INFORME ANUAL 2020

CCN-CERT IA-17/21

HACK_TIVISMO + CIBER_YIHADISMO

Informe de amenazas, movimiento y actividad hacktivista

MAYO **2021**

Edita:

Fecha de Edición: abril de 2021

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

Índice

1. Sobre CCN-CERT

CERT Gubernamental Nacional

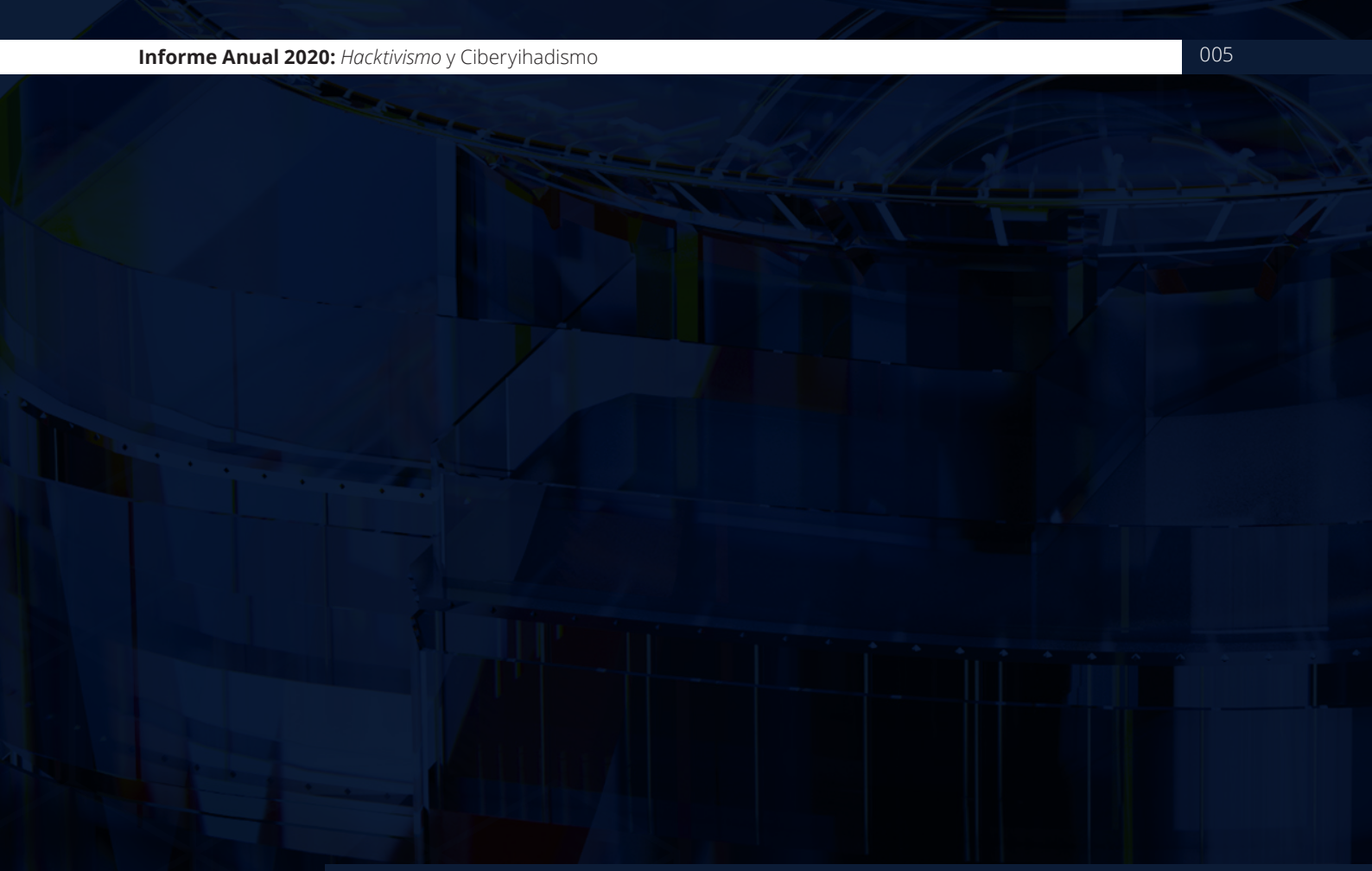
El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI.

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.



La misión del CCN es contribuir a la mejora de la ciberseguridad española.

2. Resumen ejecutivo

Durante 2020 se mantuvo la tendencia, ya reportada en años previos, de un ***hacktivismo* desideologizado y oportunista**, actuando preferentemente motivado por el exhibicionismo egocéntrico de atacantes que vulneran sitios web para inyectar sobre ellos su firma.

Continuando la tendencia de los años previos, los ataques *hacktivistas* en 2020 han descendido numéricamente respecto del año anterior, **y correlacionado en un 97% con la presencia de software vulnerable y/o desactualizado en las webs atacadas**, que puede considerarse el primer factor de riesgo para la victimización por hacktivismo.

Este conjunto de ataques *hacktivistas* oportunistas y motivados por el exhibicionismo se lleva a cabo, principalmente, por **identidades individuales sin conciencia de colectivo**, quedando reducido actualmente el papel del antaño movimiento *hacktivista* 'Anonymous' a canales testimoniales en redes sociales decorados con iconografía *hacktivista* y dedicados a buscar notoriedad y obtener "me gusta" de sus seguidores.

La debilidad de una militancia colectiva y de adhesiones ideológicas en el *hacktivismo* se ha traducido durante 2020, siguiendo el patrón de años previos, en la circunstancia de que cuando algunas identidades han intentado promover marcos de protesta *hacktivista* en países donde se estaban produciendo protestas sociales, la colectivización de esos llamamientos haya sido mínima, y la adhesión de identidades *hacktivistas* que llevaban a cabo ciberataques de protesta se haya limitado, salvo excepciones muy puntuales, a **identidades de baja peligrosidad y capacitación técnica**, que llevan a cabo mayormente ataques por denegación de servicio, inyecciones SQL de baja entidad, o desfiguraciones menores sobre webs vulnerables. Ocasionalmente en este panorama de ataques concurre la presencia de una identidad con mayor capacitación técnica que produce una brecha de seguridad en algún servidor web de mayor visibilidad o importancia, y entonces se lleva a cabo alguna desfiguración de mayor impacto, o la exfiltración de información sensible al dominio público, lo que hace que, momentáneamente, un idealista *hacktivismo* colectivo movido por razones ideológicas parezca un fenómeno con un alcance que, en realidad, no tiene.

Este *hacktivismo* individualista de oportunidad se ha concentrado durante 2020 principalmente en desfigurar webs privadas de personas o de pequeños negocios.

En ocasiones, la referida estructura atomizada de identidades individuales que llevan a cabo ataques *hacktivistas* de oportunidad se agrupan, o fingen agruparse, en pequeñas facciones *hacktivistas*, denominados genéricamente "*teams*", que utilizan un alias colectivo como firma reivindicativa de sus acciones, sin perder el carácter egocéntrico pero intentado imprimirle una suerte de apariencia de "banda cibernética". En el panorama internacional, este fenómeno de bandas utiliza, para definirse y firmar sus desfiguraciones, idioma o simbología principalmente identificativa de Brasil, Turquía, o Indonesia, como países donde estas bandas han declarado principalmente ser originarias durante 2020.

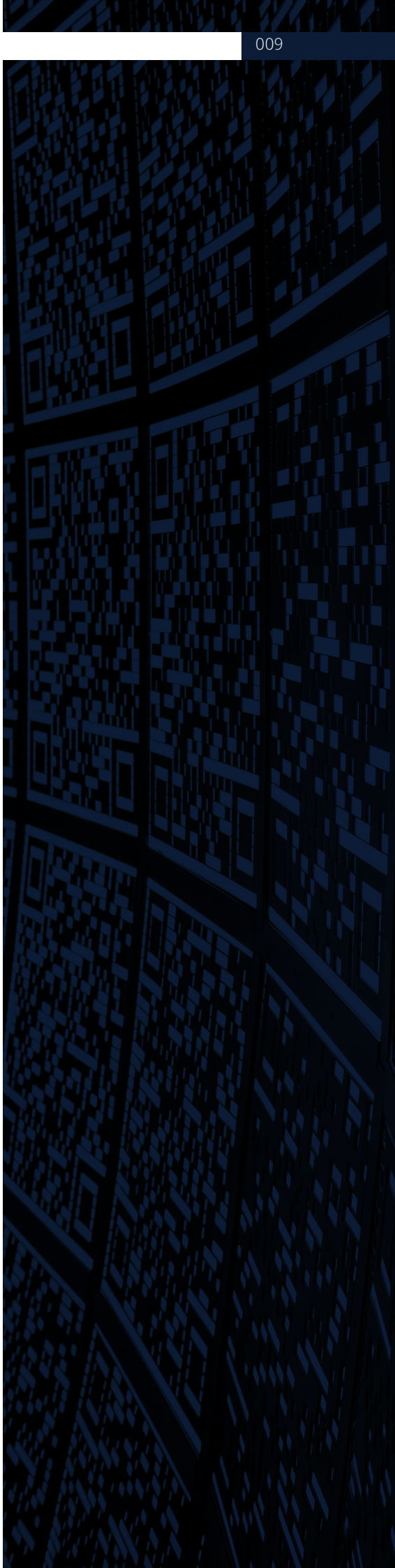
Este *hacktivismo* individualista de oportunidad que lleva a cabo ataques explotando fallos en sitios web en su mayoría provistos de software desactualizado y/o vulnerable, se ha concentrado **durante 2020 principalmente en desfigurar webs privadas de personas o de pequeños negocios**, muchas veces atacando en oleadas a un conjunto de estas webs afectadas por la misma vulnerabilidad en un mismo o en varios países. En segundo lugar, en número de webs afectadas tras la victimización de sitios privados, se cuenta la desfiguración de webs de gobierno locales y regionales, no atacadas por su naturaleza de instituciones públicas, sino por exponer fallos comunes de software visibles en Internet y detectados por los atacantes en escaneos masivos buscando webs con defectos.

El ataque sobre webs vulnerables de gobiernos locales y regionales ha sido especialmente visible en algunos países de Iberoamérica (principalmente Brasil), en Oriente Medio y en Asia. En tercer lugar, en 2020 en cuanto a número de webs afectadas, los ataques de oportunidad por desfiguración de webs han incidido en el comprometimiento de webs, programadas con software desactualizado o vulnerable, de instituciones o ministerios de gobiernos nacionales, principalmente en Oriente Medio, África, y Este de Asia.

En esta realidad a nivel mundial de carencia de conciencia ideológica y de desagregación del movimiento *hacktivista*, de individualización exhibicionista con orientación vandálica en ciberataques de baja peligrosidad de la mayoría de quienes se encuadraban en 2020 dentro del *hacktivismo*, **cohabitan un número anecdótico de identidades específicas con mayor capacitación técnica como ciberamenazas**, que actúan en solitario motivadas por una ideología antisistema, y que suponen ciberamenazas de mayor peligrosidad cuando operan ocasionalmente, comprometiendo servidores o servicios vulnerables de empresas o instituciones gubernamentales conectados a Internet. Este tipo de identidades, cuyos ejemplos prototípicos serían 'LuzlSecITA' en Italia, 'La 9ª Compañía' en España, o la inactiva durante 2020 'Phineas Fisher', pueden llevar a cabo en cualquier momento ataques técnicamente más avanzados y de mayor peligrosidad.

Por otro lado, la descripción de un *hacktivismo* en desintegración como fenómeno, así como la motivación exhibicionista y la ejecutoria de baja peligrosidad de sus atacantes, no deberían no obstante minusvalorar la posibilidad de que una porción, todavía minoritaria, de esa fenomenología, sea capaz de incrementar su potencial de ciberamenaza en el futuro. El indicador de este posible incremento de peligrosidad ya no sería propiamente *hacktivista*, sino que se adscribiría a una **derivación del *hacktivismo* hacia la pequeña cibercriminalidad con ánimo de lucro ilícito**. Esta posibilidad viene avalada por que, al menos en los últimos tres años, se está documentando que incidentes por desfiguración de sitios web se realizan, además de para inyectar una firma *hacktivista* del atacante, infectar esos sitios con código software malicioso, generalmente al servicio de la práctica conocida como ***SEO Spam***. Si en 2019 estas acciones representaban alrededor del 3% de todas las desfiguraciones en el panorama *hacktivista* mundial, **en 2020 no sólo han crecido cuantitativamente hacia un casi 25%, sino también cualitativamente con tácticas, técnicas y procedimientos de mayor peligrosidad**: el **SEO Spam** continúa, pero complementado con la inyección de script redirectores hacia webs de distribución de contenidos no deseados y/o maliciosos; y, al menos en dos casos en 2020, se ha documentado que desfiguraciones con apariencia *hacktivista* conllevaban la inyección en las webs comprometidas de infraestructuras de *phishing*, en forma de falsas tiendas de comercio electrónico cuyo propósito era robar credenciales de pago de clientes que creyeran que estaban realizando alguna compra legítima (cuando en realidad era fraudulenta) en ellas.

Finalmente, y reiterando lo advertido en informes previos, conviene acabar precisando que aunque el oportunismo egocéntrico de baja peligrosidad sea lo que caracteriza actualmente al *hacktivismo* a escala internacional, no hay que dejar de tener presente que, en sí mismo, es una **ciberamenaza irregular y por tanto de difícil predicción**, pues al estar nutrida por motivadores individuales cambiantes, aunque en general débilmente dotada técnica e ideológicamente en ocasiones puede resultar en ciberataques de impacto: ya sea porque alguna identidad con mayor habilidad técnica irrumpa atacando un objetivo de relevancia; ya 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; o porque un atacante dotado de elevadas capacidades técnicas, hasta el momento inactivo, decida que es su momento de salir a escena con una acción significativa; o, en suma, porque ciberamenazas avanzadas dedicadas a la cibercriminalidad, el



ciberespionaje o los ataques dirigidos por intereses geoeconómicos o geopolíticos, decida en alguna coyuntura que le interesa desarrollar acciones de falsa bandera disfrazadas de *hacktivismo*.

Por último, el capítulo de los fenómenos ciberyihadistas, catalogados en este informe como ***hacktivismo* de simbología proislamista**, permanece en 2020 como en 2019, s**in que se haya documentado** mediante evidencia directa o indicadores indirectos **la existencia de estructuras o identidades cibernéticas atacantes afiliadas a organizaciones islamistas o yihadistas**. Lo que se ha producido durante 2020, todavía con mayor ocasionalidad si cabe que la muy baja ocurrencia de este fenómeno en 2019, es la actividad de identidades *hacktivistas* oportunistas que desfiguran webs de alta vulnerabilidad y baja visibilidad inyectando en ellas iconografía o mensajes con apariencia islamista, sin que de esas actuaciones pueda deducirse implicación ideológica sino intención meramente provocadora o incluso de disfraz u ocultamiento. La práctica de llevar a cabo cibera taques ocultando la identidad del agresor tras una falsa bandera islamista no es ajena al ciberespacio en ninguna de las tipologías de ciberamenazas: el caso prototípico lo representa la ciberamenaza persistente avanzada de presumible origen ruso 'Fancy Bear' en su ciberataque sobre sistemas tecnológicos de la televisión francesa TV5 en 2015, donde se inyectó contenido para simular que el ataque lo llevaba a cabo el "CiberCalifato"; y ya en el ecosistema del *hacktivismo* de postureo actual, el falseamiento de identificativos proislamistas se sugiere en la actividad de 'Marwan007' o 'Mrwn007', supuestamente un nacional de Irán que se dedica a la desfiguración de sitios web para llevar a cabo una actividad cibercriminal probablemente movida por ánimo de lucro ilícito.

3. *Hacktivismo* en España

3.1 Estructura *hacktivista* en España

3.1.1 Perfilado genérico de las identidades en 2020

El panorama del *hacktivismo* de raíz autóctona en España durante 2020 no ha mostrado variación sustantiva con respecto a la pauta ya descrita para el año anterior de ausencia de un tejido *hacktivista* propiamente español o actuando desde España, que tenga un mínimo de capacidad operativa más allá de mensajes ocasionales de autocomplacencia en redes sociales, excepción hecha de la identidad conocida como 'La 9ª Compañía'.

Desde esa excepcionalidad, en términos de un posible colectivo *hacktivista* el escenario en España en 2020 se resume, precisamente, en ausencia de ese colectivo, quedando la realidad hacktivista de raíz autóctona en España representada por identidades constituidas en perfiles en redes sociales con iconografía alusiva al movimiento 'Anonymous', que principalmente transmiten desde esos perfiles contenidos de propaganda antisistema general, alusiones a otras identidades, o mayormente referencias autocentradas.

Prosiguiendo con un patrón ya observado para el marco narrativo de la #OpCatalunya el año previo, los intentos de reflotar una #OpSpain como narrativo general de protesta *hacktivista* en España durante 2020 se han topado con los mismos factores de impotencia:

1. **Ausencia de narrativas con intenciones operativas dotadas de 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- son 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. **Uso de las redes sociales digitales para proferir amenazas que no tienen materialización operativa más allá de las palabras divulgadas, y que así mismo tienen débil difusión en tanto palabras.**

Estos elementos consustanciales actualmente a un diluido *hacktivismo* asentado en España, producen un estado de ciberamenaza ocasional y de muy baja peligrosidad, dejando aparte la excepción ya mencionada así como la posibilidad de algún brote individual que pueda surgir en cualquier momento, por iniciativa propia, y que todavía no se haya manifestado: no es ajena al *hacktivismo* la eventualidad de que, de repente, aparezca una ciberamenaza con capacidades operativas más avanzadas que realice uno o varios ciberataques de impacto, presentándose con iconografía de 'Anonymous', y desencadenando por tanto la sensación puntual de que el "*hacktivismo* está vivo" en España.

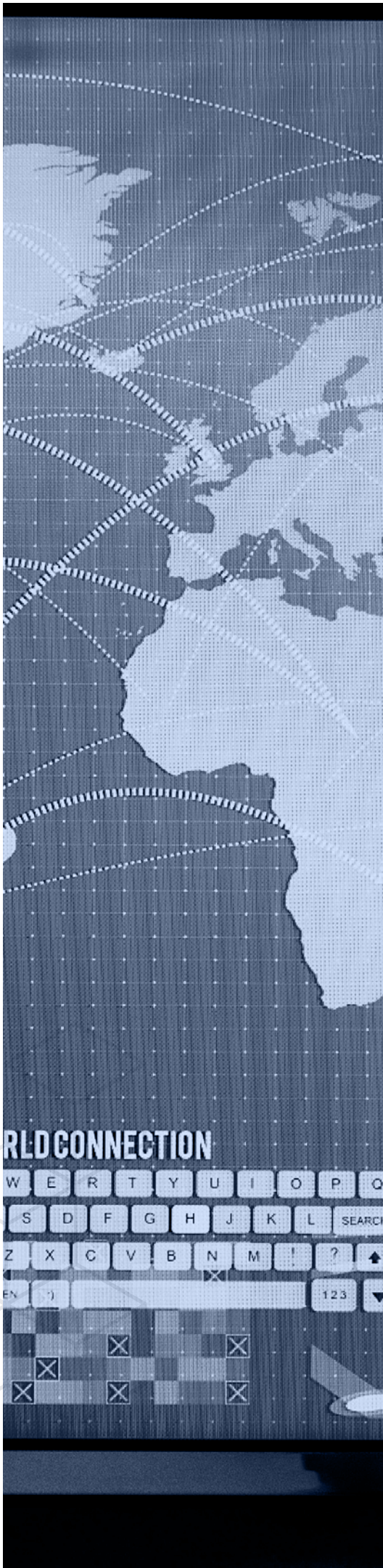
El panorama del *hacktivismo* de raíz autóctona en España durante 2020 no ha mostrado variación sustantiva con respecto a la pauta ya descrita para el año anterior de ausencia de un tejido *hacktivista* propiamente español.

3.2 Campañas y ciberataques *hacktivistas* en España

3.2.1 #OpCatalunya, #OpCatalonia, #OpSpain

Durante los doce meses de 2020, se llevaron a cabo 32 ciberataques bajo los marcos narrativos de la #OpSpain o la #OpCatalunya/#OpCatalonia, la primera una denominación genérica y recurrente de protesta *hacktivista* centrada en España, y la segunda una etiqueta que identidades *hacktivista* comienzan a utilizar en el último trimestre de 2017 en paralelo a la complicación de la situación política en Cataluña. A menudo #OpSpain y #OpCatalunya/#OpCatalonia aparecen mezcladas en contenidos reivindicativos o en amenazas *hacktivistas*.

Durante 2020 a estos dos motivadores previos se les ha unido la etiqueta **#FreeXelj** u #OpFreeXelj, un intento de visibilizar el descontento *hacktivista* por el encausamiento judicial de una persona residente en la provincia de Tarragona, que desde 2018 ha sido arrestada policialmente en un par de ocasiones por su presunta participación en actividades ilícitas ligadas a ciberataques en el contexto de la #OpCatalunya/#OpSpain. En el último tercio de 2020 varios ciberataques fueron llevados a cabo contra webs en España reivindicándolos mediante la etiqueta #FreeXelj, generalmente asociándolos a #OpSpain.



El volumen de acciones afiliadas a estos marcos narrativos durante 2020 ha caído un 30% respecto de 2019, cuando a su vez había descendido un 25% con relación al año anterior, lo que confirma el descenso paulatino de la actividad ciberofensiva *hacktivista* vinculada a estas narrativas concretas en España. Las tipologías de ciberataque desarrolladas en este contexto han sido:

- El **34% de los ataques se correspondieron con acciones por denegación de servicio**, realizados principalmente en el mes de abril de 2020 por **'Nama Tikure'** sobre un par de webs de la Administración Pública española, en ataques puntuales sin colectivización y sin sostenimiento en el tiempo. Ocasionalmente en julio de 2020 otra identidad ejecutó un ataque individual por denegación de servicio sobre la web del Departamento de Seguridad Nacional, y en noviembre de 2011 se produjo otra acción similar sobre la web de la Agencia Tributaria.

- Un **43% consistieron en desfiguraciones de webs menores**, concentradas en noviembre de 2020 y principalmente reivindicadas por **'Crystal_MSF'** y su alias colectivo **'sin1pecrew'**. En realidad, se trató de acciones de oportunidad no directamente motivadas por la #OpCatalunya, sino adscritas a la actividad sistemática de comprometimiento de sitios web provistos de software desactualizado y/o vulnerable por todo el mundo que llevaba a cabo 'Crystal_MSF' en conductas de pequeña cibercriminalidad para la inyección en esas webs de contenido ***SEO Spam***: en media docena de casos, se aprovecharon las webs desfiguradas en España por ese atacante para adscribirlas a la #OpCatalunya a través de mensajes en redes sociales, probablemente más con la intención de darle publicidad a las acciones que como adhesión genuina a la #OpCatalunya. Adicionalmente, el 10/11/2020 **'ch4rlotte'** producía la desfiguración de un subdominio de la web del Ministerio de Cultura de España, inyectando un fichero freexelj.html[1] con contenido alusivo a la "liberación de Xelj" y a #OpSpain.

- Las **inyecciones sobre bases de datos SQL**, que el año previo habían tenido un moderado protagonismo, se limitaron en 2020 a un solo intento de muy baja peligrosidad, concentrado en noviembre de 2020 sobre una web menor de noticias en Torremolinos.

- Un par de **divulgaciones de datos** de alcance limitado y de origen incierto, probablemente derivadas de algún comprometimiento de las credenciales de acceso de un usuario individual. En noviembre de 2020 **'unlawz'** reivindicaba haber logrado vulnerar un punto de acceso individual al subdominio de hospederías alojado en la web de la Guardia Civil, adjuntando capturas de pantalla que sugerirían que el acceso ilegítimo se habría producido, probablemente empleando claves de autenticación con acceso limitado obtenidas ilícitamente de algún operador de hospederías registrado en la web. Y, en el mismo mes, la identidad **'uw'**, adscrita al alias colectivo brasileño 'HighTech Brazil', junto al mensaje en portugués <<libertad para mis hermanos presos>> difundía en Twitter una captura de pantalla de lo que parecía ser una bandeja de entrada de correo electrónico donde se observaban mensajes entre noviembre de 2019 y febrero de 2020, relacionados con la Guardia Civil y el Instituto Nacional de la Administración Pública, que podrían corresponderse con la bandeja de entrada, vulnerada, de algún asistente a un curso de capacitación.

1. sede.mcu.gob.es/rpi4/webpages/publico/FreeXelj.html

Tal como ya ocurrió el año previo, a la #OpCatalunya identidades *hacktivistas* adscribieron acciones falsificadas, que en realidad no se produjeron según lo reivindicado. La más notoria fue la divulgación el dominio público en mayo de 2020 por 'Nama Tikure', una identidad que ya venía participando en ediciones de años anteriores de la #OpCatalunya, de una supuesta base de datos conteniendo un centenar de registros de lo que parecían ser credenciales de autenticación con denominaciones de dirección de correo electrónico y contraseña bajo dominio web **policia.es**. En realidad, tal como pudo acreditarse a partir del análisis del contenido exfiltrado, los datos difundidos sobre cuentas de correo de **policia.es** se correspondían mayoritariamente con una exfiltración de 2016 conocida como "anti public combo list", donde se situaron en el dominio público 458 millones de registros de credenciales de autenticación de cuentas de un conjunto de dominios web por todo el mundo ; con otra del dominio exploit.in también de 2016, donde se divulgaron 593 millones de registro; con una lista de 2019 conocida como "Collection#1", que es una combinación de diversas exfiltraciones con 2.700 millones de registros; y con la resultante de PLD Customer de 2019; y secundariamente con otros conjuntos de exfiltraciones, desde la correspondiente a Linkedin de 2016 pasando por la de Adobe en 2013.

La hipótesis es que 'Nama Tikure', o una identidad que le suministrara datos, hubiera obtenido o compuesto artesanalmente el listado referido a **policia.es** adquiriéndolo en un paquete, o configurándolo a partir de varios paquetes de datos, hasta "montar" un listado de centenar de registros compuesto a través de una búsqueda selectiva en un servicio de venta que tenga un repositorio común de grandes exfiltraciones de datos.

A partir de junio de 2020, los contenidos *hacktivistas* que circularon etiquetados como #OpSpain u #OpCatalunya estuvieron mediados por las etiquetas **#Xelj**, **#OpFreeXelj** o **#FreeXelj**, referidas a la situación judicial de un nacional español residente en la provincia de Tarragona, que fue arrestado en 2018 por su presunta participación en ciberataques en la #OpCatalunya, y que esperaba su fase de juicio oral para finales de 2020 o durante 2021, acusado de diversos delitos informáticos. En la plataforma de recogida de firmas **Change.org** hay una petición[2] dirigida al Gobierno de España en la que, en idioma inglés, se solicita la <<liberación de Xelj>> aduciendo que <<no es un cibercriminal>>, que una condena sería <<inaceptable para alguien que ha estado luchando por la libertad>> y que su propósito siempre ha sido <<hacer de este mundo un lugar mejor para todos oponiéndose a cualquier clase de tiranía, opresión y corrupción>>.

Animados por el apoyo a 'Xelj', a partir del verano de 2020 se sucedieron sobre todo contenidos de amenazas más o menos veladas circuladas a través de redes sociales, en algún caso a través de identidades creadas ad-hoc, como el vídeo de 2:03 minutos de duración difundido por la hasta entonces desconocida '**AnonyEsp**' en Youtube[3] donde una persona ataviada con indumentaria característica de 'Anonymous' y voz mecánica de audio deficiente leía una proclama con las etiquetas **#OpSpain** y **#FreeXelj** sobreimpresionadas.

2. https://www.change.org/p/spanish-government-release-anonymous-freedom-fighter-freexelj
3. https://twitter.com/4n0ny_Esp/status/1279475282890686464

En conjunto, durante 2020 la #OpSpain y la #OpCatalunya continuaban sin actividad anual, limitándose a momentos muy puntuales, sin colectivizarse y, tras reactivarse mínimamente en noviembre de 2020, discurriendo en ritmo decreciente, tanto en operativa como en menciones, hasta decaer en el último tercio del mismo mes.

La ausencia de colectivización y el bajo flujo de mensajes en redes sociales respecto de #OpSpain/#OpCatalunya se ha dejado notar especialmente en los ataques por denegación de servicio, tipología preferente en este tipo de marcos narrativos *hacktivistas*, que en la oleada de la #OpSpain de 2020 han sido ocasionales, no se han sostenido en el tiempo, y han congregado a un bajo número de identidades.

En cuanto a la adhesión a #OpSpain de identidades que pudieran aportarle mayor peligrosidad operativa ha sido, por ahora, testimonial, contribuyendo ocasionalmente algunos atacantes con desfiguraciones o accesos ilegítimos para adscribirlos a la #OpSpain/#OpCatalunya, pero sin dejar traslucir un interés concreto o una afiliación continuada al marco narrativo.

Durante 2020 la #OpSpain y la #OpCatalunya continuaban sin actividad anual, limitándose a momentos muy puntuales, sin colectivizarse y discurriendo en ritmo decreciente.

4. https://mastodon.social/@la9deanon/103690491720396366

3.2.2 La 9ª Compañía de Anonymous

Si en 2019 'La 9ª Compañía de Anonymous' había reducido sus ciberataques en un tercio con respecto al año previo, en 2020 repetía esa misma acumulación porcentual de descenso de actividad, reivindicando la ejecución de una única acción ciberofensiva en España.

En febrero de 2020 había advertido en un mensaje[4] de velada amenaza en Mastodon que durante 2020 "sólo realizarán tres acciones", y que se dirigirán contra ***<<instituciones que han protagonizado noticias de calado durante 2019-2020>>***, sin especificar víctimas más allá de sugerir que una de ellas está localizada en Latinoamérica, e insinuando que ya habrían penetrado en dos de ellas. Cuatro meses después, publicaba[5] otro mensaje intimidatorio (Figura 3-2-2-1) asegurando de que a partir del 21/6/2020, fecha en la finalizaba el primero de los estados de alarma decretados en España para afrontar la pandemia de la Covid-19, "finalizaría la tregua que La Nueve ha mantenido durante la pandemia", y a partir de entonces "dedicarán su atención" a "bancos, empresas del Ibex, y asociaciones fascistas".

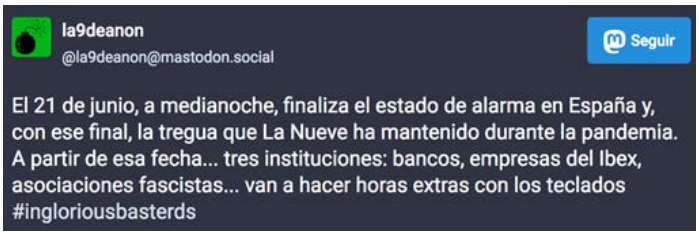


Figura 3-2-2-1

4. https://mastodon.social/@la9deanon/103690491720396366
5. https://mastodon.social/@la9deanon/104290224623328811

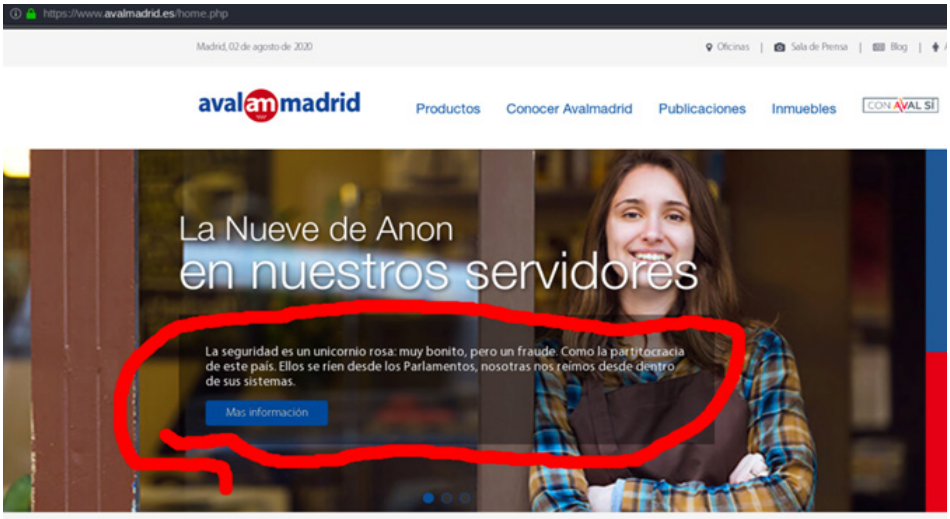


Figura 3-2-2-2

A pesar de estos contenidos de amenaza, el único ciberataque reivindicado por 'La 9ª Compañía' durante 2020 se produjo el 2 de agosto, cuando vulneraba el acceso al sitio web del servicio de préstamos financieros AvalMadrid[6] de la Comunidad de Madrid. Así mismo, desfiguraban la web con el mensaje ***<<la seguridad es un unicornio rosa: muy bonito, pero un fraude. Como la partitocracia de este país. Ellos se ríen desde los Parlamentos, nosotras nos reímos desde dentro de sus sistemas>>*** (Figura 3-2-2-2).

En la descripción que 'La 9ª Compañía' proporcionaba[7] de la acción, sugerían haber explotado alguna vulnerabilidad en el software PHP de la web y operado a través de una *shell* –tal vez completado con alguna inyección SQL, accediendo a un fichero no adecuadamente protegido en la web que ***<<codificaba y descodificaba las passwords>>***. Con las palabras de paso descodificadas, habrían penetrado la web y accedido a la información almacenada en su intranet. A partir de ahí, aunque no divulgaron en volumen información sensible, sí situaban en el dominio público capturas de pantalla de documentos y realizado afirmaciones que sugerían que han tenido acceso a variada información. También afirmaban haber accedido a documentos subidos a un servidor FTP por abogados y notarías en el contexto de la concesión de préstamos, advirtiendo ***<<toda la documentación está repleta de datos personales y capturas de LexNet que deberían tener mayores medidas de seguridad>>***, aunque sin mostrar públicamente capturas de pantalla sobre esta última afirmación.

Por tanto, en el contexto descrito de caída de su actividad durante 2020, cabe concluir que tanto el modus operandi como la motivación ideológica de 'La 9ª Compañía' no han registrado variaciones apreciables respecto de lo descrito en informes anteriores, más allá de una cierta disminución de sus comunicaciones en redes sociales pareja al decremento numérico de sus acciones ciberofensivas.

---

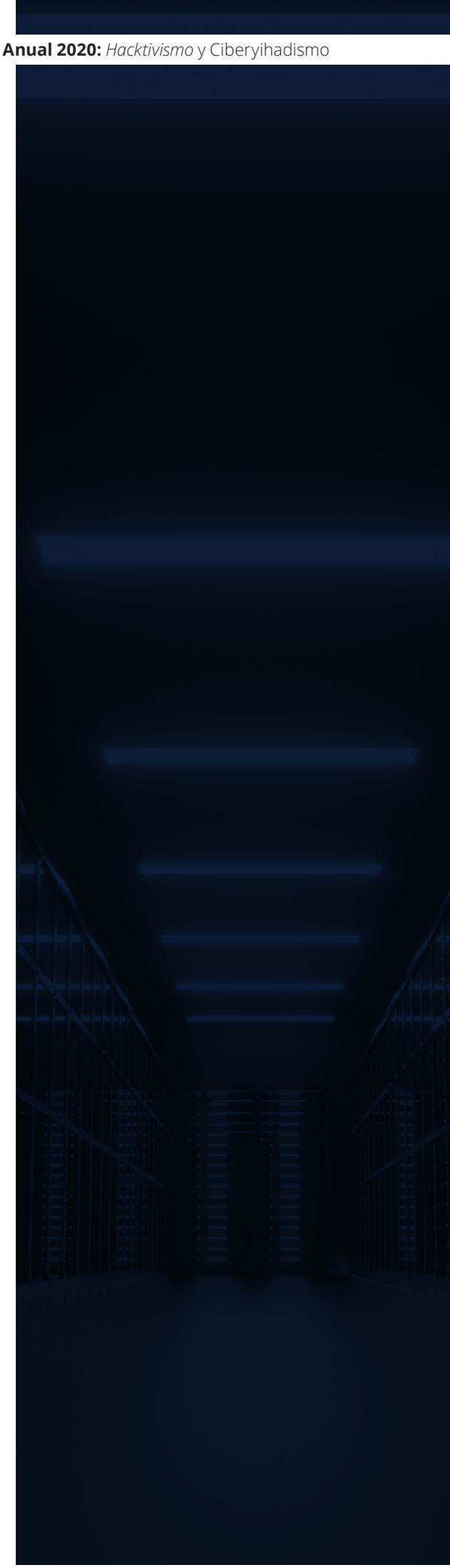
6. avalmadrid.es
7. https://la9deanon.tumblr.com/post/625357883903754240/half-track-en-avalmadrid

3.2.3 Ciberataques por entidades externas a España

En 2020 se mantuvo la pauta de los años anteriores, en la que sitios web con IP en España o dominios web de nivel geográfico para España han sido vulnerados, principalmente en ataques por desfiguración, en el curso de acciones de ciberataque por identidades que al mismo tiempo que afectaban a webs en España lo hacían en otros países.

Estos ataques se corresponden con **acciones de oportunidad** en donde los atacantes se aprovechan de vulnerabilidades en software generalmente desactualizado e instalado en las webs victimizadas, para explotarlas e inyectar sobre ellas contenido reinvidicativo general o simplemente su alias. En un porcentaje de estas acciones de oportunidad, que desde mediados de 2020 comenzaba siendo incipiente pero que ha ido creciendo paulatinamente hacia final de 2020 igual en España que en el resto de países del mundo, además de inyectar su alias en las webs comprometidas, algunos atacantes aprovechan la desfiguración de la web para insertar contenido *SEO Spam,* scripts redirectores hacia webs de distribución de contenidos no deseados o -todavía minoritariamente- estructuras dedicadas al *phishing*. Este último conjunto de conductas sugiere una intersección o solapamiento entre prácticas *hacktivistas* y pequeña cibercriminalidad con afán de lucro, o directamente la utilización de un disfraz *hacktivista* para cometer actos cibercriminales. En este estado de cosas, la situación en España no es diferente a la de la mayoría de los países con sitios web atacados en los cinco continentes.

La situación en España no es diferente a la de la mayoría de los países con sitios web atacados en los cinco continentes.



Durante 2020, atacantes mostrando rasgos que sugieren su actuación desde fuera de España desfiguraban 731 sitios radicados en el país, un 40% menos en volumetría que el año previo, que ya arrastraba un descenso del 50% con relación al año anterior. Estas cifras marcan una línea de tendencia a la baja del *hacktivismo* oportunista en España, que en general se corresponde con el panorama observado mundialmente.

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 también sucedió en los años precedentes, en 2020 se produjo un pico en noviembre en donde un mismo atacante comprometió más de ciento cincuenta webs en una misma oleada, afectando a sitios en España y en otros países, probablemente empleando procedimientos automatizados de detección y explotación de vulnerabilidades comunes en software instalado en las webs. Tal como es apreciable en la figura 3-2-3-1, el comportamiento de las curvas anuales muestra varios picos de oleadas de ciberataques, con dos evidentes en 2018 (azul claro) en enero y mayo; otros tres en enero, agosto y diciembre en 2019 (línea azul); y el ya mencionado de diciembre de 2020 (línea azul oscuro). De hecho, por tanto, si se obviaran los picos extremos, los promedios volumétricos mensuales parecerían bastante similares interanualmente.

Comparativa volumétrica de *hacktivismo* en España 2018-2020

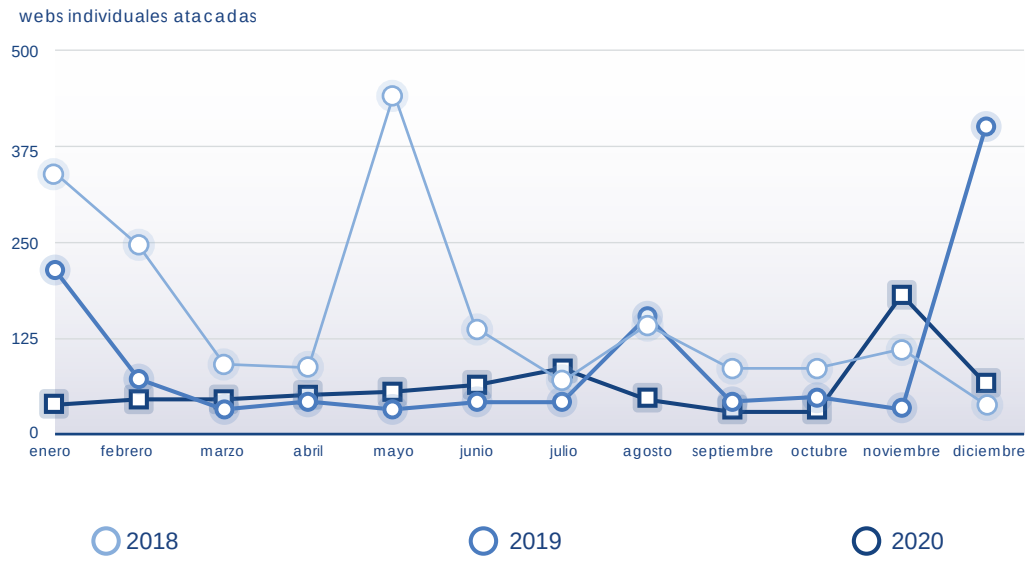


Figura 3-2-3-1

La línea promedio (línea negra punteada, figura 3-2-3-2) de los ataques por desfiguración recibidos sobre sitios web con dirección IP o dominio en España se mantuvo, durante 2020, rondando las 50 acciones mensuales. En ese sentido, es similar a la tendencia de 2019, ambas por debajo de 2018, siendo un indicador coherente con el descenso en la volumetría de las acciones, es decir, en el número de webs individuales vulneradas cada año.

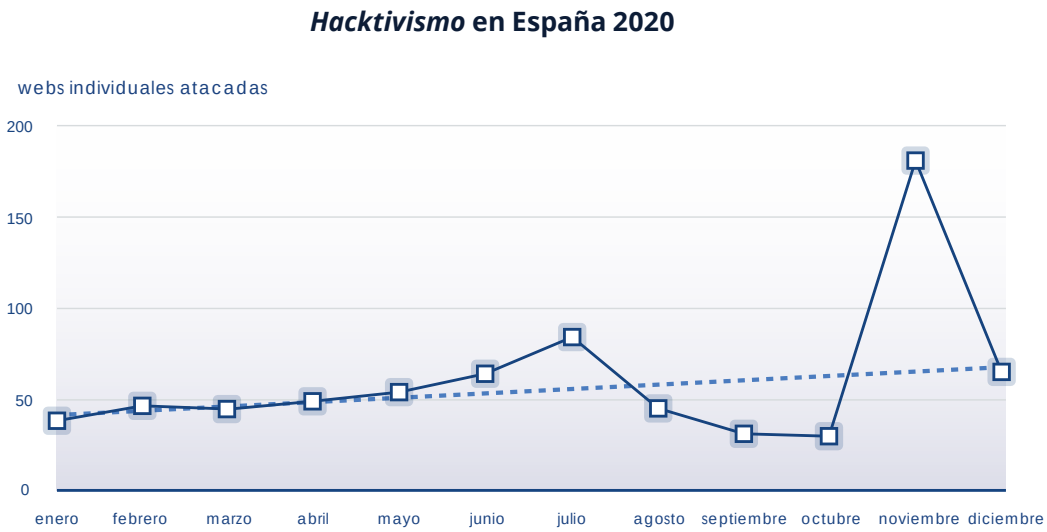


Figura 3-2-3-2

Continuando la tendencia de los años previos, los ataques *hacktivistas* en 2020 correlacionaron en un **97%** (comparado con un 93% del 2019) **con la presencia de software vulnerable y/o desactualizado en las webs atacadas**, que puede **considerarse el primer factor de riesgo para la victimización por *hacktivismo***.

Presencia de software vulnerable y/o desactualizado de las webs

Ataques hacktivistas en 2020

97%

De ese porcentaje total, un **81% de las webs victimizadas la vulnerabilidad en el software estaba relacionada con gestores comerciales de contenidos**, siendo Wordpress el más representado con un 63%, seguido de Joomla con un 18% (Figura 3-2-3-3). El descenso porcentual de la presencia de Wordpress en 2020, que el año previo acumulaba un 75% de los casos, se debe a un aumento de 7 puntos porcentuales en las webs equipadas con el habitual paquete de gestión de Microsoft (IIS para el servidor, Windows como sistema operativo, ASP. net como código operativo, y en ocasiones DotNetNuke como gestor de contenidos), presente en el 10% de los sitios web desfigurados por entidades *hacktivistas* en 2020.

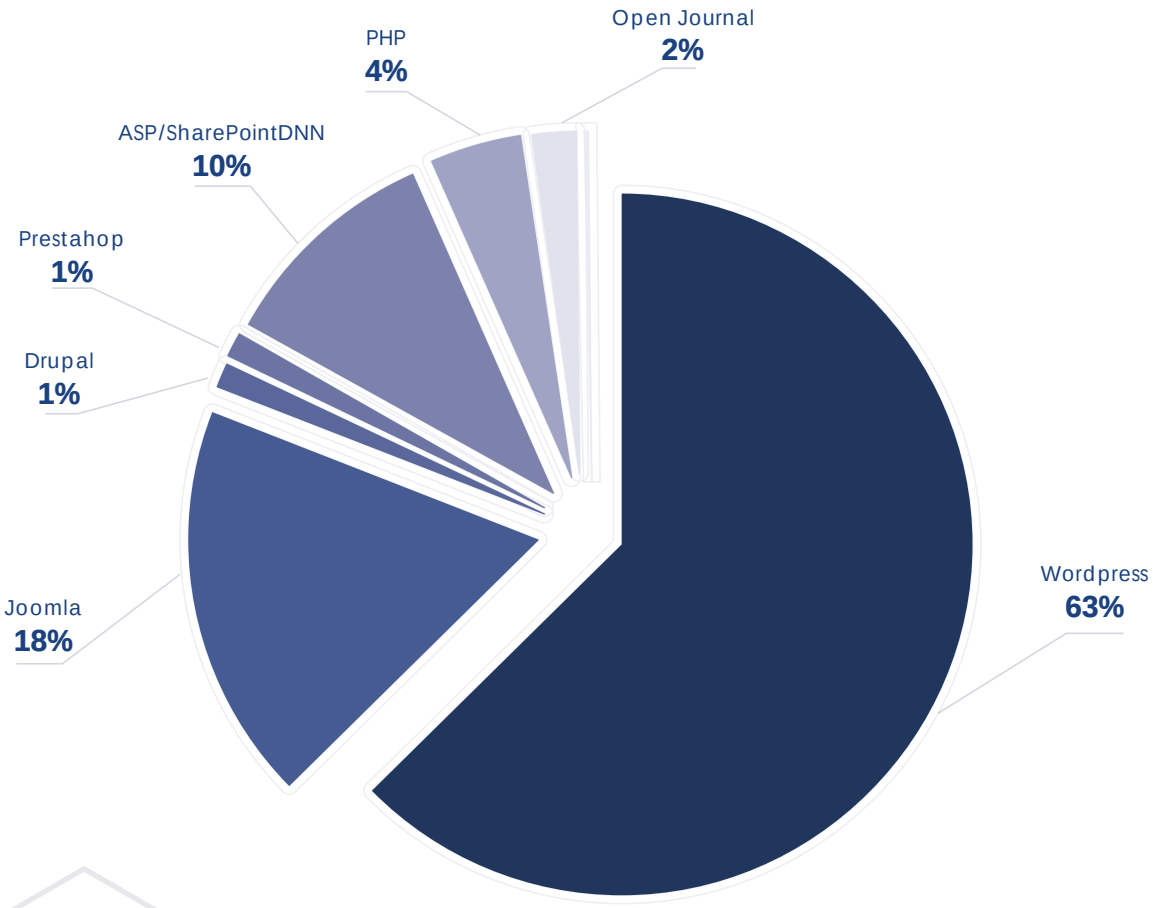


Figura 3-2-3-3

Continuando por tanto la pauta de años precedentes, igualmente en 2020 se producía una muy elevada correlación entre la alteración de sitios webs por atacantes y software desactualizado o vulnerable instalado en ellas, en ataques que cursan en oleadas llevadas a cabo por identidades que, en la mayoría de los casos, inyectan en las desfiguraciones la firma de su alias, sin más contenido reivindicativo. Esta práctica, que puede tener para los atacantes una motivación de reto, de mostrar de lo que son capaces con su pericia técnica al encontrarse con una vulnerabilidad de software, define no obstante una práctica *hacktivista* oportunista e instrumental, tal como ya se ha mencionado, desprovista en su mayor parte de las motivaciones ideológicas que caracterizaban al *hacktivismo* hace diez años. En 2020, recogiendo una tendencia reportada desde 2018, el *hacktivismo* ha sido un fenómeno principalmente desideologizado, caracterizado por identidades motivadas principalmente por la búsqueda de notoriedad y el exhibicionismo digital, y poco a poco derivando hacia la pequeña cibercriminalidad encauzada por el lucro.

En paralelo al *hacktivismo exhibicionista* como primera tipología de ciberataques contra webs en España, como se ha mencionado, crecía el volumen de acciones en donde el *hacktivismo* es un sinónimo de pequeña cibercriminalidad con ánimo de lucro. Si el año previo el porcentaje de este, todavía, segundo motivador de las acciones *hacktivistas* se situaba en el 3'2%, durante 2020 aumentaba al 24'8%, sugiriendo la significación de esta intersección cibercriminal.

Tal como se reportaba, desde 2018 se viene documentando que identidades *hacktivistas*, u otras que fingen el rol del *hacktivismo* intencionadamente para disfrazar la naturaleza lucrativa ilícita de sus acciones, desarrollan tres tipos de tácticas de pequeña cibercriminal que son concurrentes a la desfiguración de un sitio web:

01. La táctica fraudulenta que se conoce como *SEO Spam*, de *search engine optimization*, u optimización de motores de búsqueda, que consiste en incrementar ilícitamente el peso en buscadores web de contenidos comerciales alojados en webs asiáticas, principalmente japonesas -secundariamente chinas y turcas-, mediante la inyección forzada en la web atacada de contenidos comerciales a promocionar; la inclusión de estos contenidos en numerosas webs victimizadas altera el ranking de posicionamiento de esos contenidos en buscadores. En la figura 3-2-3-4 se muestra un ejemplo de contenido *SEO Spam* en idioma japonés inyectado en una web desfigurada con un atacante supuestamente *hacktivista*.

Figura 3-2-3-4

02. La inyección forzada en el código software de las webs atacadas de scripts, generalmente en lenguaje JavaScript, de funciones de redirección de visitantes hacia webs de distribución de contenidos maliciosos, de forma que alguien que conecta a una web previamente atacada es conducido automáticamente a redes de distribución de *adware*, código dañino que puede llegar incluso a la descarga de virus en el dispositivo de la víctima. En ocasiones, la inserción de scripts redirectores está mediada o complementada con la inyección de *webshells* en los sitios comprometidos. Las *webshell* es un tipo de estructura software que permite al atacante tener presencia persistente en la web. La práctica cibercriminal con las *webshells* es que el atacante acumule un número significativo de webs comprometidas, y posteriormente venda al mejor postor el conjunto de accesos a las *webshells*, y por tanto a las webs comprometidas, de forma que el comprador pueda utilizarlas como infraestructura para otras actividades cibercriminales, por ejemplo, la distribución en red de contenido malicioso o no deseado. En la figura 3-2-3-5 se aporta un ejemplo de web de distribución de contenidos maliciosos codificada en un script de redirección inyectado en una desfiguración de apariencia *hacktivista*.

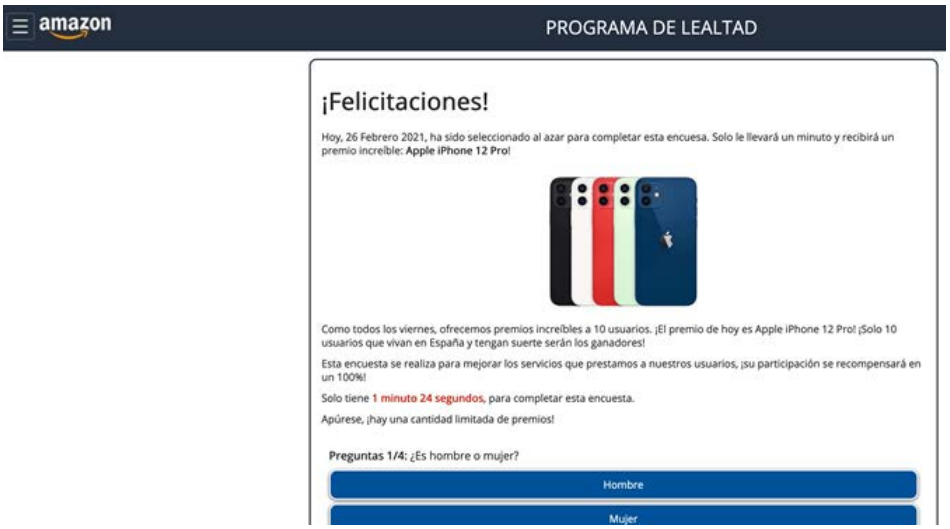


Figura 3-2-3-5

03. A partir de noviembre de 2020 con la detección de dos casos en webs alojadas en Nigeria y Burkina-Faso, identidades pretendidamente *hacktivistas* han venido inyectado en algunos de sus ataques sobre las webs victimizadas o bien una estructura completa de *phishing* o bien scripts redirectores hacia webs de *phishing*. Un primer caso de este procedimiento ya sería observado en España en 2021. Mediante el *phishing* practicado en estos casos de *hacktivismo* fraudulento, la web vulnerada, u otra hacia la que redirige, presenta al visitante una estructura que simula ser una página de autenticación de una tienda de comercio electrónico, generalmente de productos textiles o de complementos de moda, ofreciéndole el mecanismo habitual para que compre un producto -más bien, que crea que lo compra-, lo añada al carrito de compra, y lo pague con tarjeta bancaria o con otro medio digital de pago, momento en el cual los atacantes roban los datos de la tarjeta de crédito para cometer con ellos sucesivas acciones fraudulentas. En la figura 3-2-3-6 se muestra un ejemplo de web de *phishing* inyectada en un ataque *hacktivista* sobre una web comprometida, abusando de la identidad corporativa de una conocida marca de ropa deportiva.

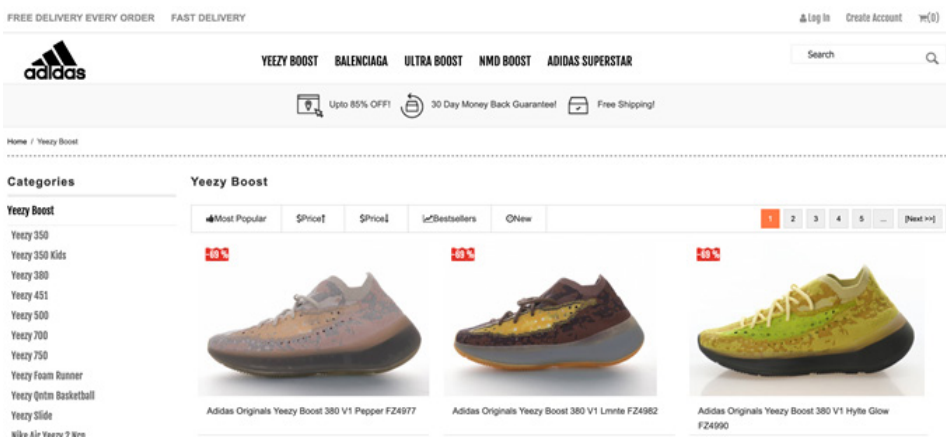


Figura 3-2-3-6

Algunas de las identidades que durante 2020 con mayor frecuencia han vulnerado webs en España en el marco de oleadas de desfiguraciones en varios países probablemente explotando vulnerabilidades en software desactualizado, y que han utilizado código malicioso adicional para actividades de SEO Spam o de inyección de scripts redirectores, han sido **'Mr.Donut's'**, con rasgos turcos y actuando principalmente sobre webs equipadas con software Wordpress; **'kaizer soze'**, también con presuntos rasgos turcos, operando sobre webs provistas de Joomla; **'Mr.L3RB1',** también conocido como 'Sorong6etar', mostrando supuestos rasgos indonesios, atacando preferentemente webs con Wordpress; **'Clash Hackers'**, que generalmente inyecta contenido contra Israel sobre las webs que vulnera; **'Dr.SiLnT HilL'**, quien se identifica como "hacker egipcio", y se decanta por webs provistas de Wordpress; o **'Dev19Feb'**, que también se presenta con iconografía alusiva a Indonesia y suele atacar también webs dotadas de Wordpress.

3.2.4 Ataques *hacktivistas* sobre instituciones públicas

Con la salvedad de lo descrito en el contexto de los marcos narrativos denominados como #OpSpain u #OpCatalunya/#OpCatalonia y sus posibles derivaciones (#FreeXelj), durante 2020 no se produjo ningún foco específico de ciberataque *hacktivista* sobre webs de instituciones públicas en España, ni de sitios web residentes en España elegidas para ser atacadas por el hecho de tener una dirección IP o un dominio web españoles.

Continuando con el patrón ya descrito, los sitios web de instituciones públicas victimizados por desfiguraciones durante 2020 lo fueron en el contexto de ataques de identidades a varias webs de diversos países elegidas por exponer vulnerabilidades comunes en software desactualizado. Los rasgos con que se mostraron las identidades atacantes involucradas en estas acciones, así como el análisis de su histórico de actividad, sugieren que se trataba de atacantes situados fuera de España.

Los ataques *hacktivistas* que lograron trastornar forzadamente de alguna manera la apariencia de sitios webs de instituciones públicas en España durante 2020, considerándose instituciones públicas de forma genérica a aquéllas que tienen dependencia orgánica del gobierno nacional, de las comunidades autónomas, o de ayuntamientos y corporaciones locales, fueron:

El 19/2/2020 '**ifactoryx**' firmaba la desfiguración de las webs de ocho ayuntamientos[8] y dos de mancomunidades[9] del noroeste de la provincia de Madrid, inyectando en todas ellas un fichero rx.html con su alias; las webs estaban desarrolladas con un gestor de contenidos DotNetNuke de Microsoft sobre una versión desactualizada (4.0.30319) del software ASP.net.

También el 19/2/2020 '**chinafans**' inyectaba su habitual fichero o.htm sobre un subdominio[10] equipado con Wordpress alojado en la Universidad de Extremadura, que además quedaba redirigido a una web de venta en línea de medicamentos con dominio en Rusia[11].

El 4/3/2020 '**SeahTheGod**' inyectaba su alias en un fichero ksh.txt sobre una URL[12] de la web del gobierno de Navarra en España, que utilizaba una versión desactualizada del gestor de contenidos Drupal.

El 8/4/2020 '**Adit Arlos**', que también utiliza el alias colectivo de 'Newbie Tersakiti', inyectaba un fichero -.php[13] sobre la web del instituto de enseñanza secundaria pública Garcilaso de la Vega en Cantabria, que estaba desarrollada con una versión desactualizada de Joomla.

8. Entre ellos pezueladelastorres.es, puebladelasierra.es
9. mancomunidad2016.org, mancomunidaddelnoroeste.org
10. ardopa.unex.es
11. helpvan.su
12. gobiernoabierto.navarra.es/es/sites/default/files/ksh.txt
13. iesgarcilasodelavega.es/-.php

El 13/4/2020 '**s1ege**' desfiguraba con una mención a 'Ghost Squad Hackers' y a la libertad de Julian Assange un subdominio[14] y un dominio[15] de la web de la Oficina Europea de Propiedad Intelectual, radicada en España y que estaba desarrollada con una versión desactualizada del gestor de contenidos Drupal.

El 23/4/2020 '**404PRESSI**' inyectaba un fichero .gif con la denominación de su alias y una mención a 'Team ZeroGroupHackers' en la web[16] de la Mancomunidad del Sureste de Gran Canaria, que utilizaba un software vulnerable para su servidor Apache.

El 28/5/2020 **'TheWayEnd'** vulneraba mediante un fichero vuln.gif con su alias el subdominio del Centro Oceanográfico de Murcia[17], que utilizaba versiones vulnerables del software PHP y del servidor Apache, y está alojado en la web del Instituto Español de Oceanografía del Ministerio de Ciencia e Innovación.

El 1/6/2020 '**KingSkrupellos**' inyectaba contenido proturco en un fichero .GIF[18] sobre un subdominio dedicado a publicaciones periódicas y programado con el gestor de contenidos Open Journal Systems en la web del Consejo Superior de Deportes, así como en el Consejo Superior de Investigaciones Científicas[19] o en varias universidades[20].

El 2/6/2020 '**Moroccan Revolution**' inyectaba un fichero ma.txt con su alias en un subdominio[21] programado en ASP.net de la web de la Comunidad de Madrid.

El 24/6/2020 '**Crystal_MSF'** alteraba con su alias una página[22] alojada en un subdominio de servicios externos de la web del gobierno foral de Navarra, que estaba programada con una versión desactualizada (2.0.50727) de ASP.net.

14. ecap.euipo.europa.eu
15. ecap3.org
16. surestegc.org
17. mu.ieo.es
18. revistasdigitales.csd.gob.es/public/site/images/adminj/kingskrupellos.gif
19. redc.revistas.csic.es/public/site/images/adminojs/kingskrupellos.gif
20. Entre ellas polipapers.upv.es/public/site/images/adminj/kingskrupellos.gif, revistas.upsa.es/public/site/images/adminj/kingskrupellos.gif, despapiro.unizar.es/ojs/public/site/images/adminj/kingskrupellos.gif
21. gestiona3.madrid.org/quadrivium/ma.txt
22. frontalnasertic.navarra.es/JumpGanasa/Temporal/EEnrS1M5bINWg0hjM83MZWO9iWEFTq/index.html

El 22/7/2020 '**Zrabba Rabba**' utilizaba contenido reivindicativo general sobre una web educativa[23] equipada con software con Java y adscrita a la Junta de Extremadura.

El 4/8/2020 '**Makato**' desfiguraba con su alias el subdominio[24] programado con Wordpress del plan internacional del gobierno de Navarra.

El 5/8/2020 '**MiSh**' comprometía sitios web de siete centros educativos[25] públicos alojados en la Junta de Extremadura y desarrollados con Joomla.

El 14/9/2020 el mismo atacante inyectaba un fichero jr.php sobre un subdominio[26] provisto con Wordpress de la Universidad de Málaga.

El 13/8/2020 de nuevo '**Moroccan Revolution**' inyectaba un fichero ma.txt con su alias en la web[27] gubernamental del Centro de Estudios Políticos y Constitucionales, que estaba desarrollada con software ASP.net desactualizado.

El 22/10/2020 '**Xyp3r2667**' deformaba con un fichero nd.txt y su alias la web de un centro de educación pública adscrito a la Junta de Extremadura y equipado con el gestor de contenidos Joomla, que ya fue vulnerado por otro atacante en agosto de 2019. En el mismo sentido, el 22/10/2020 'SeRaVo' inyectaba su alias sobre dos webs[28] programadas con Joomla de centros de enseñanza secundaria pública adscritos a la Junta de Extremadura; ambas webs ya fueron desfiguradas por el mismo atacante en octubre de 2019.

23. constructor.educarex.es/pub/cont/
24. blogpin.navarra.es/wp-content/
25. cpmdoncamilohdez.educarex.es/images/jr.gif, cpmdoncamilohdez.juntaextremadura.net/images/jr.gif, cpfcoortizlopez.juntaextremadura.net/images/jr.gif, iesodetietar.juntaextremadura.net/images/jr.gif, iesgregoriom.juntaextremadura.net/images/jr.gif, iesdrfdezsantana.juntaextremadura.net/images/jr.gif, ieseugeniofrutos.juntaextremadura.net/images/jr.gif
26. incadi.uma.es
27. cepc.gob.es/controls/ma.txt
28. iesgregoriom.educarex.es/images/nd.txt

El 30/11/2020 '**Zorrokin**' inyectaba el alias 'TurkHackTeam' sobre un subdominio[30] de la web programada con el software Liferay de la Universidad Pompeu Fabra.

En el marco de acciones en varios países contra revistas online codificadas con el software Open Journal Systems, el 2/12/2020 '**Moroccan Revolution**' comprometía una[31] alojada en la web de la Universidad de Málaga, la revista de salud pública de la Comunidad de Madrid[32], y otra[33] en la Universidad del País Vasco.

El 15/12/2020 '**aDriv4**' inyectado su alias y un anuncio para la venta de webshells en un fichero vz.txt sobre un subdominio[34] programado con PHP desactualizado y Wordpress alojado en la web gubernamental de la Agencia Española de Protección de la Salud en el Deporte, adscrita al Ministerio de Cultura y Deporte de España.

El 16/12/2020 '**Kegagalan404**' deformaba con su alias la página[35] codificada con Wordpress del departamento de informática de la web de la Universidad de Valladolid.

---

30. recursosdocents.upf.edu
31. revistas.uma.es/public/site/images/zbi/zeb.gif
32. remasp.es/public/site/images/zbii/zeb.gif
33. ojs.ehu.eus/public/site/images/zbii/zeb.gif
34. greenseal.aepsad.gob.es/vz.txt
35. infor.uva.es/gagal.html

4. *Hacktivismo* en Iberoamérica

4.1 Panorámica *hacktivista* en Iberoamérica

El *hacktivismo* en Iberoamérica mantenía en 2020 el perfil descrito en 2018 y 2019, definido principalmente por la desfiguración de sitios web de gobiernos locales y regionales provistos de software desactualizado y/o vulnerable en varios países del subcontinente.

Este patrón coincide con lo ya reportado para España y se inscribe en la tendencia general a escala mundial de un ***hacktivismo* exhibicionista de naturaleza oportunista**, lenta pero progresivamente **intersectado con un *hacktivismo* simulado de pequeña cibercriminalidad** motivado por la búsqueda de lucro ilícito, operando con los procedimientos ya descritos.

Esta pauta centrada principal, aunque no exclusivamente, en deformar por la fuerza la apariencia de webs potencialmente vulnerables de gobiernos locales y regionales en Iberoamérica, mediante la inyección en ellas de código reivindicativo en su software, se ha observado prácticamente en todos los países de la zona, pero ha sido especialmente recurrente en Brasil, con protagonismo, aunque menor incidencia, en México, Ecuador, Colombia, Perú, y Argentina.

01. Débil presencia de un tejido autóctono de *hacktivismo* organizado en la mayoría de los países, con la excepción de Brasil, donde permanece una estructura atomizada de identidades individuales agrupadas en alias locales muy centrada en desfigurar sitios web de gobiernos locales y regionales en los países de la región, actuando también en otros países, y en un porcentaje moderado instrumentando el rol *hacktivista* para llevar a cabo acciones de pequeña cibercriminalidad, mayormente la inyección de contenido *SEO Spam*.

02. Capacidad para el desarrollo de marcos *hacktivistas* de protesta antigubernamental en varios países, principalmente en Chile, Colombia, Nicaragua y Perú, promovidos por identidades actuando en su mayor parte desde el exterior de los países de la zona (como 'Lorian Synaro', o 'LiteMods') y ocasionalmente desde alguno de los países ('Anonymous T. Colombia' o 'Anonymous Chile Legion'). Habitualmente, hay un núcleo de identidades que promueven o se suman a marcos narrativos de protesta *hacktivista* en Iberoamérica que es el mismo que promueve o participa en otras protestas *hacktivistas* en diversas zonas del mundo, provistos de baja capacidad de colectivizar y sumar adhesiones a estos marcos narrativos.

03. La traducción operacional de los marcos *hacktivistas* de protestas se realiza en su mayor parte a través de ataques por denegación de servicio, que en minoritariamente se combinan en algunas ocasiones con desfiguraciones llevadas a cabo por identidades oportunistas que buscan notoriedad y lucro cibercriminal involucrándose en las campañas de ciberataque (como 'sin1pecrew'). Así mismo, se producen intentos de robo de información sensible de servidores web gubernamentales con la intención de divulgar posteriormente esos datos en el dominio público para poner en evidencia a las instituciones públicas.

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 8/3/2020 '**CKW**' divulgaba en el dominio público un fichero ecuador.zip[36] conteniendo a su vez ficheros en formato .TXT con el resultado de inyecciones SQL sobre 23 webs bajo dominio **gob.ec** en Ecuador, en su mayoría conteniendo credenciales de autenticación sobre las webs afectadas de usuarios con denominación de correo electrónico y contraseña en formato *hash*. Entre las webs vulneradas se encuentran Aviación Civil[34], la Educación de la Policía[38], el Ministerio de Trabajo[39] o el Banco Central[40].

El 1/4/2020 '**darkshadow-tn**' comprometía con un fichero ds.html de contenido general la web[41] del Centro de Respuesta ante Incidentes Cibernéticos del gobierno de Paraguay, que estaba programada con un gestor de contenidos de código abierto para PHP Concrete5.

El 10/4/2020 '**F1r3bl00d**', afiliado al alias colectivo 'Pryzraky', deformaba con contenido general y la frase "un instituto que no sirve para nada más que gastar nuestro dinero" la web[42] del Instituto Nacional de Tecnologías de la Información del gobierno de Brasil, que utilizaba una versión desactualizada del software para el servidor Apache. El 15/4/2020 de nuevo en Brasil el mismo atacante comprometía con contenido reivindicativo general la web[43] gubernamental del Departamento Nacional de Infraestructuras de Transporte, que estaba desarrollada con software Plone.

36. https://anonfile.com/l9n04fgco5/ecu
37. aviacioncivil.gob.ec
38. educacionpolicia.gob.ec
39. trabajo.gob.ec
40. bce.fin.ec
41. cert.gov.py/ds.html
42. iti.gov.br
43. iti.gov.br

El 26/5/2020 '**by dadas**' inyectaba su alias y contenido en turco sobre un subdominio[44] de la web gubernamental del Consejo de Energía Nuclear de Brasil, que estaba programada con una versión vulnerable del software Joomla.

El 1/6/2020 '**Anonymous Brasil**' situaba en Pastebin volcados de datos personales identificativos del presidente de Brasil Jail Bolsonaro[45] y de dos de sus hijos, el diputado Carlos Bolsonaro[46] y el senador Flavio Bolsonaro[47], además de datos de la Ministra de Familia del gobierno Damares Alves[48]. El propio presidente del país divulgaba un mensaje en su perfil de Twitter[49] condenado la filtración y advirtiendo de que se habían iniciado medidas legales para "tales crímenes no queden impunes". Al día siguiente un nuevo perfil en Twitter empleando iconografía de 'Anonymous' y la denominación de '**Anonymous Brazil**' divulgaba datos personales identificativos del presidente de Brasil Jail Bolsonaro, como por ejemplo un documento supuestamente acreditando gasto en gasolina[50], una declaración pública de bienes[51], o una factura de telefonía móvil[52]. Y el 5/6/2020 '**News from Around the World**' divulgaba en Twitter[53] datos identificativos completos de una tarjeta bancaria supuestamente bajo titularidad del presidente de Brasil Jair Bolsonaro.

El 6/7/2020 '**org0n'** comprometía con un fichero org0n.png[54] de contenido reivindicativo general el portal web del Gobierno de Argentina, que estaba desarrollado con una versión desactualizada del gestor de contenidos Drupal. También inyectaba el mismo contenido en la Agencia Nacional de Infraestructura[55] de Colombia, igualmente equipada con Drupal. Y el 8/7/2020 sobre el Ministerio de Ciencia[56] de Chile, dotado de Drupal.

El 30/7/2020 '**Sandalpy**' firmaba con su alias en un fichero uwu.php la desfiguración de la web[57] de las Aduanas de Honduras, que está desarrollada con Wordpress.

---

44. crcn-co.cnen.gov.br
45. https://pastebin.com/bkuVxBtE
46. http://pastebin.com/gZnsn3mc
47. https://pastebin.com/N9iwxeGi
48. https://pastebin.com/L9nu9E1t
49. https://twitter.com/jairbolsonaro/status/1267865586018762752
50. https://twitter.com/brzanonymous/status/1267821076437819394
51. https://twitter.com/brzanonymous/status/1267813388291207177/photo/1
52. https://twitter.com/brzanonymous/status/1267960452849569792
53. https://twitter.com/nfatw1/status/1268929384045576193
54. argentina.gob.ar/sites/default/files/webform/org0n.png
55. ani.gov.co/sites/default/files/webform/org0n.png
56. minciencia.gob.cl/sites/default/files/webform/org0n.png
57. aduanas.gob.hn/uwu.php

El 1/8/2020 se desfiguraba con un fichero xdxd.php[58] por parte de '**s4ndal.py**' el Ministerio de Turismo de Cuba, cuya web está desarrollada con Wordpress.

El 28/10/2020 '**HighTech Brazil**' deformaba la apariencia de un subdominio[59] de la Ventanilla Única de Comercio Exterior del gobierno de Colombia, que estaba desarrollada con software ASP.net desactualizado.

El 7/11/2020 '**By_Agent**' inyectaba contenido proturco en un fichero by_agent.asp sobre un subdominio[60] programado con ASP.net desactualizado del Ministerio de Energía de Perú.

El 7/12/2020 '**9bandz**' utilizaba el alias 'HighTech Brazil' para comprometer la web de la Policía Nacional[61] de Honduras. Al día siguiente, el mismo atacante penetraba la web del Consejo Nacional de Competencias[62] en Ecuador, que estaba programada con software Wordpress desactualizado y quedaba infectada con contenido *SEO Spam* en idioma japonés. Adicionalmente, desfiguraba del mismo modo la web[63] de la provincia de La Rioja en Argentina, así como varios de sus subdominios[64]; y la web de un gobierno regional en México, ambas provistas de Wordpress; así como un subdominio[66] programada con software Moodle de la web de la Superintendencia de Registros Públicos del Perú. El 14/12/2020 alteraba varias decenas de subdominios de la Universidad de Guayaquil[67] en Ecuador, que estaba equipada con Wordpress.

El 12/12/2020 '**s4dness**', que también emplea el alias 'Umam1337', comprometía con un fichero yolo.html de contenido general las webs de la Dirección de Ayuda Social[68] del Congreso de la Nación Argentina, que estaba desarrollada con una versión vulnerable de Wordpress; del propio Congreso[69], y de su Cámara de Diputados[70], esta última programada con una versión muy desactualizada del software OpenCMS, además de una web de gobierno municipal[71] dotada de software PHP desactualizado.

58. mintur.gob.cu/xdxd.php
59. servicios.vuce.gov.co/glpi/
60. namasenergia.minem.gob.pe/by_agent.asp
61. policianacional.gob.hn, seguridad.policianacional.gob.hn, seguridad.gob.hn
62. competencias.gob.ec/index.html
63. larioja.gob.ar
64. Por ejemplo trabajo.larioja.gov.ar, msalud.larioja.gov.ar
65. sifeet.ofstlaxcala.gob.mx
66. campusvirtual.sunarp.gob.pe
67. ug.edu.ec
68. das.gob.ar
69. congreso.gob.ar
70. hcdn.gob.ar
71. berisso.gov.ar

4.3 Marcos narrativos *hacktivistas* en Iberoamérica

El conjunto de propuestas narrativas de llamamiento a ciberataques *hacktivistas* en Iberoamérica durante 2020 se desarrolló mediante las siguientes iniciativas:

Marcos narrativos *hacktivistas* en Iberoamérica 2020

País	Operación	Promotor	Tipo de Objetivo	Tipo de Acción	Resultado
CL	#OpChile #Op18Octubre	Anonymous Chile Legión AnonDown Reizor S0u1 T-Leaks AnonLeak	Instituciones públicas de Chile	Desfiguración iSQL DDoS Exfiltraciones	Exfiltraciones de información del Ministerio de Exteriores, de la empresa Equifax en el país, y de datos personales identificativos de funcionarios. DDoS sobre webs de instituciones públicas. Desfiguración de una decena de webs institucionales. iSQL sobre universidades y algunos partidos políticos.
CO	#OpColombia #OpColombia Resiste	Anonymous Colombia AnonFury	Instituciones públicas de Colombia	DDoS Desfiguración	Afectadas por denegación de servicio media docena de webs de instituciones de gobierno. Alguna desfiguración y acciones iSQL ocasionales. Interceptación de una reunión en Zoom.

Marcos narrativos *hacktivistas* en Iberoamérica 2020

País	Operación	Promotor	Tipo de Objetivo	Tipo de Acción	Resultado
NI	#OpNicaragua	Lorian Synaro Virus-A Nama Tikure S0u1 ElixirOP Pryzraky HackDown	Instituciones públicas de Nicaragua	DDoS Exfiltraciones	Menos de media docena de webs afectadas Exfiltración de datos del Instituto Nacional Forestal, de credenciales del Ministerio de Energía, o de contenidos del Ministerio de Salud.
PE	#OpPerú	AnonOps ElixirOP LiteMods sin1pecrew	Instituciones públicas de Perú	DDoS Desfiguración iSQL	Divulgación de credenciales de un partido político, y de un gobierno regional. Desfiguración de menos de media docena de webs. Una docena de ataques DDoS sobre webs institucionales

5. *Hacktivismo* en Norte de África y Oriente Próximo

5.1 Panorámica *hacktivista* en Norte de África y Oriente Próximo

De manera similar a otras regiones en el mundo, en los países ubicados en el Norte de África y en Oriente Próximo en 2020 predominaba el ***hacktivismo* de oportunidad** explotando fallos en software vulnerable y/o desactualizado, oscilando motivacionalmente entre el exhibicionismo auto-referente y pequeña cibercriminalidad.

En comparación con Iberoamérica y España, durante 2020 en los países de Norte de África y Oriente Próximo se observaba una mayor incidencia de desfiguraciones sobre webs ministeriales o institucionales de los gobiernos nacionales, en la gran mayoría de los casos también actuando los atacantes en acciones de oportunidad sobre webs provistas de software desactualizado.

Repitiendo el patrón del año previo, únicamente dos campañas *hacktivistas* temáticas tuvieron desarrollo en la región durante 2020, la #OpLebanon y la #OpIsrael, esta última un marco narrativo recurrente de periodicidad anual que, no obstante, continuó en 2020 manteniendo su tendencia de declive de ciberataques tanto en el plano cualitativo como en el cuantitativo.

La **#OpTurkey** no tuvo actividad en 2020 más allá de un ataque ocasional sobre la web gubernamental del Sistema de Información y Monitorización Agrícola de Turquía, que estaba programada con Wordpress.

Por otro lado, los ataques adscritos a la **#OpLebanon** comenzaron en enero de 2020 con la alteración por parte de '**Syrian Revolution Soldiers**' de dos webs[72] de empresas en el Líbano inyectándoles contenido en árabe con la etiqueta #OpLebanon y reprochando a las Fuerzas Armadas del país colaborar con las milicias de Hezbollah en la <<*represión de refugiados*>>. El 26/1/2020 el mismo atacante utilizaba idéntico contenido en las webs del Consejo Económico y Social[73], y del municipio de Byblos[74]. Dos días después en el mismo país, aunque sin relación con el ataque precedente, '**lost3r'** inyectaba su alias y menciones a 'CyberTeam Portugal' en la web gubernamental[75] de la autoridad de gestión del agua del sur del Líbano, que utilizaba un software PHP desactualizado. Posteriormente en mayo de 2020, y coincidiendo con disturbios sociales acaeciendo en el país, '**Nama Tikure**' etiquetaba como **#OpLebanon** ataques por denegación de servicio sobre las webs de las Fuerzas de Seguridad Interior[76] y del Ejército[77]. Del mismo modo en julio y agosto de 2020 se produjo una leve replicación de la #OpLebanon con la desfiguración de un par de webs, una de ellas un subdominio[78] de la web programada con Drupal del Ejército del Líbano, sobre la que '**d4krstat1c**' inyectaba el logotipo de 'Ghost Squad Hackers' e infectaba con contenido *SEO Spam* en idioma japonés. Ya en septiembre de 2020 '**Ghost Egyptian**' desfiguraba con contenido reivindicativo en árabe sobre la situación social en Líbano la web[79] gubernamental de la Compañía de Electricidad de Líbano, que estaba programada con PHP desactualizado; y '**Mrb3hz4d**' alteraba con su habitual contenido de la bandera de Irán las webs de un hospital público[80], dos municipios[81], la Administración Central de Estadísticas[82], el Ministerio de Energía y Aguas[83], y las Aduanas[84] del país, todas ellas desarrolladas con versiones desactualizadas de ASP.net.

---

72. abba.com.lb, unitech.com.lb
73. ces.gov.lb
74. jbail-byblos.gov.lb
75. slwe.gov.lb
76. isf.gov.lb
77. lebarmy.gob.lb
78. lafshield2.lebarmy.gov.lb
79. edl.gov.lb
80. bguh.gov.lb
81. tannourinemunicipality.gov.lb, zahle.gov.lb
82. cas.gov.lb
83. moew.gob.lb
84. customs.gov.lb

En cuanto a la **#OpIsrael**, como viene siendo tradicional cada mes de abril anualmente, el 7/4/2020 circulaban amenazas puntuales con lanzar una oleada de ciberataques bajo este marco narrativo *hacktivista*. Las amenazas las iniciaba[85] la ya conocida identidad de propaganda y muy baja peligrosidad '**Lorian Synaro**' y recibían una colectivización marginal. Sin embargo, el 15/5/2020 los palestinos conmemoraban el denominado "día de la Nakba", que es una jornada de luto anual referenciada a la creación del Estado de Israel. Así mismo, los israelíes celebran anualmente el 21 de mayo el "día de Jerusalem". Alrededor de ambas fechas, en 2019 se produjeron amenazas y alguna acción ciberofensiva *hacktivista* bajo la etiqueta de **#OpJerusalem**. Asi, '**The Jerusalem Electronic Army**' (JEA) profería el 13/5/2020 una amenaza en Twitter[86] advirtiendo en árabe de que "llegarían sorpresas para el enemigo israelí" el 5/14/2020 en el "día de Jerusalén" (Figura 5-1-1).

Figura 5-1-1.

85. https://twitter.com/LorianSynaro/status/1247298446773628928
86. https://twitter.com/JEArmy0/status/1260507533460082688

La misma identidad utilizaba la etiqueta en árabe #TheJerusalemDay para reivindicar el 14/5/2020 la penetración de la web de la Escuela Israelí de Estudios Veterinarios[87], empleando así mismo los logos de '**Anonymous Islamic**' y de los desconocidos '**Gaza Tigers Team**', quienes estaban en ese momento inactivos en redes sociales y simplemente podrían ser otros alías[88] de JEA. Igual etiqueta en árabe #TheJerusalemDay empleaba JEA en Telegram[89] también el 14/5/2020 en una amenaza genérica, sin especificar. La composición gráfica empleada en la reivindicación (Figura 5-1-2) no evidenciaba con claridad que el ciberataque llegara a producirse, sino que más bien parecía un montaje gráfico.

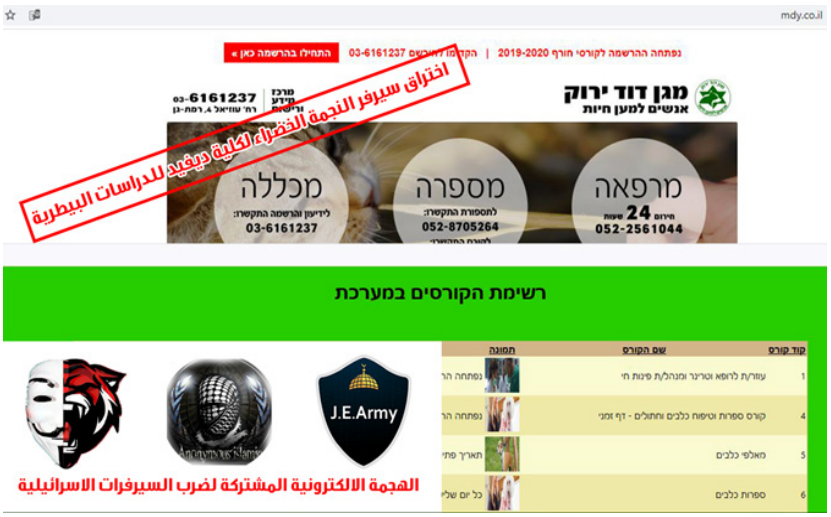


Figura 5-1-2.

El 4 y 6/5/2020 el JEA había reivindicado[90], sin atribuir las acciones al contexto narrativo de la #OpJerusalem, haber penetrado la web de una empresa de telecomunicaciones en Israel, que no identificaban por su nombre; así como varias escuelas universitarias[91] o el Ministerio de Salud de Israel[92], aunque igualmente sin aportar evidencia confirmatoria suficiente. También afirmaban haber tenido acceso a la aplicación en web Sunny Webbox de la empresa energética estadounidense[93] SMA en Tel Aviv.

87. mdy.co.il
88. https://twitter.com/avi81809
89. https://t.me/JEArmy1/3120
90. https://twitter.com/JEArmy0/status/1247157801295593472
91. Por ejemplo https://twitter.com/JEArmy0/status/1247118763339714560, https://twitter.com/JEArmy0/status/1246743387308527616
92. https://twitter.com/JEArmy0/status/1246806580617773058
93. https://twitter.com/JEArmy0/status/1247152094953402368/photo/1

Por su parte, el 21/5/2020 '**Hackers of Savior**' situaba en Youtube[94] un vídeo de muy breve duración a modo de cuenta atrás en donde advertía en inglés y hebreo a Israel que se preparase para una "gran sorpresa", puesto que "la cuenta atrás para la destrucción de Israel ha comenzado hace tiempo". Al día siguiente, desfiguraban más de 1.200 webs privadas[95] desarrolladas con el gestor de contenidos Wordpress en Israel, inyectándoles en un fichero index.php el mismo contenido (Figura 5-1-3) que aparece en Youtube.

Figura 5-1-3.

Por otro lado, el 27/5/2020 '**@lik0**' desfiguraba una docena de webs privadas[96] desarrolladas con Wordpress en Israel inyectándoles una imagen de Hasan Nasrallah, líder del grupo proiraní Hezbollah. El 18/8/2020 '**Cyb3rW0lff**' utilizaba el alias colectivo 'AnonGhost' en un fichero ghost.html para desfigurar un subdominio[97] programado en un entorno Microsoft y alojado en el Ministerio de Educación de Israel. El mismo día '**Madjid DZ**' lanzaba ataques por denegación de servicio sobre varias webs[98] de gobierno en el país. Y el 22/8/2020 '**fedi**' inyectaba contenido alusivo al conflicto palestino en la web[99] de los Archivos del Estado de Israel, que utilizaba software Wordpress. Previamente, el 18/8/2020 '**Foaad Pal**', firmando con el alias colectivo 'Gaza Hacker Team', desfiguraba veintitrés webs privadas[100] programadas con ASP.net en el mismo país, inyectándoles en un fichero index.asp contenido mencionando la muerte de un joven en Jerusalén.

---

94. https://www.youtube.com/watch?v=-8eduJrCWEA
95. Entre ellas bentoya.co.il, behaviour-analyst.co.il, levli.co.il
96. Entre ellas open.co.il, asden.co.il
97. tomtst.education.gov.il
98. Entre ellas telaviv.police.gov.il, israeltrade.gov.il, immigration.gov.il
99. archives.gov.il
100. Entre ellas vaadarkia.co.il, indra.co.il

5.2 Ciberataques *hacktivistas* destacados en Norte de África y Oriente Próximo

Entre las acciones más destacadas durante 2020 en el Norte de África y Oriente Próximo 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 7/1/2020 '**MrAxxCT**' utilizaba un fichero maxxct.htm de contenido reivindicativo general para desfigurar las webs de la Oficina de Transparencia[101] y del Gabinete del Presidente[102] del gobierno de Afganistán, que utilizaban una versión desactualizada del software de servidor Apache.

El 12/1/2020 '**Op999**' desfiguraba una treintena de subdominios alojados en la web del Ministerio de Información y Comunicaciones[103] de Irán, inyectando en una misma ruta[104] un fichero .txt con contenido en persa atribuyendo al régimen iraní ser <<*mentiroso*>> y <<*cometer crímenes contra ciudadanos de Irán y otras personas alrededor del mundo*>>; la web estaba desarrollada en un entorno Microsoft con ASP.net.

En el contexto en que Fuerzas de Seguridad de Egipto intervinieron una agencia de noticias de Turquía en El Cairo, el 14/1/2020 '**RedBeard Navy**' comprometía la web del Ministerio de Transportes[105] de Egipto, que estaba programada con Wordpress, desfigurándola con contenido alusivo al ejército de Turquía.

101. ogpa.gov.af
102. ocs.gov.af
103. ict.gov.ir
104. /content/media/dbform/2020/1/00fbb33f-a10e-4c0d-a73c-381dd3f55621.txt
105. mot.gov.eg

El 1/2/2020 '**M3sicth**' inyectaba un fichero relaz.html con su alias en la web de la Agencia de Empleo[106] del gobierno de Irán. También alteraba de la misma forma la web[107] del Ministerio de Educación en Egipto, que estaba desarrollada en un entorno Microsoft.

El 3/2/2020 '**legion**' comprometía con un fichero bd.txt y su alias las webs del Ministerio de Asuntos Exteriores[108] del Líbano, así como alrededor de quince de subdominios[109] correspondiéndose con sus Embajadas en el exterior, y las webs de la Biblioteca Nacional[110] y del Museo Nacional Virtual de Arte Moderno[111]; las webs estaban equipadas con ASP.net 4.0.30319. El mismo atacante perjudicaba de igual modo un subdominio[112] del Ministerio de Bienestar Social de Irán, y otro[113] de la Autoridad Pública Industrial de Kuwait, y una web de la Seguridad Social[114] de Afganistán, todos desarrollados bajo ASP.net 4.0.30319.

El 6/2/2020 '**Simsimi**' inyectaba un fichero galau.gif[115] con su alias en la Compañía Nacional de Petróleos de Libia, cuya web estaba desarrollada con el gestor de contenidos Joomla.

El 10/2/2020 '**NmR.Hacker**' firmaba la alteración de la web[116] del Ministerio del Interior del gobierno autónomo del Kurdistán iraquí, inyectándole contenido reivindicativo general.

El 15/2/2020 '**Dr.Mwns**' inyectaba su alias en un fichero dr.txt sobre la web de la Corporación Pública de Telecomunicaciones[117] de Yemen, que estaba programada en un entorno desactualizado ASP.net 4.0.30319.

106. aro.gov.ir
107. mohp.gov.eg
108. mfa.gov.lb, foreign.gov.lb
109. Entre ellas mexico.mfa.gov.lb, buenosaires.mfa.gov.lb o madrid.mfa.gov.lb//BD.txt
110. bnl.gov.lb
111. artmodernemv.gov.lb/BD.txt
112. sakht.mcls.gov.ir
113. gatepass.pai.gov.kw
114. socialsecurity.gov.ag
115. noc.ly/images/jdownloads/screenshots/galau.gif
116. moi.gov.krd
117. ptc.gov.ye

El 25/2/2020 '**Mrb3hz4d**', que sería otro alias de 'Mamad Warning', inyectaba su habitual contenido con la bandera de Irán sobre la web del Ministerio de Bienestar Social[118] de Kuwait, que estaba programada con ASP.net.

El 27/2/2020 '**Moroccan Revolution**' inyectaba su alias en un fichero pwd.html119 sobre la web del Ministerio de la Salud de Argelia, que estaba programada con una versión vulnerable (3.9.1) del gestor de contenidos Joomla.

El 4/3/2020 **'boogz**' comprometía la web[120] del Ministerio de Prisiones de Palestina inyectándole un fichero boogz.php; la web equipaba un software PHP desactualizado.

El 14/3/2020 **'Fahad**' comprometía con un fichero vuln.gif la web[121] de Tribunal Superior de la Sharia en el gobierno de Palestina, que estaba desarrolla con una versión desactualizada de Joomla.

El 27/3/2020 '**farzad person**' desfiguraba con un fichero farzad.txt y su alias la web[122] de la Agencia Espacial de los Emiratos Árabes, que estaba desarrollada sobre ASP.net.

El 2/4/2020 '**Gatra**' comprometía con la shell SSI[123] en un fichero 71349att_pic.shtml[124] la web del Ministerio de Información y Tecnología de Palestina, que utilizaba un gestor de contenidos Joomla desactualizado.

118. exd.gov.kw
119. sante.gov.dz/pwd.html
120. mod.gov.ps
121. ljc.gov.ps
122. space.gov.ae

El 13/4/2020 **'lakarha23'** desfiguraba con contenido proargelino la web[125] programada con una versión vulnerable de Drupal del Ministerio de Educación Superior de Marruecos.

El 3/5/2020 '**MiSh**' inyectaba un fichero mendy.txt con su alias sobre un subdominio[126] de la web de la autoridad reguladora de telecomunicaciones del gobierno de Omán, que estaba programado con Joomla desactualizado.

El 12/5/2020 '**aDriv4**' inyectaba un fichero vz.txt con su alias y contacto para la venta de *shells* en la web[127] programada con una versión vulnerable de Joomla de la Autoridad Fiscal de Egipto.

El 24/6/2020 '**Ruth72**' dañaba con un fichero ruth.htm de contenido general un subdominio[128] de la web configurada con Drupal del Ejército del Líbano.

El 6/7/2020 '**Mandra**' utilizaba un fichero man.html con su alias para desfigurar la web[129] programada con software ASP.net desactualizado (4.0.30319) del Servicio de Información del Estado en Egipto.

El 12/7/2020 '**TNT_Hacker**', actuando con el alias colectivo 'Jordanian Cyber Army', desfiguraba con contenido reivindicativo general la web[130] de la Oficina del Estado Mayor de Gaza en Palestina, que estaba configurada con versiones desactualizadas del software Apache y PHP.

125. orientation.gov.ma
126. smu.tra.gov.om
127. eta.gov.eg
128. lafshield2.lebarmy.gov.lb/ruth.htm
129. sis.gov.eg/MAN.html
130. diwan.ps

El 16/7/2020 '**Mr.L3rb1**' desfiguraba el Ministerio del Interior[131] de Libia, cuya web estaba desarrollada con Wordpress desactualizado y que quedaba infectada de contenido *SEO Spam* en idioma chino.

El 26/7/2020 '**B4x**', también actuando con el alias 'ro0t-M8n', comprometía con un fichero 4.html y su alias la web[132] del Instituto de Estudios Diplomáticos del Ministerio de Exteriores de Arabia Saudí, que estaba desarrollada en un entorno Microsoft.

El 28/7/2020 **'Hunter Bajwa**' deformaba con un fichero vuln.txt el subdominio[133] programado con Joomla del centro de excelencia en tecnologías de la información alojado en el Instituto Nacional de Correos y Telecomunicaciones de Marruecos.

El 14/8/2020 '**Freedom Cry**' comprometía la infraestructura web gubernamental de registro de dominios de Internet en Egipto, desfigurando sus principales sitios web[134] con un fichero R4BIA.htm mencionando uno de los incidentes de las protestas que ocurrieron en el país en 2011. Las webs atacadas utilizaban un entorno de software Microsoft (Windows, IIS, ASP.net) desactualizado.

El 26/8/2020 '**Angelic**' realizaba inyecciones SQL sobre varias webs[135] de gobierno en Palestina, produciendo un volcado[136] mostrando credenciales de usuarios con contraseña para algunas de las webs.

El 28/10/2020 '**Wong Galek**', utilizando el alias colectivo 'Trenggalek Cyber Army', comprometía la web de la Agencia Nacional para el Desarrollo de Inversiones[137] del gobierno de Argelia, así como una web[138] del gobierno regional de Souk Ahras, ambas programadas con Joomla.

131. moi.gov.ly
132. lms.ids.gov.sa
133. ceit.inpt.ma//images/vuln.txt
134. domain.eg, egregistry.eg, egdns.eg, nic.org.eg
135. mod.gov.ps, eportal.gov.ps, courts.gov.ps, gp.gov.ps
136. https://pastebin.com/raw/B4zHXA3Y
137. andi.gov.dz/images/gmapfp/666.jpg
138. dcwsoukahras.gov.dz

El 1/12/2020 '**moncet-1**' deformaba con su alias sobre la web del Consejo Económico y Social[139] de Jordania, que estaba programada con una versión desactualizada de ASP.net

139. esc.jo/Gallery/m-1.html

5.3 Marcos narrativos *hacktivistas* en Norte de África y Oriente Próximo

Las narrativas *hacktivistas* de llamamiento a ciberataques en el Norte de África y Oriente Próximo durante 2020 fueron:

Marcos narrativos *hacktivistas* en Norte África/Oriente Próximo 2020					
País	Operación	Promotor	Tipo de Objetivo	Tipo de Acción	Resultado
TR	#OpTurkey	s1ege	Instituciones públicas de Turquía	Desfiguración	Desfigurada una web gubernamental
IL	#OpIsrael	Lorian Synaro The Jerusalem Electronic Army Hackers of Savior	Instituciones públicas y empresas de Israel	DDoS Desfiguración	Contenidos digitales con diversas amenazas sin concretar en acciones operativas. Una treintena de webs privadas, y un par de subdominios de webs de gobierno desfigurados. Ataques DDoS ocasionales.
LE	#OpLebanon	LiteMods Nama Tikure Syrian Revolution Soldiers	Instituciones públicas y empresas del Líbano	Desfiguración iSQL DDoS	Una docena de webs de gobierno desfiguradas. iSQL sobre la agencia libanesa de noticias, y sobre el Ministerio de Finanzas. Ataques DDoS ocasionales.

6. *Hacktivismo* en ámbito internacional

6.1 Caracterización general *hacktivista* en resto internacional

Internacionalmente, el comportamiento del *hacktivismo* en el resto de los países en regiones no mencionadas en epígrafes anteriores de este informe es un reflejo de lo ya descrito en los capítulos previos, de manera que puede concluirse que las características del *hacktivismo*, con las pertinentes diferencias regionales o locales, guardan una cierta homogeneidad en todo el mundo. A saber:

01. Individualización de identidades *hacktivistas* o agrupamiento en pequeños colectivos (tipo "teams"), dedicados principalmente a las desfiguraciones de sitios webs por notoriedad y exhibicionismo personales, con patente ausencia de motivación ideológica.

02. Reducción de las antiguas configuraciones tipo 'Anonymous' a canales instalados en redes sociales dedicados prácticamente a difundir consignas que no tienen traducción en acciones.

03. Ausencia de narrativas motivadores de campañas de ciberataque en la mayoría de los contextos sociales de protesta en cualquier país. Cuando estas narrativas se producen (caso de #OpNigeria u #OpMyanmar), suelen consistir en una etiqueta sin más elaboración semántica, no logran atraer a identidades atacantes, y ni siquiera se colectivizan significativamente en redes sociales.

04. En línea con lo anterior, la mayoría de las propuestas de ciberataques de protesta *hacktivista*, poco elaboradas y débilmente colectivizadas, se articulan por un pequeño grupo de identidades de baja peligrosidad, que van de país en país intentando hacer propuestas *hacktivistas* en paralelo a los conflictos sociales que surgen en ellos, propuestas que carecen de alcance y no logran adhesiones.

05. Identidades atacantes recurrentes que llevan a cabo ciberataques de oportunidad sobre webs provistas de software desactualizado y/o vulnerable, donde mayormente se inyecta el alias o el logo del atacante como todo contenido reivindicativo.

06. Paulatina desaparición del *hacktivismo* ideológico para dar paso a un *hacktivismo* egocéntrico, cuando no a un falso *hacktivismo* o *hacktivismo* impostado, con creciente intersección entre *hacktivismo* y pequeña cibercriminalidad con ánimo de lucro ilícito.

6.2 Phishing concurrente a falso *hacktivismo*

Adicionalmente a su caracterización general, un elemento particular en el escenario *hacktivista* internacional durante 2020 fue el incremento cualitativo sobre las ya mencionadas tácticas de pequeña cibercriminalidad concurrentes al *hacktivismo*, incluso la simulación del *hacktivismo* como probable falsa bandera para desarrollar una actividad neta de cibercriminalidad, consistente ese salto cualitativo en la utilización de desfiguraciones de sitios web para inyectarles una estructura simulada de tienda de comercio electrónico -un script dirigiendo hacia ella-, que es falsa y que está diseñada como procedimiento de ***phishing***, para la captura de credenciales de pago de las víctimas que lleven a cabo una conducta de compra en una de esas tiendas fraudulentas inyectadas por desfiguración en un sitio web.

En concreto, el *phishing* concurrente a una desfiguración web con apariencia *hacktivista* comenzó detectándose en noviembre de 2020, siendo que ese año aparecieron dos casos:

01. El 7/11/2020 '**Juba_Dz**' comprometía la web de la universidad Tai Solarin[140] en Nigeria, que estaba desarrollada con software PHP desactualizado y sobre la que se alojaba contenido de *phishing* para la captura de datos de pago con tarjeta de crédito simulando ser una tienda en línea para la compra de artículos textiles (Figura 6-2-1).

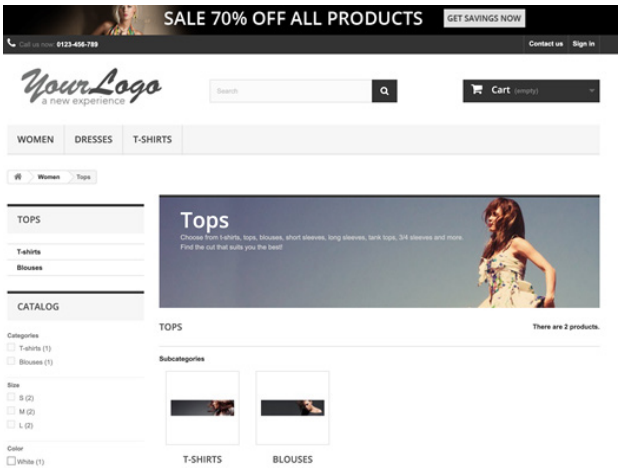


Figura 6-2-1

140. https://www.youtube.com/watch?v=-8eduJrCWEA

02.

El 14/12/2020 **'zarox**', que también emplea el alias 'Moroccanwolf', comprometía con un fichero zx.htm media docena de webs de gobierno programadas con software Joomla desactualizado en Burkina-Faso, incluyendo la Dirección General del Tesoro[141] y la Escuela Nacional de Gestión Financiera[142], sobre las que se inyectaba además un script redirector a una probable web[143] de *phishing* haciéndose pasar por una tienda de comercio electrónico (Figura 6-2-2).

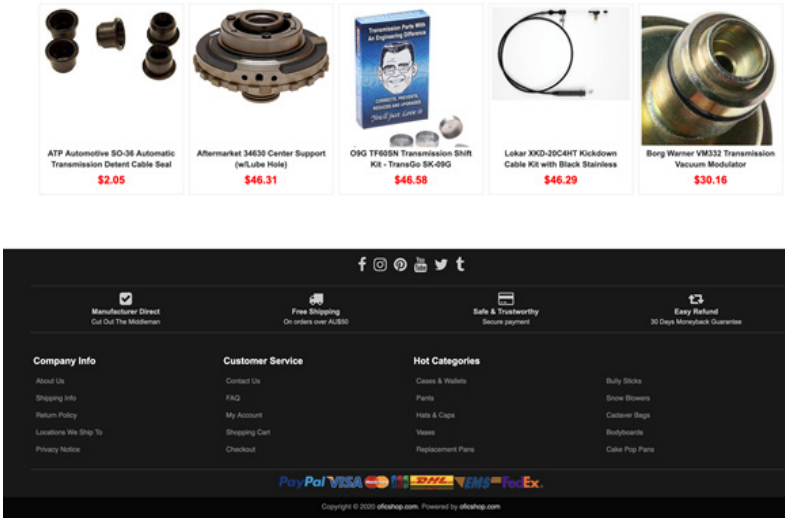


Figura 6-2-2

141. tresor.gov.bf/zx.htm
142. enaref.gov.bf/zx.htm
143. oficshop.com

6.3 Ciberataques más relevantes

Entre los ataques *hacktivistas* en países del resto del ámbito internacional no contemplados en anteriores epígrafes de este informe y que destacaron durante 2020, ya sea por su visibilidad o por comprometer sitios web significados de empresas o de gobiernos, destacaron los siguientes:

El 6/1/2020 '**MssXCode**' deformaba con su alias en un fichero boom.php la web[144] del Ministerio de Finanzas de Bosnia-Herzegovina, que usaba una versión vulnerable de Joomla.

El 18/1/2020 '**AlcatrazHackTeam**' alteraba con su fichero 13.txt la web[145] del Ministerio de Justicia de Zimbabwe, que estaba programada con una versión desactualizada de Joomla.

El 10/2/2020 '**ifactoryx**' comprometía inyectándole su alias la web[146] del Ministerio de Industria de Camboya, que estaba desarrollada cobre ASP.net 4.0.30319; posteriormente quedaba infectada con contenido *SEO Spam* en idioma japonés.

144. mft.gov.ba
145. justice.gov.zw
146. mih.gov.kh

El 25/2/2020 '**mhamdi_jeber**' alteraba con un fichero js.php y su alias la web desarrollada con Wordpress del Ministerio de Transportes[147] de Kazajistán.

El 26/2/2020 '**NullC0d3r**' inyectaban un fichero nullc0d3r.png con contenido reivindicativo general en la web de la empresa Energías de Portugal[148].

El 5/3/2020 **'MrAxxCT**' desvirtuaba la web[149] de las Aduanas de Bangladesh.

El 19/3/2020 '**NullC0d3r**' utilizaba un fichero nullc0d3r.txt con su alias y el colectivo de 'CyberTeam Portugal' para inyectarlo en un subdominio[150] de la web del Departamento de Energía del gobierno de EEUU, que estaba desarrollado con un gestor de contenidos Drupal.

El 27/3/2020 '**gh057 5p3c706**', empleando el aludido alias colectivo de 'Ghost Squad Hackers' que utiliza también 's1ege', comprometía un subdominio[151] de la web de la Policía de Tailandia y la web del Ministerio de la Marina[152] en el mismo país, ambos desarrollados con versiones desactualizadas de Joomla.

147. transportvko.gov.kz
148. edp.pt
149. bangladeshcustoms.gov.bd
150. climatemodeling.science.energy.go
151. banboek.lopburi.police.go.th
152. md.go.th

El 14/4/2020 '**NullC0d3r**' alteraba con su alias en un fichero nullc0d3r.jpg la web del Centro de Formación Europea Jacques Delors[153] del Ministerio de Asuntos Exteriores de Portugal, que estaba desarrollada con una versión vulnerable de Drupal; el 19/4/2020 el mismo atacante alteraba con su alias el Comisariado para las Migraciones[154]. En el mismo país y etiquetando sus acciones como **#Op25Abril**, la identidad colectiva '**CyberTeam Portugal**', a la que se adscribe 'NullC0der', firmaba el 20/4/2020 con un fichero cyberteam.py el comprometimiento de las webs de la biblioteca[155] del Ministerio de Salud, que estaba equipada con Wordpress; del Plan Nacional de Lectura[156]; de la Plataforma Digital de Ayuntamientos de Portugal[157]; el Centro de Investigación de Tecnologías Interactivas[158] de la Universidad de Lisboa; un subdominio de la Fundación de Ciencia y Tecnología[159]; el Observatorio de la Lengua Portuguesa[160]; algunas de las webs estaban vinculadas entre sí, de manera que era previsible que el atacante vulnerara algunas a través del acceso forzado previo sobre otras. El mismo atacante situaba el 16/4/2020 en el dominio público[161] un volcado de datos sin información sensible resultado de una inyección SQL sobre la web del proveedor portugués de telecomunicaciones Altice[162], empresa que junto a Energias de Portugal[163] recibían el 13/4/2020 ataques por denegación de servicio por parte de 'CyberTeam Portugal'.

El 14/4/2020 '**Cyberr00t**' comprometía con un fichero haruchan.htm un subdominio[164] del Ministerio de Energía de Canadá, que estaba programado con ASP.net.

El 18/4/2020 '**Aslan Neferler Tim**' deformaba con contenido proturco la web[165] programada con Wordpress del Ministerio de Juventud y Deportes de Zimbabwe, que quedaba infectada con contenido *SEO Spam* en idioma japonés. En el mismo país, el 22/4/2020 '**Saber**', también operando con el alias 'fallag kill3r', desfiguraba con su alias las webs de los ministerios de Agricultura[166], de Minas[167] y de Industria[168], que estaban equipadas con versiones desactualizadas de los gestores de contenidos Wordpress y Joomla, y que también quedaban posteriormente infectadas con contenido *SEO Spam* en idioma japonés.

153. eurocid.mne.gov.pt
154. acm.gov.pt
155. biblioteca.min-saude.pt
156. planonacionaldeleitura.gov.pt
157. pdcp.pt
158. citi.pt
159. pnl.fccn.pt
160. bibliotecalivrosdigitais.observalinguaportuguesa.org
161. https://easyupload.io/bj309w
162. telecom.pt
163. edp.pt

El 19/4/2020 el mencionado '**MrAxxCT**' inyectaba su alias en un fichero gotcha.gif sobre el Ministerio de Salud[169] de Sri Lanka, que tenía instalada una versión vulnerable del software para el servidor Apache.

El 22/4/2020 '**sorong6etar**', que también utiliza el alias 'Illusionz', desfiguraba una web[170] desarrollada con Joomla del Ministerio de Salud de Uganda, que quedaba infectada con contenido *SEO Spam*.

El 23/4/2020 '**LahBodoAmat**' alteraba con un fichero sheller.php la web[171] del Ministerio de Protección Social de Ghana, que estaba desarrollada con Wordpress y quedaba infectada con contenido *SEO Spam*.

El 2/5/2020 '**Bla3k D3vil**' comprometía con un fichero a.htm y contenido *SEO Spam* en idioma japonés la web[172] de la Embajada de Laos en Filipinas, que estaba programada con Joomla.

El 8/5/2020 '**d4rkstat1c**' comprometía con su alias y una mención a 'Ghost Squad Hackers' la web[173] del Ministerio de Justicia de Laos, que está programada con Drupal 7.

El 3/6/2020 **'Janjaweb**' comprometía la web[174] del Ministerio de Inversiones de Sudán, así como de otro par de instituciones de gobierno[175] en el país, inyectándoles un logotipo de 'Anonymous' con su alias. Las webs podrían haber estado desarrolladas con una versión desactualizada del software PHP.

169. health.gov.lk
170. nms.go.ug
171. mogcsp.gov.gh
172. laoembassymanila.gov.la
173. moj.gov.la
174. minv.gov.sd
175. hac.gov.sd, ngc.gov.sd

El 16/6/2020 '**s1ege**' desfiguraba con su alias y contenido alusivo a 'Ghost Squad Hackers' una veintena de webs[176] programadas con Joomla del gobierno de Zimbabwe, incluido el Ministerio de Defensa[177].

El 23/6/2020 '**Cherif Hadria Mohamed**' comprometía con su contenido ya conocido una página[178] del portal del Gobierno de Canadá, que utilizaba un software desactualizado para el servidor Apache. En el mismo país, el 26/6/2020 '**s4ndal.py**' vulneraba con un fichero hh.txt y su alias la web[179] de la Comisión Nacional de Capitales; la web tenía instalado software desactualizado para el servidor Nginx.

El 14/7/2020 '**s1ege**' y '**Mandra**' deformaban un subdominio[180] de la web de la Agencia Espacial Europea, que tenía desactualizado el software de su servidor Apache.

El 14/7/2020 '**Sakhavat & Ferid23**' desfiguraba el portal gubernamental[181] y la web del Primer Ministro[182] de Armenia, inyectando contenido reivindicativo sobre el carácter azerbaiyano de Karabaj; las webs tenían desactualizado el software PHP.

El 17/7/2020 '**Angelic**', que era una nueva identidad del alias colectivo 'CyberTeam Portugal', desfiguraba con contenido general la web[183] del Sindicato de Funcionarios Judiciales de Portugal, que estaba programada con Joomla. En el mismo país el 14/7/2020 '**CyberTeam Portugal**' había desfigurado con un fichero ct.html la web de la Dirección General de Educación[184], que estaba desarrollada con un gestor de contenidos Drupal 7. Y el 19/7/2020 de nuevo 'Angelic' producía una inyección SQL sobre la web del Ayuntamiento de Lisboa[185], con volcado de credenciales de usuario con contraseñas en formato SHA256 en el dominio público[186].

---

176. https://pastebin.com/f6cFxMz8
177. defence.gov.zw
178. canada.ca/nos-langues
179. ncc-ccn.gc.ca
180. business.esa.int
181. gov.am
182. primeminister.am
183. sfj.pt
184. dge.mec.pt/ct.html
185. lisboa.pt
186. https://ghostbin.co/paste/cwred

El 21/7/2020 '**Mrb3hz4d**' alteraba con un fichero .HTML un subdominio[187] desarrollado con ASP.net de la web del gobierno de Puerto Rico en EEUU. En el mismo país, el 22/7/2020 '**s1ege**' utilizaba un fichero gsh.html y contenido general para desfigurar un subdominio[188] del gobierno del Estado de Washington, que estaba codificado con ASP.net 4.0.30319. El 23/7/2020 el mismo atacante inyectaba en un fichero gsh.html alusiones a la libertad de Julian Assange sobre varios subdominios de la web[189] programada con ASP.net del Estado de Pensilvania en EEUU, mientras el 28/7/2020 hacía lo mismo con subdominios[190] del Estado de Idaho, en este caso codificados con Wordpress. Por su parte, la identidad asociada a este último atacante, '**Mandra**', comprometía el 21/7/2020 con un fichero boy.html otra web programada con ASP.net en EEUU, en esta ocasión del sistema de tribunales[191]. También en EEUU, el 26/7/2020 '**MiSh**' alteraba con su alias la web[192] desarrollada con Joomla de un gobierno local.

También el 3/8/2020 '**Moroccan Revolution**' alteraba con un fichero ma.txt y su alias o con un fichero kurd.txt y los alias 'OxSouhail' y '0x1998', una decena de subdominios alojados[193] en la web programada con software Microsoft desactualizado del gobierno estatal de Wisconsin en EEUU, así como otro[194] dotado del mismo software en el gobierno del estado de Georgia. En el mismo país, el 5/8/2020 '**xNot_RespondinGx**' comprometía otra web[195] del gobierno estatal de Utah, también desarrollada con ASP.net. El 22/8/2020 de nuevo 'Moroccan Revolution' inyectaba su alias sobre una web[196] programada con ASP.net del gobierno del Estado de Louisiana, mientras el 30/8/2020 alteraba con un fichero morocco.html y su alias las webs[197] programadas con ASP.net desactualizado de un gobierno local. Y en el mismo país, el 26/8/2020 '**Cherif Hadria Mohamed Riane**' desfiguraba con una alusión a Palestina un subdominio[198] programado con ASP.net de la web del programa de salud comunitaria del gobierno del Estado de Tennessee.

El 2/8/2020 '**s4ndal.py**' deformaba con un fichero xdxd.php y su alias la web[199] del Ministerio de Salud de Liberia, que quedaba infectada con contenido *SEO Spam* en idioma japonés.

---

187. siactest.daco.pr.gov/Mrb3hz4d.html
188. apps-trn.dcyf.wa.gov
189. Entre ellos cad.pa.gov o etran.pa.gov
190. Por ejemplo contractors.liquor.idaho.gov, cdhh.idaho.gov
191. ilnd.uscourts.gov
192. lincolnshireil.gov/media/com_acym/kroos.jpg
193. Entre ellos wistatecapitolpoliceparking.wi.gov, tn.lodi.wi.gov
194. gaprep.dhs.ga.gov
195. co.uintah.ut.us/visitoruploads/25338383883.jpg
196. lsbc.louisiana.gov/index.html
197. laceywa.gov, ci.lacey.wa.us
198. pdms.tenncare.tn.gov
199. moh.gov.lr

El 8/8/2020 '**L4663R666H05T**', también conocido como 'Laggergod', comprometía con su alias la web[200] del Ministerio de Trabajo de Laos, que utilizaba software PHP desactualizado.

Igualmente el 17/8/2020 '**IceBear7**' desfiguraba con su alias la web[201] del Ministerio de Comercio de Lesoto, que estaba desarrollada con ASP.net.

El 19/8/2020 de nuevo '**s1ege**' inyectaba un fichero g.html con el logo de 'Ghost Squad Hackers' y la frase "fuck the United Nations" sobre 75 subdominios[202] de otros tantos capítulos nacionales de la Organización Internacional para las Migraciones con sede en Suiza, que utilizaba una versión desactualizada del gestor de contenidos Drupal. El 23/8/2020 el mismo atacante inyectaba su habitual contenido alusivo a la libertad de Julian Assange en un fichero gsh.html sobre un subdominio[203] desarrollado en un entorno Microsoft de la web del Consejo de la Unión Europea.

El 23/8/2020 '**Gatra**' comprometía con su alias las webs de los Ministerios de Exteriores[204] y de Educación[205] de Zambia, que estaban programadas con Wordpress y quedaban infectadas con contenido *SEO Spam* en idioma japonés.

También el 22/9/2020 '**Gh05t66nero**' alteraba con su alias inyectado en una misma ruta URL[206] varias decenas de webs del servicio de anuncios de la empresa estadounidense Google en otros tantos países, como Suecia[207], Jordania[208] , España[209] o la República Dominicana[210].

200. molsw.gov.la
201. trade.gov.ls
202. Por ejemplo peru.iom.int, spain.iom.int
203. cimals-drmt.consilium.europa.eu
204. mofa.gov.zm
205. moge.gov.zm
206. /ddm/fls/Poisoned By Gh05t666nero
207. adservice.google.se
208. adservice.google.jo
209. adservice.google.es
210. adservice.google.com.do

El 1/10/2020 '**Anonymous Greece**' ejecutaba ataques por denegación de servicio sobre 76 webs bajo dominio gubernamental azerbaiyano gov.az, mientras el 7/10/2020 desfiguraba con un mensaje reivindicativo un subdominio[211] del Parlamento de Turquía, que utilizaba una versión desactualizada de PHP. En este mismo escenario, el 6/10/2020 '**Karabak Hacking Team**' deformaba, con el mensaje en inglés <<Karabakh is Azerbaijan!>>, 46 sitios web de primer nivel de gobierno en Armenia y en la región en disputa de Nagorno Karabaj, incluidos las presidencia de la región[212] y del país[213]; o la Policía[214], el Defensor del Pueblo[215], el Ministerio de Justicia[216] o el Ministerio de Energía[217] de Armenia; las webs comprometidas tenían desactualizado el software para el servidor Apache. El 28/10/2020, de nuevo '**Karabak Hacking Team**' desfiguraba con contenido contra Armenia la web de la empresa Pizza Hut[218] en ese país.

En el contexto del incremento de tensión en Francia con relación a caricaturas del profeta musulmán Mahoma, el 27/10/2020 '**Wong Galek**' insertaba un fichero 666.jpg sobre media docena de webs[219] programadas con Joomla de ayuntamientos en Francia. En el mismo país, el 23/10/2020 '**Achraf Dz**' había vulnerado otra[220], además de otra veintena de webs privadas[221], también provistas de Joomla, inyectando contenido rechazando "caricaturas sobre el Islam" así como contenido *SEO Spam* en idioma japonés. Del mismo modo, el 26/10/2020 '**Akincilar**' utilizaba contenido proturco para deformar la web de otro ayuntamiento[222] francés, provista de software PHP desactualizado. En el mismo contexto, '**S&A**' comprometía con contenido anti-francés mencionando el Islam treinta webs privadas[223] en Francia.

---

211. apps.tbmm.gov.tr/heyet_karsilama2/APA_HEADlist.php
212. president.nkr.am
213. president.am
214. police.am
215. ombdus.am
216. justice.am
217. minenergy.am
218. pizza-hut.am
219. Entre ellas mairie-lillers.fr, ville-poulx.fr
220. mairie-saint-marcel.fr
221. Entre ellas menuiserie-ducasse.fr, osha.fr
222. mairie-neuvillesursaone.fr
223. Entre ellas mon-electricien-paris.fr, votre-serrurier-fontainebleau.fr

El 27/10/2020 el sitio web de la campaña presidencial de Donald Trump en EEUU era desfigurado en una de sus URL[224] inyectándose contenido simulando al Departamento de Justicia del país (Figura 6-3-1), con un mensaje advirtiendo de que los atacantes tenían acceso a <<múltiples dispositivos de Trump y sus familiares>>, y a <<conversaciones secretas estrictamente clasificadas que probarían que Trump está involucrado en el origen del coronavirus>>. El contenido inyectado incluía dos direcciones electrónicas para la transferencia de divisas en Monero donde se pedía a los visitantes que transfirieran donaciones; la dirección que más donaciones recibiera determinaría si los atacantes "divulgaban" esa información que afirmaban estaba en "su posesión". Por el momento, ninguna identidad con rasgos *hacktivistas* ha reivindicado la acción, que podría ser un reclamo (o hacerlo parecer así) de pequeña cibercriminalidad dirigido a una estafa con divisas electrónicas.

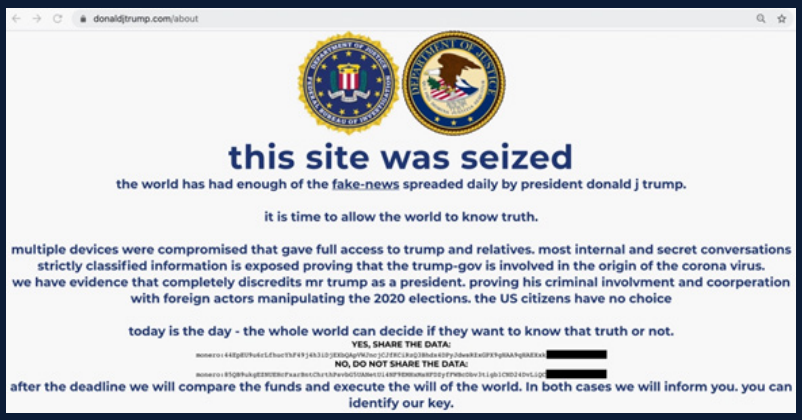


Figura 6-3-1

224. donaldjtrump.com/about

6.4 Actividad de 'LulzSecITA'

Por otra parte, en las habituales oleadas de ciberataques de '**LulzSecITA**' adscritas a sus distintos marcos narrativos ideológicos que llevan reportándose varios años, durante 2020 cabe nombrar varias de sus acciones llevadas a cabo contra sitios web en Italia, entre ellas:

El 6/1/2020, en el contexto del marco narrativo de retórica medioambientalista **#OpGreenRights**, producía desfiguraciones e inyecciones SQL sobre media docena de webs en Italia, entre ellas un subdominio del Ministerio de Política Agrícola[225], la Protección Civil de la Provincia de Lecce[226], o un subdominio de la Provincia de Foggia[227].

El 7/2/2020 producía una inyección SQL sobre la web de la Universidad Roma Tre[228] en Italia, realizando un volcado de datos en el dominio público[229]. Adicionalmente y etiquetando las acciones como **#OpLucania** dentro de su marco narrativo general **#OpGreenRights** de retórica medioambientalista, atacaba webs en el área regional de la Basilicata en Italia, protestando por lo que consideran operaciones empresariales que deterioran medioambientalmente el valle de Agri; en ese contexto, ejecutaba varias inyecciones SQL sobre algunas webs de gobierno regional[230], así como desfiguraciones con contenido alusivo en webs de gobierno local[231].

225. catalogoviti.politicheagricole.it con volcado de datos en https://bit.ly/2Fv1ZaK
226. cvpc.lecce.it con volcado de datos en https://bit.ly/2QXkPg9
227. pianificazionestrategica.provincia.foggia.it
228. uniroma3.it
229. https://privatebin.net/?111bac4997ed5b4b#5ekrF2fKqYkCnMcPx8YoP9vsAiLx25Jeh4dZ3GdEugT5
230. regione.basilicata.it con volcado en https://bit.ly/2V5he30; consiglio.basilicata.it, con volcado en https://bit.ly/2SABXub
231. comunemissanello.it, comune.pietrapertoza.pz.it

El 6/3/2020, en un nuevo incidente en el marco de la narrativa mediioambientalista #OpGreenRights, en esta ocasión etiquetando **#OpCampania** por centrar la retórica *hacktivista* en la región de Campania en Italia, ejecutaba inyecciones SQL sobre el ente público Asmez[232], la sociedad meteorológica regional[233], o la empresa de gestión del agua[234] de Nápoles.

El 20/5/2020 reivindicaba haber penetrado la infraestructura web[235] del Hospital San Rafael de Milán; más allá de la difusión de alguna captura de pantalla reivindicativa[236] o de contraseñas de usuarios individuales[237], el atacante no liberaba al dominio público contenido sensible o datos robados en la ciberincursión.

El 1/6/2020 desfiguraba la web[238] del servicio de información sobre tributación de entidades locales, que estaba desarrollada con Wordpress. Y, aunque sin producirse una reivindicación de autoría, la web de la Oficina de Transporte de Roma[239] fue infectada con contenido *SEO Spam* de naturaleza pornográfica.

El 7/7/2020 amenazaba[240] a la provincia de Trento con lanzar ciberataques bajo la etiqueta **#OpWinnieThePooh** en el contexto de la **#OpGreenRights** respecto del tratamiento que se está dando a un oso por parte de los servicios ambientales de la zona, que la amenaza considera inadecuados. De momento la amenaza no ha tenido desarrollo operativo. Así mismo, el 13/7/2020 mostraba en Twitter[241] una captura de pantalla que sugería había logrado penetrar la web de la región autónoma de Trentino-Alto Adige[242] en Italia, sin divulgar por ahora más información al respecto. Al día siguiente sugería[243] haber vulnerado la web de la Autoridad Nacional de Aviación Civil[244] en el país, aunque sin aportar evidencia concreta; y mostraba[245] resultados parciales sin publicar información sensible de una posible inyección SQL sobre la web del aeropuerto de Milán[246]. También el 22/7/2020 mostraba en Twitter[247] una captura de pantalla con el resultado de una probable inyección SQL sobre la web[248] del gobierno provincial de Foggia.

---

232. asmet.it, con volcado en https://anonfiles.com/X3icm0f2o0/asmenet_zip
233. campaniameteo.it, con volcado en https://bit.ly/2vfIK3z
234. abc.napoli.it con volcado en https://bit.ly/339qQvV
235. hsr.it
236. Por ejemplo https://twitter.com/LulzSec_ITA/status/1263116071197958144
237. Por ejemplo https://twitter.com/LulzSec_ITA/status/1263450001918898177
238. riscotel.it
239. atac.roma.it
240. https://anonitaly.blackblogs.org/2020/07/07/opwinniethepooh/
241. https://twitter.com/LulzSecurityITA/status/1282669209449791488/photo/1
242. regione.taa.it
243. https://twitter.com/LulzSecurityITA/status/1282984059996704768
244. enac.gov.it
245. https://twitter.com/LulzSecurityITA/status/1283033454976933889/photo/1
246. seamilano.eu
247. https://twitter.com/LulzSecurityITA/status/1285906024046764033
248. provincia.foggia.it

El 22/9/2020 situaba en el dominio público[249] una tabla con formato de base de datos y denominación *db_concorsopolizia* que afirma contiene datos de autenticación (dirección de correo electrónico, usuario y contraseña en formato *hash*) de más de 30 mil policías italianos. Es probable que los datos procedan de una web asociada al Ministerio del Interior de Italia, considerando que la mayoría de los registros se corresponden con usuarios bajo dominios web interno.it y poliziadistato.it. Además, el 25/9/2020 el mismo atacante situaba en el dominio público[250] el resultado parcial de una inyección SQL sobre una web no identificada donde se observa un listado de tablas de bases de datos correspondiéndose con nombres de hospitales de Italia, sin que la exfiltración expusiera más información al detalle.

El 23/10/2020 inyectaba un script redirector hacia webs de contenido pornográfico sobre la web del Instituto Nacional de la Seguridad Social[251] de Italia, que estaba desarrollada con ASP.net. El 26/10/2020 el mismo atacante divulgaba en el dominio público[252] un listado de credenciales de autenticación (denominación de dirección de correo electrónico y contraseña) de treinta usuarios con direcciones bajo el dominio web[253] de la provincia de Roma.

249. https://anonfiles.com/3al6PcXfof/33581_concorsopolizia
250. https://zerobin.net/?78c9fbcacf9281cd#XMWronaNSFl+SLVWC8Ir2Tw2FLn29OzdDlIJY3kGGrA=
251. inps.ita
252. https://zerobin.net/?f9a773898c6157e5#CH7OFtOtsGTGBqVDfB4LDSLoC/+guLVOmg2y4dYEOnY=
253. provincia.roma.it

6.5 Ciberataques en EEUU reactivos a muerte de iraní Soleimani

Durante el primer mes de 2020 se produjeron varias acciones por desfiguración de webs en EEUU y otras partes del mundo donde se inyectaron contenidos proiraníes y/o de protesta contra la muerte del General iraní Qasem Soleimani, acaecida el 3/1/2020 por una acción militar estadounidense en Iraq. Esta reacción *hacktivista* no llegó a configurar una campaña ni organizada ni sostenida en el tiempo, sino que se desarrolló a partir de ataques individuales coyunturales llevados a cabo por identidades en función de criterios de oportunidad. Entre las desfiguraciones producidas en este contexto constan:

El 3/1/2020 '**JavidH373**' inyectaba un fichero iran.html con contenido gráfico alusivo al General iraní Qasem Soleimani en una veintena de webs privadas[254] con dominio en Italia e IP en España; las webs estaban equipadas con la versión desactualizada ASP.net 4.0.30319.

El 5/1/2020 el alias '**Iran Cyber Security Group**', que se correspondería con la identidad '**Iran-Cyber**' que opera con desfiguraciones inyectando el mismo contenido proiraní al menos desde 2015, deformaba la web[255] del Programa Federal de Bibliotecas en EEUU, que estaba desarrollada con el gestor de contenidos Joomla, inyectándole su acostumbrado mensaje proiraní con el añadido de un contenido de burla sobre Donald Trump (Figura 6-5-1); la web ya había sido previamente desfigurada por otros atacantes en 2012 y 2014.

254. Entre ellas fooditalia.com, studiogrifasi.it
255. fdlp.gov

Figura 6-5-1

El 7/1/2020 '**Shield Iran**' inyectaba contenido alusivo al general iraní Qasem Soleimani sobre la web[256] de Banco Comercial de Sierra Leona, que opera con una versión vulnerable (4.0.30319) de ASP.net.

El 8/1/2020 '**invisibleegle1**' firmaba la desfiguración, con contenido alusivo a Irán, de un subdominio[257] del Departamento de Tráfico de la web del gobierno del distrito federal de Washington.

256. slcb.com
257. artsprod.mvis.dmv.washingtondc.gov

El 28/1/2020 '**lulzkid**' inyectaba una alusión a 'Anonymous Iranian' desfigurando con un fichero index.html un subdominio de la web[258] del gobierno del Estado de Texas en EEUU, que estaba desarrollado con una versión desactualizada (4.0.30319) de ASP.net. Con el mismo alias '**Anonymous Iranian**' se alteraba el 30/1/2020 la web de un gobierno local[259] en EEUU también configurada con ASP.net 4.0.30319. Igualmente, el 31/1/2020 probablemente el mismo atacante, pero operando con el alias '**Vis3c**', alteraba con el mismo fichero otros tres gobiernos municipales[260] en el mismo país, también equipados con ASP.net.

Posteriormente, ya el 4/10/2020 '**Bax 026 of Iran**', que también emplea el alias de 'Mamad Warning', desfiguraba con contenido proiraní tres webs[261] desarrolladas con ASP.net de gobiernos locales en EEUU. En el mismo país y día '**1TED**' también inyectaba contenido proiraní en la web[262] de otro gobierno local. Igualmente, el 2/10/2020 '**Rhm4tFnx**' dañaba con un fichero mat.html de contenido general la web[263] de una oficina de derechos del consumidor del gobierno estatal de Texas, también programada con ASP.net. Y el 7/10/2020 '**Dr.3V1L'**, firmando con el nombre 'Hossein Hezami', alteraba un subdominio[264] la web programada en un entorno Microsoft del gobierno estatal de Alaska.

258. puc.texas.gov
259. brevardfl.gov
260. flatoniatx.gov, fairviewnc.gov, dalharttx.gov
261. cmbuslic.ci.monterey.ca.us, service.hiltonheadislandsc.gov/PSI/, alerts.rochestermn.gov
262. citykankakee-il.gov
263. opuc.texas.gov/mat.html
264. dot.alaska.gov/_RECYCLE/cftest/logview.cfm

En este contexto de ciberataques por desfiguración sobre webs de EEUU inyectando contenidos de temática proiraní, cabe mencionar que en septiembre de 2020 el Departamento de Justicia de EEUU presentaba cargos criminales[265] contra dos nacionales de Irán acusados de los ataques por desfiguración de sitios web en EEUU, algunos de los cuales se reseñan en este informe, en el contexto de las oleadas de protesta por la muerte del general Qasem Soleimani. El Departamento Federal de Investigación (FBI) del Departamento de Justicia tiene identificados a esos dos nacionales iraníes como **Behzad Mohammadzadeh**[266], con el alias 'Mrb3hz4d'; y **Marwan Abusrour**[267] como 'Mrwn007'.

Adicionalmente, en enero de 2021 la empresa de ciberseguridad Clearsky afirmaba en un informe[268] que la ciberamenaza persistente avanzada (APT) conocida como '**Lebanese Cedar**', que las atribuciones de esta empresa consideran un "cibercomando" de la milicia proiraní libanesa **Hezbollah**, está utilizando, entre las herramientas de penetración y persistencia en servidores web en sus ataques, una webshell denominada 'Mamad Warning Sheller', que coincidiría con la denominación del alias empleado por la identidad varias veces mencionada en ciberataques en este informe utilizando los sobrenombres 'Mamad Warning', 'Bax 026 of Iran' o 'Mrb3hz4d'.

Tanto la acción judicial del Departamento de Justicia de EEUU como las atribuciones de ClearSky sitúan en la órbita de Irán a 'Mamad Warning', y a sus alias potencialmente asociados, lo que es coherente con el hecho de que el contenido proiraní con que estos alias firman la mayoría de sus desfiguraciones web. La utilización por una APT de una webshell con la denominación de 'Mamad Warning' es también compatible con que la actividad *hacktivista* -o de apariencia *hacktivista*- de este alias esté vinculada a una sistemática de pequeña cibercriminalidad, principalmente traducida en el *SEO spamming*, en la inyección de scripts redirectores hacia webs de distribución de contenidos maliciosos o, como es el caso, a la venta de *webshells*, práctica a la que también se dedican otras reportadas identidades pretendidamente *hacktivistas* como 'aDriv4'. La webshell[269] de 'Mamad Warning' está diseñada para el ataque a servidores programados en un entorno Microsoft, lo que coincide con la tipología de desfiguraciones llevadas a cabo por este alias y sus sobrenombres asociados.

265. https://www.justice.gov/usao-ma/pr/two-alleged-hackers-charged-defacing-websites-following-killing-qasem-soleimani
266. https://www.fbi.gov/wanted/cyber/behzad-mohammadzadeh
267. https://www.fbi.gov/wanted/cyber/marwan-abusrour
268. https://www.clearskysec.com/cedar/
269. https://valhalla.nextron-systems.com/info/rule/WEBSHELL_ASPX_MamadWarning_Jul20_1

6.6 Vulneración de accesos a cuentas de Twitter

En los primeros compases de 2020 la identidad '**OurMine**', que en años previos había sido reportada comprometiendo el acceso a cuentas en Twitter de alta visibilidad, principalmente en EEUU, repetía la operación el 27/1/2020 interviniendo sobre diversas cuentas en la red social de equipos estadounidenses de fútbol americano (entre ellas Kansas City Chiefs[270], Green Bay Packers[271], o Chicago Bears[272]), además de la propia Liga Nacional[273], emitiendo a través de ellas y para varios millones de seguidores (la Liga tiene 25 millones de ellos) el mismo tipo de mensaje aludiendo a que pretenden <<*mostrar a la gente que todo es hackeable*>>. De nuevo el 7/2/2020 el mismo atacante vulneraba el acceso a las cuentas corporativas del propio Facebook en Twitter[274] e Instagram[275], donde tiene 13.4 y 3.5 millones de seguidores, respectivamente. Como es habitual, 'OurMine' secuestró brevemente el acceso a los perfiles emitiendo a través de ellos el mensaje en inglés <<*incluso Facebook es hackeable, pero al menos su seguridad es mejor que la de Twitter*>> (Figura 6-6-1).

Figura 6-6-1

270. @Chiefs
271. @Packers
272. @ChicagoBears
273. @NFL
274. https://twitter.com/facebook
275. https://www.instagram.com/facebook/

El 15/2/2020 el mismo atacante vulneraba igualmente los accesos a Twitter de los perfiles del movimiento olímpico internacional[276], que tenía 6.1 millones de seguidores; y del Fútbol Club Barcelona[277], con 32 millones en ese momento. Desde ambos perfiles, el atacante emitía sus típicos mensajes reivindicativos (Figura 6-6-2); se da la circunstancia de que 'OurMine' ya hubo vulnerado la misma cuenta en Twitter del FC Barcelona el 23/8/2017.

Figura 6-6-2

Por otro lado, el 26/2/2020 la cuenta en Twitter[278] del Real Madrid Club de Fútbol, que tenía en aquel momento 33.7 millones de seguidores, emitía un par mensajes poco comunes (por ejemplo <<*@CR7Violador Esto es #RealFootball*>>, Figura 6-6-3) que sugerían que podría haber sido objeto de un acceso ilegal del tipo del descrito para la cuenta de Fútbol Club Barcelona por parte de '**OurMine**'. En este caso, no obstante, ni la empresa interesada confirmaba la posibilidad de un ciberataque ni los contenidos inyectados se ajustaron, en su momento, al patrón habitualmente desarrollado por 'OurMine'.

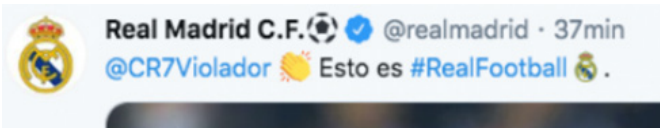


Figura 6-6-3

276. @olympics
277. @fcbarcelona
278. @RealMadrid

6.7 *Hacktivismo* en el contexto pandémico del Covid-19

Durante la pandemia del Covid-19 no se desplegó una reacción *hacktivista* específica en términos operativos de ciberataque en ningún país, más allá de la divulgación de contenidos digitales de tonalidad antisistema en redes sociales.

No obstante, el 8/4/2020 el portal internacional de información anarquista '**Anarchists Wordwide**' divulgaba un texto en inglés[279] en donde hacía un llamamiento para, en el contexto de la pandemia de Covid-19, "golpear al capitalismo en el ciberespacio, que es donde está estructurado" para compensar que no se pueden realizar "expropiaciones" (entiéndase robos) debido a que la mayoría de comercios están cerrados. En la misma línea sugerían la utilización de ransomware, denominándolo 'Covid-19', para llevar a cabo cibersabotajes en donde soliciten un rescate de 2 mil dólares por víctima, un 35% de los cuales irían a fondos para el apoyo a "prisioneros anarquistas". El texto proporcionaba una dirección de correo electrónico de contacto[280]. Con todo, ninguna acción operativa que respondiera a ese llamamiento fue reportada.

279. https://anarchistsworldwide.noblogs.org/post/2020/04/08/call-for-action-expropriationist-anarchy-in-crisis-times-ransomware-covid-19/
280. non.existant.comittee@elude.in

Adicionalmente, el 21/4/2020 se reivindicaba de manera genérica como '**Anonymous**' inicialmente a través de hilos en la plataforma 4chan[281], la exfitración al dominio público[282] de varios listados de credenciales de autenticación (usuario de correo electrónico y contraseña) correspondientes a dominios web del Centro de Control de Enfermedades[283] de EEUU, el sistema nacional de salud británico[284], la Organización Mundial de la Salud[285], el Banco Mundial[286], el Instituto de Virología de Wuhan en China[287], o la Fundación Gates[288]. En realidad, aunque la identidad '**Usa Hackers**' afirmaba[289] en aquel momento (Figura 6-7-1) ser nada más que el canal de difusión de la exfiltración, cuya autoría atribuía a una supuesta "milicia de extrema derecha" '**κατέχον**', se trataba de una reivindicación fraudulenta, puesto que los datos exfiltrados en ese momento se correspondían con una compilación de datos ya expuestos en brechas de seguridad masivas sobre distintas plataformas de servicios de Internet ocurridas principalmente en 2019, pero también en años anteriores[290]. Es decir, era un ejercicio desinformativo en el contexto de la pandemia del Covid-19, pretendiendo haber afectado a organizaciones representativas en la gestión de la crisis como la OMS o el instituto de Wuhan. Al menos durante doce horas tras su reivindicación, numerosos canales informativos sobre ciberseguridad le otorgaron crédito, ejerciendo el asunto su efecto desinformativo: incluso un medio de prensa global como el The Washington Post[291] dedicó una reseña al asunto titulando "Casi 25 mil direcciones de correo y contraseñas del NIH y de la Fundación Gates son divulgadas online".

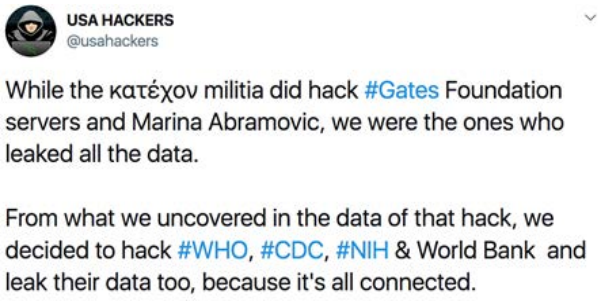


Figura 6-7-1

281. Por ejemplo https://boards.4chan.org/pol/thread/254429595
282. https://pastebin.com/egF5YNyd
283. http://archive.is/IyApN
284. http://archive.is/WkHpk
285. http://archive.is/MkhgD
286. http://archive.is/0XJEL
287. http://archive.is/UtQGz
288. http://archive.is/j6sgo
289. https://twitter.com/usahackers/status/1252653263280881664
290. Por ejemplo, la primera dirección de correo electrónico de la lista de Wuhan ya estaba en cuatro exfiltraciones previas (una sobre Linkedin) circulando en el dominio público entre 2016 y 2019; otra dirección escogida al azar de la lista de la Organización Mundial de la Salud constaba ya en tres exfiltraciones previas de 2019, una de ellas de la plataforma verifications.io.
291. https://www.washingtonpost.com/technology/2020/04/21/nearly-25000-email-addresses-passwords-allegedly-nih-who-gates-foundation-are-dumped-online/

6.8 Marcos narrativos *hacktivistas* en resto internacional

Las narrativas *hacktivistas* que convocaron a ciberataques durante 2020, en países en el ámbito internacional no mencionados en epígrafes dedicados a otras regiones en este informe, fueron:

Marcos narrativos *hacktivistas* en resto internacional 2020

País	Operación	Promotor	Tipo de Objetivo	Tipo de Acción	Resultado
PT	#Op25Abril	CyberTeam Portugal	Gobierno de Portugal	Desfiguración iSQL DDoS	Breves ataques ocasionales por denegación de servicio. Una iSQL defectuosa. Casi una decena de webs de gobierno desfiguradas.
USA	#OpFloyd	Nama Tikure x4Amon YourAnon Central	Instituciones de gobierno en Minneapolis, EEUU	DDoS Exfiltración Desfiguración iSQL	Una decena de DDoS sobre instituciones. Desfiguración de Senado de Minneapolis Divulgación de datos identificativos de funcionarios, así como #BlueLeaks con documentos de servicios policiales locales y regionales. Una iSQL sobre web universitaria.

Marcos narrativos *hacktivistas* en resto internacional 2020

País	Operación	Promotor	Tipo de Objetivo	Tipo de Acción	Resultado
RS	#OpSerbia	Lorian Synaro ElixirOP systemD	Instituciones de gobierno en Serbia	DDoS Desfiguración iSQL	Media docena de DDoS sobre instituciones de gobierno. iSQL sobre Ministerio de Educación. Desfiguración de subdominio de Ministerio de Energía, y de web de unidad contra blanqueo de capitales.
MY	#OpMalaysia	CyberWare Litemods	Instituciones de gobierno en Malasia	DDoS Desfiguración	Una desfiguración y un ataque DDoS sobre webs de gobierno.
NG	#OpNigeria	Lorian Synaro LiteMods systemD	Instituciones públicas en Nigeria	DDoS Desfiguración ISQL	Una decena de webs de gobierno desfiguradas. Media docena de iSQL sobre webs de gobierno. Una docena de ataques DDoS sobre webs de gobierno.
FR	#OpFrance	HackDown	Instituciones públicas de Francia	Sin ataques	No hubo desarrollo.

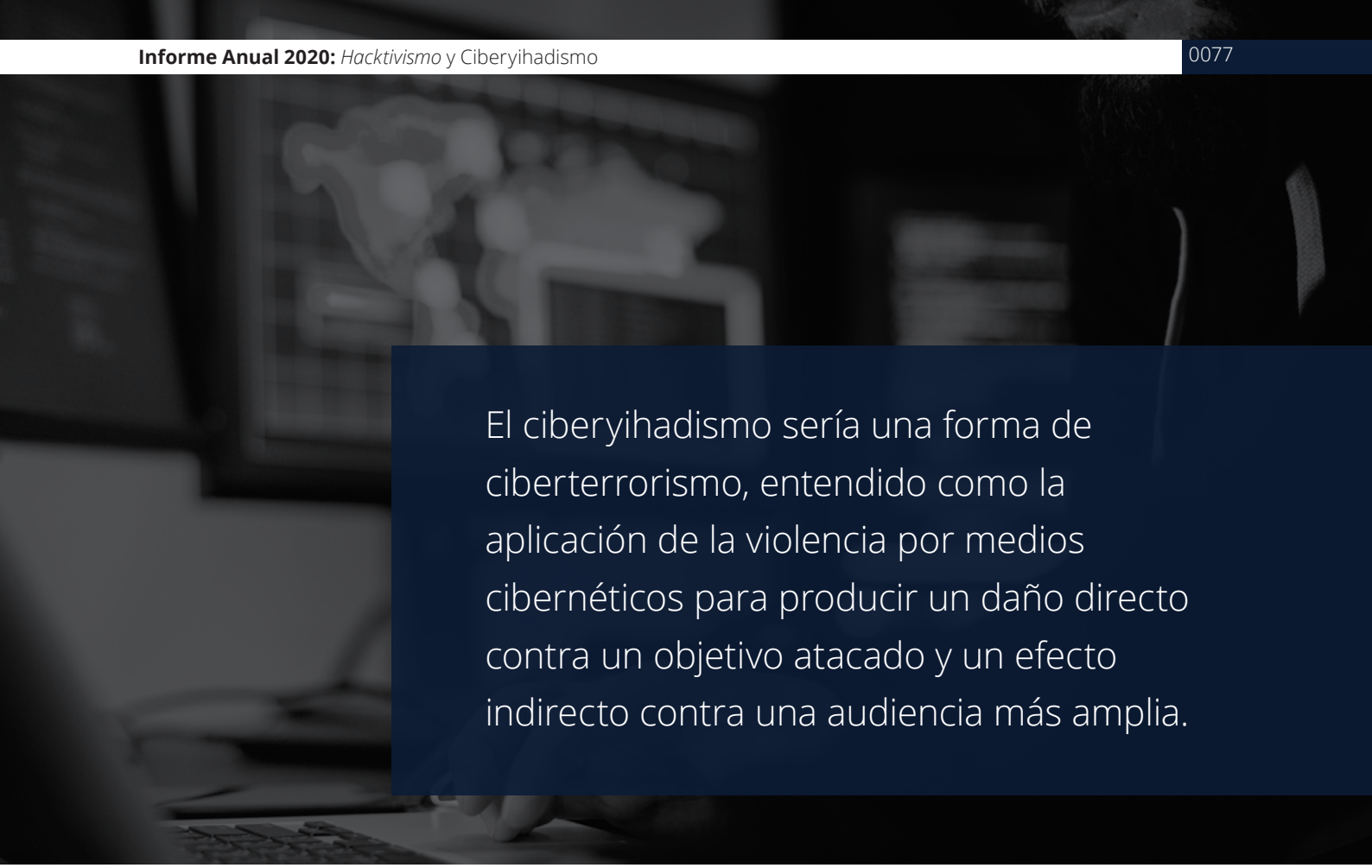
7. *Hacktivismo* proislamista o proyihadista

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.



El ciberyihadismo sería una forma de ciberterrorismo, entendido como la aplicación de la violencia por medios cibernéticos para producir un daño directo contra un objetivo atacado y un efecto indirecto contra una audiencia más amplia.

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 y 2019, durante 2020 no detectó ningún incidente que sea calificable de ciberyihadismo.

Así mismo, la información de incidentes cibernéticos durante 2020 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 para clasificar en el ámbito del ciberyihadismo sino del *hacktivismo*, de 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 y 2019 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 2020** esa pauta queda consolidada, con la **inactividad operativa de cualquier variante del 'Cibercalifato'** y con **la ausencia de incidentes significativos** siquiera clasificables netamente como "**hacktivismo proislamista**".

Dentro de esta pauta, los únicos incidentes que durante 2020 han inyectado en desfiguraciones de sitios web contenidos con alguna insinuación "islamista", en un sentido de provocación ocasional desprovista de motivaciones ideológicas, fueron dos:

01. El 8/1/2020 '**marwan 007**', que podría ser un alias del ya identificado como Behzad Mohammadzadeh en el capítulo de ciberataques sobre EEUU de este informe, inyectaba contenido reivindicativo general con el texto "*Islamic hacker*" y una imagen simbólicamente alusiva a la yihad (Figura 7-2-1) en la web privada[292] de una empresa educativa en Israel, que estaba desarrollada con Wordpress. No obstante, la utilización así mismo del texto <<*do not tell anyone that you got hacked that's very shame*>> sugería que el recurso por el atacante a contenido proyihadista no tenía intención ideológica sino meramente provocadora.

Figura 7-2-1

292. hagiva.org.il

02. El 3/9/2020 '**ifactoryx**' desfiguraba más de un millar de webs privadas[293] programadas con ASP.net –y ocasionalmente además utilizando Joomla- en Australia, inyectándoles en un fichero rx.html contenido (Figura 7-2-2) consistente en el símbolo de *Shahada*, que es la representación gráfica de la profesión de fe islámica. Aunque es un símbolo instrumentalizado maliciosamente por grupos yihadistas como el Daesh, la Shahada no es en sí misma más que un testimonio de adhesión religiosa al Islam. En el caso de 'ifactoryx', el escenario más plausible es que lo estuviera utilizando como provocación, pues es una identidad atacante con un largo historial de actividad que no aparece conducida por ningún tipo de ideología más allá del afán de notoriedad con la inyección de diversos tipos de contenidos.

Figura 7-2-2

Finalmente, en este panorama de desactivación operativa de identidades que instrumentan provocativamente sobrenombres que intentan apropiarse de variantes del término 'Cibercalifato', al igual que ya hiciera en algunas ocasiones previas, en abril y junio de 2020 la identidad '**Caliphate Cyber Shield**' circulaba vídeos de autopropaganda mostrando capturas de pantalla supuestamente acreditativas de vulneraciones de acceso a diversas webs de baja visibilidad en varias partes del mundo[294] (por ejemplo Figura 7-2-3), sin acreditar las acciones y probablemente refiriéndose a antiguas desfiguraciones llevadas a cabo por atacantes con intenciones provocadoras.

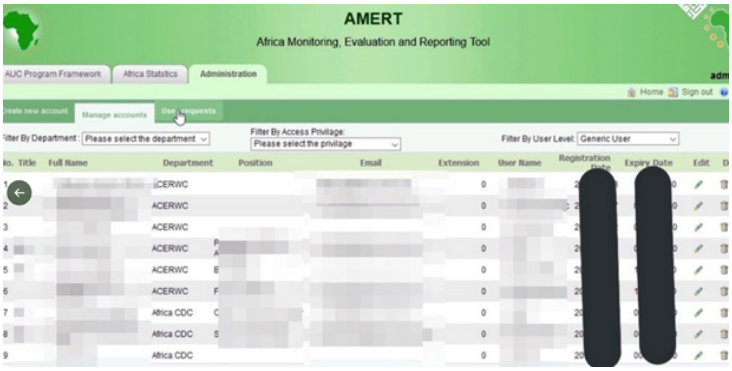


Figura 7-2-3

293. Entre ellas stockinettebags.com.au, pathwayswa.org.au
294. Por ejemplo amert.org en África o la Hermandad de Policías de Nueva Jersey en EEUU (njlepba.com)

8. Tendencias 2021-2022

+ Continuidad de '**Anonymous**' como **fenómeno de propaganda testimonial en contenidos digitales difundidos por redes sociales**, sin actividad operativa más allá de la apropiación iconográfica que algunos atacantes hagan de su simbología para desfigurar sitios web vulnerables o para proferir ciberamenazas de baja peligrosidad.

+ Consolidación del ***hacktivismo*** en un fenómeno desideologizado y concentrado en acoger la **actividad de un conjunto menor de identidades que actúan por motivaciones egocéntricas** y afán de notoriedad para acumular seguimiento en redes sociales.

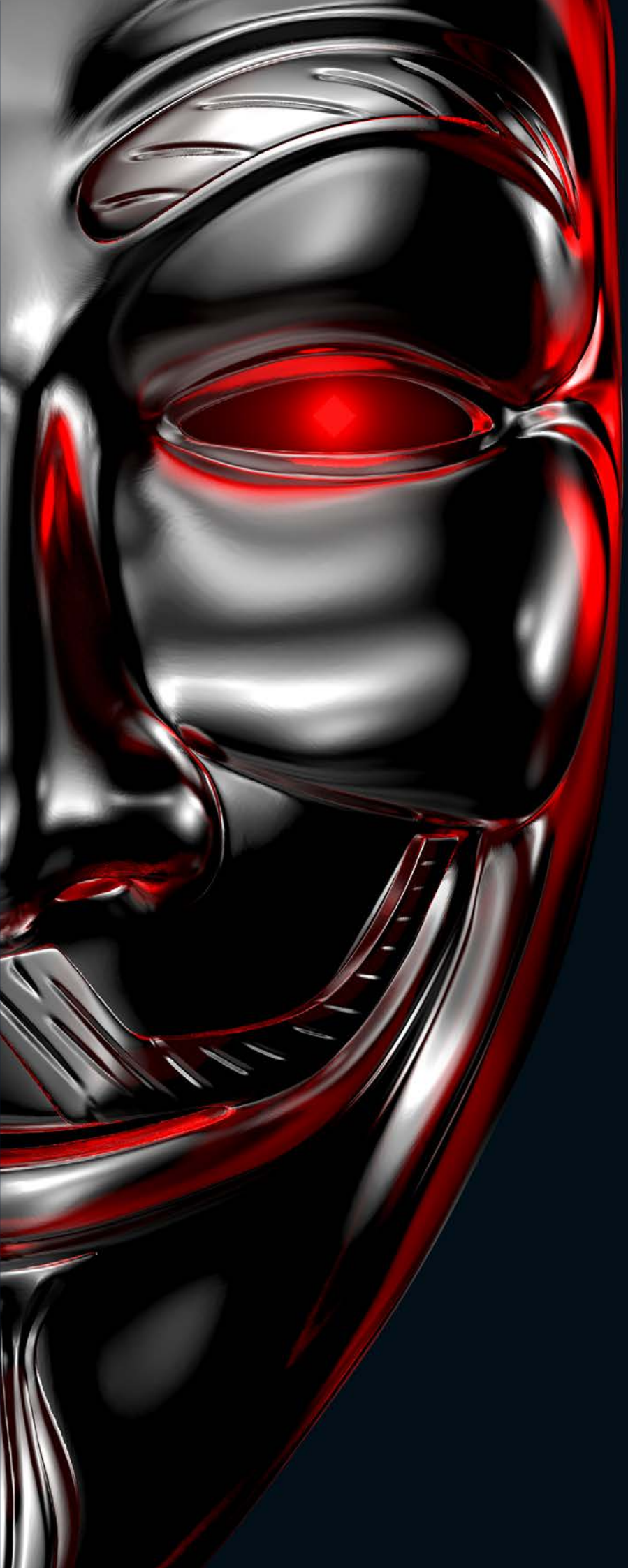
+ **Debilidad, desorganización, escasa peligrosidad técnica, baja colectivización e impacto menor** en el intento de un grupo de identidades, generalmente las mismas en torno a una decena, de **organizar protestas *hacktivistas*** en forma de ciberataques cibernéticos en paralelo a protestas sociales en varios países. Ocasionalmente alguna identidad *hacktivista* dotada de mejores habilidades técnicas podría tomar parte en esos marcos narrativos de protesta *hacktivista* con algún ataque de mayor impacto, ya sea por algún motivador ideológico coyuntural, por afán de notoriedad, o para enmascarar alguna actividad cibercriminal subyacente.

+ La actividad de **identidades individuales de peligrosidad moderada o alta, movidas por razones ideológicas antisistema**, y dotadas de suficientes capacidades técnicas como para llevar a cabo ciberataques por penetración sobre servidores web de significación nacional o internacional, con el propósito de inscribir esos ciberataques en un *hacktivismo* militante y de protesta, continuará siendo muy esporádica y limitada **a menos de media docena de atacantes en el mundo**.

- En un panorama general de *hacktivismo* oportunista de motivación egocéntrica, continuarán **creciendo en número los ciberataques a servidores webs que intenten enmascarar con una firma hacktivista intereses cibercriminales de lucro personal**, traducidos a través de prácticas de *SEO Spam*, inyección de scripts redirectores de tráfico o de distribución de *malware*, o inserción de estructuras dedicadas al *phishing*. Tampoco es descartable que, según cada coyuntura de intereses geopolíticos, ciberamenazas persistentes avanzadas al servicio de Estados puedan adoptar falsos roles, tácticas, técnicas y procedimientos *hacktivistas* para llevar a cabo ciberataques puntuales.

- Los ciberataques *hacktivistas* tendrán en **la explotación de vulnerabilidades en sitios web provistos de software desactualizado** su principal **vector de ciberataque**.

- El denominado "**ciberyihadismo**" tiene probabilidad de continuar siendo un **fenómeno inexistente**, parasitado instrumentalmente en sus símbolos y semánticas por identidades provocadoras, o por otras **intenciones de falsa bandera**.



CCN
centro criptológico nacional

CCN-CERT
centro criptológico nacional