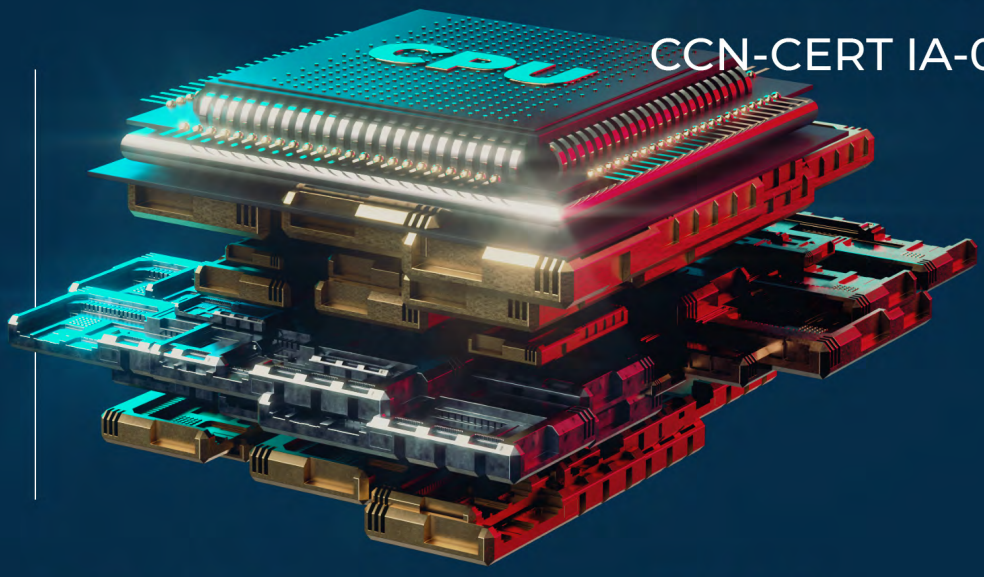
MARZO **2020**

INFORME ANUAL 2019

HACKTIVISMO Y CIBERYIHADISMO

CCN-CERT IA-04/20



INFORME DE AMENAZAS, MOVIMIENTO Y ACTIVIDAD HACKTIVISTA

CCN centro criptológico nacional

ccn-cert centro criptológico nacional

Edita:

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

Fecha de Edición: Marzo de 2020

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2020.03.21 01:53:05 +01'00'

Índice

1. SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como **CERT Gubernamental Nacional** español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la información clasificada (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo a esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

2. RESUMEN EJECUTIVO

Durante 2019 el escenario *hacktivista* internacional ha proseguido la tendencia degenerativa observada en los últimos años en cuanto a paulatina desideologización, atomización en identidades individuales desorganizadas y sin conciencia alguna de movimiento colectivo, y motivadas casi exclusivamente por afán de notoriedad. Los vertebradores ideológicos antisistema y contestatarios que configuraron al movimiento *hacktivista* antes de la década de 2010, casi diez años después están prácticamente desaparecidos, sustituidos por atacantes individuales cuyo propósito general es desfigurar sitios web para firmarlos con su alias. De esta forma, **el *hacktivismo* de 2010 acabará convirtiéndose en 2020 en una clase de *cibergraffitismo***.

En cuanto a tácticas, técnicas y procedimientos, este panorama internacional definido por un ***hacktivismo* oportunista** está configurado por identidades individuales la mayor parte de las veces desconectadas entre sí que desfiguran con el *cibergraffiti* de sus alias sitios web; en más del 90% de los incidentes, la desfiguración correlacionaba con el equipamiento por parte de las webs victimizadas de software desactualizado presentando vulnerabilidades comunes fácilmente explotables.

En **España** está presente **la misma realidad *hacktivista* internacional pero muy devaluada** en cuanto a identidades dotadas de habilidades técnicas para suponer una ciberamenaza. Con alguna excepción ('La 9ª Compañía'), prácticamente todos los atacantes *hacktivistas* sobre los que se puede inferir que operan desde el interior de España atacando a webs en el mismo país presentaban perfiles de muy baja peligrosidad debido a su carencia de un mínimo de habilidades técnicas ciberofensivas; una minoría de esas identidades es capaz de utilizar software de usuario disponible en paquetes de libre circulación empleados en auditoría y seguridad informáticas, para llevar a cabo ciberataques rudimentarios generalmente ejecutados con impericia sobre webs de alta vulnerabilidad. La mayor parte de los ataques *hacktivistas* sobre webs alojadas en infraestructura en España se llevan a cabo por identidades presumiblemente en el exterior del país, cuyo perfil responde al del *hacktivismo* oportunista *cibergraffitero* ya apuntado.

La degradación ideológica y colectiva del escenario *hacktivista* internacional conlleva así mismo una muy baja producción de marcos narrativos motivacionales para desarrollar campañas de ciberataque en los distintos países. Las que se llevan a cabo suelen estar privadas de una retórica militante elaborada, tener muy débil colectivización, recibir el apoyo de identidades sin habilitación técnica y de baja peligrosidad, carecer de impacto e influencia atractiva, y de nuevo caracterizar a sus promotores por la intención de obtener menciones en redes sociales, deseo que logran muy marginalmente.

Trasladada a España, esta insuficiencia ideológica, narrativa y técnica de un *hacktivismo* oportunista sólo ha tenido en la #OpCatalunya un llamamiento a llevar a cabo ciberataques. Este marco narrativo ha tenido en 2019 un desarrollo irregular, configurado por unas pocas identidades desorganizadas y realizando ataques de baja peligrosidad (generalmente por denegación de servicio, o inyecciones SQL deficitarias) con una cronología discontinua. A fin de lograr notoriedad en redes sociales, algunas de las identidades participantes falsificaban reivindicaciones simulando ciberataques que en realidad no habían realizado.

También **en el marco de la #OpCatalunya** pudiera estarse dando el caso de que se llevan a cabo divulgaciones de información sensible al dominio público por parte de alguna identidad amparada en una **táctica de falsa bandera**: simular ser un militante *hacktivista* que por otro lado no muestra indicio de poseer ningún tipo de habilidad técnica, para divulgar a través de redes sociales información sensible que reivindica haber obtenido por medio de ataques cibernéticos, cuando en realidad pudiera tratarse de una identidad simpatizante prosecesionista en el contexto de Cataluña que se hace pasar por *hacktivista* para hacer pública información que obtendría no necesariamente por medios cibernéticos ofensivos, o que le sería suministrada por terceras partes con intereses en la #OpCatalunya.

Por otro lado, de una manera muy incipiente y a escala internacional, representando en España un 3'2% de los incidentes, continúan observándose incidentes por desfiguración de web en donde, además del alias del atacante, se inyecta contenido en forma de código software no

deseado que conduce a los visitantes de la web victimizada a contenidos comerciales sobre los que el atacante pretende, fraudulentamente, incrementar su peso referencial en el algoritmo de buscadores web. Esta **práctica fraudulenta se conoce con el nombre de *SEO Spam***, y es practicada desde hace al menos tres años por un porcentaje de momento menor de atacantes *hacktivistas* mostrando rasgos o iconografía en idioma turco.

No obstante este diagnóstico, internacionalmente todavía operan menos de media docena de identidades a la que se puede atribuir afiliación ideológica *hacktivista*, y que tienen **habilidades técnicas suficientes** como para presentar un riesgo de nivel moderado o alto, dependiendo del objetivo al que decidan atacar. Este tipo de identidades, de las cuales 'Phineas Fisher' sería el prototipo, puede traducirse en una amenaza operativa en cualquier momento y contra cualquier objetivo que tenga sistemas tecnológicos conectados a Internet.

Del mismo modo, aunque el *hacktivismo* oportunista que configura la realidad internacional presente en general una baja peligrosidad, **no conviene pasar por alto que supone una ciberamenaza irregular y de compleja predicción**, pues al estar operado por motivadores individuales y de búsqueda de notoriedad, aunque en general débilmente dotado técnica e intelectualmente en ocasiones puede resultar en cibertaques de impacto: ya sea porque puntualmente alguna identidad con mayor habilidad técnica entre en acción atacando un objetivo de relevancia; ya sea porque un ciberataque menor sea sobredimensionado por la evaluación imprecisa de medios de comunicación o profesionales de la ciberseguridad, resultando en impacto reputacional o mediático.

En lo que tiene que ver con el **ciberyihadismo**, 2019 se ha desarrollado y concluye del mismo que el año anterior: **ausencia de evidencia directa o indicadores indirectos que sugieran que exista alguna estructura o identidad atacantes afiliadas a organizaciones islamistas o yihadistas**. Sin embargo, permanece la actividad, disminuida respecto del año previo, de identidades *hacktivistas* oportunistas que desfiguran webs de alta vulnerabilidad y baja visibilidad inyectando en ellas iconografía o mensajes parasitados de contenidos islamistas, sin que de esas actuaciones pueda deducirse implicación ideológica sino intención meramente provocadora.

3. HACKTIVISMO EN ESPAÑA

3.1 ESTRUCTURA *HACKTIVISTA* EN ESPAÑA

3.1.1 PERFILADO GENÉRICO DE LAS IDENTIDADES EN 2019

En 2019 se cumplen **cinco años consecutivos de carencia de una infraestructura *hacktivista* en España** con capacidad coordinada de planear y ejecutar ciberataques con un mínimo de peligrosidad.

Al contrario, la realidad *hacktivista* en España está conformada por identidades individuales de nula o baja capacitación técnica como ciberamenazas, con débil o inexistente colectivización o identidad de grupo, y motivadas fundamentalmente por lograr notoriedad mediante menciones en redes sociales, redes en las que no obstante carecen de influencia, de canales informativos de referencia con un seguimiento que pueda considerarse mínimamente significativo.

La nulidad operativa de las identidades individuales que se apropian de iconografía y lemas *hacktivistas* para tratar de destacar en redes sociales está explicada por la deficiente capacitación técnica de los individuos que adoptan esas identidades digitales. Por lo que respecta a la incapacidad de generar colectivización o sentimiento de pertenencia a un colectivo *hacktivista*, así como la ausencia de influencia en redes sociales, están así mismo determinadas por el abandono de motivadores ideológicos en el *hacktivismo*, que tanto en España como internacionalmente está dominado por intenciones exclusivamente egocéntricas y autoreferenciales de obtener visibilidad en redes sociales circulando cualquier tipo de contenido que "suene" a *hacktivista*, incluso si para ello hay que falsear reivindicaciones de ciberataques o impostar llamamientos a la acción en determinados escenarios.

Esa impostura en cuanto a la implicación *hacktivista* en escenarios de protesta social, junto a la individualización autoreferencial de los implicados, se traduce en un marcado déficit narrativo a la hora de componer llamamientos al activismo cibernético. En España, al igual que sucede en otros países, los escenarios de tensión social o política no logran ser traducidos en narrativas motivacionales de implicación *hacktivista* más allá de la fabricación de una etiqueta meramente simbólica que difundir en redes sociales.

El ejemplo más evidente de esta **degeneración hacktivista en España**, **hasta convertirse en una impostura**, es la denominada #OpCatalunya, en donde a pesar de correlacionar con un escenario de conflictividad y contestación sociales en una determinada realidad política, la implicación *hacktivista* no ha pasado de ser una etiqueta en redes sociales, aderezada a veces por reivindicaciones sobredimensionadas en esas mismas redes sociales o en medios de comunicación, y en definitiva caracterizada por:

1. Ausencia de una narrativa con una mínima redacción motivacional;
2. Ausencia de un núcleo activo de identidades con capacidades operativas cibernéticas;
3. Ausencia de colectivización, donde incluso los ataques por denegación de servicio -tradicionalmente un asunto colectivo- han sido individuales;
4. Predominio de actores utilizando software automático, que no requiere habilidades técnicas en el atacante, para llevar a cabo inyecciones SQL, la mayoría defectuosas;
5. Incremento de las reivindicaciones falsificadas o amañadas para dar apariencia de credibilidad;
6. Apropiación de iconografía y rasgos *hacktivistas* para llevar a cabo exfiltraciones de información con intenciones prosecesionistas.

Estos parámetros identificativos en torno a la #OpCatalunya, que son extensibles al resto del *hacktivismo* en España, configuran un escenario de ciberamenaza ocasional, inexistente como grupo y restringida a ocurrencias individuales de muy baja peligrosidad, de débil impacto e influencia, y sin un trasfondo ideológico o motivacional que pronostique un cambio de tendencia a corto plazo si esos parámetros se mantienen como hasta el momento.

La única ciberamenaza doméstica en España con rasgos de peligrosidad, capacitación técnica para llevar a cabo ciberataques, y motivación ideológica de naturaleza *hacktivista*, continúa siendo la identidad digital conocida como '**La 9ª Compañía**', que no obstante ha disminuido significativamente su actividad durante 2019.

Este escenario de una única identidad *hacktivista* aislada digna de mención en cuanto a su capacidad para representar una ciberamenaza no es exclusivo de España, sino común a todos los países europeos: en ningún otro país de la Unión Europea cabe hacer referencia a una entidad similar a 'La 9ª Compañía' salvo en el caso de Italia, con '**LulzSecITA**', una mutación de 'Anonymous Italia'.

3.1.2 NUEVAS IDENTIDADES INDIVIDUALES OPERANDO EN 2019

En el contexto de este panorama de continuidad en la inarticulación de un tejido *hacktivista* en España, durante 2019 han venido apareciendo y desapareciendo algunas pocas nuevas identidades de muy baja peligrosidad caracterizadas, tal como ya se ha descrito en el perfilado general de identidades, por su:

- Afán de notoriedad en redes sociales traducida en cambio en una débil influencia incluso para lograr darse a conocer u obtener seguidores. Carencia de motivaciones ideológicas, sustituidas por claras intenciones de auto-referencia, de conseguir rápidamente menciones y notoriedad por parte de otras cuentas en redes sociales o de medios de prensa.
- Nula o baja capacidad técnica para llevar a cabo ciberataques, que algunas de ellas han tratado de compensar falsificando ciberataques mediante la simulación de que los llevaban a cabo, para lo cual por lo general han difundido información fabricada para tratar de sostener la impostura de que eran identidades *hacktivistas* operativas, cuando en realidad no han pasado de ser un icono creado en un perfil de Twitter o Facebook.

Entre ese tipo de identidades, el 5/1/2019 el portavoz de la asociación de consumidores FACUA Rubén Sánchez revelaba a través de un hilo en Twitter[1] la identidad administrativa de una persona a la que atribuye gestionar el perfil en Twitter[2] de '**Anonymous ES**', entonces una identidad con 31.300 seguidores constituida en 2013 de la que no se conoce ni participación en, ni promoción de, ciberataques, y que utilizaba iconografía y denominación de 'Anonymous' para difundir informaciones diversas, en su mayoría ajenas al *hacktivismo*; en general este perfil venía siendo calificado por otras identidades ciberatactivistas como de "ultraderecha".

Por otro lado, a partir del 7/2/2019 la identidad probablemente radicada en España y constituida en Twitter[3] '**DigitalResearchTeam**' iniciaba una campaña de diseminación de mensajes para divulgar información y documentos públicamente disponibles en sitios web y localizables mediante una sencilla búsqueda; o datos situados en el dominio público resultado de la aplicación de iSQL por parte de identidades *hacktivistas* en el pasado; o ejecutaba inyecciones XSS que en realidad eran redirecciones de navegador de usuario hacia montajes gráficos intentando simular una acción de penetración en realidad no realizada; para con toda esa información reivindicar ciberataques -en última instancia falsos- a esos sitios web intentando transmitir la impresión de que los había vulnerado y obtenido de ellos "información sensible", y solicitando a las supuestas víctimas que le contacten por correo electrónico[4] para "resolver la vulnerabilidad encontrada". Con esta pauta, intentaba hacer pasar por información sensible la que cualquier ciudadano obtiene en abierto y públicamente de webs como la correspondiente a los Ministerio de Justicia, Asuntos Exteriores, o Hacienda, del Partido Socialista, del Principado de Asturias, o de varias universidades, todos ellos en España.

[1] https://twitter.com/RubenSanchezTW/status/1081503092460453888
[2] https://twitter.com/Anonymus_ES
[3] @digitalrteam
[4] digitalresearchteam@secmail.pro

En este mismo elenco de identidades, el 31/3/2019 el nuevo alias en Twitter[5] '**g0tze**' emitía un mensaje advirtiendo en inglés y catalán de que "*atacarán hoy la web de la junta electoral*" de España. Inmediatamente después de emitirlo, el mensaje era borrado por el propio usuario. La cuenta no llegó en ningún momento a emitir más mensajes, y permanece inactiva.

En el mismo contexto, el 4/3/2019 la identidad '**0xDazzer**' emitía un mensaje[6] sugiriendo haber obtenido ilícitamente datos de la Dirección General de Protección Civil y Emergencias de España, aunque sin establecer sobre qué dominio web habría presuntamente actuado. Como muestra de los datos supuestamente obtenidos adjuntaba una captura de pantalla de lo que parecía ser una hoja de Excel con dos columnas: una con direcciones de correo electrónico (sólo denominación, sin contraseñas) la mayoría bajo dominio guardiacivil.org; y otra con nombres o puestos de trabajo, de los cuales la mayoría han sido censurados para no ser visibles, dejando a la vista diez puestos de trabajo con denominación de Guardia Civil. Posteriormente la identidad borraría su perfil en Twitter, sin más desarrollo, y sin esclarecer el origen de los datos divulgados, que tenían la apariencia de corresponderse con listados de asistentes a un curso.

Por otra parte, en el capítulo de identidades que, aun manteniendo el patrón de baja peligrosidad de las anteriores, han mostrado no obstante alguna capacidad principiante para llevar a cabo ciberataques menores utilizando software automático para intentar escanear y explotar vulnerabilidades comunes en sitios web, durante 2019 ha venido operando en España y en algún otro pais '**al1ne3737**'[7], que el 21/3/2019 adscribía varias acciones por inyección SQL a la #OpCatalonia y que posteriormente participa en varios ataques también principalmente por iSQL, con alguna desfiguración menor, en el contexto de la #OpEcuador. Esta identidad dejó de estar activa a partir de la segunda mitad de 2019.

Por último en cuanto a nuevas identidades, en 2019 también ha venido operando '**ChalecosAmarillos**', el alias de un militante antisistema con presencia en Twitter[8] desde 2018 que sobre todo ha destacado por afirmar haber iniciado una huelga de hambre en julio de 2019 en protesta por la entrega por parte de Ecuador a Reino Unido de Julian Assange, y que ha participado en varios puntos de protesta sobre el terreno en Barcelona[9] en apoyo a las tesis prosecesionistas. Esta actividad militante sobre el terreno la llegaría a completar durante 2019 en el plano cibernético con el lanzamiento de varios ataques testimoniales por denegación de servicio: en marzo sobre las webs de los ayuntamientos de Salou y Reus; en abril y en el contexto de la campaña electoral de las elecciones generales al Parlamento en España sobre webs del partido político Vox, sin producir más impacto; y en mayo sobre la web del Partido Socialista en Cataluña, sin más recorrido que situar en Pastebin[10] un listado de direcciones de correo electrónico bajo dominio psoe.es, sin contraseñas ni información sensible ni contextual de otro tipo, y fácilmente obtenible por medios abiertos legítimos.

[6] https://twitter.com/0XDAZZER/status/1102575132340555777
[7] https://twitter.com/al1ne3737
[8] https://twitter.com/ChalecosAmarill
[9] Por ejemplo https://twitter.com/ChalecosAmarill/status/1200212079766097920
[10] https://pastebin.com/h4WyqtbB

3.2 CAMPAÑAS Y CIBERATAQUES HACKTIVISTAS EN ESPAÑA

3.2.1 #OPCATALUNYA, #OPCATALONIA, #OPSPAIN

Durante los doce meses de 2019, se han llevado a cabo 43 ciberataques en el marco narrativo de la #OpCatalnuya, que lleva activo con distintas denominaciones desde el último trimestre de 2017. El volumen de acciones durante 2019 representa el 25% de la actividad adosada a la #OpCatalunya el año previo y, por tanto, una sustantiva caída de la ofensiva *hacktivista* afiliada esta narrativa. De entre las acciones llevadas a cabo:

- Un **60% fueron inyecciones sobre bases de datos SQL**, en un 35% de los casos fracasadas o defectuosas en sus resultados. La mayoría tuvieron como objetivos webs privadas menores, o centros de educación secundaria. En este capítulo intervino principalmente la mencionada '**al1ne3737**', y también '**NightStroke**', '**alph4numer1c**', '**Reizor**' o la identidad instrumental y rápidamente desaparecida **OpC4tal0ni42019.**
- El **30% de los ataques se correspondieron con acciones por denegación de servicio**, realizadas al igual que el año anterior principalmente sobre web de la Administración Pública española. En la gran mayoría de casos, se trató de ataques sin colectivizar y, salvo alguna instancia puntual, sin prolongarse en el tiempo, quedando por tanto en acciones meramente testimoniales. Los actores que llevaron a cabo estos ataques fueron principalmente '**Mr Whiteanon**', '**Andr4x**' o '**CataloniaLegion**'.
- Un **9% consistieron en desfiguraciones de webs menores** de pequeños negocios o empresas, inyentando contenido generalmente alusivo a la #OpCatalunya o al alias del atacante, que en todos los casos fue una identidad genérica '**Anonymous España**'.

Con la mayoría del año prácticamente en blanco, el grueso de las acciones en el contexto de la #OpCatalunya se concentró en menor medida en enero, y principalmente en marzo y en octubre, siendo este último mes cuando se conoció la sentencia judicial por la Causa Especial 20907/2017, que se seguía en el Tribunal Supremo contra los organizadores del referéndum secesionista en Cataluña el 1/10/2017.

No obstante, en este panorama general de actividad residual y baja peligrosidad en la #OpCatalunya, destaca la implicación de '**Anonymous Catalonia**' en varias acciones de difusión de información sensible en el dominio público:

- El 2/3/2019 situaba en el dominio público[11] un fichero en formato MS Excel conteniendo datos personales identificativos (nombre, DNI, teléfono, dirección postal) de supuestos afiliados al partido político Vox en la localidad de Sabadell. No mostraba ningún indicador que sugiera que los datos habían sido obtenidos por procedimientos de ciberataque; tampoco se encuentran públicamente disponibles en abierto.

[11] https://anonfile.com/w80fC0vbb4/afiliados_sabadell_xlsx

- Posteriormente y en el contexto del juicio en el Tribunal Supremo sobre la causa respecto del referéndum independentista del 1/10/2017 en Cataluña, la misma identidad divulgaba a través de Twitter[12] datos personales identificativos en redes sociales y de correo electrónico de Montserrat del Toro López, Secretaria Judicial del Juzgado de Instrucción número 13 de Barcelona; no hay constancia de que los datos se obtuvieran por una acción de ciberataque, pero tampoco que estén públicamente disponibles.

- En junio de 2019 situaba un hilo en Twitter[13] de varios mensajes en donde insinuaba que la "cuenta de correo electrónico profesional" del presidente del Tribunal de la Causa Especial 20907/2017, Manuel Marchena, estaría protegida por un "código de 7 letras con el nombre de alguien querido". En el hilo de mensajes se afirmaba que la información sobre Marchena formaría parte de una base de datos de "más de 9 millones de códigos que fueron filtrados en su día" y que serían "accesibles a cualquiera". Como supuesta muestra de esa base de datos, la identidad hacktivista difundía una captura de pantalla donde mostraría una visión muy restringida y censurada de supuestas credenciales de autenticación de cuentas de correo electrónico comenzando por las iniciales "mm" (siguiendo la retórica de 'Anonymous Catalonia', probablemente haciendo referencia a Manuel Marchena) bajo diversos dominios de servicios gratuitos en internet, varios con referencia geográfica a Rusia (.ru), que como Yandex.ru se considera improbable que representen a Manuel Marchena.

  Posteriormente, y en otro mensaje del hilo mostraba una captura de pantalla de Microsof Outlook que afirmaba se correspondería con el acceso web al buzón de correo electrónico de una dirección electrónica de Manuel Marchena, que sugería que trataría de m.marchena@poderjudicial.es, a partir de la cual intentan forzar el descubrimiento en Gmail de una cuenta personal para el mismo juez, intento que se muestra en idioma francés (probablemente debido al uso, por el intruso, de algún sistema de anonimización de IP como Tor o una VPN).

- Por último, el 19/9/2019 difundía un mensaje en Twitter[14] donde a su vez referenciaba a otro mensaje previo[15] de tres minutos antes donde se mostraba la captura de pantalla del icono de un fichero .VCF con el nombre Todos _los_contactos; en el segundo mensaje haciendo referencia al primero, 'Anonymous Catalonia' mencionaba los perfiles en Twitter de Albert Rivera[16] y Carina Mejías[17], respectivamente Presidente y Diputada en el Congreso del partido político Ciudadanos. Al día siguiente de nuevo divulgaba a través de Twitter[18] un enlace a carpetas almacenadas en la plataforma Keybase[19], dando a entender que se trataba de información sobre el partido político Vox.

[12] https://twitter.com/anonktalonia/status/1103289931311562752
[13] https://twitter.com/anonktalonia/status/1144936578298601472
[14] https://twitter.com/anonktalonia/status/1174792660260966420
[15] https://twitter.com/anonktalonia/status/1174791932331118595
[16] @Albert_Rivera
[17] @CarinaMejias
[18] https://twitter.com/anonktalonia/status/1175058424641523713
[19] https://keybase.pub/anoncatalonia/VOX/

El 21/9/2019 ‘Anonymous Catalonia’ continuaba con el partido político Ciudadanos y difundía tres mensajes en Twitter insinuando que había tenido acceso a nombres de grupos de Whatsapp del presidente del partido Albert Rivera, mencionando algunos nombres de supuestos grupos de Whatsapp que atribuía a Rivera estar suscrito.

‘Anonymous Catalonia’ tiene un histórico de comportamiento que la define como un canal de propaganda desinformativa prosecesionista catalana operando con una interfaz hacktivista probablemente como “falsa bandera”.

Del análisis de sus exfiltraciones de información se infiere la hipótesis de que ‘Anonymous Catalonia’ es una identidad ciberactivista militante centrada específicamente en promover propaganda secesionista en Cataluña a través de redes sociales (actualmente en Telegram), probablemente desprovista de habilidades técnicas ciberofensivas, pero también probablemente conectada con otra fuente de información principal que la instrumenta como canal de exfiltración al dominio público de información sensible, información ésta que originariamente habría sido obtenida por un atacante distinto a ‘Anonymous Catalonia’ mediante procedimientos cibernéticos o directamente a partir de algún tipo de acceso (en el caso del comprometimiento de credenciales de autenticación de cuentas de correo electrónico de miembros del Poder Judicial) incluso a terceras fuentes (como foros de mercado negro cibercriminal de compra/venta de contraseñas) o tercera parte interesada.

3.2.2 LA 9ª COMPAÑÍA DE ANONYMOUS

Durante 2019 ‘La 9ª Compañía de Anonymous’ ha disminuido su actividad ofensiva aproximadamente al equivalente a un tercio del promedio anual que venía mostrando.

Tanto su modus operandi como su motivación ideológica no han registrado variaciones apreciables, dando continuidad a ciberataques por penetración sobre servidores web en un despliegue de técnicas y procedimientos que revela una cuidada fase preparatoria de análisis del objetivo a atacar, de su arquitectura tecnológica, del software empleado y, principalmente, de las vulnerabilidades que expone; para continuar con una fase de explotación operativa de esas vulnerabilidades, con el propósito de acceder a bases de datos de negocio o de identificación personal, datos que extrae y sustrae para mantenerlos en su poder; finalizando con una fase reivindicativa en donde generalmente no disemina al dominio público los datos sustraídos en el servidor web victimizado, sino que a través de sus canales sociales ofrece capturas de pantalla censurando los datos personales al objeto como evidencia de que ha llevado a cabo el ciberataque. Habitualmente la fase reivindicativa de los ataques conlleva la exposición de motivos para cada acción, en el contexto de una narrativa sustancialmente ideológica de naturaleza insurgente y de sesgo antisistema y anticapitalista de tintes anarquistas.

En abril de 2019 quedaba suspendida por Twitter el perfil en esa red social de 'La 9ª Compañía', momento a partir del cual optaba por canalizar sus comunicaciones sociales a través de las cuentas que venía manteniendo en Mastodon[20] y Tumblr[21], aunque creando en octubre de 2019 una nueva en Twitter[22] que de momento no está empleando.

En cuanto a ciberataques, durante 2019 ha llevado a cabo tres acciones, con una cuarta meramente anecdótica:

1. El 6/2/2019 comprometía el punto de acceso que la web que la empresa de ventas El Corte Inglés tiene para las "listas de la Comunión", inyectando sobre ella varios contenidos irónicos con alusiones a políticos españoles.
2. El 22/5/2019 penetraba la web de venta de entradas al recinto de la Alhambra en Granada, desfigurándola y accediendo potencialmente a datos personales identificativos y de pago de usuarios de la web, que no ha divulgaba en el dominio público.
3. El 21/11/2019 lograba acceso ilegítimo al portal de noticias de la agencia de noticias EFE.
4. Ya como anécdota, el 2/11/2019 apuntaba a una vulnerabilidad XSS en una web de servicios a empresas de Telefónica inyectándole un texto reivindicativo[23] que, como ocurre con este tipo de inyecciones, no modifica ni vulnera la web sino que la muestra deformada en el navegador web del visitante que acceda a ella mediante el hipervínculo con el mensaje inyectado por 'La 9ª Compañía'.

[20] https://mastodon.social/@la9deanon
[21] https://la9deanon.tumblr.com/
[22] https://twitter.com/9deAnon
[23] empresas.blogthinkbig.com

3.2.3 CIBERATAQUES POR ENTIDADES EXTERNAS A ESPAÑA

Continuando el patrón de años precedentes, durante 2019 sitios web con direcciones IP en España o dominio web correspondiente a España, se han visto afectado al igual que los residentes en otros países por oleadas de ciberataques llevados a cabo por identidades *hacktivistas* que llevan a cabo acciones explotando vulnerabilidades comunes en sitios web, principalmente en los provistos de software desactualizado, con el propósito final de inyectar en ellos contenido reivindicativo general, principalmente el alias del atacante. Este patrón es general a nivel mundial y la situación en España no es más que un reflejo de lo ocurrido en el resto de países.

En los doce meses de 2019 se han atacado 1.153 sitios web con dirección IP o dominio territorial en España, lo que representa una disminución superior al 50% respecto del año previo. La comparativa interanual, no obstante, tiene una interpretación muy relativa, y no sirve en general para determinar por sí sola si la amenaza *hacktivista* es mayor o menor. Esto es así porque la variación de cifra total de webs individuales atacadas en un año depende de que haya habido una o varias oleadas de explotación masiva de vulnerabilidades en sitios web: por ejemplo, como ha sido el caso tanto en 2018 como en 2019, en enero y diciembre se produzcan varias oleadas de desfiguración de decenas de sitios web a la vez, donde el atacante utiliza procedimientos automatizados para explotar una misma vulnerabilidad en un elevado número de sitios web individuales; en este caso, dependiendo de si hay una o varias oleadas, o de si cada oleada implica a varias decenas de webs o varios cientos de webs, el número total anual de webs afectadas se ve o no incrementado. Como es observable por la figura 3-2-3-1, en 2019 (línea roja) se produjeron picos de ataques en masa en enero, agosto y diciembre, mientras en 2018 (línea verde) se produjo adicionalmente un gran pico en mayo y la volumetría también fue mayor en el primer trimestre del año.

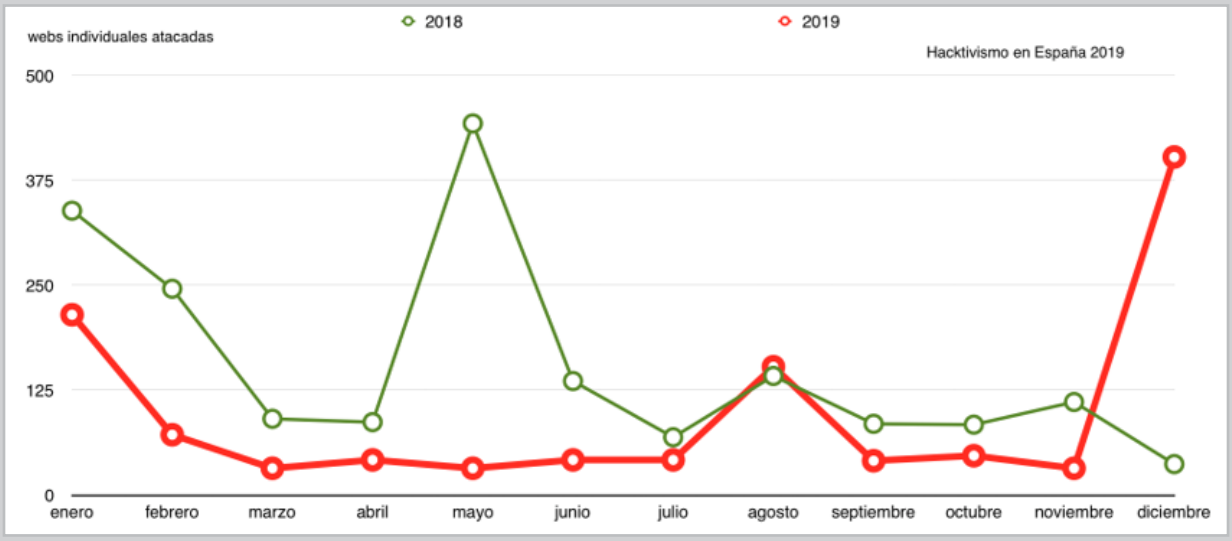


Figura 3-2-3-1

Al igual que años precedentes, los ataques *hacktivistas* correlacionan en un **93% con la presencia de software vulnerable en las webs atacadas**, que puede **considerarse el primer factor de riesgo para que la victimización por *hacktivismo***.

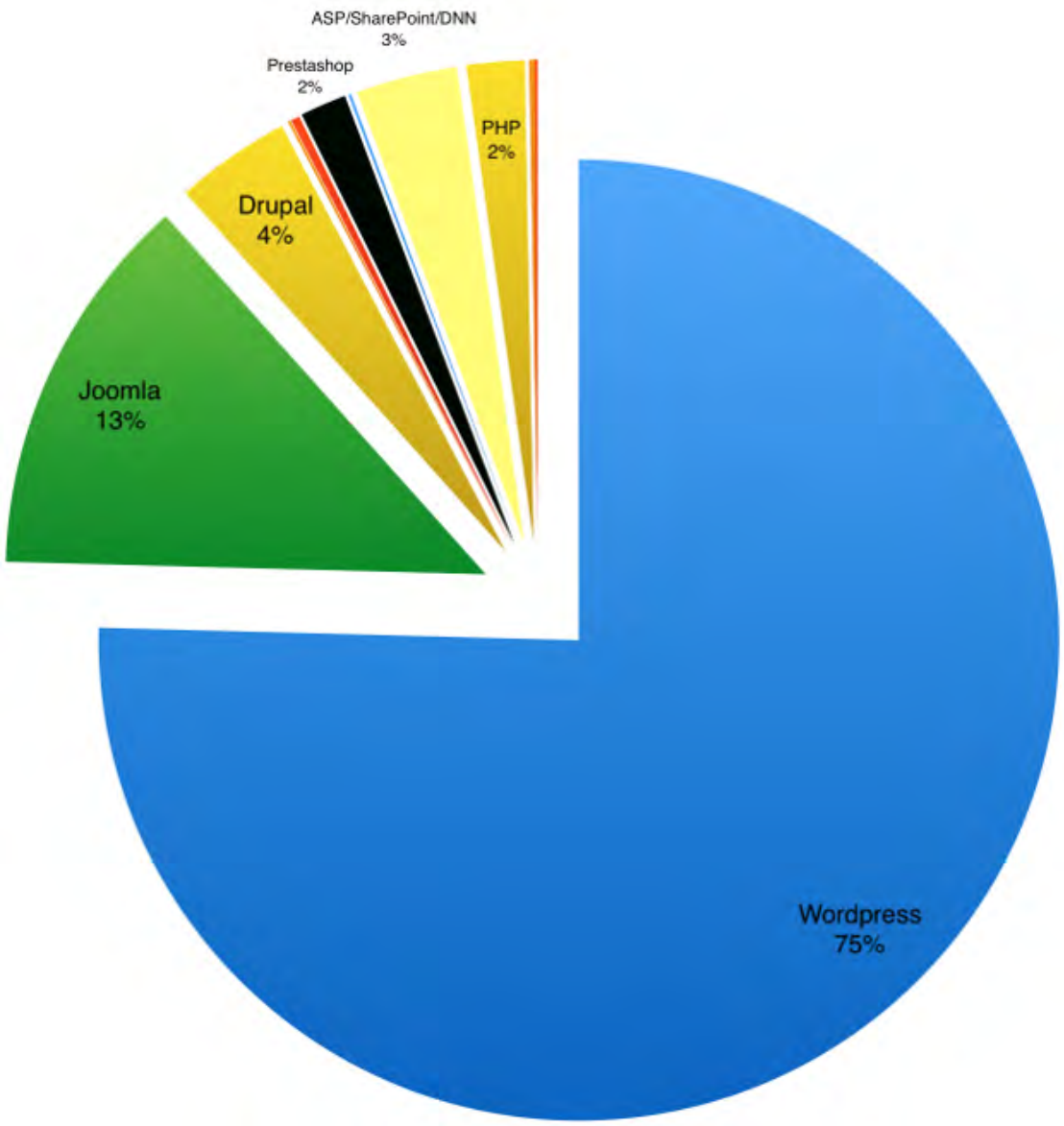


Figura 3-2-3-2

De ese porcentaje total, un **89% de las webs victimizadas la vulnerabilidad en el software estaba relacionado con gestores comerciales de contenidos**, siendo Wordpress el más representado con un 75% de los casos, seguido de Joomla con un 13% (Figura 3-2-3-2).

Por tanto, también coincidiendo en ello con años previos, la muy elevada correlación entre victimización de sitios web y software vulnerable instalado en ella, junto a la circunstancia de que numerosos de los ataques cursen en oleadas de desfiguración masiva de webs con la

misma vulnerabilidad de software en varios países, llevadas a cabo por identidades atacantes cuyo propósito general es inyectar contenido reivindicativo de autoafirmación (en la mayoría de los casos, su propio alias), confirma la tendencia de considerar el ***hacktivismo* actualmente** prevalente a nivel internacional como una **actividad oportunista motivada por criterios egocéntricos y de búsqueda de notoriedad** y alejada de las palancas ideológicas que supuestamente definían el *hacktivismo* en sus orígenes como movimiento de protesta cibernética. En 2019, confirmando una tendencia de los últimos años, el ***hacktivismo* es una actividad de pequeña cibercriminalidad motivada por la búsqueda de notoriedad y el exhibicionismo digital** por parte de sus ejecutantes.

Además de ese exhibicionismo digital como primer motivador del *hacktivismo*, en 2018 comenzó a observarse que algunos atacantes aprovechaban la desfiguración *hacktivista* de sitios web para inyectarles código malicioso en forma de scripts generalmente programados en JavaScript. Este patrón se confirma en 2019.

Estos script han venido cumpliendo dos funciones: la principal, incrementar el peso en buscadores web de contenidos comerciales alojados en webs asiáticas, principalmente japonesas, mediante la inclusión en la web atacada de contenidos comerciales a promocionar; la inclusión de estos contenidos en numerosas webs victimizadas altera el ranking de posicionamiento de estos contenidos en buscadores web, en un táctica fraudulenta que se conoce como SEO Spam, de *search engine optimization*, u optimización de motores de búsqueda.

Tras esta función principal, una secundaria de los scripts inyectados ha sido incluir entre su código HTML *metadata* promocionando webs de contenido pornográfico en Turquía; o directamente insertar scripts redirectores desde la web atacada hacia las webs pornográficas.

Este **escenario de intersección entre dos áreas de pequeña cibercriminalidad** (el **hacktivismo y el SEO Spam**) continúa en 2019 y ha sido observada principalmente en acciones llevadas a cabo por atacantes que muestran rasgos turcos, ya sea en las denominaciones de sus alias o en los contenidos reivindicativos inyectados. De momento, no obstante, esta práctica representa un porcentaje menor del *hacktivismo* tanto en España como en el exterior: del total de webs victimizadas en España en 2019, **sólo el 3'2%** incluían algún tipo de técnica *SEO Spam* inyectada en su desfiguración.

Finalmente, algunas de las identidades que durante 2019 con mayor frecuencia han vulnerado webs en España en el marco de oleadas de desfiguraciones en varios países probablemente explotando vulnerabilidades en gestores comerciales de contenidos han sido, entre otras: '**Mister Spy**', probablemente argelina, afectando webs basadas en Wordpress; '**Imam**', probablemente norteafricano, sobre webs equipadas con Joomla; '**Simsimi**' actuando sobre webs equipadas con Wordpress; '**KingSkrupellos**', probablemente turco, sobre webs basadas en SPIP y en Open Journal; '**Ayyildiz Tim**', probablemente turca, sobre webs con distintos tipos de software vulnerable; '**chinafans**', sin rasgos definidos de nacionalidad pero que podría ser turca, actuando sobre webs con Wordpress; '**Mr.Donut's**', con rasgos turcos y actuando sobre Wordpress; '**hector**',

también inyectando contenidos turcos sobre gestores de contenidos Drupal y Wordpress; '**eRRoR 7rB**' operando sobre Wordpress; '**zakiloup**', probablemente norteafricano, sobre webs basadas en Wordpress; '**Seravo**', sobre webs basadas en Joomla; '**UnM@SK**' explotando software desactualizado basado en ASP.net; '**Dev19Feb**' actuando sobre Wordpress; y la también mostrando indicadores turcos '**Oscar**', igualmente sobre Wordpress,

3.2.4 ATAQUES HACKTIVISTAS SOBRE INSTITUCIONES PÚBLICAS

La realidad del *hacktivismo* sobre España en 2019 no muestra un foco específico de hostilidad ofensiva sobre el país que lleve a atacantes *hacktivistas* a atacar webs por su españolidad. De idéntica manera, no se observa **ninguna intencionalidad específica de atacar sitios web de instituciones públicas en España**, más allá de lo ya consignado para la #OpCatalunya. En esta realidad, las webs de instituciones de los distintos niveles y órganos de la Administración Pública en España que se han visto afectadas por desfiguraciones durante 2019, lo han sido en el mismo contexto general ya informado de haber sido **victimizadas por exponer algún tipo de vulnerabilidad en su equipamiento software**.

Las acciones *hacktivistas* que han afectado de manera variada a instituciones públicas en España durante 2019, considerándose instituciones públicas de manera genérica a aquéllas que tienen dependencia orgánica del gobierno nacional, de las comunidades autónomas, o de ayuntamientos y corporaciones locales, han sido:

- El 17/1/2019 '**Akem**' producía inyecciones SQL sobre las webs de la Universidad de Extremadura[24], la Universidad de Málaga[25], la Universidad Politécnica de Cartagena[26] y Laboral Ciudad de la Cultura[27] efectuando volcados de usuarios en el dominio público; también se afectaba parcialmente a la Universidad de Alicante, pero únicamente exfiltrando las tablas de un subdominio[28]. También el 21 y 22/1/2019 el mismo 'Akem' reclamaba haber realizado inyecciones de una imagen con su alias en una URL de un subdominio de la web del Instituto de Mayores y Servicios Sociales[29].
- El 18/1/2019 '**nadya**' desfiguraba cuatro webs[30] también desarrolladas con Joomla, inyectando sobre ellas un fichero f.gif con su alias; una de ellas se corresponde con un subdominio del Ayuntamiento de Burriana[31].

[24] [uex.es] https://ghostbin.com/paste/fgkec
[25] [uma.es] https://ghostbin.com/paste/tk55w
[26] [upct.es] https://pastebin.com/JBkxsavL
[27] [laboralciudaddelacultura.com] https://pastebin.com/JBkxsavL
[28] [iuii.ua.es] https://pastebin.com/JBkxsavL
[29] sede.imserso.gob.es/carpetaCiudadano/jsp/adjuntarDocumento.jsp?id=akem
[30] montealduide.org, albertolajo.es, celiacosmalaga.es
[31] arxiu.burriana.es

- El 6/2/2019 '**Mr.Whiteanon**' lanzaba un ataque individual por denegación de servicio sobre la web[32] de Instituciones Penitenciarias del Ministerio del Interior de España, sin enmarcar la acción en ningún tipo de narrativa. El 9/2/2019 el mismo atacante repetía la operación, sin colectivización ni narrativa específica, sobre otras webs[33] de partidos políticos y de la ciudad de Barcelona.
- El 18/2/2019 '**Mr.Inbetween**' insertaba un fichero inbetween.html con su alias en la web[34] de las jornadas de ciberdefensa de 2018.
- El 5/3/2019 '**PaWL**' inyectaba su alias en un fichero algeria.txt sobre un subdominio[35] desarrollado con Wordpress y alojado en la web del gobierno de Navarra.
- El 27/3/2019 '**Mister Spy**' utilizaba un fichero def.gif con su alias contra la web de espacios naturales protegidos[36] de la Comunidad de Madrid, que está desarrollada con una versión vulnerable del gestor de contenidos Joomla.
- El 10/4/2019 '**eRRoR 7rB**' alteraba con contenido general diez subdominios[37] equipados con versiones vulnerables de Wordpress y alojados en la web del Consejo Superior de Investigaciones Científicas.
- El 9/5/2019 '**Mr.Kro0oz.305**' inyectaba un fichero kro.html con su alias en la web del Ayuntamiento de Maracena[38] en Granada, que está desarrollada con una versión vulnerable del gestor de contenidos Joomla.
- El 26/7/2019 '**Xmed_Falleg**' deformaba la web[39] del Consejo Comarcal de la Selva en Cataluña mediante un fichero xmed.html; la web usa versiones vulnerables de Joomla y PHP, además de soportar el habitualmente vulnerable Adobe Flash.
- El 28/7/2019 '**Html404**' desfiguraba tres webs[40] que podrían estar utilizando el gestor de contenidos Drupal, una de ellas correspondiente al Ayuntamiento de La Oliva, inyectando sobre ellas un fichero exz.txt con su alias; alguna de las webs quedaba contaminada con contenido *SEO Spam* en idioma japonés.
- El 5/8/2018 '**Seravo**' inyectaba un fichero db.txt con su alias en la misma ruta[41] de diez webs[42] correpondientes a centros de enseñanza pública alojados en las webs de la Junta de Extremadura[43]; las webs emplean un gestor de contenidos Joomla. El 21/9/2019 el mismo atacante vulneraba otra web[44] de un centro de enseñanza pública adscrito a la Junta de

[32] institucionpenitenciaria.es
[33] falange.es, alternativaespanola.com y portdebarcelona.cat
[34] jornadasciberdefensa.es
[35] blogpin.navarra.es
[36] espaciosnaturalesmadrid.org
[37] Entre ellos mbg.csic.es, nanocosmos.csic.es, swi.csic.es
[38] maracena.es
[39] selva.cat
[40] losanimalesmehablan.com, o2pos.com, laoliva.es
[41] .../images/db.txt
[42] Entre ellas cpfcoortizlopez.educarex.es, cpmdoncamilohdez.juntaextremadura.net
[43] educarex.es y juntaextremadura.net
[44] cpralmendralejo.juntaextremadura.net/images/db.gif

Extremadura, que está desarrollada con el gestor de contenidos Joomla. Igualmente el 12/10/2019 desfiguraba con un fichero db.txt y su alias dos subdominios[45] de centros de enseñanza pública en la Junta de Extremadura, que también están desarrollados con el gestos de contenidos Joomla.

- El 13/8/2019 '**DeadsOul**' dañaba con su alias la web[46] del proyecto Red Natura, que está adscrito a la Junta de Extremadura, inyectando un fichero s0ul.txt con su alias; la web utiliza un gestor de contenidos Joomla y equipa versiones vulnerables del software Apache y PHP; ya fue alterada de la misma forma por otro atacante en mayo de 2019.
- El 3/9/2019 '**Death Student**' inyectaba contenido general en un fichero death.gif sobre la web de un centro de enseñanza secundaria pública[47] adscrito a la Junta de Extremadura, que está desarrollada con Joomla.
- El 7/9/2019 '**Quizy Squad**' deformaba con un fichero 0x.html y contenido general la web de la Fundación Madridi+d[48] de la Comunidad de Madrid, que utiliza un gestor de contenidos Drupal y está dotada de versiones desactualizadas del software PHP y del servidor Nginx.
- El 24/12/2019 '**Ayyildiz Tim**' inyectaba su acostumbrado contenido proturco en el subdominio[49] desarrollado con Wordpress del Laboratorio de las Artes del ayuntamiento de Valladolid, que quedaba posteriormente infectado con contenido *SEO Spam* en idioma japonés.

3.2.4.1 VULNERACIÓN DE PERFILES INSTITUCIONALES EN TWITTER

Hacia el último tercio de julio de 2019, y principalmente concentrándose en todo el mes agosto, se desarrollaba una campaña de vulneración de accesos de cuentas en Twitter de ayuntamientos e instituciones públicas, para una vez logrado acceso ilegítimo por un atacante, emitir a través de la cuenta comprometida mensajes alusivos a la corrupción y amenazas a cargos políticos electos correspondientes al país o localidad de referencia de la cuenta en Twitter vulnerada.

Durante la mañana del 14/10/2019 era vulnerada la cuenta en Twitter[50] de la Universidad Pública de Navarra (UPNA), que difundía mensajes con amenazas de muerte al Alcalde de Pamplona (Figura 3-2-4-1-1).

Figura 3-2-4-1-1

[45] iesloustauval.juntaextremadura.net, cptrajano.juntaextremadura.net
[46] infonatur.es
[47] cptrajano.educarex.es
[48] madrimasd.org/0x.html
[49] lava.valladolid.es
[50] @UNavarra

Posteriormente, en la tarde del mismo 14/10/2019 el perfil en Twitter[51] de la Universitat Jaume I de Castellón era comprometido, emitiendo mensajes maliciosos y amenazas de muerte contra la alcaldesa de la ciudad Amparo Marco: <<*si alguien se encuentra con esta especie por la calle, animamos a que la matéis*>>.

El 15/10/2019 la cuenta de atención al cliente de la empresa Correos en Twitter[52], con 16.800 seguidores, fue comprometida y comenzaba a emitir mensajes maliciosos.

Seguidamente y el mismo día 15/10/2019, el perfil en Twitter del Servicio Andaluz de Empleo[53] era comprometido, emitiendo mensajes maliciosos para sus 112 mil seguidores, incluyendo amenazas de muerte para el presidente del Partido Popular Pablo Casado.

Las tácticas, técnicas y procedimientos (TTP) de las acciones descritas vulnerando cuentas en Twitter en España coinciden con las llevadas a cabo durante julio y agosto de 2019 en Iberoamérica por un atacante del que de momento se conoce el alias '**Lullz DL'**, y que son descritas en el apartado correspondiente a Iberoamérica en este informe.

Considerando que el epicentro de esta oleada de vulneraciones de accesos a cuentas institucionales en Twitter durante 2019 estaba en Iberoamérica, se establece la hipótesis de que la variante en España fue un reflejo de la actividad en Iberoamérica, probablemente facilitada por el factor idiomático en el atacante.

Por tanto, la información sobre los incidentes no sugiere un foco específico de amenaza sobre cuentas en redes sociales de instituciones públicas españolas, sino el resultado de un efecto puntual y colateral de una acción ciberofensiva atacando a este tipo de objetivos en varios países de Iberoamérica, con probable epicentro en El Salvador.

[51] @UJI_noticias
[52] https://twitter.com/correosatiende
[53] https://twitter.com/saempleo

4. HACKTIVISMO EN IBEROAMÉRICA

4.1 PANORÁMICA HACKTIVISTA EN IBEROAMÉRICA

La realidad *hacktivista* iberoamericana en 2019 ha sido continuista respecto del año previo, definiéndose principalmente por ciberataques mediante la **deformación del contenido de sitios web de gobiernos locales, regionales y federales**, o de otros órganos como instituciones educativas, que **exponían vulnerabilidades explotables en su equipamiento software**. Este patrón ha sido especialmente incidente en Brasil, seguido de México, Ecuador, Colombia y Perú.

Esta panorámica general se ha complementado con las siguientes características, unas tendenciales como la primera y la segunda, y otras más coyunturales:

1. Debilidad o presencia anecdótica, limitada a identidades digitales en redes sociales, de configuraciones nacionales *hacktivistas* o de la marca 'Anonymous' en los países de Iberoamérica. En algunos casos, como en Colombia o Brasil operan algunas identidades individuales (como 'org0n' o 'Umbrella Gang') con capacidad para llevar a cabo ataques por desfiguración sobre webs vulnerables. En otros, como Chile o Perú, el mínimo tejido hacktivista en torno a 'Anonymous' se ha debilitado sustancialmente hasta prácticamente quedar en anecdótico. En Chile, por ejemplo, el marco narrativo contestatario de la #OpChile ha mostrado como la denominación 'Anonymous Chile' era empleada para realizar exfiltraciones que como #PacoLeaks o #MilicoLeaks no está claro que procedieran de ciberataques llevados a cabo por identidades hacktivistas, sino probablemente de acciones híbridas ejecutadas tal vez por activos de movimientos insurgentes o antisistema que han utilizado el canal 'Anonymous Chile' para sus exfiltraciones.

2. Ausencia de narrativas elaboradas y con suficiente impacto colectivo para articular campañas nacionales de ciberataque en paralelo a situaciones de contestación social en algunos países. La conflictividad social con protestas durante 2019 en los casos de Chile, Guatemala, Venezuela u Honduras se ha saldado con ataques *hacktivistas* desorganizados –más incidentes en Chile, y menos en el resto de países- en una ausencia de campañas con una mínima sustanciación, ataques promovidos generalmente por unas pocas identidades digitales con baja influencia y débil o nula capacitación técnica.

3. Visibilización ocasional en la identidad brasileña 'VandaTheGod' (por otro lado, desarticulada en diciembre de 2019 al ser arrestado su presunto responsable en Brasil) de esa intersección ya mencionada en ataques por identidades extranjeras en España entre la pequeña cibercriminalidad *hacktivista* motivada por la búsqueda de notoriedad, y la pequeña cibercriminalidad asociada al *SEO Spam* o a la venta de exploits para llevar a cabo ciberataques.

4. En diciembre de 2019 intentaba ocupar de nuevo un espacio en el *hacktivismo* iberoamericano la identidad colectiva 'Anonymous Ibero', que en los inicios de la década de 2010 pretendió, sin demasiado éxito, organizarse en configuraciones nacionales de 'Anonymous' en varios países del subcontinente con el objetivo de generar narrativas *hacktivistas* para el llamamiento a ciberataques. De momento, en esa búsqueda de la "reentrada" en el escenario, 'Anonymous Ibero' no pasa de ser una identidad digital con muy baja influencia en redes sociales, sin habilidades técnicas, y sin capacidad (ni perspectiva de tenerla) de lograr articular un colectivo.

5. En claro mimetismo a otras identidades atacantes a nivel internacional, en varios países de Iberoamérica y con foco originario en El Salvador, un atacante vulneraba el acceso a cuentas en Twitter de instituciones de gobierno en varios países tanto del subcontinente

como de España. El modus operandi se centraba en divulgar mensajes amenazantes contra gobernantes locales a través del perfil en Twitter mientras permanecía comprometido. A partir de uno de los incidentes en España, se corrobora que el vector de ataque para estos comprometimientos de cuentas en Twitter es el *phishing*, correos electrónicos dirigidos a buzones de personas que podrían tener las claves de acceso a la cuenta en Twitter que se pretende vulnerar, personas a las que se aplican tácticas de ingeniería social para robarles las credenciales de acceso, que posteriormente serán empleadas por el atacante para tomar el control coyuntural del perfil en Twitter.

4.2 CIBERATAQUES HACKTIVISTAS DESTACADOS EN IBEROAMÉRICA

Dentro del contexto general descrito, no obstante, han destacado algunas acciones particulares ya sea por la visibilidad o por la relevancia institucional de las webs victimizadas:

- El 7/1/2019 '**TuNovato**' desfiguraba las webs de la Armada[54], de la Oficina de Defensa del Consumidor[55] y de la Seguridad Social del Ministerio de Trabajo y Empleo[56] de Paraguay, inyectando en ellas contenido general; la primera y tercera de las webs están desarrolladas con el gestor de contenidos Concrete5 y la segunda con Wordpress.
- El 4/4/2019 '**STR0NG**' alteraba la web de la Autoridad Portuaria[57] en República Dominicana, que está programada con un gestor de contenidos Drupal 8, inyectando sobre ella contenido reivindicativo genérico y un fichero 404javascript.js con su alias.
- El 15/4/2019 '**Kec0a_T3rbang**' desfiguraba la web[58] del Ministerio de Industria en Jamaica, que está montada sobre un gestor de contenidos Drupal y utiliza una versión desactualizada de PHP.
- El 25/4/2019 '**FakeSmile**' comprometía la web de la Dirección General de Aeronáutica Civil[59] en Guatemala, inyectando sobre ella un fichero blink.php con su alias y contenido general; la web equipa versiones desactualizadas del gestor de contenidos Joomla y del software PHP.
- El 27/5/2019 '**Anonymous Venezuela**' dañaba la web programada con Drupal del Ministerio del Poder Popular para el Transporte Acuático y Aéreo[60] de Venezuela, inyectando sobre ella un fichero anonymous.php con contenido reivindicativo general

[54] armadaparaguaya.mil.py
[55] sedeco.gov.py
[56] seguridadsocial.mtess.gov.py
[57] portuaria.gob.do
[58] moa.gov.jm
[59] dgac.gob.gt
[60] mpptaa.gob.ve

- El 12/5/2019 '**Inocent**' desfiguraba con contenido reivindicativo general la web[61] en Brasil de la distribuidora cinematográfica Warner Bros.
- El 14/6/2019 '**GeNErAL**' comprometía con un fichero by.htm de contenido general y alusiones al Islam y a la liberación de Siria y Palestina diecisiete webs de marcas automovilísticas en Ecuador[62], Colombia[63], Perú[64], México[65] y Uruguay[66]; las webs tienen en común estar desarrolladas en un entorno Microsoft (IIS, ASP.net, Windows) y estar alojadas en infraestructura de Google; también haber sido programadas por la empresa *Exagono Software*, cuya web[67] utiliza una versión desactualizada de ASP.net (4.0.30319).
- El 3/7/2019 '**Legion BOmb3r**' atacaba la web de la Organización de las Naciones Unidas[68] en Ecuador, inyectándole contenido reivindicativo general en un fichero legito.txt; la web emplea una versión vulnerable de Wordpress. El mismo atacante desfiguraba el 13/7/2019 la web[69] de turismo del Gobierno de Belice. En la República Dominicana, el mismo atacante afectaba a la web del Servicio Militar Voluntario[70] y de otras tres instituciones gubernamentales[71], inyectándoles un fichero bd.txt con su alias; del mismo modo que los ataques del día anterior en el pais, estas webs emplean un entorno Microsoft y versiones desactualizadas de ASP.net (por ejemplo 2.0.50727).
- El 12/8/2019 la identidad '**LaGorraLeaks**' reivindicaba[72] haber comprometido sistemas de la Policía Federal de Argentina. Como resultado de la acción, el atacante produjo la exfiltración en Tor[73] de diversos documentos de interés policial (transcripciones de escuchas policiales, fichas personales de agentes de policía); la desfiguración de una web[74] del Ministerio de Seguridad de la Provincia de Buenos Aires; y el secuestro momentáneo del perfil en Twitter de la Prefectura Naval Argentina[75], que difundió un falso mensaje afirmando que buques argentinos habían sido <<*atacados por misiles británicos*>> y que <<*la Armada ha respondido con éxito a esta violación de nuestro territorio*>>.
- El 19/8/2019 '**nine**' utilizaba un fichero nine.html con su alias sobre la web[76] de la Asamblea Legislativa de la Paz en Bolivia, que está desarrollada con una versión desactualizada de Wordpress.

[61] warnerexibidor.com.br
[62] Dodge.com.ec
[63] jeep.co
[64] ram.pe, Dodge.pe
[65] mopar.com.mx, Chrysler.com.mx
[66] Chrysler.com.uy, jeep.com.uy
[67] exagono.net
[68] un.org.ec
[69] belizetourism.gov.bz
[70] smv.mil.do
[71] procomunidad.gob.do, losbotados.gob.do, corepol.gob.do
[72] https://zggtzf2fjdaoazu7777zhlz2qwtwbchpkl5lgca53htfvf2i7umvudid.onion.pet/
[73] http://zggtzf2fjdaoazu7777zhlz2qwtwbchpkl5lgca53htfvf2i7umvudid.onion/
[74] http://zggtzf2fjdaoazu7777zhlz2qwtwbchpkl5lgca53htfvf2i7umvudid.onion/
[75] @PrefecturaNaval
[76] asamblealapaz.gob.bo

- El 23/8/2019 '**Mr.Onion**' dañaba la web[77] programada con Wordpress de la Agencia de Aeronáutica Civil de Honduras, inyectándole un fichero 69.htm con contenido en indonesio; la web quedaba infectada con contenido *SEO Spam* en idioma japonés.
- El 8/10/2019 '**M1r0x**' desfiguraba con contenido alusivo a 'Ghost Squad Hackers' la web del Parlamento Centroamericano[78], que está programada con DotNetNuke y ASP.net, y que ya fue atacada de la misma forma en agosto de 2019.
- En el marco narrativo de la **#OpChile**, el 25/10/2019 '**Anonymous Chile**' reivindicaba[79] haber situado en el dominio público[80] y la denominación general de **#PacoLeaks** lo que reclamaba era datos personales identificativos de personal de los Carabineros de Chile. Durante los dos días posteriores fueron situados sucesivos volcados, contiendo documentos con supuestos datos personales identificativos de funcionarios, nombre, RUT, zona y comisaría de destino o cargo; manuales de usuario de la plataforma de documentación electrónica (DOE) de los Carabineros de Chile; o grabaciones sobre operativos policiales. En este escenario pudiera darse el caso de que 'Anonymous Chile' fuera la identidad reivindicativa y **Rebeldeside.pw** el canal de exfiltración, mientras el atacante que lleva a cabo la supuesta ciber-intrusión en el sistema tecnológico de Carabineros fuera una identidad no visibilizada.
- El 6/11/2019 '**0x1998**' vulneraba la web del Ministerio de Salud de Nicaragua, que está desarrolla con una versión vulnerable de Joomla, inyectándole[81] un fichero 0x1998.txt con su alias. También el 20/11/2019 el mismo atacante vulneraba con un fichero 0x1998. txt y su alias la web[82] de la Dirección General de Minería del gobierno de la República Dominicana, que equipa una versión vulnerable del gestor de contenidos Joomla.
- De nuevo en el contexto de la **#OpChile**, el 13/12/2019 era situada[83] en la plataforma de exfiltraciones DdoSecrets una colección de varios ficheros descritos como *<<3.475 correos electrónicos de oficiales superiores del Ejército de Chile, incluyendo los Directores de Inteligencia, Operaciones, Finanzas, y Relaciones Internacionales*>>. La colección de ficheros, que era etiquetada colectivamente como **#MilicoLeaks**, no fue reivindicada en una acción con autoría específica, sino acompañada de un texto con retórica militante general antisistema contra el Gobierno de Chile.

[77] ahac.gob.hn
[78] parlacent.int
[79] Por ejemplo https://www.facebook.com/AnonOpsChile/posts/1148373638692656
[80] pacoleaks.rebelside.pw
[81] minsa.gob.ni/images/0x1998.txt
[82] dgm.gob.do/images/0x1998.txt
[83] https://hunter.ddosecrets.com/collections/65

4.2.1 VULNERACIÓN DE PERFILES INSTITUCIONALES EN TWITTER

Tal como se mencionaba en el epígrafe 3.2.4.1 de este informe anual, hacia el último tercio de julio de 2019, y principalmente concentrándose en todo el mes agosto, se desarrollaba una campaña de vulneración de accesos de cuentas en Twitter de ayuntamientos e instituciones públicas, para una vez logrado acceso ilegítimo por un atacante, emitir a través de la cuenta comprometida mensajes alusivos a la corrupción y amenazas a cargos políticos electos correspondientes al país o localidad de referencia de la cuenta en Twitter vulnerada.

El epicentro originario de los ataques se radicaba en Iberoamérica, y concretamente en El Salvador, para posteriormente extenderse por otros países de la región hispanoamericana y por España. Las acciones hostiles fueron ejecutadas por un atacante cuya operativa responde a los siguientes parámetros:

- Por el momento no ha revelado indicadores identificativos más allá del hecho de expresarse en español y de firmar con un alias desconocido;
- Probablemente esté poniendo en práctica tácticas de ingeniería social por correo electrónico con *phishing* para robar credenciales de autenticación de las cuentas de Twitter a atacar;
- Utiliza una narrativa contra la corrupción en los mensajes inyectados en las cuentas comprometidas;
- Profiere amenazas gruesas contra representantes políticos de las localidades cuyos perfiles en Twitter vulnera.

En este contexto, el 23/7/2019 el Ministerio de Justicia y Seguridad Pública de El Salvador reconocía[84] que el perfil personal en Twitter[85] del Ministro de Seguridad del país había sido atacado, emitiendo mensajes de insulto y amenazas contra el ministro. Al día siguiente era coyunturalmente secuestrada la cuenta en Twitter[86] de la Dirección General de Migración y Extranjería de El Salvador, que emitía el conocido mensaje "*esta cuenta ha sido hackeada*".

Posteriormente, el 29/7/2019 fue atacado el perfil en Twitter[87] de la Dirección de Cultura de la Intendencia de Montevideo en Uruguay, comenzando por el típico mensaje "*esta cuenta ha sido hackeada*" y siguiendo por amenazas a Rogelio Rivas, Ministro de Justicia y Seguridad Pública de El

[84] https://twitter.com/SeguridadSV/status/1153766936469266432
[85] @RogelioRivasSS, modificada por el atacante a @RogelioRivasSS_
[86] @Migracion_SV, modificada por el atacante a @Migracion_SV_
[87] @IMCultura, modificada por el atacante a @IMCultura_

Salvador. Y el 30/7/2019 era comprometido el perfil personal en Twitter[88] de Óscar Ortiz, Secretario General del Frente Farabundo Martí de Liberación Nacional de El Salvador y expresidente del país, que emitía la hasta el momento única firma identitaria del atacante en esta oleada de acciones sobre cuentas de Twitter, haciendo constar en un mensaje (Figura 4-2-1-1) la reivindicación "*hacked by **Lullz DL***", cuyo alias no coincide con ninguna identidad *hacktivista* conocida.

Figura 4-2-1-1

El 1/8/2019 había sido vulnerada de la misma forma la cuenta en Twitter[89] de la Caja Seguro Social de Panamá, comenzando por la frase "*esta cuenta ha sido hackeada*" y emitiendo posteriormente los mensajes habituales ya conocidos, además de amenazas al Presidente del país Nito Cortizo.

Tras esta primera oleada de ciberataques en Iberoamérica, comenzaron acciones contra cuentas en Twitter de ayuntamientos en España, afectándose de la misma manera y con igual narrativa que la observada en Iberoamérica las cuentas en Twitter del Ayuntamiento de Valencia[90], el Ayuntamiento de Pamplona[91], y el Ayuntamiento de Albacete[92].

El mismo día 5/8/2019 donde se afectaba a ayuntamientos en España se actuó sobre otros dos perfiles en Twitter del gobierno de Ecuador, el correspondiente al Viceministerio de Promoción e Inversiones[93], y otro de la cuenta oficial de las Fuerzas Armadas. Al día siguiente se comprometía el perfil en Twitter[94] del Instituto Nacional de Formación Técnico Profesional de la República Dominicana, y de nuevo a la semana siguiente volvían a victimizarse cuentas en España, vulnerándose las cuentas del Ayuntamiento de Berga[95] en Cataluña, del Ayuntamiento de Palma[96] en las Islas Baleares, pasando de nuevo el 13/8/2019 a la cuenta de la Gobernación del Azuay[97] en Ecuador, donde se inyectaban amenazas al presidente del país Lenin Moreno.

[88] @OscarOrtiz
[89] @CSSPanama, modificada por el atacante a @CSSPanama_
[90] https://twitter.com/AjuntamentVLC
[91] https://twitter.com/PamplonaIruna_
[92] https://twitter.com/aytoalbacete
[93] @Pro_Ecuador
[94] @InfotepRD_
[95] @AjBerga_, actualmente en @AjuntamentBerga
[96] @AjuntPalma_, actualmente en @AjuntPalma
[97] @GoberAzuay_, actualmente en @goberazuay

Adicionalmente, 15/8/2019 era vulnerado el perfil en Twitter de la provincia de Chubut[98] en Argentina, y al día siguiente la cuenta del Ayuntamiento de Arona[99] en Tenerife, con varias amenazas contra el alcalde del municipio José Julián Mena.

Tras el consistorio en Tenerife, alrededor de nueve horas más tarde del mismo 16/8/2019 era comprometida la cuenta en Twitter de la Fiscalía General del Estado de Jalisco[100] en México, y al día siguiente el Twitter de la Secretaría de Seguridad Pública del Estado de Quintana Roo[101] también México.

El 18/8/2019 un nuevo ataque afectaba al perfil del Ayuntamiento de Jaén[102], y el mismo día era alterado el Twitter del medio de comunicación dominicano Diario Digital RD[103], mientras el siguiente se vulneraba la cuenta del Ayuntamiento de Jerez[104] en España.

En el caso de Jerez se confirmaba que el posible vector de ataque para el comprometimiento del perfil era sido la ingeniería social: correos electrónicos maliciosos enviados a buzones del ayuntamiento simulando proceder de Twitter, conduciendo a la víctima a una web de *phishing*, y solicitando número de teléfono y claves de verificación del perfil en la red social, en uno de los cuales al menos una víctima con conocimiento de esta información la proporcionó al procedimiento malicioso.

Estas oleadas ponían su punto final el 20/8/2019 con las cuentas en Twitter de la Alcaldía de Coyoacán[105] y de la Alcaldía de Gustavo A. Madero[106] ambas en México; y el 28/8/2019 y de nuevo en El Salvador, comprometiendo el perfil de la Iniciativa Social para la Democracia[107], que emitía el mensaje "*esta cuenta ha sido hackeada por corrupción*", para difundir posteriormente amenazas contra el presidente del país Nayib Bukele.

[98] @GobiernoChubut, modificada por el atacante a @GobiernoChubut_
[99] Modificado por el atacante a @AytoArona_, actualmente en @AytoArona
[100] Modificado por el atacante a @FiscaliaJal_, actualmente en @FiscaliaJal
[101] Modificado por el atacante a @SSP_QROO_, actualmente en @SSP_QROO
[102] Modificado por el atacante a @AytoJaen_, actualmente en @AytoJaen
[103] @DiarioDigitalDo
[104] @CiudadJerez
[105] @Alcaldia_Coy
[106] @TuAlcaldiaGAM, modificada por el atacante a @TuAlcaldiaGAM_
[107] @ISDemocracia, modificada por el atacante a @ISDemocracia_

4.3 MARCOS NARRATIVOS HACKTIVISTAS EN IBEROAMÉRICA

El conjunto de propuestas narrativas de llamamiento a ciberataques hacktivistas en Iberoamérica durante 2019 se ha compuesto de las siguientes iniciativas:

MARCOS NARRATIVOS HACKTIVISTAS EN IBEROAMÉRICA 2019					
PAÍS	OPERACIÓN	PROMOTOR	TIPO DE OBJETIVO	TIPO DE ACCIÓN	RESULTADO
CL	#OpChile	Anonymous Baskerfield Xelj Yaupon Pitt Reizor Anonymous Chile AnonDown	Instituciones públicas de Chile	Desfiguración iSQL DDoS Exfiltraciones	Un par de grandes exfiltraciones de información sensible sobre Carabineros y el Ejército de Chile. DDoS sobre webs de instituciones públicas. Desfiguración de una veintena de webs de segundo y tercer nivel de gobierno. iSQL sobre universidades e instituciones de segundo nivel.
HO	#OpHonduras	Lorian Synaro SystemD	Instituciones públicas de Honduras	Desfiguración	Afectadas media docena de webs de instituciones de gobierno.
NI	#OpNicaragua	Lorian Synaro Anonymous Nicaragua Lancelot Udrich	Instituciones públicas de Nicaragua	DDoS	Menos de media docena de webs afectadas
EC	#OpEcuador #OpAssange	YourAnon Network Al1ne3737	Instituciones públicas de Ecuador	DDoS Desfiguración iSQL	Una veintena de acciones por DDoS contra instituciones públicas de Ecuador. Alrededor de iSQL sobre webs de gobierno. Desfigurada alguna web institucional, como la Corte Constitucional
BR	#OpAmazonia	Anonymous Brasil	Instituciones públicas y empresas internacionales en Brasil	iSQL DDoS Desfiguración	Casi medio centenar de webs de tercer nivel de gobierno desfiguradas. Algunos ataques DDoS puntuales sobre instituciones públicas. iSQL ocasionales fallidas.
VE	#OpVenezuela	Anonymous Venezuela	Instituciones públicas de Venezuela	DDoS Desfiguración iSQL	Una decena de acciones afectando a webs de segundo nivel de gobierno

5. HACKTIVISMO EN NORTE DE ÁFRICA Y ORIENTE MEDIO

5.1 PANORÁMICA HACKTIVISTA EN NORTE DE ÁFRICA Y ORIENTE MEDIO

Al igual que el año previo, en los países del Norte de África y de Oriente Medio el hacktivismo de 2019 ha venido protagonizado por **ataques de oportunidad mediante la desfiguración de sitios web llevados a cabo por identidades individuales**, que no se adscriben en su mayoría a colectivos hacktivistas y están motivadas por la búsqueda de notoriedad inyectando su alias en las webs deformadas. Al igual que en resto de regiones del mundo, estos ataques de oportunidad son ejecutados en su gran mayoría mediante la **explotación de vulnerabilidades del software, generalmente desactualizado**, que equipan las webs victimizadas.

Aparte ciberataques ocasionales en el contexto de la **#OpTurkey**, y acciones de un atacante individual en Líbano etiquetadas como **#OpLebanon**, el único marco narrativo hacktivista con traducción operativa en 2019 en las regiones del Norte de África y Oriente Medio ha sido la **#OpIsrael**, que aunque en marcado declive continúa su convocatoria anual cada mes de abril para atacar sitios web en Israel.

Durante 2019 la #OpIsrael ha continuado la tendencia de años previos de congregar desorganizadamente y durante un breve período a algunas identidades dispersas que lanzan ataques por denegación de servicio de baja peligrosidad sobre webs de gobierno en Israel, o desfiguran webs privadas menores de alta vulnerabilidad.

No obstante, este año se ha presentado la novedad de que una ciberamenaza, de la que se sospecha que utilizaba rasgos *hacktivistas* como envoltura de falsa bandera, pretendía diseminar una cepa de ransomware sobre ordenadores Windows en Israel utilizando en el código malicioso para distribuir el malware desde webs comprometidas el texto en inglés <<*"#OpJerusalem, Jerusalem is the capital of Palestine*>>. El intento no pasó de ser una amenaza, y no consta que la cepa de ransomware empleada (*JCry*) pasara de la anécdota en cuanto a su distribución.

Otro elemento diferencial observado en agosto de 2019 ha sido la utilización por un atacante *hacktivista*, probablemente turco, de un script redirector de tráfico para conducir a visitantes de una web desfigurada en el Ministerio de Planificación de Libia hacia una web de aterrizaje fraudulenta diseñada para capturar credenciales de autenticación de usuarios de tarjetas American Express. La intersección entre pequeña cibercriminalidad hacktivista y pequeña cibercriminalidad dedicada al *SEO Spam* o a la redirección de tráfico de usuarios, como ya se ha destacado en otros capítulos de este informe, representa una pequeña aunque tímidamente creciente proporción de las acciones hacktivistas principalmente ejecutadas por algunos atacantes mostrando rasgos turcos. No obstante, el caso de la web desfigurada en Libia supone un salto cualitativo, aunque de momento puntual, desde la pequeña cibercriminalidad del *SEO Spam* al *phishing* con pretensiones de robo de credenciales de autenticación bancaria de usuarios victimizados.

5.2 CIBERATAQUES HACKTIVISTAS DESTACADOS EN NORTE DE ÁFRICA Y ORIENTE MEDIO

Entre las acciones más destacadas durante 2019 en el Norte de África y Oriente Medio debido a que lograron alterar webs de instituciones públicas de relevancia como ministerios u órganos gubernativos o empresas públicas de visibilidad en los países afectados, cabe individualizar las siguientes:

- El 6/1/2019 '**Clash Hackers**' comprometía la web, desarrollada con Wordpress, del Ministerio de Asuntos Exteriores[108] de Palestina, inyectando sobre ella contenido reivindicativo general.
- El 25/1/2019, coincidiendo con el que está considerado el aniversario de la denominada "revolución del 25 de enero de 2011" en Egipto, '**Freedom Cry**' desfiguraba con un fichero 25Jan.htm y contenido alusivo varias webs en el país: las más significativas fueron las correspondientes al Ministerio de Salud[109] y a la autoridad nacional de registros de dominios de internet[110], que están desarrolladas en un entorno Microsoft (IIS, Windows, ASP.net) y alguna de ellas utiliza el habitualmente vulnerable Adobe Flash; afectando también a portal de la red egipcia de universidades[111], que utiliza el gestor de contenidos Wordpress.
- El 28/1/2019 '**Syrian Revolution Soldiers**' comprometía media docena de webs en Líbano, entre ellas los municipios de Aley[112] y Saida[113], así como el aeropuerto de Beirut[114] y la Embajada de Argelia en el país[115], inyectando sobre ellas contenido reivindicativo general con la etiqueta **#OpLebanon**, aunque sin desarrollar narrativa militante específica; alguna de ellas (como el aeropuerto o la embajada) tienen en común el desarrollo por parte de *OpenTech*. El mismo día, aunque en una acción aparentemente no relacionada, '**Sniper Egypt**' afectaba a un subdominio[116] de la web desarrollada con el gestor de contenidos SharePoint del Ministerio para la Reforma Administrativa, inyectando contenido reivindicativo general con alusiones al conflicto en Siria.

[108] mofa.gov.ps
[109] mohealth.gov.eg, mohp.gov.eg
[110] nic.net.eg, egdomain.net.eg, domain.com.eg, egdns.eg
[111] portal.eun.eg
[112] aley.gob.lb
[113] saida.gob.lb
[114] beirutairport.gov.lb, beirutairport.net
[115] embalgeria-lb.net
[116] afkar.omsar.gov.lb

- El 5/2/2019 '**Dr.SHA6H**', que es un alias alternativo de '**Syrian Revolution Soldiers**', desfiguraba con contenido general las webs de la Autoridad de Competencia y Antimonopolio[117], de una exposición nacional en la feria de arte de Basilea[118], de la Compañía de Electricidad de Homs[119], del Ministerio del Petróleo y Recursos Naturales[120], y de la Organización Central de Auditoría[121] del Gobierno de Siria; varias de ellas desarrolladas con Joomla.
- El 21/2/2019 '**mathio**' comprometía la web de la Comisión de Regulación de la Electricidad y el Gas del Ministerio de Energía de Argelia, que está programada con una versión desactualizada del gestor de contenidos Joomla, inyectando en una de sus URL[122] un fichero id.php de contenido general. El mismo día, inyectaba su alias en otra URL[123] de la Alta Instancia Independiente de Vigilancia de las Elecciones en el país, también programada con Joomla. El 28/2/2019 comprometía la web de la Dirección de Educación del Estado de Tlemcen[124], en el mismo país, que está desarrolla con Wordpress.
- El 26/2/2019 '**Wolftartous**' y '**Nightmare**' firmaban conjuntamente la alternación de la web de Defensa Civil[125], de un subdominio del Ministerio de Medio Ambiente[126], y de una web del Ministerio de Cultura[127] en Líbano, inyectando sobre ellas contenido reivindicativo en árabe de la "unidad" entre Siria y Líbano; las webs están alojadas en un entorno Microsoft, utilizan un gestor de contenidos *CMS Made Simple*, y una versión desactualizada del lenguaje PHP.
- El 8/3/2019 '**SnOw WoLF**' comprometía con un fichero done.htm de contenido general la web[128] del Poder Judicial de Palestina, que está desarrollada en un entorno Microsoft. El 12/5/2019 el mismo atacante vulneraba seis webs de gobierno en Palestina, entre ellas las más relevantes el Ministerio de la Mujer[129] o la Fiscalía[130], inyectando sobre ellas un fichero done.htm con su alias; las webs equipan versiones vulnerables del software del servidor Apache y de PHP, y la segunda de ellas el gestor de contenidos Wordpress.
- El 23/4/2019 '**Worms**' comprometía la web de la entidad de ciberseguridad[131] del gobierno de Libia, inyectando sobre ella un fichero worm.php de contenido reivindicativo general; la web utiliza un gestor de contenidos Wordpress.

[117] competition.gov.sy
[118] albasselfair.gov.sy
[119] hec.gov.sy
[120] mopmr.gov.sy
[121] cofc.gov.sy
[122] creg.gov.dz/pdf/id.php
[123] hiise.dz/index.php/ar/contacteznous-hiise-ar
[124] detlemcen.dz
[125] civildefense.gov.lb
[126] hunting.moe.gov.lb
[127] beirutworldbookcapital.com
[128] courts.gov.ps
[129] mowa.gov.ps
[130] gp.gov.ps
[131] nissa.gov.ly

- El 10/6/2019 '**mohamed.xo**' desfiguraba con contenido general y su alias una decena de subdominios del Ministerio de Recursos Hídricos[132] de Iraq, cuya web está dotada del gestor de contenidos Drupal y de una versión desactualizada de PHP.
- El 14/6/2019 '**PaWL**' comprometía la web equipada con Wordpress del Ministerio de Asuntos Religiosos[133] de Egipto, inyectando sobre ella un fichero A.php con la palabra "Algeria"; posteriormente, la web quedaba inyectada con contenido *SEO Spam* en idioma japonés.
- El 2/7/2019 '**Syrian Volcano**' comprometía tres webs[134] de instituciones de gobierno en Siria, incluido el Ministerio de Industria[135], inyectándoles contenido reivindicativo contra el presidente del país; las webs utilizan una versión vulnerable de PHP.
- En Jordania, '**Legion BOmb3r**' deformaba con un fichero bd.txt las webs del Ministerio de Hacienda[136] y de una institución del Ministerio de Cooperación Internacional[137], también desarrolladas en un entorno Microsoft.
- El 1/8/2019 '**Mr.Donut's**' (también conocido como 'Krayzie Haxor'[138]) desfiguraba con su alias la web programada con Wordpress del Ministerio de Planificación[139] en Libia; posteriormente quedaba infectada con contenido *SEO Spam* en idioma japonés y un redireccionamiento a una web[140] de *phishing* para el robo de credenciales de autenticación de clientes de American Express.
- El 7/8/2019 y actuando contra una web provista de ASP.net 4.0.30319 y DotNetNuke, '**VandaTheGod**' atacaba el Ministerio de Medio Ambiente[141] de Iraq con un fichero vanda.htm.
- El 26/9/2019 '**m4xpr0**' vulneraba hasta once webs de instituciones de gobierno en Iraq con IP en Reino Unido, entre ellas la empresa pública de informática y telecomunicaciones[142], el Ministerio de Comercio[143], el propio CERT (equipo de respuesta a incidentes de ciberseguridad) gubernamental[144], o el Consejo de Seguridad Nacional[145], inyectando sobre ellas un texto en árabe de rechazo al denominado "equipo de seguridad Sabrani (السابراني)", supuestamente dedicado a proporcionar seguridad en el país.

[132] mowr.gov.iq
[133] awkaf.gov.eg
[134] epsda.gov.sy, geci.gov.sy
[135] moid.gov.sy
[136] mof.gov.jo
[137] inform.gov.jo
[138] https://www.facebook.com/donathaxor
[139] planning.gov.ly
[140] shrilaxmiband.com/calendar/as/78d19/Suziko.php?Sef=4147
[141] moen.gov.iq
[142] itpc.gov.iq
[143] mot.gov.iq
[144] cert.gov.iq
[145] nsa.gov.iq

- El 8/11/2019 '**torgod**' inyectaba contenido reivindicativo general[146] sobre la web del Ministerio del Interior de Libia, que está desarrollada con Wordpress.
- El 9/12/2019 '**Black Python**' desfiguraba las webs de la Guardia de Fronteras[147] y de la Agencia Meteorológica[148] de Pakistán inyectándoles un fichero pwned.html con contenido de burla; al menos la segunda web está desarrollada con ASP.net.
- El 29/12/2019 '**3bad**' inyectaba su alias sobre las webs de la División de Refugiados[149] del movimiento de resistencia islámica Hamas, y sobre el Sindicato de Comités de Salud[150], ambas en Palestina. También en Palestina, el 28/12/2019 de nuevo '**0x1998**' inyectaba contenido despectivo contra los árabes en un fichero fuckpalestine.html sobre un subdominio[151] del Ministerio de Asuntos Religiosos.

[146] moi.gov.ly/wp-includes/torgod/index.html
[147] fc.gov.pk
[148] pmd.gov.pk
[149] drah.ps
[150] gaza-health.com
[151] dawa.palwakf.ps

5.3 MARCOS NARRATIVOS HACKTIVISTAS EN NORTE DE ÁFRICA Y ORIENTE MEDIO

Las narrativas *hacktivistas* de llamamiento a ciberataques en el Norte de África y Oriente Medio durante 2019 han sido:

MARCOS NARRATIVOS HACKTIVISTAS EN NORTE ÁFRICA/ORIENTE MEDIO 2019					
PAÍS	OPERACIÓN	PROMOTOR	TIPO DE OBJETIVO	TIPO DE ACCIÓN	RESULTADO
TR	#OpTurkey	Anonymous	Instituciones públicas de Turquía	Desfiguración DDoS	Desfiguradas una veintena de webs privadas. DDoS ocasionales sobre instituciones de gobierno.
IL	#OpIsrael	Minion Ghost Electron Libre NewSec Mauritania Attacker AnonGhost Palestine	Instituciones públicas y empresas de Israel	DDoS Desfiguración iSQL Amenaza de ransomware	Amenaza fallida de ransomware con cepa JCry distribuida en un fichero .EXE con la etiqueta #OpJerusalem Medio centenar de webs privadas desfiguradas. Ataques DDoS ocasionales.
LE	#OpLebanon	Syrian Revolution Soldiers	Instituciones públicas y empresas de Líbano	Desfiguración	Una veintena de webs de primera línea de gobierno afectadas.
KS	#OpHouseofSaud	News2Tor	Instituciones públicas de Arabia Saudí	DDoS	Sin desarrollo operativo más allá de su propuesta narrativa.

6. HACKTIVISMO EN ÁMBITO INTERNACIONAL

6.1 PANORÁMICA HACKTIVISTA EN RESTO INTERNACIONAL

Internacionalmente en el resto de países en regiones no mencionadas en epígrafes anteriores de este informe se reproduce, precisamente, lo ya diagnosticado para otras regiones en capítulos previos de este informe:

1. Atomización de identidades *hacktivistas* y desaparición de configuraciones nacionales tipo 'Anonymous';
2. Incapacidad para articular narrativas atractoras de campañas de ciberataque en contextos nacionales de conflictividad social, contextos que en el pasado, sobre todo en la década de los 2010, venían siendo atractores para el *hacktivismo* en torno al movimiento 'Anonymous', una pauta que ha decaído sustantivamente hasta ser anecdótica.
3. Desideologización a cambio de una motivación basada en la búsqueda egocéntrica de notoriedad;
4. Ciberataques en masa explotando vulnerabilidades en software desactualizado, principalmente gestores comerciales de contenidos y durante 2019 en software basado en un entorno ASP.net,
5. Un de momento bajo volumen de intersección entre pequeña cibercriminalidad *hacktivista* egocéntricamente motivada por el afán de notoriedad y pequeña cibercriminalidad dedicada al *SEO Spam*.

Adicionalmente a esta caracterización general, algunos elementos particulares en el escenario hacktivista internacional durante 2019 han sido:

- El comprometimiento en un país (Laos) de servidores de sistemas de nombres de dominio (DNS) , que se traduce en que el atacante tiene capacidad de acceder a la desfiguración de dominios web de alta visibilidad internacional. Este patrón ya ha sido observado en años previos, y de momento tiene una incidencia ocasional que no supone una tendencia.
- El secuestro puntual de acceso a perfiles en redes de alta visibilidad en redes sociales, probablemente obtenido a través de la aplicación de técnicas de ingeniería social, lo que posibilita al atacante inyectar contenidos reivindicativos en ese perfil y obtener una atención aumentada que hace que su acción sea muy eficiente en términos reputacionales del propio atacante. Durante 2019 ha destacado en esas prácticas la identidad '**Chuckling Squad**', mientras que 2020 se iniciaba con el mismo tipo de acciones firmadas por '**OurMine**'. Este tipo de atacantes no es necesariamente *hacktivista* en el sentido ideológico clásico, y podría más bien tratarse de otra clase de ciberamenaza actuando para servir a intereses geopolíticos o cibercriminales.
- El regreso a la escena pública mediante un ciberataque a un banco de la Isla de Man de la ciberamenaza *hacktivista* avanzada '**Phineas Fisher**'.
- La posibilidad de que algunas *ciberamenazas avanzadas* que despliegan operaciones ciberofensivas de intenciones geopolíticas o cibercriminales puedan estar coyunturalmente adoptando rasgos y prácticas *hacktivistas* como táctica de falsa bandera.

Entre los ataques *hacktivistas* en países del resto del ámbito internacional no contemplados en anteriores epígrafes de este informe y que han destacado ya sea por su visibilidad o por comprometer sitios web significados de empresas o de gobiernos, destacan los siguientes:

- El 12/1/2019 '**Simsimi**' comprometía la web desarrollada con Joomla del Ministerio de Justicia[152] de Zimbabwe, inyectando sobre ella un fichero simi.txt con su alias.
- El 25/1/2019 '**Negat1ve**' comprometía un subdominio de la web programada con Wordpress del Ministerio de Defensa[153] de Kenia, inyectando un fichero 1.php con su alias; posteriormente quedaba lleno de páginas con contenido comercial en idioma japonés.
- El 19/3/2019 '**xeo-neo**' comprometía la web[154] del Ministerio de Industria en Myanmar, inyectando sobre ella contenido en inglés atribuyendo al país ejercer "propaganda"; la web está desarrollada con versiones desactualizadas del gestor de contenidos Drupal, y los software para PHP y Apache.
- El 18/4/2019 '**Akincilar**' inyectaba contenido proturco con advertencias a Italia y Francia en cinco webs[155] desarrolladas con Wordpress de institutos de enseñanza secundaria pública en Italia. El 22/4/2019 comprometía la web de distribución de vídeos[156] de Asamblea

[152] justice.gov.zw
[153] soi.mod.go.ke
[154] industry.gov.mm
[155] Entre ellas comprensivoscilla.gov.it, icpaolovicampanella.gov.it
[156] assemblee-nationale.tv

Nacional de Francia, que utiliza el habitualmente vulnerable Adobe Flash. El 30/4/2019 afectaba a algo más de quince webs[157] del municipio de Arezzo en Italia, inyectando sobre ellas su habitual contenido proturco; las webs están desarrolladas en un entorno Microsoft. También comprometía varias decenas de webs alojadas en la Universidad de Córcega[158], que está desarrollada con versiones vulnerables de Wordpress y Apache. El 6/5/2019 y continuando con la inyección de contenidos negativos sobre Italia y Francia, se vulneraban alrededor de quince webs[159] de pequeños ayuntamientos en Francia, que están desarrolladas con Wordpress. Posteriormente, el 14/5/2019 operaba sobre la web[160] del servicio de Protección Civil de la provincia de Arezzo en Italia, que está desarrollada sobre un entorno Microsoft [IIS, ASP.net, Windows].

- El 22/4/2019 '**Hexolzwolf**' alteraba una de las webs del registrador nacional de dominios[161] de Senegal, inyectando sobre ella contenido proturco; la web está desarrollada con Wordpress.
- El 28/4/2019 '**Kurd Electronic Team**' comprometía la web del banco central[162] del gobierno de Eritrea, que utiliza una versión desactualizada del software del servidor Apache (la 2.0.40) sobre la que se han informado históricamente hasta 52 vulnerabilidades distintas.
- El 17/5/2019 '**Anonymous Fox**' comprometía dieciocho webs de órganos de gobierno y ministeriales en Burkina Faso, entre ellos la Policía[163] o los Ministerios de Transporte[164] o de Minas[165], inyectando sobre ellas un fichero F0x.php con su alias y logotipo; las webs equipan versiones desactualizadas del gestor de contenidos Joomla y de PHP.
- El 5/6/2019 '**Goodzilam**' había deformado con su alias e iconografía iraní la web del Ministerio de Cultura[166] de Tailandia, que está programada con versiones desactualizadas de PHP y Apache.
- El 8/7/2019 '**CoolDrax1337**' desfiguraba la webs del Parlamento[167], de la empresa Citroen[168] y del Tribunal Central Administrativo[169] en Portugal, inyectando sobre ellas contenido reivindicativo general; al menos las dos webs del sector gubernamental tienen en común equipar versiones vulnerables (4.0.30319) de ASP.net.
- El 21/7/2019 el mencionado '**ifactoryx**' actuaba contra tres webs ministeriales[170] de Mali, así como sobre una web de la Administración de Justicia Criminal[171] de Nigeria,

[157] Entre ellas vittoriacolonna.gov.it, comune.foiano.ar.it
[158] universita.corsica
[159] Entre ellas ville-saintagreve.fr, saint-laurent-les-bains.fr
[160] protezionecivile.provincia.ar.it
[161] nicsenegal.sn
[162] boe.gov.er
[163] police.gov.br
[164] transports.gov.bf
[165] mines.gov.bf
[166] culture.go.th
[167] parlamento.pt
[168] gsp.citroen.pt
[169] tca-sul.net
[170] education.gouv.ml, culture.gouv.ml, primature.gov.ml
[171] acjmc.gov.ng

- El 24/7/2019 el mismo '**M3sicth**' utilizaba contenido general para comprometer webs gubernamentales basadas en una versión vulnerable (4.0.30319) de ASP.net en varios países: la alcaldía del condado de Putnam[172] en EEUU; la Agencia para la Seguridad del Estado[173] en Sudáfrica; la Fiscalía General[174] en Trinidad Tobago; la Autoridad de Recursos Minerales[175] de Papúa Nueva Guinea; así como un par de decenas alojadas en un dominio de la administración pública[176] de Vietnam.
- El 6/8/2019 '**Ateam Tersolid**' comprometía un subdominio[177] de la web de Google en Togo, inyectándole su alias. El mismo día, '**1337**' dañaba otra media docena de subdominios[178] en la misma web. Es probable que estos ataques se deban a una acción sobre los servidores DNS gestionados por la infraestructura institucional pública o por los proveedores de servicios DNS de Togo: tanto Google como otras empresas de alta visibilidad en el país ya sufrieron desfiguraciones por un ataque a servidores DNS de Togo en ambos meses de noviembre de 2017 y 2018, en sendos casos por atacantes turcos.
- El 26/8/2019 'Mamad Warning', actuando bajo el alias '**Bax 026 of Iran**', inyectaba su habitual contenido con la bandera de Irán sobre las webs corporativas[179] de la empresa de ciberseguridad ESET en Croacia, que están programadas con ASP.net 4.0.30319.
- El 14/9/2019 '**s1ege**' comprometía con un fichero gsh.html conteniendo el aludido contenido sobre 'Ghost Squad Hackers' las webs del Ministerio de Equipamiento[180] de Níger; de la Comisión Nacional de Gestión de Desastres[181] del gobierno de Etiopía; de la Imprenta Nacional[182] de Monzambique; del Ministerio de Salud[183] de Gambia; y de la Agencia Metereológica[184] de Nigeria; que están desarrollada con un gestor de contenidos Drupal 7.
- El 24/10/2019 '**b0z1**' afectaba con su alias a la web corporativa de Yahoo[185] en Laos, probablemente sometiéndola a un ataque por redireccionamiento DNS, técnica mediante la cual otras webs del mismo operador han sido comprometidas en el pasado en países con menores estándares de ciberseguridad.
- Por otro lado, el 30/8/2019 la identidad '**Chuckling Squad**' comprometía el acceso a la cuenta en Twitter[186] de uno de sus fundadores, Jack Dorsey, difundiendo desde ella mensajes de tónica racista en inglés. Al parecer, el ataque se habría realizado comprometiendo la

[172] putnamcountyohio.gov
[173] ssa.gov.za
[174] ag.gov.tt
[175] mra.gov.pg
[176] vieclamvietnam.gov.vn
[177] edu.google.tg
[178] images.google.tg o books.google.tg
[179] eset.hr, nort.hr
[180] equipement.gouv.ne
[181] dppc.gov.et
[182] inm.gov.mz
[183] moh.gov.gm
[184] nimet.gov.ng
[185] yahoo.la
[186] @Jack

cuenta de Dorsey en un servicio asociado a Twitter, **Cloudhopper** (que permite utilizar Twitter mediante mensajes SMS), a la que los atacantes habrían accedido mediante la técnica del *SIM Card Swap*[187], que consiste en llamar por teléfono a la asistencia técnica de un proveedor de telefonía (en este caso el que sirva a Jack Dorsey), hacerse pasar por la víctima, y obtener del proveedor de telefonía un duplicado de la tarjeta SIM del teléfono de la víctima (para lo cual hay que conocer el número de teléfono usado por esa víctima); una vez el atacante en poder del duplicado de la tarjeta SIM, puede acceder a los mensajes SMS de la víctima, incluidos los códigos de segundo factor de verificación de Cloudhopper.

- El 6/9/2019 el mismo atacante comprometía el perfil en Instagram[188] del actor estadounidense Robert Downey Junior, con más de 43 millones de seguidores. Y el 31/12/2019 las cuentas en Twitter del actor estadounidense Adam Sandler[189] (2.4 millones de seguidores) y de la cantante del mismo país Mariah Carey[190] (21.4 millones de seguidores) fueron igualmente vulneradas, para pasar a emitir o retuitear contenidos ofensivos y racistas, de orientación provocadora y "gamberra".

Por su parte, en las sucesivas oleadas de ciberataques de '**LulzSecITA**' adscritas a sus distintos marcos narrativos ideológicos, durante 2019 han destacado varias de sus acciones llevadas a cabo contra sitios web en Italia, entre ellas:

- El 21/2/2019 deformaba con contenido reivindicativo alusivo la web del Ministerio de Medio Ambiente[191] de Italia, situando además en el dominio público[192] un volcado de contenido de la web, incluyendo acceso al webmail en Outlook de alguna cuenta bajo dominio del Ministerio; la web está equipada con un gestor de contenidos Drupal y está alojada en un servidor Apache con su software desactualizado. También se alteraba otra web del ministerio[193], igualmente equipada con Drupal.
- El 24/4/2019 vulneraba el acceso a la web del Sistema Informativo de Archivos del Estado[194] del Ministerio de Bienes Culturales de Italia y situaba un volcado de datos en el dominio público[195].
- El 7/5/2019 comprometía las webs del Colegio de Abogados de Roma[196], y de la empresa de servicios de identificación, certificación y factura electrónica Visura[197] en Italia, situando contenido de mensajes privados de webmail de ambas webs en el dominio público[198], incluyendo datos de identificación personal[199] de profesionales de la abogacía; ambas webs están equipadas con versiones vulnerables del gestor de contenidos Wordpress, y la primera de ellas además del software PHP.

[187] https://attack.mitre.org/techniques/T1451/
[188] @RobertDowneyJr
[189] https://twitter.com/adamsandler
[190] https://twitter.com/MariahCarey
[191] minambiente.it
[192] https://anonfiles.com/80u0Bcu1b1/minambiente_db_zip
[193] reach.gov.it
[194] archivi-sias.it
[195] https://tinyurl.com/y6ye6l7q
[196] ordineavvocatiroma.org
[197] visura.it

- El 19/11/2019 mostraba en Twitter[200] capturas de pantalla que sugerían habían tenido acceso a un subdominio[201] que expone datos personales identificativos y comerciales de contacto de empleados de la empresa farmacéutica Bayer en Italia.

6.2 IDENTIDADES *HACKTIVISTAS* AVANZADAS

Al margen del contexto ya descrito de identidades *hacktivistas* oportunistas de baja peligrosidad que actúan en comportamientos de pequeña cibercriminalidad movidos por motivaciones autoreferenciales de obtener notoriedad principalmente a través de redes sociales, durante 2019 han destacado dos casos que, aún pudiéndose adscribir al movimiento *hacktivista*, no se ajustan al patrón general.

El primero de ellos es la identidad '**Phineas Fisher**', ya conocida porque en 2014 y 2015 llevó a cabo ataques contra las empresas de ciberseguridad *Gamma International* y *Hacking Team*, y en 2016 una acción contra el Sindicato de los Mossos d'Esquadra en España. 'Phineas Fisher' no se ajusta al patrón de *hacktivismo* oportunista de baja peligrosidad predominante internacionalmente a todos los países por dos razones:

1. Es un atacante de alta peligrosidad, técnicamente muy dotado no sólo para explotar vulnerabilidades comunes, sino para analizar distinto tipo de arquitecturas de red y de software, y desarrollar su propio código malicioso para atacarlas en distintas fases de complejidad y con diversas técnicas de ciber-penetración; y
2. Su motivación atacante no es autoreferencial, sino la más propiamente *hacktivista* en origen de actuar ilegalmente contra sistemas tecnológicos movido por presupuestos ideológicos, que en su caso son de naturaleza antisistema, anticapitalista, en una orientación general identificable con alguna corriente anarquista de corte insurgente.

Con estas premisas, el 13/3/2019 'Phineas Fisher' enviaba un mensaje en inglés a través de Twitter[202] afirmando que "*como una pesadilla para #hackingteam y #gammagroup, vuelvo al hackeo en 2019*", sin proporcionar más detalles en aquel y siendo inmediatamente clausurada la cuenta en Twitter que había utilizado.

El 17/11/2019, la plataforma de exfiltraciones Distributed Denial of Service divulgaba[203] un conjunto de información resultado de la supuesta vulneración de servidores web[204] del Cayman National Bank and Trust de la Isla de Man. La acción estaba firmada por 'Phineas Fisher', que

[198] https://mega.nz/#F!5LJU2Qhb!WqUXAu84t6-h_Ebgr52riQ!pXYhSIxb
[199] https://privatebin.net/?733c77b53f0a18bb#mOfP7ehglNAogRlakrBvJqi/LUil8ld4tm6VoECNZqw=
[200] https://twitter.com/LulzSec_ITA/status/1196774442166312962/photo/1
[201] drugtraceabroad.bayer.it
[202] https://twitter.com/Phineas_Fisher/status/1105952749349289984
[203] https://data.ddosecrets.com/file/Sherwood/
[204] caymannational.im

divulgaba un texto reivindicativo[205], escrito en un español[206] correcto aunque rígido, en donde presentándose como el "Subcowmandante Marcos" proporcionaba una amplia introducción de retórica antisistema y anticapitalista, animando a los "militantes *hacktivistas*" a embarcarse por motivos ideológicos en acciones contra los bancos, para aportar posteriormente una descripción del procedimiento supuestamente utilizado para vulnerar el banco en la Isla de Man. En principio y según la información divulgada, la acción no formaba parte de una operación general contra entidades bancarias, sino que se trataba de un ciberataque de impacto individual ejecutado por 'Phineas Fisher' por motivos ideológicos principalmente anticapitalistas, igual que en el pasado atacó a empresas de ciberseguridad.

La otra excepción de identidades con una fisonomía aparentemente *hacktivista* pero que no se ajusta al perfil internacionalmente más común, ya descrito, de las identidades hacktivistas, ha sido en 2019 '**PokemonGo**'. Al igual que 'Phineas Fisher', 'PokemonGo' no se ajusta al perfil común de identidad *hacktivista* debido a que muestra capacidades técnicas ciberofensivas avanzadas que son ajenas a la comunidad *hacktivista* internacional; sin embargo, al contrario que 'Phineas Fisher', las motivaciones que son deducibles a partir de la breve y concentrada actividad de 'PokemonGo' durante 2019 no sugieren una impronta ideológica en su motivación, sino tal vez geopolítica en su sentido más instrumental, incluso con la posibilidad de que la "indumentaria" hacktivista que pretendía vestir 'PokemonGo' fuera fingida, a modo de un táctica de *falsa bandera*.

El 11/4/2019 la hasta el momento desconocida identidad 'PokemonGo Team' anunciaba en un perfil en Twitter[207] casi inmediatamente clausurado la exfiltración de un conjunto de datos correspondientes a los Asociados de la Academia Nacional de la Agencia Federal de Investigación de EEUU, abreviadamente FBINAA. Aunque relacionada nominalmente con el FBI, la FBINAA es una organización privada con forma de empresa mercantil, constituida por 17 mil funcionarios de policía, y cuyo propósito es impartir cursos de liderazgo y gestión entre las comunidades policiales.

La exfiltración la producía 'PokemonGo Team' a través de su propia web[208] (que en mayo de 2019 ya no estaba operativa) en un fichero comprimido .ZIP protegido por una contraseña que proporcionaban, mostrándose que era el producto de haber afectado a tres sitios web de la FBINAA en Carolina del Norte, Washington y Florida. La exfiltración contenía datos personales identificativos de agentes del FBI y de otros cuerpos de policía en EEUU, probablemente participantes en programas de formación de la FBINAA.

El 13/4/2019 de nuevo exfiltraban información[209] sobre varias entidades asociativas relacionadas con funcionarios de gobiernos locales o federales en EEUU[210], con algunas de las webs evidenciando vulnerabilidades de software PHP.

[205] https://data.ddosecrets.com/file/Sherwood/HackBack.txt
[206] El español en que está escrito el comunicado no es deficiente, pero sí algo rígido, dando la impresión de que se trata de una traducción automática posteriormente corregida por un humano.
[207] @PokemonGoICU
[208] pokemongo.icu/files/fbiinfo.zip
[209] pokemongo.icu/files/web_government1.zip
[210] Entre ellas Asociación Nacional de Profesionales de Webs de Gobierno (nagw.org), Sociedad de Reuniones de Funcionarios (ncsgmp.org), Asociación de Funcionarios Fiscales de Oregón (ogfoa.org).

'PokemonGo' se definía en su web como un "grupo de profesionales" dedicados, en genérico, a diversas tareas de ciberseguridad. En otro momento afirman que son un "*grupo hacker que ha trabajado en la sombra desde 2014 sin atraer atención, aunque ha llegado el momento de cambiar el mundo*".

Además de las exfiltraciones comunicadas, el histórico de 'PokemonGo mostraba el desarrollo de una cepa de ransomware a la que han denominado '**CryptoPokemon**', cuyo código fuente situaron también el 11/4/2019 en la plataforma Github[211], donde afirman radicarse en Ucrania. La pieza de ransomware, que había sido desarrollada en VisualStudio para Windows, tenía la peculiaridad de que no atacaba a máquinas que mostraran en su configuración estar alojadas en alguno de los países correspondientes con las antiguas repúblicas soviéticas.

En definitiva, la información disponible sobre esta nueva identidad, por lo que parece rápidamente desactivada, sugiere la hipótesis de que no se trataba de la típica identidad *hacktivista*, sino más bien de una ciberamenaza que empleaba entre sus tácticas, técnicas y procedimientos (TTP) una apariencia y operativa *hacktivistas* con algún propósito específico, probablemente llamar la atención sobre sí misma y confundir en las atribuciones.

Esta intención de confundir en las atribuciones era muy apreciable en su evidente uso de rasgos rusos: el ransomware no atacaba en países de la órbita rusa, tenía presencia en Exploit. in (tradicional web de intercambio y compra-venta de código dañino cuyo idioma principal es el ruso), y consignaban localización en Ucrania; todos son elementos demasiado visibles como para adoptarlos como ciertos, considerando que en la "ciencia de las atribuciones" en ciberseguridad es un hecho que las ciberamenazas emplean elementos atributivos con propósito claro de confundir, precisamente, sobre las atribuciones que sobre ellas se realizan. Que 'PokemonGo Team' mostrara pistas tan evidentes de su vinculación con Rusia podía significar tanto que tenían esa vinculación; como que no la tenían (*falsa bandera*) y pretendían hacer ver que la tenían; o incluso que la tenían pero querían hacer ver que la tenían para que quienes realizan atribuciones los descartaran como rusos, sabiendo ellos de antemano que con pistas tan evidentes iban a ser descartados como rusos por la mayoría de los evaluadores.

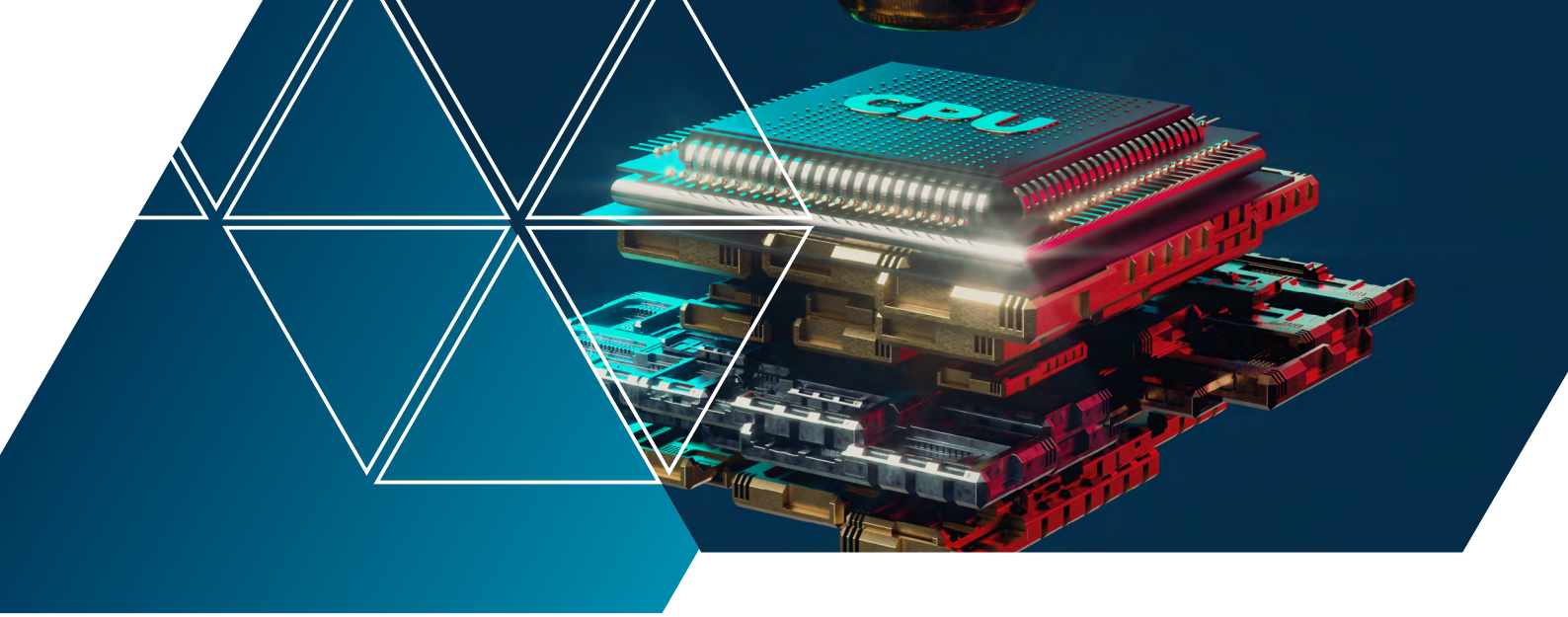
Fueran o no rusos, su modelo de actuación era muy similar al empleado por '**Fancy Bears**', supuestamente representando a la presumiblemente ciberamenaza rusa APT28 y que desde 2016 han venido contando con canales en Twitter y en web. 'Fancy Bears', que está inactiva desde 2018, ha venido realizando en los últimos años exfiltraciones centradas en organismos internacionales de gestión del deporte olímpico en el contexto de la **#OpOlympics**. Considerando la similitud entre ambas identidades, si 'PokemonGo Team' fuera una mutación de 'Fancy Bears' no sería sorprendente; tampoco si se tratara de una ciberamenaza con la intención de hacer creer que es una mutación de 'Fancy Bears'. Lo que parece más probable, a la luz de la información disponible, es que se trataba de una ciberamenaza con intenciones tal vez geopolíticas o incluso puramente de lucro criminal, haciéndose pasar por una identidad *hacktivista* con el fin de confundir las atribuciones que sobre ella fueran propuestas.

[211] https://github.com/PokemonGoTeam/CRYPTOPOKEMON

6.3 MARCOS NARRATIVOS HACKTIVISTAS EN RESTO INTERNACIONAL

Las narrativas hacktivistas convocando a ciberataques durante 2019 en países en el ámbito internacional no mencionados en epígrafes dedicados a otras regiones en este informe han sido:

MARCOS NARRATIVOS HACKTIVISTAS EN RESTO INTERNACIONAL 2019					
PAÍS	OPERACIÓN	PROMOTOR	TIPO DE OBJETIVO	TIPO DE ACCIÓN	RESULTADO
CN	#OpTibet	Ayn Oneemooz	Gobierno de China	DDoS	Sin desarrollo operativo más allá del marco narrativo.
UK	#OpUK #OpAssange	AnonNews YourAnon Net	Instituciones de gobierno en Reino Unido	DDoS Desfiguración	Una decena de DDoS sobre instituciones. Algún iSQL sobre gobiernos locales. Media docena de webs de universidades desfiguradas.
ID	#OpIndonesia	Lorian Synaro NewSec	Instituciones de gobierno en Indonesia	DDoS	Media docena de DDoS sobre instituciones de gobierno.
Varios	#OpCopyWrong	Anonymous Germany Mecz1nko Markov Al1ne3737	Webs de Unión Europea	DDoS iSQL	Media docena de DDoS sobre partidos políticos e instituciones europeas en Alemania, Portugal y Estrasburgo. Algunas iSQL ocasionales sobre webs privadas.
IT	#OpNessunDorma #OpGreenRights #OpNoTAV #OpSardegna #OpPharma #OpPulizia	LulzSecITA	Instituciones públicas y empresas en Italia	Desfiguración iSQL	Alrededor de 65 de webs de gobiernos regionales y locales, de asociaciones gremiales, y de empresas de energía y de trabajo temporal a nivel local en Italia afectadas por inyecciones SQL. Alrededor de media docena desfiguradas.
SD	#OpSudan	Lorian Synaro	Instituciones públicas en Sudán	DDoS	Medio centenar de webs de gobierno atacadas por DDoS Una docena de webs institucionales desfiguradas.
ZW	#OpZimbadwe	Lorian Synaro	Instituciones públicas de Zimbadwe	DDoS	Un par de webs de gobierno atacadas mediante DDoS



7. HACKTIVISMO PROISLAMISTA O PROYIHADISTA

7.1 PANORAMA HACKTIVISTA PROISLAMISTA O PROYIHADISTA

El ciberyihadismo sería la utilización de medios cibernéticos para desarrollar ataques ("atentados cibernéticos" podrían denominarse) sobre la base de una motivación ideológica yihadista. Por tanto, el ciberyihadismo se diferenciaría del yihadismo propiamente dicho únicamente en los medios a utilizar para el ejercicio de la violencia:

- mientras el **yihadismo** emplea la violencia física (asaltos armados, atentados con bomba, despliegue de fuerzas armadas sobre el terreno) para actuar sobre objetivos en un plano físico predominantemente analógico: instalaciones de Gobierno o de empresas, personas, infraestructuras críticas, poblaciones.
- el **ciberyihadismo** recurriría potencialmente a armas cibernéticas (*malware*, *exploits*, *remote access tools*, *remote control systems, ransomware*) para intentar producir un perjuicio o daño en los sistemas cibernéticos de un objetivo a atacar.

De este modo, el ciberyihadismo sería una forma de **ciberterrorismo**, entendido como la aplicación de la violencia por medios cibernéticos (ciberataques) para producir un daño directo contra un objetivo atacado y un efecto indirecto contra una audiencia más amplia (generación del terror en la sociedad, advertencia a las instituciones estatales).

Con este espacio terminológico de partida como criterio de observación, al igual que ocurrió en 2018 durante 2019 no se ha detectado ningún incidente que sea calificable de ciberyihadismo.

Así mismo, la información de incidentes cibernéticos durante 2019 confirma la inexistencia de evidencias que sugieran que el 'Daesh' (Estado Islámico) haya desarrollado una división *ciberarmada* específica destinada a la comisión de atentados terroristas por medios cibernéticos.

7.2 HACKTIVISMO PARÁSITO DE SIMBOLOGÍA PROISLAMISTA

Desde 2015 la denominación '**Cibercalifato**' o alguna de sus variantes ha venido siendo el reclamo utilizado por identidades hacktivistas en ataques por desfiguración sobre sitios webs en varios países, generalmente de baja entidad y exponiendo vulnerabilidades comunes, sobre los que se inyectaba contenido provocativo mencionado al 'Daesh' o incluyendo algún tipo de iconografía con insinuaciones proislamistas o proyihadistas.

Tanto el análisis del histórico de actividad de los atacantes que empleaban esos contenidos, como la propia baja elaboración de esos mismos contenidos, sugiere que su utilización no ha venido teniendo una intencionalidad ideológica sino una motivación de notoriedad acompañada de provocación por parte de las identidades *hacktivistas* actuantes.

Del mismo modo, la información disponible sirve para sostener la hipótesis plausible de que la denominación 'Cibercalifato' no está asociada a ninguna entidad ni vinculada orgánica o infraestructuralmente al 'Daesh' ni a ningún otro grupo yihadista o islamista conocido. Más bien, se sugiere que 'Cibercalifato' es un término de conveniencia instrumentado por un conjunto cambiantes de sobrenombres, que podrían corresponderse realmente con un solo atacante o con un conjunto muy reducido de ellos tal vez localizados en India o Indonesia, que realizan cibertataques por desfiguración contra sitios webs de baja visibilidad y alta vulnerabilidad en cualquier país del mundo insertando menciones concretas al 'Daesh' como modo de provocación.

Por tanto y a la luz de la evidencia disponible, el 'Cibercalifato' como tal no habría de ser una denominación a clasificar en el ámbito del ciberyihadismo sino del *hacktivismo*, una clase de hacktivismo que por emplear conceptos e iconografías proislamistas a modo de provocación de un potencial auditorio podría calificarse como "**hacktivismo parasito de simbología proislamista**".

En este contexto, mientras en 2018 se apreciaba con respecto al año previo una disminución de incidentes de desfiguración de sitios web empleando la marca 'Cibercalifato' o alguna de sus variaciones, durante 2019 esa pauta queda confirmada con la utilización sólo ocasional de algunos alias atacantes que han incluido el término en inglés 'Cybercaliphate', pero en un contexto donde ha predominado la inyección forzada de contenidos en sitios web firmados por identidades con alias individuales.

Al igual que el año previo, la identidad *hacktivista* predominante en la utilización de contenidos de significante proislamista, con baja tonalidad ideológica y con rasgos que denotan una finalidad de provocación y de notoriedad ha sido '**Mujahidin313**', que comenzaba en enero y marzo desfigurando webs en India y Nueva Zelanda inyectando sobre ella contenido proislamista, favorable al denominado "*califato islámico*" pero contrario al 'Daesh' (Figura 7-2-1). Entre abril y junio producía nuevas desfiguraciones en webs privadas menores en en Vietnam, Esloveniam, Italia, Indonesia, Tanzania, Polonia, Birmania y Argentina, inyectando contenido que mezclaba un saludo a los "musulmanes del mundo" con una mención a Palestina. A partir de junio de 2019 'Mujahidin313' no ha mostrado actividad ciberofensiva.

Figura 7-2-1

A partir de los contenidos inyectados por 'Mujahidin313' en desfiguraciones se aprecia que: 1) se introduce grafismo que sería incompatible con una visión estricta del islamismo, lo que sugiere que en efecto las menciones al "Estado Islámico" en sus acciones no son una "profesión ideológica" sino que tienen intención provocadora y se utilizan como alusiones instrumentales; 2) realiza una mención a su origen en Indonesia, que coincide con rasgos de probable relación geográfica observados otra identidad *hacktivista* parásita que utiliza provocativamente contenidos proislamistas: '**Munashir Cyber Section**', que en marzo de 2019 desfiguraba webs privadas de baja entidad y con software vulnerable en Sudáfrica.

Otras tres identidades que han empleado en 2019 contenidos proislamistas con intenciones de provocación en desfiguración de sitios web han sido:

- '**Morrocanwolf**' en junio (que es una identidad conocida por utilizar contenido generalista en sus desfiguraciones, incluso últimamente sólo su alias), que procedía a vulnerar la web de una pequeña empresa en EEUU empleando en esta ocasión contenido con iconografía y texto mencionando al ISIS (Figura 7-2-2), contenido al que recurrió esa misma identidad en ataques puntuales en 2015; '**c0d3Lib**', que así mismo en junio y después en julio alteraba media docena de webs privadas en Dinamarca, sobre las que inyectaba una reivindicación general junto a un saludo en inglés a todos los "hackers musulmanes" y una imagen que se corresponde con el conocido como "sello de Mahoma", que habitualmente es empleado por militantes islamistas;

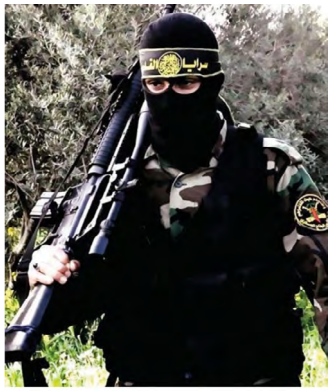


Figura 7-2-2

- '**marwan007**', que en septiembre inyectaba contenido gráfico que mostraba una imagen típica de militantes proyihadistas armados en la web de una pequeña empresa en Arabia Saudí. A ese contenido se le añadía un mensaje en inglés pidiéndole al administrador de la web que no "le diga a nadie" que la "web ha sido hackeada", sugiriendo esta frase que el contenido proyihadista inyectando tiene intención provocadora, y no ideológica.

En cuanto a las desfiguraciones que han empleado de alguna forma variantes del término 'Cibercalifato' constan:

- La desfiguración firmada en enero por '**0x.Terrorist**' y '**0x.Shadow**' de desfiguraban dos webs menores con IPs en EEUU y Sudáfrica inyectándose contenido con una alusión al "Islamic State" y al '**United Cyber Caliphate**' pero con texto en inglés mencionado el Kurdistán.
- La deformación en marzo y junio de cuatro webs menores en India y Canadá con contenido bajo denominación '**Caliphate Cyber Shield**', conteniendo una mención al "Islamic State".
- El comprometimiento en mayo de una web menor en India por parte una nueva identidad bajo la denominación '**Cyber Revenge Army**', que también lanzaba un ataque por denegación de servicio sobre la -muy específica- web del servicio de Policía del Estado de Karnataka en India; la especificidad de esta acción sugiere, a priori y sin más información de contexto, algún tipo de vinculación territorial del atacante.
- Por otro lado, el 30/6/2019 una nueva identidad en Twitter bajo la denominación de '**Blackhawk Cyber Caphilates**' difundía una mensaje[212] comunicando un hipervínculo a un repositorio público en Github[213] donde aseguraba haber situado el resultado de la "mayor brecha de datos sobre India con datos de 13 millones de usuarios y funcionarios de gobierno incluyendo chats, emails y constraseñas". Una exploración de los datos exfiltrados sugería que se trata de datos de usuarios de una tienda de comercio electrónico, tal vez vinculada a una universidad, quizás al Instituto Indio de Comercio Exterior[214].

[212] https://twitter.com/caphilates/status/1145390103277105152
[213] https://github.com/caphilates/IndianPrivataDataLeak/
[214] iift.ac.in

8. TENDENCIAS 2020

- **Permanencia del movimiento *hacktivista* 'Anonymous' en su estado de desmembramiento internacional en términos operativos**, con alguna identidad *hacktivista* ocasionalmente empleando alguna de sus denominaciones a efectos testimoniales, pero sobre todo reduciéndose la realidad de 'Anonymous' a identidades digitales creadas en redes sociales a efectos propagandísticos, privadas de influencia y de capacidad de elaboración narrativa.
- En coherencia con la inhabilitación de 'Anonymous' como atractor de militancia *hacktivista*, **profundización en la conversión del *hacktivismo* de movimiento de ciberinsurgencia a categoría a la que se afilian identidades oportunistas individuales, mayormente no relacionadas entre sí, dedicadas a la pequeña cibercriminalidad**, expresada principalmente en la desfiguración de sitios web con meras motivaciones de notoriedad, sin sustrato ideológico. Con una baja representación en el volumen general de la pequeña cibercriminalidad de las desfiguraciones, un pequeño número de identidades atacantes aprovecharán las acciones de ataque sobre las webs para complementarlas con otras actividades de pequeña cibercriminalidad, principalmente el *SEO Spam* y, en mucha menor medida, el *phishing* y la venta de *exploits*.

- Los ataques de este *hacktivismo* oportunista sobre sitios web continuarán desarrollándose técnicamente mediante la **explotación de vulnerabilidades en webs equipadas con software desactualizado**.
- En el contexto del *hacktivismo* de oportunidad, seguirán apareciendo **casos puntuales de ciberamenazas que se hagan pasar por identidades hacktivistas para llevar a cabo ataques de falsa bandera**, principalmente divulgaciones de información sensible al dominio público, o comprometimiento de perfiles de alta visibilidad en redes sociales. Estas acciones de falsa bandera podrían involucrar potencialmente, en algún momento, la diseminación de malware por parte de ciberamenazas con intereses geopolíticos o cibercriminales; o también ataques avanzados por penetración del tipo del llevado a cabo en 2015 sobre la televisión francesa TV5 presuntamente por parte de atacantes con origen en Rusia que se hicieron pasar por atacantes ciberyihadistas.
- En 2020 **tampoco se observará evidencia sobre la existencia de ciberyihadismo**. Algunas identidades *hacktivistas* insistirán en utilizar contenidos de provocación con iconografía proislamista para inyectarlos en sus desfiguraciones de oportunidad de sitios web de alta vulnerabilidad.

CCN
centro criptológico nacional

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA