puede ser el descubrimiento de procesos ejecutados en el sistema o carpetas de red compartidas, entre otros.

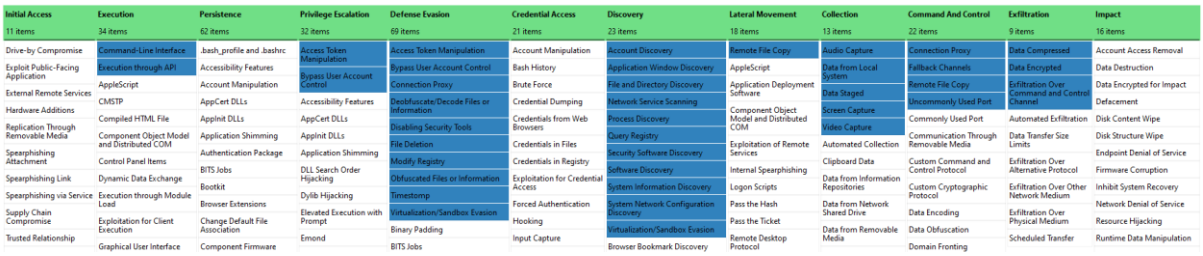
- Táctica de movimiento lateral. Disponemos de **una única técnica** detectada, siendo la transferencia de archivos de manera remota.

- Táctica de colección. Han sido detectadas **5 técnicas** asociadas a esta táctica, siendo la captura de audio, pantallazo del escritorio, captura de datos de dispositivos de entrada de los usuarios y datos obtenidos del sistema.

- Táctica de comando y control. Dentro de este bloque han sido detectadas un total de **4 técnicas**, como pueden ser la utilización de

canales de comunicación alternativos o de puertos no comunes y la utilización de proxies en las conexiones, entre otros.

- Táctica de exfiltración. Dentro de esta táctica hemos detectado **3 técnicas**, siendo la compresión y el cifrado de los datos y la exfiltración de información utilizando canales de comando y control.



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	34 items	62 items	32 items	69 items	21 items	23 items	18 items	13 items	22 items	9 items	16 items
Drive-by Compromise	Command-Line Interface	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Remote File Copy	Audio Capture	Connection Proxy	Data Compressed	Account Access Removal
Exploit Public-Facing Application	Execution through API	Accessibility Features	Bypass User Account Control	Bypass User Account Control	Bash History	Application Window Discovery	AppleScript	Data from Local System	Fallback Channels	Data Encrypted	Data Destruction
External Remote Services	AppleScript	Account Manipulation	Connection Proxy	Deobfuscate/Decode Files or Information	Brute Force	File and Directory Discovery	Application Deployment Software	Data Staged	Remote File Copy	Exfiltration Over Command and Control Channel	Data Encrypted for Impact
Hardware Additions	CMSTP	AppCert DLLs	Accessibility Features	Disabling Security Tools	Credential Dumping	Network Service Scanning	Component Object Model and Distributed COM	Screen Capture	Uncommonly Used Port	Exfiltration Over Alternative Protocol	Defacement
Replication Through Removable Media	Compiled HTML File	AppInit DLLs	AppCert DLLs	File Deletion	Credentials from Web Browsers	Process Discovery	Exploitation of Remote Services	Video Capture	Commonly Used Port	Automated Exfiltration	Disk Content Wipe
Spearphishing Attachment	Component Object Model and Distributed COM	Application Shimming	AppInit DLLs	Modify Registry	Credentials in Files	Query Registry	Internal Spearphishing	Automated Collection	Communication Through Removable Media	Data Transfer Size Limits	Disk Structure Wipe
Spearphishing Link	Control Panel Items	Authentication Package	Application Shimming	Obfuscated Files or Information	Credentials in Registry	Security Software Discovery	Logon Scripts	Clipboard Data	Custom Command and Control Protocol	Exfiltration Over Physical Medium	Endpoint Denial of Service
Spearphishing via Service	Dynamic Data Exchange	BITS Jobs	DLL Search Order Hijacking	Timestomp	Exploitation for Credential Access	Software Discovery	Pass the Hash	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Other Network Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Dylib Hijacking	Virtualization/Sandbox Evasion	Forced Authentication	System Information Discovery	Pass the Ticket	Data from Network Shared Drive	Data Encoding	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Elevated Execution with Prompt	Binary Padding	Hooking	System Network Configuration Discovery	Remote Desktop Protocol	Data from Removable Media	Data Obfuscation		Network Denial of Service
	Graphical User Interface	Change Default File Association	Emond	BITS Jobs	Input Capture	Virtualization/Sandbox Evasion			Domain Fronting		Resource Hijacking
		Component Firmware				Browser Bookmark Discovery					Runtime Data Manipulation

Imagen 6. TTPs RC2CL

Si analizamos los TTPs asociados a **InvisiMole**, **RC2FM** y **RC2CL** en su conjunto podemos apreciar la presencia de **10 tácticas** y **82 técnicas empleadas** en total.

En la Imagen 7 hemos añadido todas los TTPs relacionados con los tres malware para identificar el número de apariciones de cada una de las técnicas detectadas.

Para las detecciones hemos utilizado un código de colores en función del número de apariciones de una técnica en cada panel de los 3 malwares. El código de colores empleado ha sido el siguiente:

- **Tres coincidencias (fondo rojo)**. Si la técnica es identificada en las tres matrices de TTPs, dichas técnicas serán coloreadas con un fondo rojo.

- **Dos coincidencias (fondo amarillo).** Si la técnica solo es identificada en dos de las tres matrices de TTPs, dichas técnicas serán coloreadas con un fondo amarillo.

- **Una coincidencia (fondo azul).** Si la técnica solo es identificada en una de las tres matrices de TTPs, dichas técnicas serán coloreadas con un fondo azul.

Imagen 7. TTPs comunes en los tres malware

Como conclusión, si nos fijamos en los TTPs utilizados en los tres tipos de malware, podemos apreciar la presencia de **8 tácticas** y **21 técnicas empleadas** en común entre los tres malwares, InvisiMole, **RC2FM** y **RC2CL.**

Análisis de los indicadores de compromiso

En la presente sección vamos a investigar qué tipo de relaciones tienen los diferentes indicadores de compromiso entre sí, aunque centrándonos en los dominios y direcciones IP. Para dicho fin, vamos a utilizar Yeti, una Plataforma de Threat Intelligence (TIP) y la herramienta VirusTotal.

Análisis de relaciones entre los IoCs en Yeti

En esta primera subsección procedemos a realizar una investigación de los IoCs para ver cómo están relacionados entre sí por medio de Yeti. En la Imagen 8 puede visualizarse el grafo de las relaciones entre los dominios y las direcciones IP detectados como IoCs.

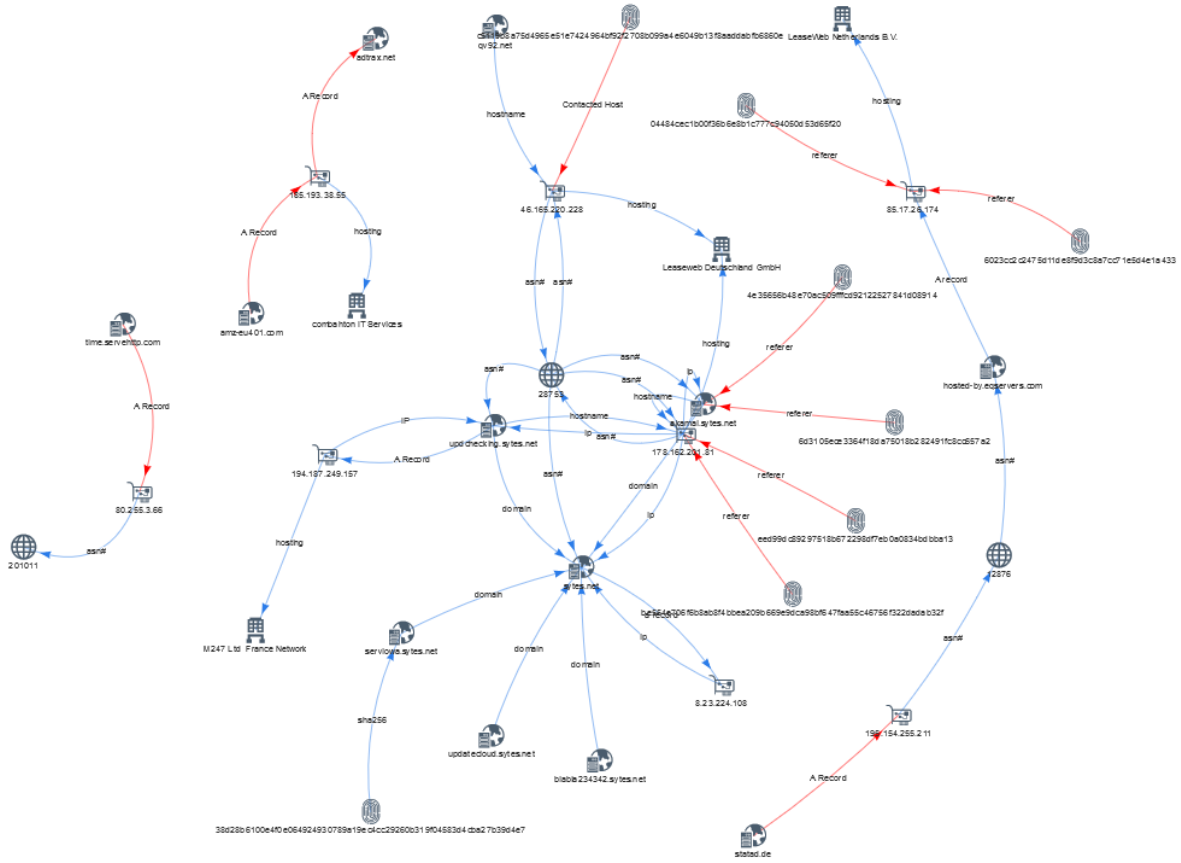


Imagen 8. Grafo de relaciones de IoCs con Yeti

Tal como puede apreciarse en la Imagen 8 existen varios tipos de relaciones entre los IoCs analizados, tanto de primer como de segundo nivel. Si lo analizamos más en detalle podemos identificar cuatro bloques de relaciones.

En el **primer bloque** (ver Imagen 9) disponemos de una relación entre dos de los IoCs analizados, siendo el hostname **time.servehttp.com** y la dirección IP **80.255.3.66**, en el cual el primero apunta al segundo. Este último indicador está englobado dentro del **ASN AS201011**, situado en Alemania (ver Imagen 10).

Imagen 9. Relaciones del primer bloque

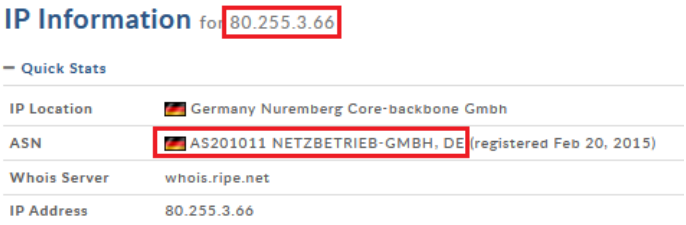


Imagen 10. Información de la IP 80.255.3.66

En el **segundo bloque** (ver Imagen 11) disponemos de una relación entre dos de los IoCs analizados, el dominio **adtrax.net** y la dirección IP **185.193.38.55**, en el cual el primero apunta al segundo. Este último indicador tiene relación con el hosting **combahton IT Services** y se detecta que el ASN (**AS30823**) y la propia IP están alojados en Alemania (ver Imagen 12).

A su vez, dicha dirección IP está relacionada con otro IoC, en este caso **amz-eu401.com**.

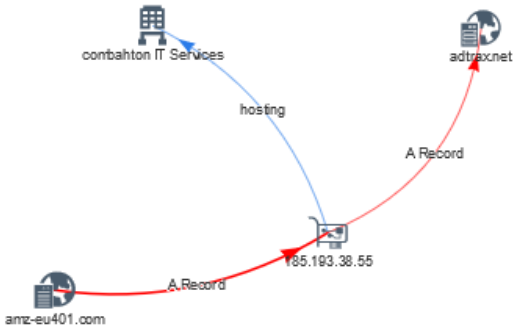


Imagen 11. Relaciones del segundo bloque

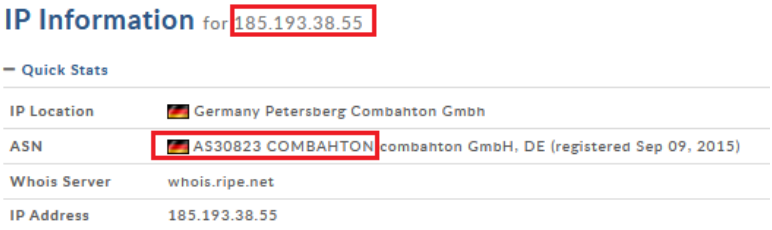


Imagen 12. Información de la IP 185.193.38.55

En el **tercer bloque** (ver Imagen 13) disponemos de dos relaciones entre tres de los IoCs analizados, el dominio **statad.de** y las direcciones IP **195.154.255.211** y **85.17.26.174**. El dominio mencionado apunta a la IP

195.154.255.211, el cual está relacionada con el ASN **AS12876** que está alojado en Francia (ver Imagen 14).

Dentro de este ASN está englobado el hostname **hosted-by.eqservers.com** que a su vez está relacionado con un IoC asociado con la amenaza, la dirección IP **85.17.26.174**. Tal como puede apreciarse en la Imagen 15, dicha IP apunta a Holanda (englobado dentro del ASN **AS60781**) utilizando el hosting **LeaseWeb Netherlands B.V.** Además, la IP **85.17.26.174** está relacionada con dos hashes identificados como maliciosos.

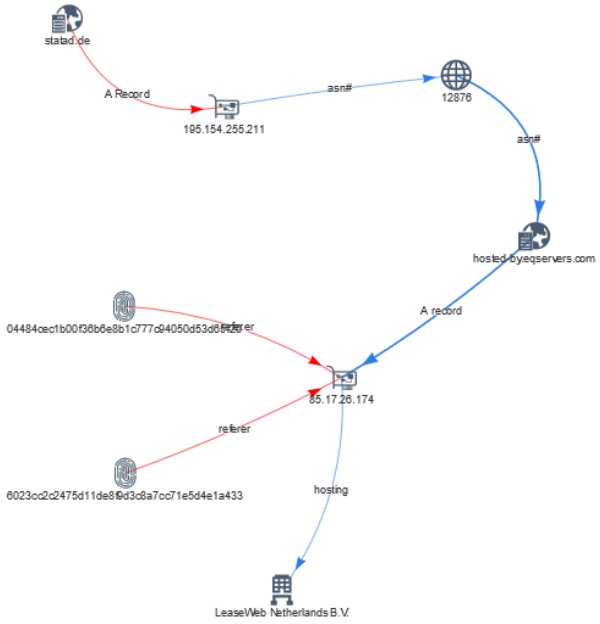


Imagen 13. Relaciones del tercer bloque

IP Information for 195.154.255.211

Quick Stats

IP Location	France Paris Online S.a.s.
ASN	AS12876 Online SAS, FR (registered Dec 20, 1999)
Resolve Host	195-154-255-211.rev.poneytelecom.eu
Whois Server	whois.ripe.net
IP Address	195.154.255.211

Imagen 14. Información de la IP 195.154.255.211

IP Information for 85.17.26.174

Quick Stats

IP Location	Netherlands Amsterdam Leaseweb Netherlands B.v.
ASN	AS60781 LEASEWEB-NL-AMS-01 Netherlands, NL registered May 13, 2013)
Resolve Host	hosted-by.Eqservers.com
Whois Server	whois.ripe.net
IP Address	85.17.26.174

Imagen 15. Información de la IP 85.17.26.174

En el **cuarto y último bloque** (ver Imagen 20) disponemos de varias relaciones entre 7 IoCs analizados de partida. Los hostnames **blabla234342.sytes.net**, **updatecloud.sytes.net, updchecking.sytes.net** y **akamai.sytes.net** están relacionados directamente con el dominio **sytes.net**. Analizando dicho dominio hemos identificado que apunta a la dirección IP **8.23.224.108**, alojada en Estados Unidos dentro del ASN **AS14627**. Otras relaciones disponibles del dominio **sytes.net** son con el hostname **serviowa.sytes.net**, que a su vez tiene relación con un hash malicioso, y con el **ASN AS28753**. Este ASN mencionado tiene conexión directa con los hostnames **akamai.sytes.net** y **updchecking.sytes.net**, el dominio **sytes.net** y la dirección IP **46.165.220.228**.

Analizando dicha dirección IP descubrimos relaciones con el dominio **qv92.net**, el hosting **Leaseweb Deutschland GmbH**, un hash malicioso y la geolocalización situada en Alemania (englobado dentro del ASN **AS28753**).

Imagen 16. Información de la IP 8.23.224.108

Imagen 17. Información de la IP 46.165.220.228

El hostname **updchecking.sytes.net** tiene relación directa con la dirección IP **194.187.249.157**, el cual está ubicado en Francia, englobado dentro del ASN **AS9009** (ver Imagen 18) y utilizando el hosting **M247 Ltd France Network**.

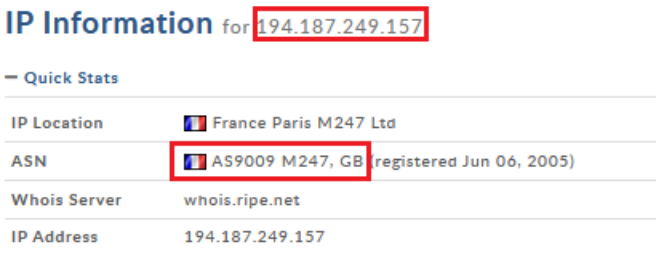


Imagen 18. Información de la IP 194.187.249.157

El hostname **akamai.sytes.net** tiene relación directa con la dirección IP **178.162.201.81**, el cual está ubicado en Alemania (englobado dentro del ASN **AS28753**) y utiliza el hosting **Leaseweb Deutschland**. Ver Imagen 19.

Tanto con la dirección IP **178.162.201.81** como con el dominio **akamai.sytes.net** hemos detectado dos hashes maliciosos.

Imagen 19. Información de la IP 194.187.249.157

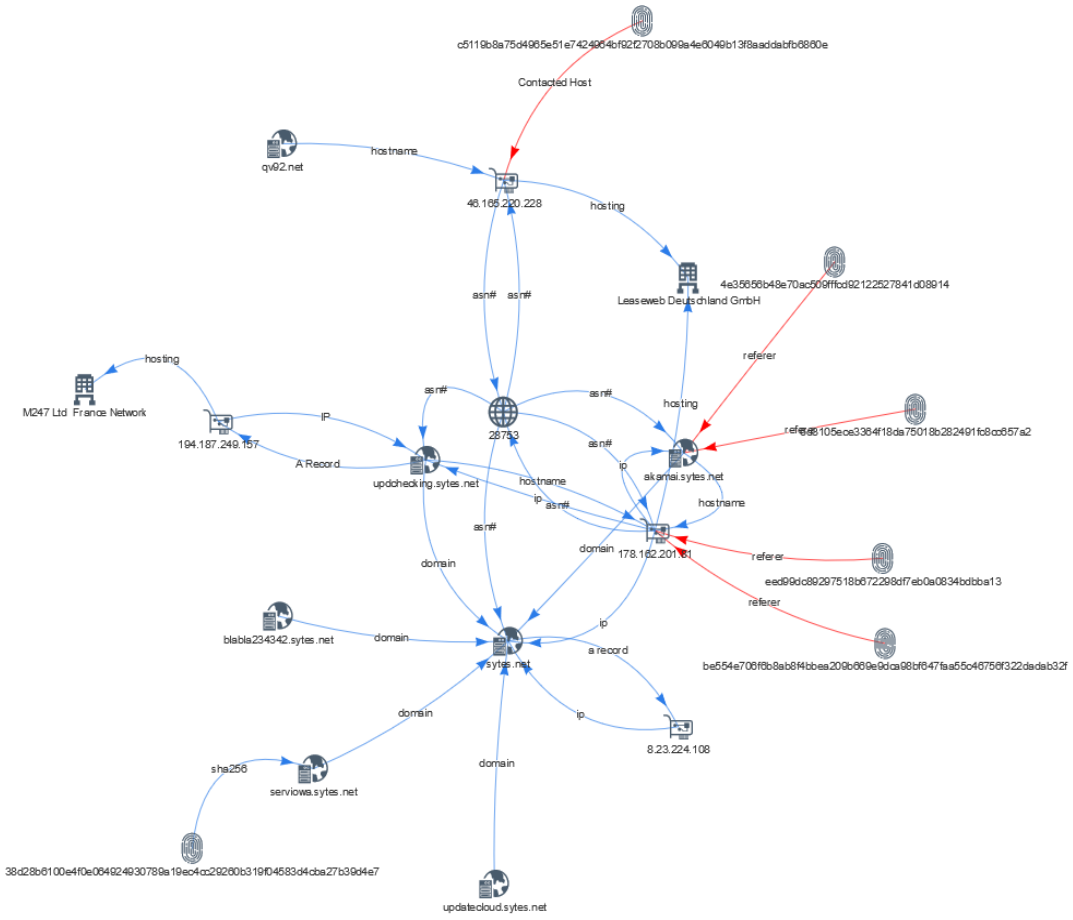


Imagen 20. Relaciones del cuarto bloque

Análisis de relaciones entre los IoCs en VirusTotal

En esta subsección procedemos a realizar una investigación de todos los IoCs para ver cómo están relacionados entre sí dentro de una herramienta de inteligencia de amenazas como VirusTotal. En la Imagen 21 puede visualizarse el grafo de las relaciones entre los dominios y las direcciones IP detectados como IoCs.

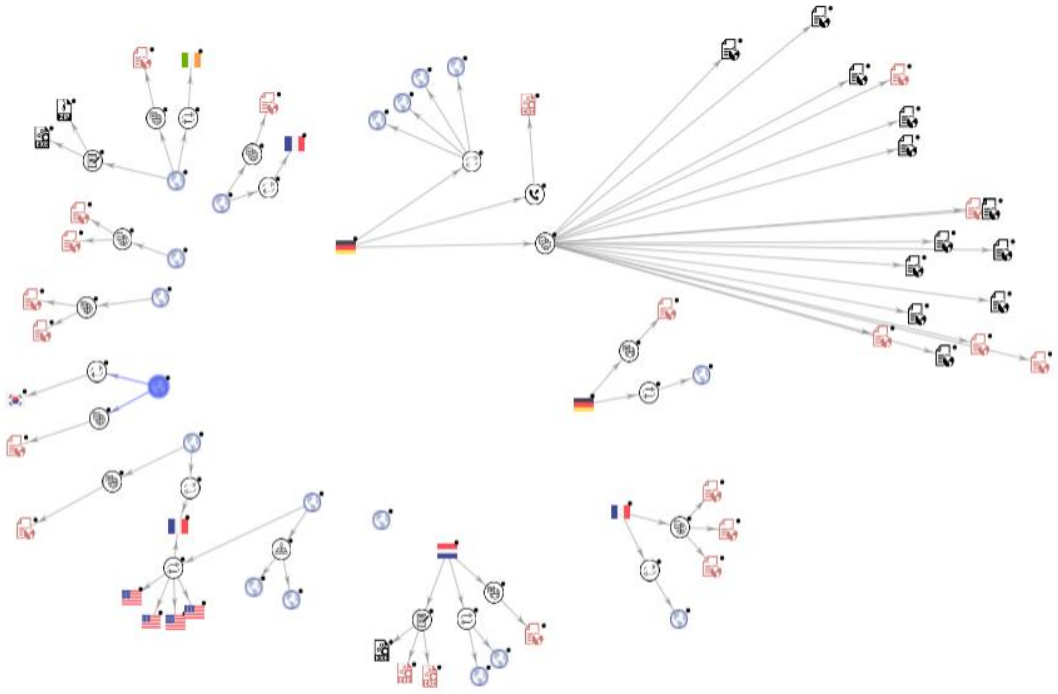


Imagen 21. Relaciones obtenidas en VT

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

- **<u>IoC 1. Dirección IP 46.165.220.228:</u>**

    - La dirección apunta a **Alemania, su ASN es 28753 y su owner es Leaseweb Deutschland GmbH**

    - Relación existente entre la dirección IP con cuatro URLs, una de ellas detectada como maliciosa por 5 motores antivirus updatecloud.sytes.net

- Se han encontrado **18 ficheros** que hacen referencia a la dirección IP, **5 de ellos** han sido detectados como **maliciosos**

- Hay una comunicación con un ejecutable llamado "**AlcRmv.exe**", el cual ha sido detectado como malicioso por 55 antivirus

- **IoC 2. Dirección IP 80.255.3.66:**

  - La dirección IP apunta a **Alemania, su ASN es 201011 y su owner es AS33891 Netzbetrieb GmbH**

  - Relación existente entre la dirección IP con una URL (**time.servehttp.com**) detectada como maliciosa por 5 motores de antivirus

- **IoC 3. Dirección IP 194.187.249.157:**

  - La dirección IP apunta a **Francia, su ASN es 9009 y su owner es M247 Ltd**

  - Relación existente entre la dirección IP con una URL (**updchecking.sytes.net**) detectada como maliciosa por 7 motores de antivirus

  - Se han encontrado **3 ficheros** que hacen referencia a la dirección IP, **todos ellos** han sido detectados como **maliciosos**

- **IoC 4. Dirección IP 85.17.26.174:**

  - La dirección apunta a **Holanda, su ASN es 60781 y su owner es LeaseWeb Netherlands B.V.**

  - Relación existente entre la dirección IP con dos URLs, sin detectarse ningún tipo de actividad maliciosa

- Se han encontrado **3 ejecutables** que hacen referencia a la dirección IP, **2 de ellos** han sido detectados como **maliciosos**

- **IoC 5. Dominio statad.de:**

  - Este dominio ha sido **detectado como malicioso por 4 motores antivirus**

  - El dominio apunta a una **dirección IP francesa (195.154.255.211), su ASN es 12876 y su owner es Online S.a.s**. Esta dirección IP ha sido detectada como maliciosa por **4** motores antivirus

- **IoC 6. Dominio mx1.be:**

  - Este dominio ha sido **detectado como malicioso por 4 motores antivirus**

  - El dominio apunta a una **dirección IP de Irlanda (54.72.9.51), su ASN es 16509 y su owner es Amazon.com, Inc**. Esta dirección IP no ha sido detectada como maliciosa

- **IoC 7. Dominio adstat.red:**
  - Este dominio ha sido **detectado como malicioso por 4 motores antivirus**

- **IoC 8. Dominio update.xn--6frz82g:**
  - Este dominio ha sido **detectado como malicioso por 2 motores antivirus**

- **IoC 9. Dominio wlsts.net:**

  - Este dominio ha sido **detectado como malicioso por 4 motores antivirus**

- El dominio apunta a una **dirección IP de Corea del Sur (49.50.51.52), su ASN es 10049 y su owner es SK Co**. Esta dirección IP no ha sido detectada como maliciosa

- **IoC 10. Dominio amz-eu401.com:**

  - Este dominio ha sido **detectado como malicioso por 5 motores antivirus**

  - El dominio apunta a una **dirección IP de Francia (185.193.38.55), su ASN es 30823 y su owner es combahton GmbH**. Esta dirección IP ha sido detectada como maliciosa por 3 motores antivirus. Esa IP a su vez se ha visto relacionada con 4 direcciones IPs de Estados Unidos, de las cuales una es maliciosa.

- **IoC 11. Dominio adtrax.net:**

  - Este dominio ha sido **detectado como malicioso por 3 motores antivirus**

  - Se han detectado **dos subdominios (ns2.adtrax.net y ns3.adtrax.net)**. Ninguno ha sido detectado como malicioso

  - Este dominio está relacionado con el dominio anterior (**amz-eu401.com)** en que también apunta a las mismas 4 direcciones IPs de EEUU

- **IoC 12. Dominio 153.re:**

  - Este dominio ha sido **detectado como malicioso por 3 motores antivirus**

Conclusión del análisis de relaciones entre los IoCs

Este análisis ha mostrado que sólo hay una aparente relación entre las 5 direcciones IP y los 7 dominios que han sido relacionados con InvisiMole. Esto no es de extrañar ya que estamos analizando IoCs de un grupo que se especializa en operaciones encubiertas a gobiernos extranjeros. Por lo tanto, es muy probable que el grupo esconda su infraestructura utilizando dominios/direcciones IP que no tengan relación entre sí para evitar su descubrimiento.

Sodinokibi / REvil

Luis Diago de Aguilar – Derecho de la Red

El ransomware sigue siendo una de las principales amenazas. Estos meses hemos visto muchas noticias hablando sobre ello, sin irnos más lejos, el caso de Adif puede ser un ejemplo de que este tipo de sucesos están ocurriendo continuamente.

Desde que estos actores hacen sus víctimas públicamente, todo el sistema evolucionó.

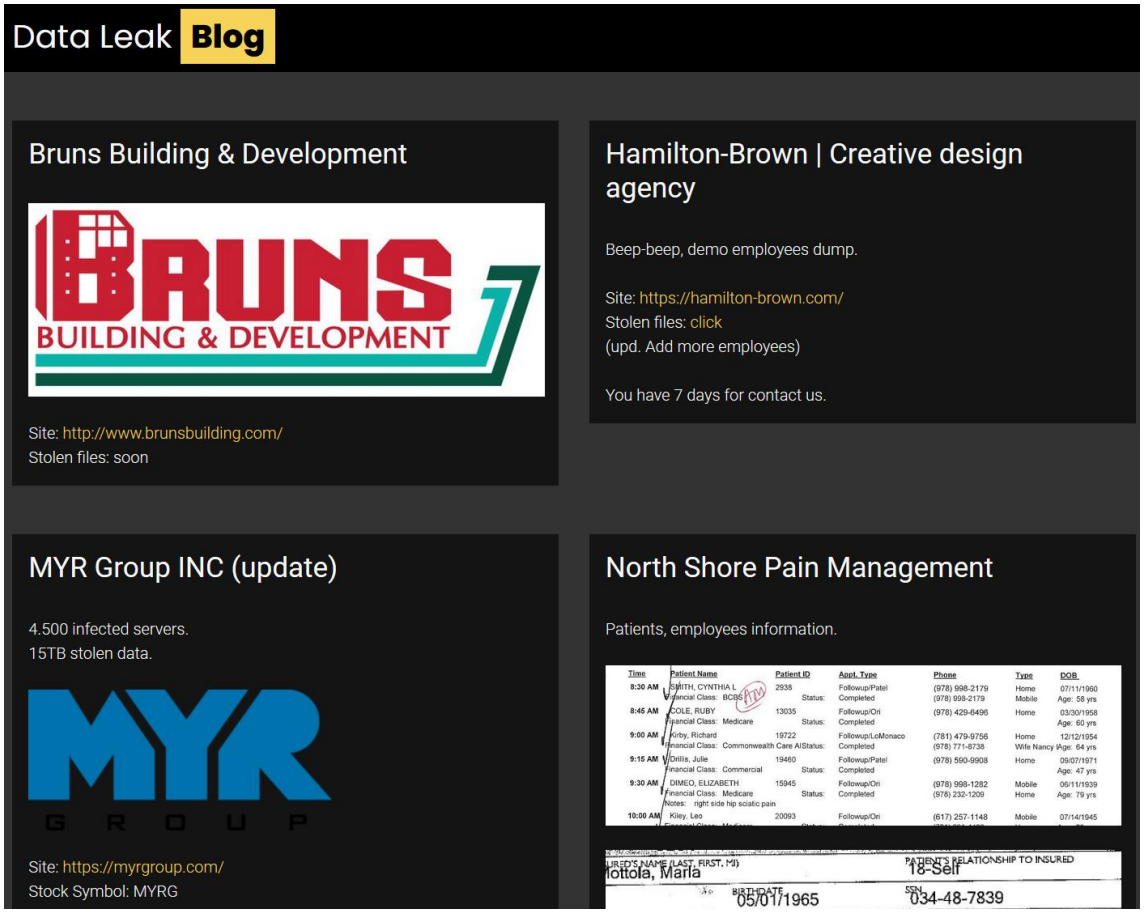
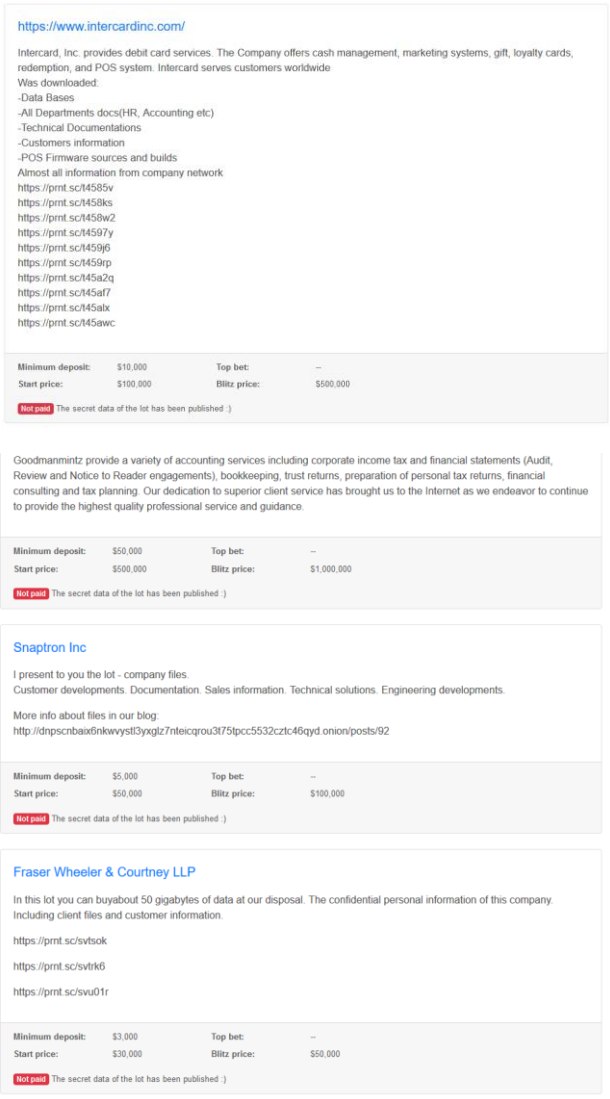


Imagen de uno de estos blogs de ransomware. Algunos otros de estos malware son, Nefilim, MAZE, NetWalker, RAGNAR… y el propio blog de REvil que publica sus víctimas y realiza subastas con los datos (ver imagen siguiente).



Un poco de historia

Este malware llega sobre abril de 2019, obtiene el nombre de Sodinokibi de un archivo ".exe" interno con el hash ccfde149220e87e97198c23fb8115d5a.

Su otro nombre, quizás el más común, REvil.

Al principio se propagaba mediante una vulnerabilidad en el servidor WebLogic de Oracle. Pero, debido a que se trata de un RaaS, un Ransomware as Service, o Ransomware como Servicio en español, el código va variando.

Un grupo de personas se encarga de ir mejorando el código, y otro, por medio de asociación difunde el ransomware.

Esto permite que los encargados de distribuirlo puedan hacerlo de diversas formas y con un alto grado de personalización si lo requieren.

Muchos de los distribuidores prefieren realizar campañas de phishing y de kits de exploits, pero, otros prefieren enfocarse en ataques específicos. Por ejemplo, acceso RDP.

Para más detalles técnicos os dejamos con un informe aquí.

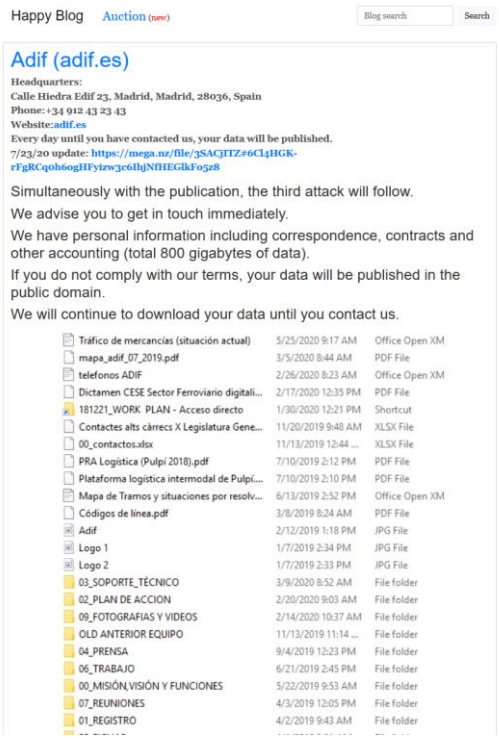
Pero continuemos con la historia, REvil, sucesor de GrandCrab. Este ransomware canceló sus actividades, pero, el grupo de desarrollo detrás del mismo, ¿paró realmente de programar malware? Algunos investigadores piensan que no, que tratándose de un negocio tan lucrativo continuaron desarrollando REvil.

Los objetivos eran los mismos que los de GrandCrab, durante abril de 2019, REvil estuvo distribuyendo muestras de GrandCrab. Además en diversos foros underground se encontraron diferentes conversaciones en las que se trataba de convencer a distribuidores/afiliados para la distribución de un nuevo ransomware.

Tal vez, este malware fuera reemplazado por REvil, siendo distribuido a los mismos afiliados, que usaban las mismas técnicas y lo propagaban sobre los mismos objetivos puesto que históricamente era un método funcional, ¿por qué cambiarlo?

Seguramente, estas técnicas seguirán variando, por lo que tendremos que seguir vigilando de cerca este malware por las alteraciones que pueda sufrir.

Como no somos expertos en malware, os dejamos toda la información recabada a la hora de hacer el artículo para que podáis ver toda la documentación.



Reglas Yara

```
rule Sodinokobi
{

/*

This rule detects Sodinokobi Ransomware in memory in old samples and perhaps future.

*/

meta:

author      = “McAfee ATR team”

version     = “1.0”

description = “This rule detect Sodinokobi Ransomware in memory in old samples and perhaps future.”

strings:

$a = { 40 0F B6 C8 89 4D FC 8A 94 0D FC FE FF FF 0F B6 C2 03 C6 0F B6 F0 8A 84 35 FC FE FF FF 88 84 0D FC FE FF FF 88 94 35 FC FE FF FF 0F B6 8C 0D FC FE FF FF }

$b = { 0F B6 C2 03 C8 8B 45 14 0F B6 C9 8A 8C 0D FC FE FF FF 32 0C 07 88 08 40 89 45 14 8B 45 FC 83 EB 01 75 AA }

condition:

all of them

}
```

```
/* ------------------------
------ Revil/Sodinokibi Ransomware-----------
-------------------------- */

rule RevilRansomwareByName
{
meta:
 author = "@neonprimetime"
 description = "Revil/Sodinokibi Ransomware"
strings:
 $string1 = "Sodinokibi" nocase
 $string2 = "For google: Revil" nocase
```

```
condition:
 any of them
}


rule RevilRansomwareByKeyword
{
meta:
 author = "@neonprimetime"
 description = "Revil/Sodinokibi Ransomware"
strings:
 $string1 = "decryptor.top" nocase
 $string2 = "nbody" nocase
 $string3 = "bedbg" nocase
condition:
 3 of them
}
```

Fuentes

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-atr-analyzes-sodinokibi-aka-revil-ransomware-as-a-service-what-the-code-tells-us/

https://blogs.protegerse.com/2019/07/17/tras-la-desaparicion-de-gandcrab-otros-ransomware-toman-su-relevo/

https://blog.talosintelligence.com/2019/04/sodinokibi-ransomware-exploits-weblogic.html

https://www.tesorion.nl/aconnection-between-the-sodinokibi-and-gandcrab-ransomware-families/

https://neonprimetime.blogspot.com/2019/02/malware-yara-rules.html

https://www.cyber.nj.gov/threat-center/threat-profiles/ransomware-variants/sodinokibi