GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

CCN-CERT
centro criptológico nacional

HACKTIVISMO Y CIBERYIHADISMO

Informe Anual 2021

CCN-CERT IA-03/22
USO OFICIAL

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2022.05.18 20:52:46 +02'00'

Fecha de Edición: mayo de 2022

ÍNDICE

01
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.

02
RESUMEN EJECUTIVO

En 2021 se ha consolidado la tendencia, documentada en años previos, de una derivación del **hacktivismo ideológico de aspiraciones colectivas hacia un hacktivismo vandálico individualista** que, haciendo una explotación oportunista de vulnerabilidades de código informático, desfigura sitios web por todo el mundo para inyectar sobre ellos contenidos autorreferenciados al atacante.

Este tipo de hacktivismo oportunista que se ha instalado en paralelo a la paulatina desaparición efectiva del hacktivismo que, en el pasado, se adscribía al colectivo 'Anonymous', correlaciona cada vez en mayor medida con la implicación de los atacantes en **fases preparatorias de la diseminación de código dañino y contenidos maliciosos o no deseados**. Esta propagación de código dañino se inscribe mundialmente en la actividad de ciberamenazas organizadas. Esa organización comporta una periferia de actuaciones en donde participan numerosas identidades individuales que aportan funciones instrumentales y que, sin pertenecer a la infraestructura orgánica de las ciberamenazas avanzadas, realizan tareas preparatorias de las tácticas, técnicas y procedimientos de esas ciberamenazas organizadas.

De este modo, un porcentaje de identidades que ocasionalmente llevan a cabo ciberataques hacktivistas reivindicativos, también participa como identidades instrumentales con tareas preparatorias de esa secuencia de las ciberamenazas organizadas. Ese porcentaje está creciendo desde hace tres años.

El ejemplo más evidente de esta intersección entre hacktivismo y las fases preparatorias de la diseminación de código dañino para servir a ciberamenazas avanzadas, lo refleja cómo miles de **desfiguraciones mensuales por todo el mundo**, comprometiendo sitios web provistos de software vulnerable, sirven para **articulan toda una malla de sitios web donde puede plantarse código dañino** para servir de infraestructura para su propagación. Está acreditado[1], por ejemplo, que el envenenamiento de procesos de optimización de búsquedas en web (SEO) se utiliza como técnica sistemática por ciberamenazas organizadas para generar y mantener infraestructuras de propagación de código informático dañino (malware).

[1] Entre otras fuentes, https://news.sophos.com/en-us/2021/03/01/gootloader-expands-its-payload-delivery-options/, https://www.godaddy.com/garage/godaddy-small-business-website-security-report/, https://www.welivesecurity.com/la-es/2021/08/11/iiserpent-malware-para-realizar-fraude-seo-como-servicio/, http://blog.talosintelligence.com/2017/11/zeus-panda-campaign.html, https://news.sophos.com/en-us/2022/02/01/solarmarker-campaign-used-novel-registry-changes-to-establish-persistence/

Durante 2021 y dependiendo del momento y de las regiones del mundo, **entre un 10% y un 30%** de las **desfiguraciones de sitios web** por parte de atacantes con rasgos hacktivistas, ha **correlacionado con estas prácticas de intoxicación SEO o de inserción de código software malicioso** redireccionando tráfico de visitas desde las webs comprometidas hacia infraestructuras de diseminación de código informático no deseado o dañino.

Tanto en España como en el resto del mundo, los ataques por desfiguración, que han venido siendo la principal técnica hacktivista, mantienen una **senda contenida y descendente en volumetría, pero ascendente en peligrosidad**. Aunque la cantidad de acciones hacktivistas disminuye moderadamente a nivel mundial, principalmente debido a la descomposición del tejido hacktivista, la peligrosidad de los ciberataques por desfiguración de webs aumenta debido al incremento en el porcentaje en que las webs victimizadas están siendo instrumentados como tácticas en secuencias iniciales o preparatorias de propagación de código dañino o de contenidos no deseados. **Un número de webs vulneradas mediante desfiguraciones pasa a formar parte de infraestructura de diseminación de malware**.

Del mismo modo, en todas las regiones mundiales se mantiene una **correlación muy significativa entre los ataques por desfiguración de sitios web y la presencia de software desactualizado en esas webs**. La coincidencia entre la victimización de sitios web y la presencia de software WordPress desactualizado continúa siendo la mayoritaria, seguida por software Microsoft desactualizado (ASP.net, DotNetNuke, SharePoint o servidores IIS), que en 2021 ha relegado a la tercera posición a las webs provistas de versiones desactualizada de software Joomla.

En lo que respecta a las características de perfilado de las identidades atacantes, en España continuaba rigiendo en 2021 el mismo patrón que para el resto del mundo: **individualidades atacantes**, ocasionalmente agrupadas en pequeños grupos de menos de media docena, con capacidades técnicas para ejecutar **ataques procedimentados para la explotación de vulnerabilidades** comunes de código informático, en la gran mayoría de los casos sin motivación ideológica e impulsados por el afán de notoriedad o, en el caso de las ciberamenazas que participan en la diseminación de código dañino o contenidos no deseados, el ánimo de lucro. En esos pequeños agrupamientos de ciberatacantes, a la manera de "bandas cibernéticas", Brasil, Turquía, o Indonesia continúan siendo los países respecto de los cuales estas bandas muestran rasgos identificativos de probable origen.

El colectivo hacktivista 'Anonymous', antaño aglutinante de la militancia hacktivista en numerosos países, está tan ausente en España como inexistente es en términos operativos en la mayoría del mundo, quedando reducido a expresiones narrativas o iconográficas testimoniales en redes sociales, que en ocasiones profieren amenazas que no se materializan o falsifican acciones que no han llevado a cabo.

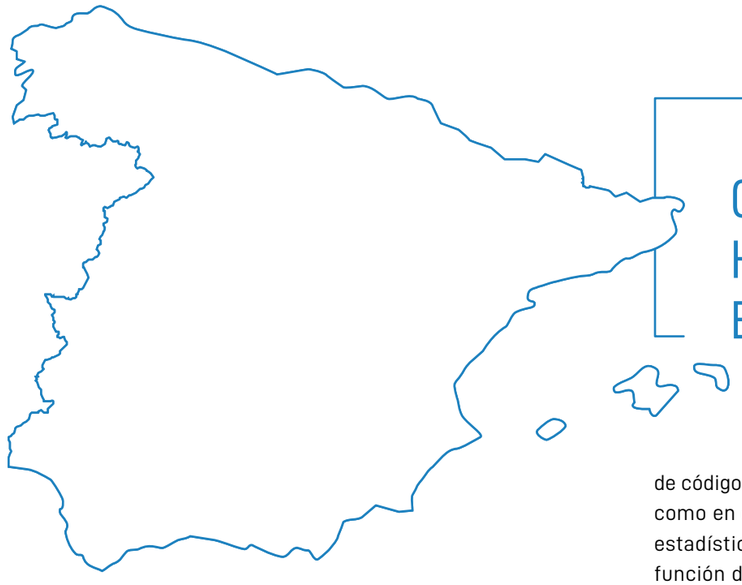
Al igual que el año precedente, durante 2021 en el perfil predominante de webs victimizadas han continuado destacando las webs privadas de personas o pequeños negocios, provistas de software desactualizado, que muchas veces son comprometidas en oleadas en varios países buscando los atacantes sitios web expuestos a la misma vulnerabilidad.

Este perfil es el habitual en los países europeos. 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 continúa siendo especialmente visible en algunos países de Iberoamérica (principalmente Brasil, Perú y México), en Oriente Medio y en Asia. En tercer lugar, en 2021 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 este escenario de un hacktivismo vandálico individualista dedicado preferentemente a la desfiguración oportunista de webs vulnerables, conviven un **número mínimo de identidades atacantes muy ideologizadas** que llevan a cabo acciones ofensivas selectivas y ocasionales contra sistemas informáticos conectados a Internet. Esta clase de atacantes está técnicamente más capacitada, y puede ejecutar ciberataques de mayor peligrosidad en cualquier momento y localización donde encuentren una oportunidad y un objetivo factible que victimizar, buscando producir el mayor impacto en la opinión pública. Durante 2021 la actividad de este tipo de atacantes ha sido **anecdótica**.

Finalmente, y reiterando lo advertido en informes previos, conviene acabar precisando que, aunque el hacktivismo vandálico 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**. Esto se debe a que, 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, continúa constatándose la **inexistencia de una fenomenología netamente ciberyihadista**. Lo que muchas veces se cataloga de ciberyihadismo, erróneamente en función de la evidencia empírica, es en realidad un **hacktivismo de falsa bandera** que utiliza simbología proislamista como una impostura tanto para provocar o alcanzar notoriedad, como para disfrazar la participación de ciertas identidades atacantes en acciones por desfiguración sobre sitios web para convertirlos en parte de infraestructuras de diseminación de contenidos no deseados o de código dañino.



03 HACKTIVISMO EN ESPAÑA

3.1. Estructura hacktivista en España

3.1.1. Perfilado genérico de las identidades en 2021

Las características del hacktivismo autóctono en España durante 2021 no han mostrado diferencias respecto al año anterior y, en general, la última media década. En resumidas cuentas, en España no opera un tejido hacktivista propiamente originado en el país, más allá de una mínima actividad de propaganda en redes sociales por parte de identidades que utilizan iconografía hacktivista. La única excepción en este escenario de carencia de hacktivismo de raíz española es la identidad conocida como '**La 9ª Compañía**' o '**La9deAnon**' que, no obstante, viene desarrollando una actividad de ciberataques que lleva declinando hacia la ocasionalidad desde 2018.

Esta ausencia de un hacktivismo propiamente español no implica que el ciberespacio de España esté libre de ciberataques llevados a cabo por identidades cuyas actividades podrían encuadrarse, aunque sea parcialmente, en la órbita del hacktivismo. Por el contrario, España se encuadra en el común de los países de cualquier continente, en el sentido de que sitios web con dominio y/o dirección IP residente en su ciberespacio son atacados mediante acciones por penetración y desfiguración, llevadas a cabo por atacantes de varias procedencias geográficas, que suelen explotar vulnerabilidades comunes en software desactualizado para ejecutar desfiguraciones en serie o en masa sobre webs en varios países. Este tipo de hacktivismo de oportunidad, cada vez más intersectado con prácticas en la secuencia inicial de ciberamenazas para la propagación de código dañino, ha sido tan corriente en España en 2021 como en el resto de los países del mundo, variando las estadísticas mensuales y geográficas en cada caso en función de la coyuntura de los atacantes para explotar vulnerabilidades de software allá donde las encuentren.

Si bien el año previo se produjeron algunas acciones menores de ciberataque adscribiéndolas a los marcos narrativos hacktivistas latentes de la #OpSpain o la #OpCatalunya, en 2021 ambos referentes de militancia hacktivista han estado desprovistos de actividad ciberofensiva, limitándose a algunas menciones esporádicas de esas etiquetas en mensajes en redes sociales, de naturaleza individual y sin pauta de colectivización, y además desprovistas de semántica amenazante explícita.

Por tanto, durante 2021 se repite el perfilado genérico del hacktivismo en España que viene decantándose desde años previos, configurado por:

1. Práctica inexistencia de identidades hacktivistas autóctonas, mientras webs en España forman parte de las comúnmente atacadas en cualquier país por identidades operando en base a criterios de oportunidad basados en la explotación de vulnerabilidades comunes de software.

2. Un par de identidades hacktivistas activas en España que puedan hipotetizarse como originarias del país: '**La 9ª Compañía**', una ciberamenaza centrada en la técnica y el método, es decir, provista con suficientes habilidades técnicas informáticas como para producir ciberataques por penetración de servidores web expuestos a vulnerabilidades de software, utilizando para ello herramientas a su conveniencia; y '**jibar0**', de cuyo historial hacktivista se deduce una capacitación técnica entre baja y moderada, correspondiéndose con una ciberamenaza centrada en el uso de herramientas, es decir, que puede utilizar algunas herramientas básicas de explotación de vulnerabilidades de software, pero no tiene habilidad ni conocimientos informáticos suficientes como para desarrollar técnicas de ciberataque basadas en la generación o manipulación manual de código software, debiéndose apoyar para ello, a modo de cualquier usuario, en herramientas de terceros, generalmente de software libre.

3. Ausencia o inactividad de marcos narrativos militantes que promuevan hacktivismo en España, así como indigencia de cualquier discurso con intención hacktivista.

4. Salvando algunos intentos puntuales que por el momento no han logrado impacto[2], descomposición de cualquier base organizada de propaganda hacktivista que pudiera animar a la revitalización de un tejido hacktivista agotado desde el primer tercio de la década de 2010.

Esta serie de características del hacktivismo en España durante 2021 da lugar a una ciberamenaza general ocasional y de baja peligrosidad, con tres excepciones:

A) Alguna identidad autóctona conocida –'La 9ª Compañía'- o desconocida que lleve a cabo un ciberataque de mayor impacto, comprometiendo algún servidor web y exponiendo información sensible.

B) Alguna ciberamenaza hacktivista procedente del exterior de España, provista de habilidades técnicas por encima de la media, y que se fije en España como objetivo para atacar un servidor web con el propósito de publicitar una acción hacktivista de impacto.

C) Alguna ciberamenaza avanzada del exterior de España que ejecute un ataque contra un recurso informático público o privado de importancia, y que reivindique esa acción en un procedimiento de "falsa bandera", es decir, disfrazando el ataque con propósito hacktivista cuando, en realidad, el propósito de la ciberamenaza es otro (geopolítico, ánimo de lucro, híbrido).

[2] Por ejemplo, el proyecto sataniccat.com

3.2. Campañas y ciberataques hacktivistas en España

3.2.1. #OpCatalunya, #OpCatalonia, #OpSpain

Durante 2020 había en España tres marcos narrativos hacktivistas, herederos de mayor o menor actividad de años previos, establecidos para justificar propaganda y acciones de ciberataque hacktivista: **#OpSpain**, que es una etiqueta genérica y recurrente que sirve como banderín de enganche instrumental para cualquier protesta hacktivista que pudiera producirse en España; **#OpCatalunya**/#OpCatalonia, una etiqueta que identidades hacktivistas comenzaron a utilizar en el último trimestre de 2017 en paralelo al incremento entonces de la tensión política en torno a Cataluña; y **#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 este contexto, mientras en 2020 se adscribieron 32 ciberataques de baja entidad principalmente a los dos primeros de esos marcos narrativos, en 2021 no se produjo ninguna acción ciberofensiva contra sistemas informáticos que se reivindicara a través de esas etiquetas hacktivistas.

La actividad de propaganda utilizando cualquiera de las denominaciones #OpSpain, #OpCatalunya o #FreeXelj fue menor también en 2021, limitándose a menciones ocasionales en redes sociales, con nula o baja colectivización, esencialmente en el caso de actividad militante contra el encausamiento judicial de 'Xelj', y sin constituir una propuesta mínimamente organizada de hacktivismo.

3.2.2. jibar0

El 20/11/2021 la identidad '**jibar0**', una identidad probablemente originaria de España pero que podría residir fuera del país, publicaba[3] un mensaje en Mastodon anunciando su retorno al hacktivismo (Figura 3-2-2-1).

Figura 3-2-2-1

'jibar0' es un alias que se correspondería con la denominación de '**Anon_Jibaro**', que estuvo presente en el conjunto de identidades que orbitaba acerca de la posibilidad, luego no fructificada, de intentos de una tercera reconstitución de la facción 'OpSpain' de 'Anonymous' en España a finales de 2012 y durante 2013, después de dos operaciones policiales de desarticulación de las anteriores facciones. También habría empleado en el pasado el alias '**cl4nd3stin0**'[4]. En aquellos primeros compases intervino en actividades de propaganda hacktivista (por ejemplo, Figura 3-2-2-2).

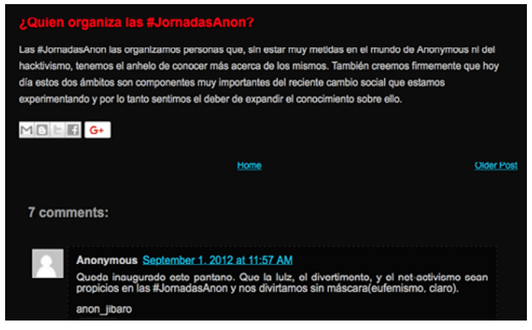
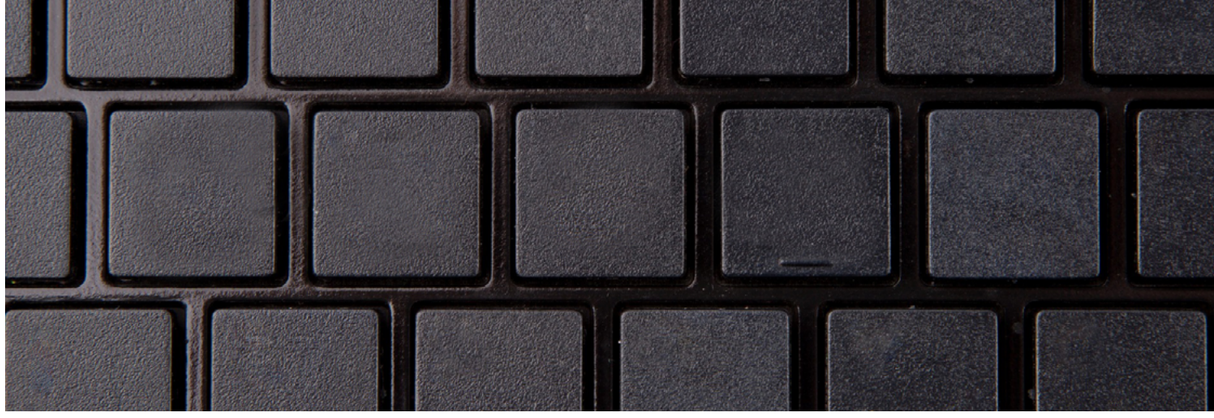


Figura 3-2-2-2

Durante al menos sus seis primeros años de militancia hacktivista no mostró implicación, al menos en abierto, en actividades ciberofensivas, más allá, por ejemplo, de animar ataques por denegación de servicio en las primeras fases de la #OpCatalunya en 2017 (por ejemplo, Figura 3-2-2-3).

Figura 3-2-2-3

[3] https://mastodon.social/@jibar0/107310651104786821
[4] http://cl4nd3stin0.tumblr.com



Ya en 2018 mostraba en Twitter capturas de pantalla que sugerían que había logrado accesos ilegítimos a varios sitios web[5], sin que divulgara entonces evidencia de que hubiera realizado ninguna modificación forzada en las webs, más allá de los accesos.

En su declarado regreso al hacktivismo en noviembre de 2021, situaba en el dominio público[6] un listado de datos personales identificativos con formato de volcado de base de datos conteniendo los campos de nombre y apellidos y dirección de correo electrónico, sin contraseña, provincia española, y en algunos casos número de teléfono móvil con formato de España. En un mensaje[7], la identidad afirmaba que los datos se correspondían con 30.107 suscriptores del partido político Vox. Tras ser analizados, se constata que los datos tienen la misma fisonomía que los sustraídos por '**La 9ª Compañía'** en un ciberataque reivindicado por esta identidad en diciembre de 2018 sobre una web de Vox[8].

En los últimos dos meses de 2021, 'jibar0' publicaba varios mensajes[9] en Mastodon, sin divulgar información sensible, sugiriendo haber logrado acceso forzado al foro Todopolicía[10]; haber aplicado con éxito una inyección SQL, y logrado acceso ilegítimo, sobre la web[11] de la Asociación de Empresas de Transporte de Cantabria; o advirtiendo de que el Hospital Central Universitario de Asturias (HUCA) estaría expuesto a <<una vulnerabilidad crítica en uno de sus sistemas que deja al descubierto las comunicaciones de citas a sus usuarios>>.

[5] Conferencia de Rectores de Universidades Españolas, Asociación de Militares Españoles, Colegio de Procuradores de Madrid, Sociedad General de Autores y Editores
[6] https://share.riseup.net/#Z_s5UNkGYgiyF5dE4b26Dg
[7] https://mastodon.social/@jibar0/107311147464988682
[8] voxespana.com
[9] https://mastodon.social/@jibar0/107344790672988211, https://mastodon.social/@jibar0/107344871374238019, https://mastodon.social/@jibar0/107610784599871586
[10] todopolicia.com
[11] asemtrasan.com
[12] https://ia801507.us.archive.org/18/items/codigo-fuente-t-1-e-10-con-la-9de-anon/Codigo%20Fuente%20-%20T1E10%20con%20La9deAnon.mp3

3.2.3. La 9ª Compañía de Anonymous / La9deAnon

'**La9deAnon**' o 'La 9ª Compañía de Anonymous' lleva desde 2019 marcando una trayectoria de descenso anual de su desempeño hacktivista. Si en 2018 finalizaba con un promedio de un ciberataque mensual, los años siguientes iba reduciendo en tercios progresivos su volumen de actividad, hasta quedarse en 2020 con una sola acción reivindicada. Ese mismo único ciberataque anual ha sido la tasa de visibilidad ciberofensiva que 'La 9ª Compañía' ha mantenido durante 2021.

En cuanto a su actividad militante de propaganda, si bien en el último trimestre de 2016 se habían marcado del objetivo de "mantener y ampliar el plano ideológico", en paralelo a una mayor selectividad de sus acciones, su comunicación al exterior, esencialmente a través de sus canales en Tumblr y Mastodon, ha disminuido también sensiblemente desde 2020.

En este apartado de las narrativas hacktivistas, no obstante, en agosto de 2021 se divulgaba[12] una entrevista de audio que el espacio de radio digital sobre temas informáticos Código Fuente le hacía a 'La 9ª Compañía'. En la entrevista (Figura 3-2-3-1), de unos quince minutos de duración, la identidad hacktivista respondía en texto transcrito a audio mediante software de voz. El contenido no es relevante a efectos de aportar elementos identificadores ni de la identidad ni de su actividad hacktivista, y versa en general sobre cuestiones ideológicas, donde la 'La 9ª Compañía' reitera sus ya conocidos postulados libertarios, antisistema y anticapitalistas como motivadores de su actividad.

Figura 3-2-3-1

En un momento de la entrevista (minuto 9'15'') en la que está nombrando empresas o instituciones victimizadas por sus ciberataques, 'La 9ª Compañía' se adjudica una acción contra el Sindicato de los Mossos d'Esquadra; no obstante, ese ataque, ocurrido en mayo de 2016, fue entonces reivindicado[13] por la identidad '**Phineas Fisher**'. Inicialmente, salvo información que sugiera otra interpretación, esta auto-adjudicación por 'La 9ª Compañía' podría entenderse, en un escenario más probable, como formando parte de una distracción, enmarcada en el "espíritu juguetón" que 'La 9ª Compañía' considera parte de sus tácticas, técnicas y procedimientos. Esta distracción implicaría además un reconocimiento mutuo entre dos identidades, 'La 9ª Compañía' y 'Phineas Fisher', que tienen muchos elementos en común tanto ideológica como técnicamente. Respecto a la posibilidad de que ambas identidades sean máscaras del mismo o los mismos atacantes, ninguna evidencia la sugiere, de momento.

En cuanto al ciberataque llevado a cabo por 'La 9ª Compañía', se dirigía el 2/11/2021 a victimizar el sitio web de la edición de 2021 de la FEINDEF[14], la Feria Internacional de Defensa y Seguridad que se celebraba en Madrid entre el 3 y 5 de noviembre. Como evidencia del comprometimiento del sitio web, el atacante divulgaba capturas de pantalla (Figura 3-2-3-2) de usuarios de la web supuestamente comprometida, donde censuraba las contraseñas; y de contactos de asistentes a la feria, con muestras de mensajes intercambiados entre ellos o de proyectos presentados a la feria.

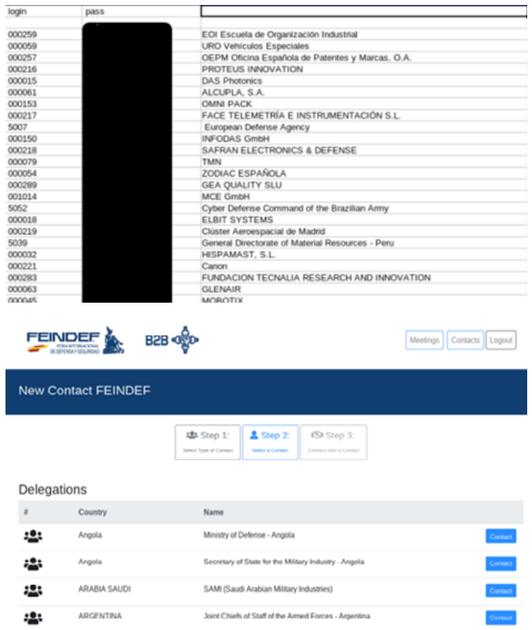


Figura 3-2-3-2

El texto reivindicativo no aportaba más información, terminando con una proclama militante: <<este es un evento de compra y venta de materiales para masacrar a poblaciones enteras e individuos concretos si es necesario. Y se lleva a cabo en la capital del reino, en el famoso recinto ferial del IFEMA que, si echáis un vistazo rápido en Wikipedia, está formado por la Comunidad de Madrid (31%), el Ayuntamiento de Madrid (31%), la Cámara de Comercio (31%) y la Fundación Montemadrid (7%). Congrega a numerosos ministros de defensa y a multitud de empresas de muerte con fondos públicos que financian nuestros impuestos y, más especialmente, los impuestos de las vecinas de Madrid>>[15].

Aunque el atacante no describía el método mediante el cual produjo el comprometimiento de la web de FEINDEF, en varios mensajes subsiguientes insinuaba que tanto el software de gestión del servidor Apache[16] como el sistema operativo Windows[17] del servidor estaban desactualizados, además de afirmar que la web almacenaba en texto en claro[18] las contraseñas de autenticación de usuarios.

[13] A través de https://pastebin.com/keMTZYGZ, no disponible actualmente, pero transcrito en https://www.wifi-libre.com/topic-551-hackeando-el-sindicato-de-los-mossos-d-esquadra-sme.html
[14] feindef.com
[15] https://la9deanon.tumblr.com/post/666759745649164288/invitadas-entrella-en-la-feindef21
[16] https://mastodon.social/@la9deanon/107213158525737355
[17] https://mastodon.social/@la9deanon/107213153830209970
[18] https://mastodon.social/@la9deanon/107212974008542627

3.2.4. Ciberataques por entidades externas a España

Durante 2021 continuaba la tendencia instalada desde hace varios años de comprometimiento mediante desfiguraciones de sitios web con dirección IP o nombre de dominio radicados en España, como parte de acciones de ciberataque llevadas a cabo por identidades actuando desde el exterior de España sobre webs en cualquier parte del mundo, que tienen en común exponer algún tipo de vulnerabilidad en el software instalado.

En ese sentido, España no ha constituido un foco diferencial o específico de ofensiva hacktivista en comparación con otros países, sino una porción más del ciberespacio mundial donde residen webs que son detectadas como vulnerables a un ciberataque por parte de identidades que escanean Internet localizando fallos de software comunes para explotarlos en **ciberataques de oportunidad**, desfigurándolas para inyectar contenido militante generalmente autorreferenciado al propio atacante.

Del mismo modo, en 2021 se consolidaba un patrón, que venía conformándose desde 2020, de aprovechamiento de ataques hacktivistas de desfiguración de sitios webs para la inyección, en las webs victimizadas, de contenidos de intoxicación de resultados de motores de búsqueda (práctica conocida como envenenamiento SEO, de Search Engine Optimization), de scripts redirectores de tráfico hacia webs de distribución de contenidos maliciosos, o de inserción o redireccionamiento hacia contenidos simulando entornos de comercio electrónico que, en realidad, son trampas de phishing para el robo de datos personales identificativos y de pago con tarjeta bancaria o servicios financieros digitales.

Este patrón es mundial y se manifiesta en España como en el resto de los países, con las diferencias mensuales de volumen de webs atacadas y de geografías que son inherentes a los ciberataques de oportunidad. En semejante pauta de actuación, identidades atacantes que ejercen militancia hacktivista en otros contextos, dedican una parte porcentual de sus ciberataques por desfiguración a actividades preparatorias de ciberamenazas para la propagación de código dañino, como son el envenenamiento SEO y la inserción de scripts redirectores de tráfico. Durante 2021 en España identidades que han mostrado esa doble dedicación han sido, entre otras, las probablemente turcas '**Fajar Ganz**', '**Rayzky**' o '**Aslan Neferler Tim**', que igual que se involucran en envenenamiento SEO participan con desfiguraciones militantes sobre webs en el contexto de la #OpIsrael, por ejemplo; o la probablemente iberoamericana '**Crystal_MSF**', que igual disemina contenidos de intoxicación SEO que participa en desfiguraciones militantes para la #OpColombia.

Es previsible que, al igual que el antiguo hacktivismo ha ido solapándose desde 2020 con estas prácticas preparatorias de ciberamenazas organizadas, una parte de esa actividad vaya implicando, así mismo y progresivamente, la diseminación de código dañino tipo troyano. Este último vector es todavía incipiente en el panorama hacktivista mundial y, aunque todavía no ha sido observado en España, durante 2021 ya se ha documentado un caso de diseminación de código dañino tipo troyano a través de la desfiguración de una web en Libia, y durante el primer trimestre de 2022 se han registrado ya otros dos incidentes en Honduras y Macedonia.

En lo que tiene que ver con ciberataques de oportunidad por desfiguración de webs con IP o dominio en España, llevados a cabo por identidades que se suponen actuando principalmente desde el exterior de España, durante 2021 se produjeron 580 de estas acciones, que representan un 20% menos que el año anterior.

Las comparaciones interanuales, no obstante, son relativas, pues la volumetría de ataques se cuantifica por el número total de webs afectadas durante un año. Ese número de webs puede cambiar sustancialmente en la estadística de un año concreto si en una oleada de ciberataque, por

ejemplo, un atacante ha encontrado una vulnerabilidad que puede explotar en masa en quinientas o un millar de webs, y resulta que un escaneo sobre webs en España revela que, en ese ciberespacio, reside ese millar de webs del ejemplo. Esta posibilidad de llevar a cabo desfiguraciones en masa, que los atacantes desarrollan a través de scripts más o menos automatizados una vez han detectado vulnerabilidades explotables en webs concretas, puede generar en algunos años picos mensuales de ciberataques que abultan el total de la estadística anual, pero que no son representativos de la actividad promedio.

Tal como se refleja en la figura 3-2-4-1, el comportamiento de las curvas anuales muestra varios picos de oleadas de ciberataques, con dos evidentes en 2018 (línea verde) en enero y mayo; otros tres en enero, agosto y diciembre en 2019 (línea amarilla); y otro en noviembre de 2020 (línea roja); mientras que en 2021 los ataques se han ajustado a una línea anual más suavizada (línea gris gruesa), con un incremento puntual en junio (se aprecia mejor en la figura 3-2-4-2), pero sin altibajos destacables a lo largo del año. De hecho, por tanto, si se obviaran los picos extremos, los promedios volumétricos mensuales parecerían bastante similares interanualmente.

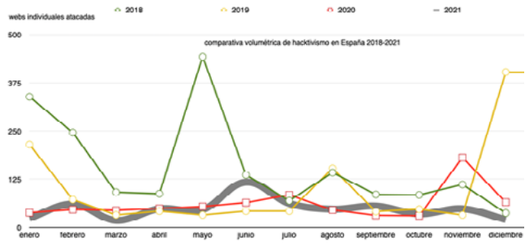


Figura 3-2-4-1

La línea promedio (línea negra punteada, figura 3-2-4-2) de los ataques por desfiguración recibidos sobre sitios web con dirección IP o dominio en España se mantuvo, durante 2021, por encima de las 45 acciones mensuales. En ese sentido, es similar a la tendencia de 2020 y 2019, ambas por debajo de 2018, siendo un indicador coherente con el descenso en la volumetría de las acciones desde 2018, es decir, en el número de webs individuales vulneradas cada año.

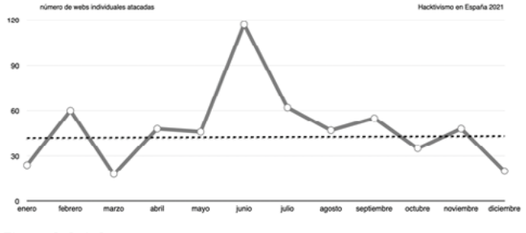


Figura 3-2-4-2

Continuando la tendencia de los años previos, los ataques hacktivistas en 2021 correlacionaron en un **81%** (un descenso de diez puntos en comparación con los dos años previos) **con que se detectara presencia de software vulnerable y/o desactualizado en las webs atacadas**. Aunque este dato haya disminuido con respecto a los años anteriores, continúa siendo claramente definitorio, pues implica que 8 de cada 10 webs victimizadas por desfiguraciones en 2021 presentaban algún tipo de fallo de seguridad en el software, circunstancia que continúa siendo **el primer factor de riesgo para la victimización por hacktivismo**.

En la práctica totalidad de estas webs desfiguradas en 2021, los atacantes no inyectaban contenido reivindicativo con carga ideológica, sino meramente sus alias o menciones autorreferenciadas, como si se tratara de la firma de un grafiti en un acto vandálico, en este caso de **cibervandalismo**.

De ese porcentaje total, en un **58%** (81% en 2020) **de las webs victimizadas la vulnerabilidad detectada en el software estaba relacionada con gestores comerciales de contenidos**, siendo WordPress el más representado con un 47%, seguido del DotNetNuke o SharePoint (entorno Microsoft) con un 26% (Figura 3-2-4-3). Estas cifras implican un descenso de alrededor de veinte puntos con respecto a los mismos parámetros del año anterior en cuanto a webs provistas de gestores de contenidos y al papel representado por WordPress, que sigue encabezando interanualmente la suma de las webs que lo equipan y que son vulneradas en ataques por desfiguración. En la misma magnitud sube el entorno de software Microsoft (IIS para el servidor, Windows como sistema operativo, ASP.net como código operativo, y DotNetNuke o SharePoint como gestores de contenidos) que, si en 2020 era victimizado en un 10% dentro del conjunto del software de gestión de contenidos, en 2021 ocupaba el segundo lugar en el baremo porcentual con un 26%. La victimización de webs desarrolladas en un ecosistema Microsoft ya había crecido en 2020 con respecto a 2019, de manera que lleva un patrón ascendente.

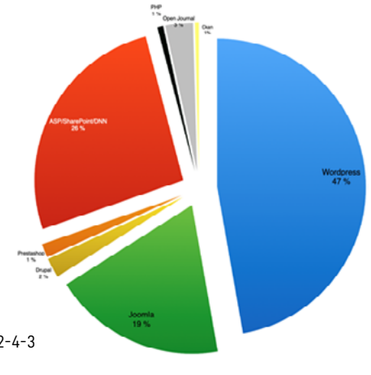


Figura 3-2-4-3

En consonancia con este hacktivismo de oportunidad y orientación vandálica, puede ya considerarse un patrón tendencial, tanto en España como en el resto del mundo, la correlación entre la desfiguración vandálica de webs y **tácticas preparatorias de la secuencia de actividad de ciberamenazas organizadas**. Si en 2020 el porcentaje de procedimientos de inyección de código para la propagación de contenidos maliciosos inscrito en el hacktivismo vandálico fue del 24,8%, en 2021 ese volumen se consolidaba por encima del 28%.

Resumiendo lo que ya consta en informes anuales previos, este volumen de coincidencia de acciones iniciales en la secuencia de ciberamenazas para la propagación de código dañino en alrededor de un cuarto de los ciberataques de identidades pretendidamente hacktivistas, se extiende principalmente hacia la inyección de contenido, mayormente en idioma japonés, para el envenenamiento de procesos de optimización de resultados en buscadores web (SEO). Esa intoxicación SEO se acompaña secundariamente con la inserción de scripts redirectores de tráfico hacia webs de distribución de contenidos maliciosos, que en un porcentaje menor incluye además la desviación de tráfico hacia páginas web que simulan ser tiendas de comercio electrónico y que, en realidad, se inscriben en esquemas de phishing para el robo de datos personales identificativos y de pago.

Uno de los incidentes que más prototípicamente ejemplificó durante 2021 esta deriva de "doble dedicación" de hacktivismo junto a tácticas preparatorias de ciberamenazas organizadas lo protagonizó '**Moroccan Revolution'**, una identidad colectiva que actúa con varios alias individuales ('Neige_Ma', 'MoroccanHack Team' o 'moroccohack_team', entre otros) al menos desde 2016 mediante ataques por desfiguración en varios países, en su más alto porcentaje de actividad coincidiendo en su victimización con sitios web equipados con software Microsoft desactualizado. Pues bien, el 22/5/2021 '**Moroccan Revolution**' desfiguraba seis webs privadas[19] provistas de software ASP.net desactualizado, inyectándoles un tipo de contenido que podría ser considerado típicamente hacktivista por su tono reivindicativo, cual es el mensaje en inglés "free Morocco" junto a imágenes de inmigración en la costa española de Ceuta (Figura 3-2-4-4); al mismo tiempo, aprovechaba las desfiguraciones para monetizarlas insertando en algunos de los sitios webs victimizados contenido de envenenamiento SEO en idioma japonés.

[19] idrometeo.es, davidcanovas.es, cdlaalmunia.es, casaruralsantana.es, skema.eu/index.html, marykayintouch.es/index.html, cowama.es/index.html

Figura 3-2-4-4

Otro ejemplo también característico de intersección entre hacktivismo vandálico y ciberamenazas propagando código dañino o malware, ocurrido en España en 2021 pero que es perfectamente representativo de la misma pauta en el resto de los países, es el de '**Mr.QLQ**', una identidad que opera al menos desde 2015 inyectando en sus desfiguraciones contenido alusivo a la <<defensa de los musulmanes en el mundo>> y, más en concreto, en contra del conflicto bélico en Yemen (por ejemplo, Figura 3-2-4-5). El 7/6/2021 esa misma identidad 'Mr.QLQ' dañaba con contenido reivindicativo general una web privada[20] desarrollada con software WordPress desactualizado, sobre la que inyectaba además la webshell '**Mini Mani Mo Shell**' (Figura 3-2-4-6), que se emplea habitualmente en el ámbito de las ciberamenazas como puerta trasera para dejar preparado un sitio web para la inserción de código dañino con diferentes funciones, generalmente monetizables.

[20] impremtasolber.com/abd.html

Figura 3-2-4-5

Figura 3-2-4-6

De manera similar a 'Mr.QLQ' operaba '**Ahd404**', que en noviembre de 2021 inyectaba contenido alusivo a "Al-Andalus" (Figura 3-2-4-7) en cuatro webs de comercio electrónico[21] programadas con WordPress y radicadas en España, pero con IPs en Lituania y Estados Unidos. Como suele ser habitual en oleadas de desfiguraciones, las acciones de 'Ahd404' no tenían centralidad en España, pues el mismo día el mismo atacante desfiguraba con contenido general otras webs en la propia Lituania[22] o, dos días más tarde, en Turquía con IP en Alemania[23]. A pesar de que, en un primer vistazo, los contenidos inyectados por el atacante podrían inscribirse en la orientación reivindicativa propia del hacktivismo, el análisis del histórico de la identidad, que apareció en junio de 2021, y de su perfil en redes sociales[24], la muestra interesada en la explotación de vulnerabilidades en WordPress, sin mostrar sesgo ideológico ninguno, desfigurando webs en diversos países. En alguna de las webs vulneradas por 'Ahd404' aparecen scripts de redirección hacia webs de comercio electrónico[25] que podrían ser trampas de phishing, de lo que se infiere que la motivación de 'Ahd404' se decanta menos hacia el hacktivismo y más hacia la secuencia de ciberamenazas que propagan malware.

Figura 3-2-4-7

Finalmente, otro ejemplo clarificador de una identidad muy prolífica internacionalmente durante 2021, en desfiguraciones de sitios webs mayormente provisionados con software Microsoft desactualizado, ha sido '**chinafans**', que se ha prodigado menos en inyección de contenido militante y se ha dedicado más a la inserción de envenenamiento SEO y de scripts redirectores hacia webs de distribución de adware[26]. Entre otras acciones durante el año, el 10/7/2021 inyectaba su alias en un par de webs privadas[27], en ese caso programadas con software Joomla desactualizado, sobre las que inyectaba scripts de redirección hacia una web de venta de relojes falsificados (Figura 3-2-4-8), que podría ser un engaño con propósitos de phishing, con dominio en Islandia[28] y declarando ser un servicio "comercial" operando desde China.

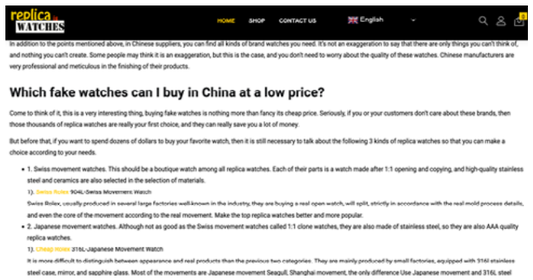


Figura 3-2-4-8

[21] Entre ellas, cuerpofuerte.es/Andalus.html, happybay.store/Andalus.html
[22] bodyimpuls.lt/Ahd404.html, bodypower.lt/Ahd404.html
[23] Entre ellas, imajosgb.com/Ahd404.html, ansiklopedist.com/Ahd404.html
[24] https://twitter.com/a_h_d0
[25] Por ejemplo, buytomato.fun o saleac.top
[26] En el caso de 'chinafans' y de otras identidades con pretensiones hacktivistas como 'Anonymous Arabe', el código malicioso inyectado en las desfiguraciones ha sido relacionado con la posible vinculación a redes de distribución del código dañino '**Ramnit**'.
[27] manasalmoradi.com/o.htm, getxobizi.com/o.htm
[28] replica-watches.is

3.2.5. Ataques hacktivistas sobre instituciones públicas

Al igual que en años previos de manera general en el panorama de identidades hacktivistas atacantes desde el exterior de España, durante 2021 las instituciones públicas españolas no han tenido centralidad en campañas o acciones dirigidas de ciberataque en ese capítulo, más allá de incidentes en donde algunos sitios web se han visto victimizados por su posible exposición de vulnerabilidades de software ante escaneos de atacantes en búsqueda activa de webs a comprometer.

Este patrón de victimización de webs de entidades públicas en España, que estaban exponiendo algún tipo de vulnerabilidad de software, se ha inscrito durante 2021 en acciones de identidades atacantes afectando en serie a webs del mismo tipo localizadas en varios países. Esta inscripción de los ataques a webs vulnerables en oleadas de desfiguraciones en varios países vuelve a subrayar que este tipo de acciones están dirigidas por las vulnerabilidades de software, y no por la localización geográfica de los dominios web o de sus direcciones IP.

En general, las webs de las administraciones públicas victimizadas durante 2021 en España se adscriben a alguno de estos tres tipos de categorías:

1. Webs de universidades y centros de enseñanza secundaria, dependientes del gobierno de Comunidades Autónomas, que exponen software desactualizado, generalmente Joomla o WordPress pero también para la gestión de servidores Apache.

   a. En esta primera categoría se inscriben desfiguraciones sobre páginas web de las universidades de Barcelona[29], de Zaragoza[30], de Lleida[31], de Salamanca[32], o de la Politécnica[33] o la Complutense[34] de Madrid, entre otras, generalmente subdominios de algún departamento o unidad docente alojados en espacios específicos de las webs de las universidades.

   b. También destaca el compromotimiento de webs programadas con software Joomla desactualizado de centros de enseñanza secundaria adscritos a la Junta de Extremadura[35], por ser una pauta que se repite interanualmente.

2. Webs provistas de versiones desactualizadas del gestor de contenidos Open Journal Systems, que alojan revistas digitales de universidades o de otras instituciones públicas.

   a. En este capítulo cabe mencionar que el comprometimiento a escala mundial de webs de revistas digitales desarrolladas con software Open Journal Systems es constante por parte, al menos, de dos identidades que utilizan en sus desfiguraciones contenidos con rasgos turcos: '**KingSkrupellos**' y '**Mr.Kro0oz.305**', al menos la segunda de las cuales instrumentaliza sus ataques para la inyección de contenido de envenenamiento web. De este modo ocurrió en diciembre de 2021, cuando la primera de ellas desfiguró (Figura 3-2-5-1) un subdominio[36] dedicado a revistas digitales y alojado en la web del Ministerio de Justicia, así como otro[37] en la web de la Universidad de Málaga.

Figura 3-2-5-1

[29] morfeo.ffn.ub.es
[30] gesport.unizar.es/gss.php
[31] bigdssagro.udl.cat
[32] sociocav.usal.es/web/
[33] cbgp.upm.es/images/ejderbub.jpg, maca.aq.upm.es/b4.html, hypermedia.aq.upm.es/b4.html, doca.aq.upm.es/b4.html
[34] repositorios.fdi.ucm.es/ciberia/krd.html
[35] Por ejemplo, iesloustauval.educarex.es/images/fighter.gif, iesdrfdezsantana.juntaextremadura.net/images/0x.jpg, o cptrajano.educarex.es/images/idolsex.txt
[36] ojs.mjusticia.gob.es/public/site/images/adminojs/kingskrupellos.jpg
[37] revistas.uma.es/public/site/images/adminojss/kingskrupellos.jpg

3. Webs de ayuntamientos o corporaciones locales provistas de software desactualizado, generalmente vulnerable.

a. Esta práctica de desfigurar webs de gobiernos locales y regionales es general y sistemática semanalmente en todo el mundo, con mayor incidencia en Iberoamérica y Asia, secundariamente en Estados Unidos de América y Europa. Está favorecida por la circunstancia de que, sobre todo en el caso de webs de corporaciones locales, los atacantes encuentran una considerable incidencia de desactualización en el software, que aprovechan en muchos casos para inyectar contenido de envenenamiento SEO o scripts redirectores de tráfico hacia webs maliciosas.

b. En el caso de España durante 2021 quedaron victimizados los ayuntamientos de Montcada[38] en Barcelona, Alcadozo[39] en Albacete, una web de promoción turística municipal[40] en Peñafiel en Valladolid, la biblioteca pública[41] del municipio de Dos Hermanas en Sevilla, o la mancomunidad[42] de municipios del Bagés en Cataluña. En alguno de los incidentes, los atacantes seguían el patrón ya descrito de desarrollar tácticas preparatorias de diseminación de código dañino: por ejemplo, en la acción sobre la mancomunidad del Bagés, llevada a cabo por 'KimiHmei7' en octubre de 2021, se inyectaba contenido de envenenamiento SEO relacionado con la descarga de software para videojuegos (Figura 3-2-5-2), que conducía a webs de distribución de contenidos maliciosos[43].

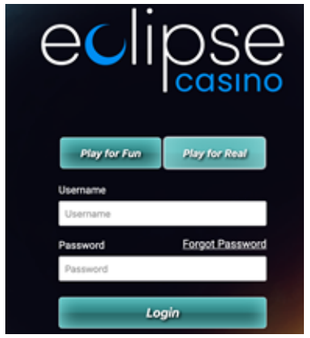
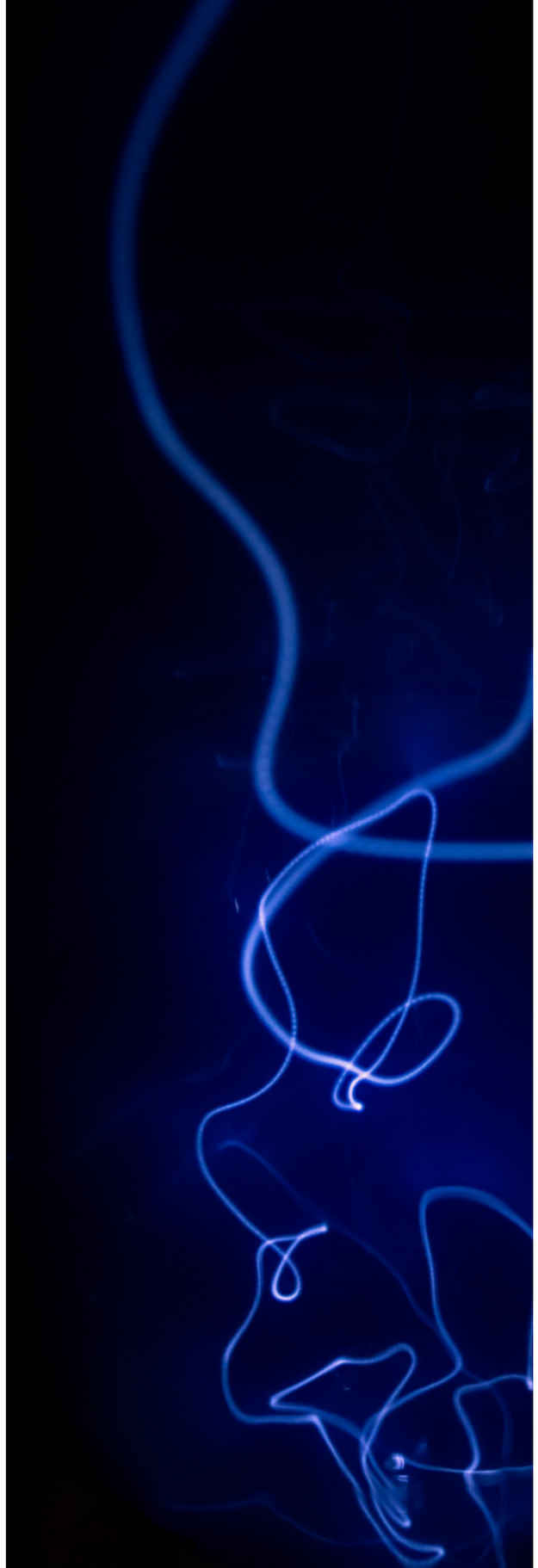


Figura 3-2-5-2

[38] pam.montcada.cat/o.htm, biblioteques.montcada.cat/o.htm, inclusio.montcada.cat/o.htm
[39] alcadozo.com/album/albums/userpics/ess.txt
[40] casita.turismoruralpenafiel.es
[41] bibliotecamontequinto.doshermanas.es/o.htm
[42] mnbagessanejament.cat/Fitxers/pwn.gif
[43] Por ejemplo, rungamepc.ru/?load=Biomutant%20Crack%20PC



04 HACKTIVISMO EN IBEROAMÉRICA

4.1. Panorámica hacktivista en Iberoamérica

El hacktivismo en Iberoamérica mantenía en 2021 el perfil descrito para los años previos, destacando la tendencia de desfigurar webs, provistas de software desactualizado, de gobiernos locales y regionales en la mayoría de los países, pero principalmente en Brasil, Perú y México, secundariamente en Colombia, Argentina y Ecuador.

Al igual que en el resto del mundo, el hacktivismo en Iberoamérica continúa siendo oportunista y de orientación vandálica, con un porcentaje de acciones por desfiguración aprovechados por los atacantes para involucrarse en tácticas preparatorias de ciberamenazas que diseminan código dañino, como el envenenamiento SEO o la inyección de scripts redirectores de tráfico, que en ocasiones desembocan en webs con apariencia de comercio electrónico provistas código software malicioso para robo de credenciales de pago en servicios digitales. Durante 2021, el porcentaje de este tipo de tácticas subsidiarias de ciberamenazas organizadas, concurrentes con desfiguraciones, por parte de identidades adscritas a un hacktivismo oportunista ha oscilado en una horquilla del 20% y el 40% en Iberoamérica.

En conjunto, el hacktivismo en Iberoamérica durante 2021 ha continuado mostrando el perfil de **declive ideológico, de descomposición orgánica y de atomización de identidades** iniciado alrededor de media década.

La infraestructura hacktivista autóctona decrece en Iberoamérica en cuanto a configuraciones que antaño adoptaban la simbología del colectivo 'Anonymous', actualmente prácticamente desaparecida, y aumenta en cuanto a la desagregación de configuraciones de tres o más identidades reunidas en identidades colectivas atacantes con la denominación genérica de teams (equipos).

En el primer caso, el de las configuraciones tipo 'Anonymous', durante 2021 actuaban principalmente en el ámbito de la propaganda o de las amenazas no concretadas en '**Anonymous Brasil**', '**Anonymous Venezuela**' o '**Anonymous Chile**'. Por ejemplo, en el contexto de las elecciones presidenciales celebradas en Chile, el 17/12/2021 '**Anonymous Chile Legion**' amenazaba en un vídeo situado en YouTube[44] con <<atacar la candidatura de José Antonio Kast>> (Figura 4-1-1). No obstante, a pesar de que '**Lorian Synaro**' ejecutaba ataques por denegación de servicio entre el 16 y 19/12/2021 contra varias webs institucionales[45] en el país, la convocatoria no se colectivizó ni generó una campaña hacktivista específica.

Figura 4-1-1

Por lo que respecta a la identidad colectiva 'Anonymous Iberoamérica', que en el pasado pretendió erigirse como un paraguas de hacktivismo en el subcontinente, tras varios años inactiva, recuperó capacidad ciberofensiva durante 2021 probablemente al ser ese alias colectivo asumido por un atacante individual actuando principalmente como 'CyberPhantom' y también como 'AnonDoor'. Esta marca colectiva de 'Anonymous Iberoamérica' se empleaba en contenido reivindicativo (Figura 4-1-2) de una serie de desfiguraciones adscritas a la #OpColombia durante la mitad del año, principalmente contra webs de gobierno regional o local, como la Gobernación de Nariño[46] o la Personería del municipio de Armenia[47], entre otras.

[44] https://www.youtube.com/watch?v=JLzprRFJxu8
[45] mtt.gob.cl, partidorepublicanodechile.cl, apoderadosdemesa.cl
[46] aplicaciones.narino.gov.co/.ssh/6402.html
[47] personeriarmenia.gov.co/ibero.html, personeriarmenia.gov.co/6402.html

Figura 4-1-2

En lo que respecta a configuraciones de tres o más identidades reunidas en identidades colectivas (teams), si bien hace años era común observarlas en varios países como Chile, Argentina, Colombia o Brasil, durante 2021, y siguiendo un patrón de años previos, este tipo de agrupamientos se limitaba principalmente a Brasil. Desde ese país probablemente actúan '**Shawty Boy**', operando con el alias colectivo 'Paraná Cyber Mafia'; '**sanninja**', '**bandz**' y 'sh3llc0de_' como 'Noias do Amazonas'; 'Aj4x', adscrito al alias colectivo 'Sharp Crew'; '**Global Illusion Crew**'; o '**son1x**', afiliado a '**theMx0nday**'.

Otra identidad colectiva, que así mismo podría ser brasileña, es 'sin1pecrew', que ataca principalmente a través de '**Crystal_MSF**', y que durante 2021 ha venido participando tanto en ataques preparatorios de diseminación de código dañino, como en acciones adscritas a marcos narrativos hacktivista, firmando desfiguraciones algunas veces como 'Anonymous Colombia' y otras como 'Anonymous Venezuela' (por ejemplo, Figura 4-1-3).

Figura 4-1-3

[48] https://www.las2orillas.co/persecucion-de-la-policia-a-anonymous-colombia/
[49] https://streamable.com/a7qpre
[50] https://ghostbin.co/paste/fwkr3
[51] https://mega.nz/folder/8lFzzQSQ#_B3plVHLPgxUz3JMtpHobA
[52] simfac.mil.co

4.2. Ciberataques y marcos narrativos hacktivistas destacados en Iberoamérica

Al igual que un hacktivismo centrado en el modelo 'Anonymous' ha pasado a la historia, los marcos narrativos hacktivistas alrededor de los cuales, a partir de una declaración militante, se colectivizaba un llamamiento a ciberataques, generalmente sobre el ciberespacio de un país, en el que participan identidades atacantes de distintas procedencias bajo la guía de una o varias identidades convocantes, llevan también varios años en decadencia, en Iberoamérica como en el resto del mundo.

Durante 2021 en Iberoamérica ha sido principalmente la **#OpColombia** en el segundo trimestre del año la que ha logrado aglutinar algún tipo de adhesión, generalmente por un reducido grupo de atacantes que no han logrado colectivizar ni sostener un marco de ciberataque en paralelo, como pretendían, a protestas sociales que se estaban sucediendo en el país. Aparte de ese escenario, hubo un atisbo, sin llegar a fructificar, de iniciar una **#OpCuba** en paralelo a un incremento de tensión social en el país durante el final del verano de 2021; acciones muy ocasionales y dispersas adscritas a la **#OpNicaragua**; y un llamamiento a iniciar una **#OpBrasil/#OpAmazonia**, que se quedó en intentona individual.

En la #OpColombia, tras intentos a comienzos de año por '**AnonFury**' y '**Anonymous T. Colombia**' de activar un contexto de ciberataques hacktivistas, al que se sumó '**s0u1**' con algunos ataques menores por distribución de servicio contra webs colombianas, no es hasta abril de 2021, cuando el blog '**las2orillas**' publicaba[48] un texto en donde titulando <<Persecución de la policía a Anonymous Colombia>>, que varias identidades atacantes aplicaran durante varias semanas ciberataques, principalmente por desfiguración, sobre webs en el país. '**Lorian Synaro**', que durante al menos los dos años previos había sido una identidad muy activa en la promoción de varios marcos narrativos hacktivistas en distintos países del mundo, pasó en 2021 prácticamente desapercibida, sin lograr que un llamamiento[49] que hizo en mayo de 2021 para atacar sitios web en Colombia[50] llegara a colectivizarse. Aunque identidades como 'GhostSec' realizaron intentos de divulgar informaciones supuestamente sensibles presuntamente obtenidas de webs gubernamentales (por ejemplo, en octubre un volcado[51] de información supuestamente procedente de la web[52] de la Subdirección de Meteorología de la Fuerza Aérea Colombiana), en realidad esas divulgaciones no llegaron a contener información privilegiada.

En la #OpBrasil participó principalmente 'EterSec', una identidad, probablemente del país, que ha tratado de impulsarse como referente hacktivista tipo 'Anonymous' en 2021 a través de la constitución de una web[53] (Figura 4-2-1) y de realizar llamamientos militantes, por ahora sin conseguirlo más allá de llevar a cabo sus propias acciones individuales. Entre ellas, en junio de 2021 ejecutaba una inyección SQL sobre la web gubernamental del Instituto Brasileño de Medio Ambiente[54], y en septiembre desfiguraba con contenido reivindicativo la web[55] de la empresa financiera brasileña Fib Bank, situando en el dominio público[56] un fichero comprimido RAR de 649MB con información exfiltrada supuestamente procedente de la acción sobre el servidor web atacado.

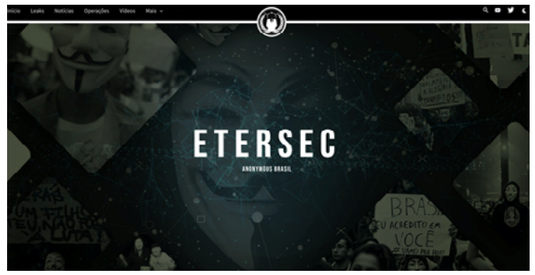


Figura 4-2-1

En lo que respecta a la incipiente #OpCuba, se quedó en un marco narrativo reactivo a las protestas populares que acaecieron en la isla en julio de 2021, pero sin transcender, ni colectivizarse ni mantenerse más allá de algunas acciones puntuales, como ataques por denegación de servicio de baja intensidad sobre webs gubernamentales llevados a cabo por '**s0u1**', '**EyenSoft**', 'Lorian Synaro' o '**Anonymous Iberoamérica**' o por la identidad, creada para la ocasión, '**Anonymous Cuba**'.

Aparte esos pocos marcos narrativos hacktivistas que, en el mejor de los casos, no han pasado de ser testimoniales, y de los ataques por desfiguración que mensualmente se ajustan a la habitualidad mundial de este tipo de acciones, cabe mencionar algunas acciones que sirven para visibilizar algunas de las tácticas, técnicas y procedimientos que se están produciendo en esa intersección del hacktivismo con las fases iniciales de las ciberamenazas que propagan código dañino.

Por ejemplo, el 10/12/2021 '**LAPSUS$**' desfiguraba la web[57] del Ministerio de Salud de Brasil, dejando una nota que pretende falsamente asemejar los ataques por ransomware y advirtiendo el atacante de que había robado 50TB de "datos internos del sistema" (Figura 4-2-2), solicitando ser contactado para recuperarlos.

La web estaba provista de un software de gestión de contenidos Plone. Ese mismo alias fue utilizado en julio de 2021 por un atacante que pretendía extorsionar[58], con una exfiltración de datos presuntamente robados, a la empresa de videojuegos EA Sports; y también era reportado[59] en agosto de 2021 como el firmante de mensajes SMS (Figura 4-2-3) extorsionando a usuarios individuales con revelar datos privados y con hacer compras en su nombre en servicios digitales.

Figura 4-2-2

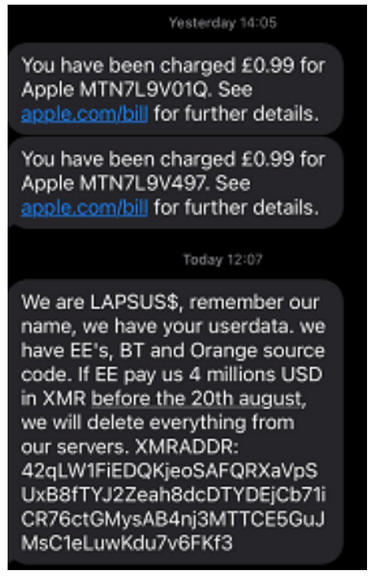


Figura 4-2-3

[53] https://etersec.org
[54] ibama.gov.br
[55] fib-bank.com
[56] https://gofile.io/d/B9B6wf, https://drive.etersec.org/0:/Leaks/FibBank/?__cf_chl_managed_tk__=pmd_MDvvjKrzCZpLMEGgu.9zP1nkwE8hKEL3IKt4EWHggBc-1631182554-0-gqNtZGzNArujcnBszRDl
[57] saude.gov.br
[58] https://raidforums.com/Thread-The-Biggest-EA-Data-Leak, https://raidforums.com/Thread-EA-Leak-Fifa-SOURCE-CODE-MIRROR
[59] https://www.reddit.com/r/applehelp/comments/ovqhi0/anyone_else_had_this_very_odd_that_it_happened_as/

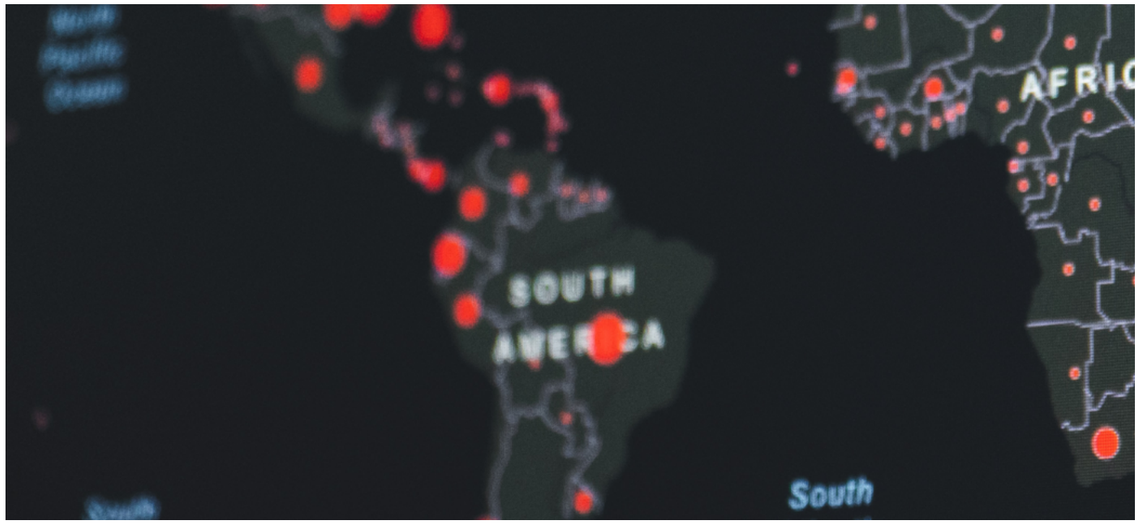
En otro escenario similar, el ya mencionado '**EterSec**' situaba en junio de 2021 en Vimeo[60] un vídeo de alrededor de 5 minutos de duración en donde, a través de un montaje gráfico, sugería haber infectado servidores web[61] de la Procuraduría General de la Nación (PGN) de Colombia con la cepa de ransomware '**Petya**' (Figura 4-2-4). En realidad, el montaje del vídeo mostraba a un usuario operando un panel de control de la proveedora de servicios de protección y gestión de datos Commvault supuestamente sobre algún activo tecnológico de la Procuraduría, así como una escena final en donde un usuario en un terminal Windows con el logotipo en el escritorio de la PGN parecía pulsar un fichero infectado con el ransomware. A partir del montaje del vídeo, se infería que el contenido difundido por 'EterSec' era un ejercicio de desinformación propio de la actividad hacktivista.

Figura 4-2-4

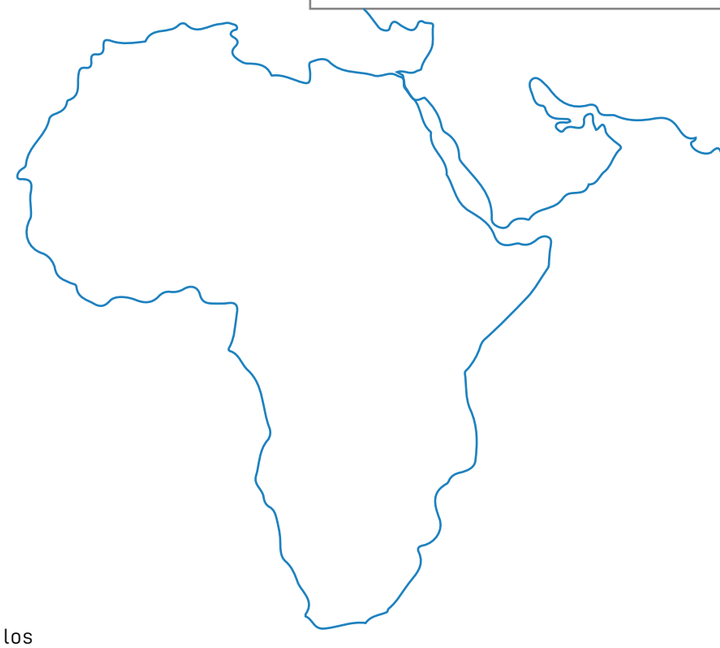
Y como instancias que muestran cómo identidades que en algún momento han ejercido militancia hacktivista se involucran en ciberataques preparatorios para la diseminación de código dañino, cabe reseñar cómo '**bky992**', que es otro alias para 'theMx0nday', inyectaba su alias sobre una web[62] de un gobierno municipal en Ecuador, en la que se insertaba un script redirector de tráfico de visitantes hacia una web[63] de phishing simulando una tienda de comercio electrónico. Lo mismo hacía en septiembre de 2021 '**aDriv4**', una identidad con varios años de recorrido, que comprometía con su alias las webs desarrolladas con WordPress desactualizado de un gobierno regional[64] en Venezuela y de otros dos, regional[65] y municipal[66], en Perú, en el último de los casos infectando con contenido SEO Spam en idioma japonés y con scripts redirectores hacia webs[67] de comercio electrónico que podrían ser trampas de phishing (Figura 4-2-5).

Figura 4-2-5

[60] https://vimeo.com/566819147
[61] procuraduria.gov.co
[62] tundayme.gob.ec
[63] Por ejemplo, uastore.es
[64] tifm.gob.ve/vz.txt
[65] copasa.gob.pe/vz.txt
[66] munipichanaqui.gob.pe/vz.txt
[67] Por ejemplo, newsale.yjbestbud.com



05 HACKTIVISMO EN NORTE DE ÁFRICA Y ORIENTE MEDIO



5.1. Panorámica hacktivista en Norte de África y Oriente Medio

De modo similar a otras geografías del mundo, los ciberataques que podrían encuadrarse dentro del hacktivismo, afectando a sitios web radicados en los países del Norte de África y en Oriente Medio durante 2021, se han desarrollado sobre ese doble eje de **hacktivismo vandálico de oportunidad**, por un lado, y **tácticas preparatorias de la secuencia de ciberamenazas para la propagación de código dañino**, por otro. La correlación entre ambas dimensiones de ese doble eje ha oscilado, durante 2021, en una horquilla entre el 10% y el 25% en estos países.

Un ejemplo prototípico de este desdoblamiento de personalidad ciberatacante lo ha mostrado en 2021 '**Moroccan Revolution**', una identidad colectiva que opera al menos desde 2016 con ataques por desfiguración contra webs en todo el mundo, y que actúa a través de una serie de alias individuales ("Ox Souhail", "r00t-kech", "Neige_ma", "Aliester-Crowley", "AnonGhost", "MoroccoHack_Team", entre otros) que suelen mostrar rasgos identificativos marroquíes. Generalmente, 'Moroccan Revolution' altera sitios web programados con software Joomla, ASP.net y WordPress en versiones desactualizadas, donde suele inyectar o bien su alias o bien contenido con iconografía reivindicativa marroquí (por ejemplo, Figura 5-1-1).

Figura 5-1-1

En varios momentos durante 2021 'Moroccan Revolution' vulnerado webs provistas de software vulnerable en Argelia, inyectando en ellas contenido promarroquí, lo que desde algún prisma podría ser interpretado como un cierto hacktivismo en el contexto de la rivalidad geopolítica entre Argelia y Marruecos, sobre todo si puntualmente alguna de esas desfiguraciones correlacionan con ciberataque en sentido inverso, es decir, por identidades supuestamente argelinas afectando a webs en Marruecos, como ocurrió nada más que ocasionalmente en noviembre de 2021, cuando 'Juba_Dz' desfiguraba con contenido proargelino (Figura 5-1-2) media docena de webs[68] privadas en Marruecos, incluyendo adicionalmente las webs[69] de gobierno abierto del Ministerio de Transición Informática.

Figura 5-1-2

Este tipo de acciones de 'Moroccan Revolution' en 2021 contra webs gubernamentales argelinas mayormente provistas de software Joomla o WordPress desactualizado afectaban en agosto al Ministerio de Turismo[70], de la Dirección General de Presupuestos[71], de la Agencia para la Transición Energética[72], y probablemente del Ministerio

[68] Entre ellas, fmje.ma, liverado.ma/Ju.php
[69] ogp.ma, gouvernement-ouvert.ma
[70] mta.gov.dz
[71] mfdgb.gov.dz
[72] cerefe.gov.dz

de Medio Ambiente[73], mientras en septiembre a las webs de la Dirección General de Prisiones del Ministerio de Justicia[74] de Argelia, que está programada con una versión desactualizada de software Drupal, así a las desarrolladas con software Joomla del Ministerio de Transición Energética[75], de la Autoridad Reguladora de Hidrocarburos[76], así como contenido promarroquí sobre la web[77] del Órgano Nacional de Prevención y Lucha contra la Corrupción, que estaba provista de WordPress.

Sin embargo, mostrando esa instrumentación de desfiguraciones para servir a fases subsidiarias de ciberamenazas para la propagación de código dañino, en noviembre varias acciones de 'Moroccan Revolution' sobre webs argelinas correlacionaba con la inyección de contenido de envenenamiento SEO en idioma japonés como, por ejemplo, la producida contra la web de Naciones Unidas en Argelia[78], que estaba desarrollada con software WordPress.

Por otro lado, y en conjunto, la situación de identidades hacktivistas operando desde los países de Norte de África y Oriente Medio se asemeja en cierta medida al escenario iberoamericano, aunque con una mayor atomización de identidades individuales y la configuración de menos agrupamientos de ellas en alias colectivos.

De entre los atacantes con mayor actividad en 2021, además de los ya aludidos bajo el paraguas de 'Moroccan Revolution' o la potencialmente argelina 'Juba_Dz, se mencionan '**djebbaranon**' (también conocido como '1337_H4x0rs_Dz'), '**Sofian X35 DZ**', '**B14ck_Dz**', '**Sc0rp10n.Dz**' o '**Admiral Zino**', con rasgos argelinos, y esta última involucrada en la venta de webshells; las presuntamente kuwaitíes '**sherlouk alenezi**', o '**B4x**'; las probablemente turcas '**Ayyildiz Tim**' o '**Aslan Neferler Tim**'; '**Error 7rB**', '**Shadow Officlle**' o '**ro0t-M8n**', que no muestran rasgos de procedencia identificables; '**Moroccanwolf**', que pasa por ser marroquí; '**Dr.SHA6H**', que se declara egipcia; '**cyber hacker-ly**', '**Alansary_Ly**', o **Ly Kermit**' en Libia; '**DesTroTN**' en Túnez; o el ya conocido agrupamiento de identidades iraníes '**Bax 026 of Iran**', '**Mamad Warning**' y '**Mrb3hz4d**'.

[73] me.gov.dz
[74] dgapr.mjustice.dz/ma.html
[75] mteer.gov.dz/index.php/fr/34-evenements/392-HackedMOROCCO
[76] arh.gov.dz/index.php/fr/presentation/139-17-1961
[77] onplc.org.dz
[78] un-algeria.org/ma.htm

5.2. #OpIsrael

La recurrente #OpIsrael es el único marco narrativo hacktivista que se ha configurado entre los países del Norte de África y Oriente Medio durante 2021. Esa etiqueta es empleada cada año por identidades hacktivistas que llevan a cabo desfiguraciones contra sitios webs en Israel generalmente para inyectarlos contenidos reivindicativos respecto de la situación en Palestina.

Lo habitual es que, cada año, identidades diversas, casi siempre mostrando iconografía y narrativa reivindicativa propalestinas, hagan un llamamiento a lanzar ciberataques contra sitios webs en Israel durante el mes de abril. Desde hace algunos años, estos llamamientos cursan en declive en cuanto a colectivización y a alcance de peligrosidad, tanto por la ausencia de identidades organizadoras con influencia suficiente como para aglutinar a su alrededor a participantes hacktivistas, como por la paulatina desideologización de los atacantes hacktivistas en todo el mundo.

En 2021 el mismo llamamiento se produjo en abril, distinguiéndose de los reciente años precedentes en tener una mayor adhesión de identidades atacantes, pero igualándose a ellos en la baja peligrosidad de la campaña, limitada a ataques de menor entidad sobre webs privadas, en general desfiguraciones de oportunidad sobre software vulnerable, con alguna exfiltración limitada de contenidos extraídos por inyección SQL y ataques testimoniales por denegación de servicio sobre algunas webs gubernamentales. En la campaña participaron una veintena de identidades inyectando en sus desfiguraciones contenido militante (Figura 5-2-1).

Figura 5-2-1

Tras ataques preliminares de '**ALkNsOle**', que también utiliza el alias colectivo 'Army Hacker Islamic', o '**Anonymous Ghost Gaza**' desfigurando con contenido propalestino (Figura 5-2-2) webs privadas provistas de software ASP.net en Israel, ya en mayo, tras desfiguraciones por parte de **'Hackers of Savior**', tanto '**El Armagttos**' como '**Y0urAnonOPS**' hacían sendos llamamientos[79] en inglés <<a todos los hacktivistas>> a alistarse en la #OpIsrael (Figura 5-2-3). El 30/5/2021 la indonesia '**Muslim Cyber Army**' convocaba[80] a un "Tweet Storm" (difusión masiva de mensajes reivindicativos en Twitter) sobre la cuestión palestina para el 4/6/2021 a las 20.00 GMT.

Figura 5-2-2

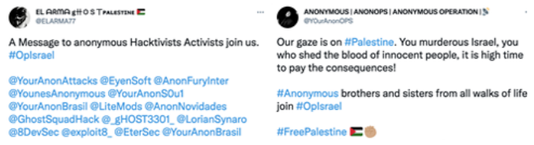


Figura 5-2-3

También en mayo 'EterSec' realizaba una inyección SQL sobre la web[81] del Departamento Central de Estadísticas en Israel, produciendo un volcado de contenido en el dominio público[82], incluyendo datos de autenticación de algunos usuarios.

[79] https://twitter.com/ELARMA77/status/1392269967874215936, https://twitter.com/Y0urAnonOPS/status/1392383549119074304
[80] https://twitter.com/MCAOps/status/1398833782304645127
[81] cbs.gov.il
[82] https://doxbin.org/upload/EterSecDBLEAKEDcbsgovilOpIsrael?bp=UpRDQ4HmXItZVORzxTg6JxUDMHLF7JjO|FEHriR5wE4lNYn4djXJmzRajZVouqAH6
[83] https://mega.nz/file/5HAQmJYb#1_9aLnDM5RG3-cO50pjLNFqzosszzd485ycWtxPHVcU
[84] https://raidforums.com/Thread-SELLING-Israel-municipal-databases-are-on-sale
[85] gettr.com
[86] https://gettr.com/user/jasonmillerindc

En junio, varias identidades asociadas al alias colectivo 'Dragon Force Malaysia' llevaron a cabo un nuevo llamamiento proponiendo ciberataques contra webs en Israel utilizando el etiquetado habitual de #OpIsrael y así mismo #OpSBedil, en donde identidades asociadas llevaron a cabo una serie de desfiguraciones sobre webs privadas provistas de software vulnerable (mayormente WordPress), sin lograr una respuesta colectiva a la convocatoria. 'T3Dimension' situaba un fichero en el dominio público[83] conteniendo imágenes escaneadas de documentos de identidad de quienes define como "ciudadanos israelíes" (Figura 5-2-4), imágenes que probablemente provengan de la reutilización de contenidos de alguna exfiltración generalista de información privada afectando a Israel y que identidades hacktivistas emplean recurrentemente simulando que provienen de nuevos ciberataques, como hacía por ejemplo 'SANGKANCIL', ya en septiembre de 2021, reivindicando en Telegram[84] tener acceso a 7 millones de datos personales identificativos de ciudadanos israelíes.

Figura 5-2-4

Finalmente, como una acción nominalmente no adscrita a la #OpIsrael, pero sí evaluable como hacktivismo militante en el contexto de su misma narrativa, saliéndose además de la técnica de desfiguración de webs para encaminarse por el comprometimiento de accesos a cuentas en redes sociales, cabe mencionar que el 4/7/2021 '**JubaBaghdad**' inyectaba su alias y una fase sobre la "liberación de Palestina" (Figura 5-2-5) en la declaración biográfica de varios de los perfiles de alto seguimiento de la entonces recién inaugurada red social GETTR[85] en Estados Unidos de América, incluida la cuenta de su fundador Jason Miller[86].

Figura 5-2-5

5.3. Phishing y malware concurrentes a impostado hacktivismo

Al igual que en el resto del mundo, en el área geopolítica del Norte de África y Oriente Medio, la acción de atacantes hacktivistas ha mezclado las acciones de oportunidad de expresión vandálica con tácticas preparatorias de ciberamenazas para la difusión de código dañino.

Aunque es común que los scripts redirectores hacia webs de difusión de contenidos maliciosos acaben conduciendo a los visitantes que llegan a esas webs a través de una ruta que finalizará con la descarga en sus dispositivos informáticos de algún tipo de fichero no deseado o quizás dañino, durante 2021 se documenta un caso de desfiguración por parte de una identidad hacktivista que es concurrente con **la inserción en la web victimizada de un malware de la familia de los troyanos de acceso remoto (RAT) contra dispositivos Android**. El incidente se produjo el 9/6/2021, cuando '**cyber hacker-ly**' comprometía con su alias la web[87] de la Cámara de Representantes de Libia, alojándose en esa web un fichero[88] de instalación para dispositivos Android infectado con el troyano de acceso remoto (RAT) '**SpyNote**'.

Otro caso de código informático malicioso directamente inyectado en un sitio web instrumentando una desfiguración con apariencia hacktivista se había producido en febrero de 2021, cuando '**cyber00t**' comprometía la web[89] provista de software PHP desactualizado de una agencia de publicidad en Túnez, que se infectaba con probable código tipo skimmer incrustado en varios ficheros Javascript[90], además de contenido SEO Spam en idioma japonés.

[87] ppsb.gov.ly/fuck.htm
[88] ppsb.gov.ly/app/APP.apk
[89] stock.cap.tn/task.htm
[90] add-to-cart.min.js, jquery-migrate.min.js, jquery.themepunch.revolution.min.js
[91] lis.edu.eg
[92] misternezq.com
[93] ahri.gov.eg
[94] elevenkicks.com

Además de este par de incidentes involucrando código informático tipo malware, que en 2021 ha distinguido al área regional del Norte de África y Oriente Medio del resto del panorama hacktivista mundial, y lo ha hecho no por cuestiones geográficas, sino por mero oportunismo de los atacantes, también se han documentado ciberataques en donde las desfiguraciones eran concurrentes a la inserción de scripts de redireccionamiento hacia webs de distribución de contenidos maliciosos o hacia phishing. Entre ellas, por ejemplo, dos en Egipto, una protagonizada el 17/5/2021 por '**Ayyildiz tim**', que alteraba con contenido proturco una web[91] educativa en el país, en la que además inyectaba un redireccionamiento hacia una web[92] probablemente de phishing; y otra en junio, cuando '**Ren4Sploit**' desfiguraba con su alias la web[93], programada con ASP.net, del Instituto de Investigación Animal del gobierno, en la que además insertaba una redirección hacia una web[94] probablemente dedicada al phishing simulando el comercio electrónico de productos textiles (Figura 5-3-1).

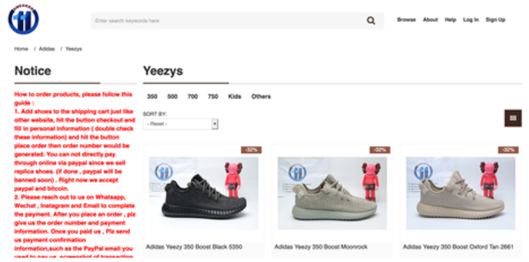
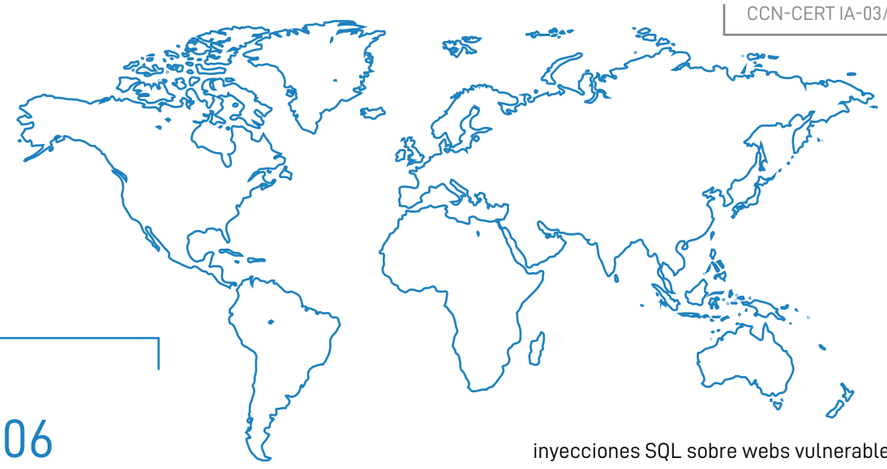


Figura 5-3-1



06 HACKTIVISMO EN ÁMBITO INTERNACIONAL

6.1. Caracterización general hacktivista en resto internacional

En áreas locales o regionales del mundo no contempladas en epígrafes anteriores de este informe, el hacktivismo ha seguido la misma pauta oportunista de desfiguraciones de sitios web adscritas a un doble eje, por un lado vandálico y por otro subsidiario de ciberamenazas para la propagación de código informático dañino.

En general, el perfilado del hacktivismo internacional ha seguido durante 2021 las mismas pautas que el año previo:

1. Atomización de identidades atacantes, con desaparición efectiva de agrupamientos tipo 'Anonymous' para dar paso a una sucesión de pequeñas configuraciones con denominación de identidades colectivas, que llevan a cabo generalmente ataques por desfiguración de tipo oportunista y vandálico, sin motivación ideológica.

2. Fracaso en el intento de movilizar colectivamente a identidades hacktivistas en campañas de ciberataque bajo una narrativa concreta de protesta contra algún país, quedándose las propuestas en escenarios testimoniales: intentos de convocar a una **#OpUganda** en enero de 2021 por parte de '**Lorian Synaro**'; a una **#OpMyanmar** de narrativa antigubernamental en ese país, en paralelo a protestas populares en sus calles en febrero, por parte de '**Union of Underground Myanmar Hackers**'; a una **#OpParis** por '**EterSec**' en julio; se limitaron, en el mejor de los casos, a concentrar puntualmente algunos ataques por denegación de servicio, desfiguraciones de webs de bajo impacto por parte de identidades actuando aisladamente, y algunas inyecciones SQL sobre webs vulnerables o, por lo general, a amenazas que no han llegado a tener recorrido, como la #OpParis de 'EterSec' (Figura 6-1-1). En este mismo contexto de fracaso de llamamientos, en Estados Unidos de América una nueva identidad bajo la denominación '**Hackers of Estradiol**', afiliándose a 'Anonymous', situaba el 13/9/2021 en el dominio público[95] un conjunto de información identificativa de clientes supuestamente procedente del comprometimiento del sitio web Epik[96], un servicio digital de gestión de dominios y alojamiento web al que el atacante atribuye dar soporte a "grupos de extrema derecha". En su reivindicación, el atacante pedía apoyo para la **#OperationJane**, un marco narrativo contra la legislación limitativa del aborto en Texas, cuya web del Partido Republicano también era desfigurada[97] (Figura 6-1-2) el 11/9/2021 con contenido alusivo a 'Anonymous'. La #OperacionJane no tuvo recorrido.

Figura 6-1-1

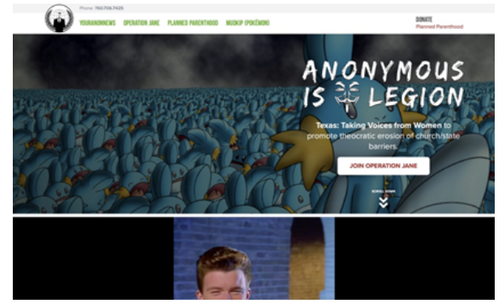


Figura 6-1-2

[95] https://4chan.partyvan.epikfail.win:55899/, https://ddosecrets.com/wiki/Epik
[96] epik.com
[97] texasgop.org

En cuanto a geografías de los ciberataques por desfiguración, algunos puntos comunes mantenidos durante 2021 han sido:

- La materialización de desfiguraciones sobre webs ministeriales y de instituciones de gobierno en países de África, en la mayoría de los casos actuando los atacantes sobre servidores web provistos de software vulnerable, y correlacionando esas desfiguraciones en un rango de entre el 10% y el 20% con tácticas preparatorias de ciberamenazas para la propagación de código software dañino.

- Recurrencia de desfiguraciones sobre gobiernos locales y regionales en Estados Unidos de América, generalmente actuando los atacantes sobre webs que emplean software vulnerable, mayormente distintas herramientas de software Microsoft desactualizado. Por ejemplo, en septiembre de 2021 coincidía que '**Mamad Warning**' inyectaba su habitual contenido proiraní sobre una web de gobierno municipal[98] programada con software ASP.net y provista de software Microsoft-IIS desactualizado para la gestión de su servidor; '**0x1998**' firmando con el alias 'KrdSec' sobre una web[99] de gobierno tribal programada con ASP.net, que además quedaba infectada con contenido SEO Spam en idioma japonés; y '**Moroccan Revolution**', desfigurando con su alias la web[100], también codificada con ASP.net, de un gobierno local en California.

- Oleadas de desfiguraciones sobre gobiernos asiáticos como Indonesia o Bangladesh, generalmente por parte de atacantes locales explotando debilidades de software desactualizado en las webs.

[98] officestatus.loslunasnm.gov/public/026.html
[99] lvd-nsn.gov/kurd.html
[100] laquintaca.gov/morocco.txt
[101] galacticgames.co.uk

6.2. Hacktivismo subsidiario de ciberamenazas de propagación de malware

Las identidades más persistentes en 2021 en cuanto a la instrumentación de desfiguraciones de webs para inserción de código informático para apoyar a ciberamenazas de propagación de algún tipo de contenido dañino o no deseado han sido '**LahBodoAmat**', '**Panataran**', '**chinafans**', '**Mr. Kro0oz.305**', '**ManzHERE**', '**Clash Hackers**' así como, a partir de la segunda mitad del año, varias identidades actuando alrededor de '**KrdSec**' bajo la nueva denominación '0x1998' y sus alias asociados.

Del mismo modo que en todos los países del mundo, en 2021 ha sido común la inyección de contenido de envenenamiento SEO concurrente a desfiguraciones (por ejemplo, Figura 6-2-1).

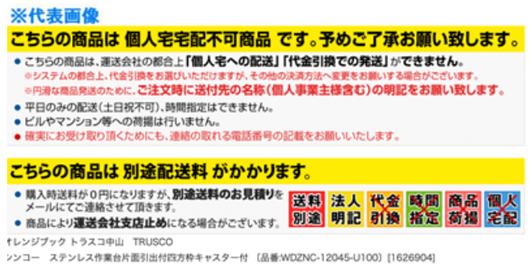


Figura 6-2-1

Además, en una desfiguración firmada por '**LingsCarsDotCom**' en marzo de 2021 sobre una web[101] desarrollada con el software para comercio electrónico OpenCart en el Reino Unido, se infectada con código Javascript tipo skimmer (Figura 6-2-2) para la captura de datos de pago con tarjeta de clientes que realizaran compras en esa web.

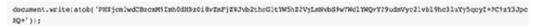


Figura 6-2-2

También en algunos incidentes se documentaba que las desfiguraciones vandálicas se instrumentaban para la inserción en la web comprometida de código informático tipo puerta trasera (webshell), como los protagonizados en mayo de 2021 por '**Fighter Kamrul**' sobre web privada[102] desarrollada con WordPress (Figura 6-2-3); o por '**Fnug**' en septiembre, cuando inyectaba una webshell[103] (Figura 6-2-4) sobre la Oficina Nacional de Medicamentos de Camerún.

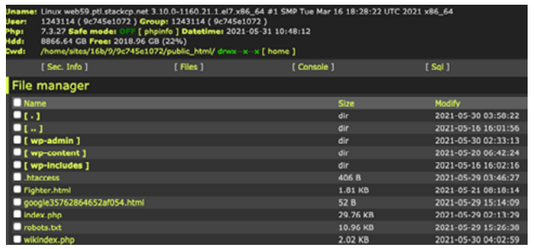


Figura 6-2-3

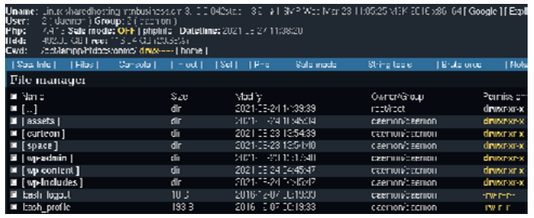


Figura 6-2-4

Además del envenenamiento SEO en idioma japonés y del redireccionamiento a falsas webs de comercio electrónico como trampas de phishing, un par de ataques por parte de '**angga1337**' sobre webs ministeriales[104] en Malawi y de '**xIdontknow**' sobre un subdominio[105] de la web del Departamento de Irrigación del gobierno de Malasia, coincidían en la inserción de intoxicación SEO redirigiendo a tiendas de comercio electrónico de relojes falsificados (por ejemplo, Figura 6-2-5) probablemente dispuestas como phishing.

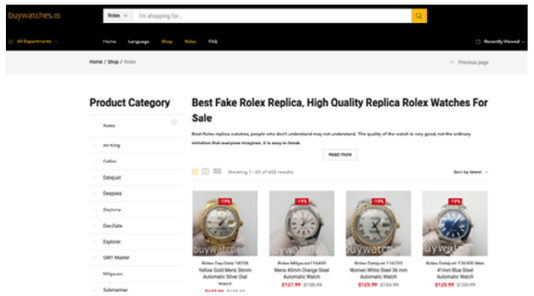


Figura 6-2-5

[104] education.gov.mw, malawi.gov.mw/hacked.php, finance.gov.mw/hacked.php, nao.gov.mw
[105] aseaniwrm.water.gov.my

6.3. Ciberataques colindantes con el hacktivismo

Durante 2021 se han producido algunas acciones ciberofensivas que, apartadas de las habituales técnicas de las desfiguraciones y también de las inyecciones SQL o de las exfiltraciones de información, por su intención o expresión reivindicativas podrían considerarse colindantes o relacionadas con el hacktivismo.

6.3.1. Campaña contra la difusión de mensajes de odio en Twitch

El 6/10/2021 una identidad anónima difundía a través del foro 4Chan[106] (Figura 6-3-1-1), que fue epicentro del movimiento 'Anonymous' en la década de 2000, un fichero de 125 GB en formato torrent[107] que identificaba como el código fuente del servicio digital de vídeo estadounidense Twitch, incluyendo entre la información exfiltrada datos personales identificativos y de autenticación de usuarios de la plataforma.


[Return] [Catalog] [Bottom] Archived // 1169 / 140

File: bezos-pogchamp.jpg (9 KB, 186x295)

twitch leaks part one Anonymous 10/05/21(Tue)22:34:18 No.83691438

We bring to you today an extremely poggers leak:

Twitch is an American video live streaming service that focuses on video game live streaming, including broadcasts of esports competitions, operated by Twitch Interactive, a subsidiary of Amazon.com, Inc.

Their community is also a disgusting toxic cesspool, so to foster more disruption and competition in the online video streaming space, we have completely pwned them, and in part one, are releasing the source code from almost 6,000 internal Git repositories, including:

> Entirety of twitch.tv, with commit history going back to its early beginnings
> Mobile, desktop and video game console Twitch clients
> Various proprietary SDKs and internal AWS services used by Twitch

> Every other property that Twitch owns including IGDB and CurseForge
> An unreleased Steam competitor from Amazon Game Studios
> Twitch SOC internal red teaming tools (lol)

AND: Creator payout reports from 2019 until now. Find out how much your favorite streamer is really making!

Torrent (128GB):

Repository listing:

Jeff Bezos paid $970 million for this, we're giving it away FOR FREE.

#DoBetterTwitch

Figura 6-3-1-1

El mismo día Twitch reconocía[108] la brecha de seguridad. El incidente se atribuyó a un ciberataque al repositorio Github privado del propio departamento de desarrollo de software de Twitch. La reivindicación por una identidad anónima en 4Chan enmarcaba la acción de ciberataque en una "respuesta a las incursiones de odio" en forma de mensajes que otras identidades difunden en las páginas de comentarios de vídeos de Twitch, y que había sido objeto de una campaña de rechazo de usuarios de Twitch durante el último mes mediante la etiqueta de protesta **#ADayOffTwitch**, que llamaba a una desconexión por un día de la comunidad de usuarios para reclamar mayor control sobre esos "mensajes de odio" que se sugiere estarían circulando en las páginas de comentarios.

[106] https://boards.4chan.org/bant/thread/13578558/twitch-leaks-part-one
[107] magnet:?xt=urn:btih:N5BLZ6XECNEHHARHJOVQAS4W7TWRXCSI&dn=twitch-leaks-part-one&tr=udp%3A%2F%2Fopen.stealth.si%3A80%2Fannounce
[108] https://twitter.com/Twitch/status/1445770441176469512

6.3.2. Vulneración de accesos a cuentas de Twitter para propagación de mensajes sobre Bitcoin

A finales de 2021, continuando con varios incidentes en los primeros meses de 2022, se producían vulneraciones de accesos a cuentas en Twitter, de instituciones gubernamentales o de figuras sociales representativas, principalmente en India, para publicar a través de ellas mensajes de promoción de la divisa electrónica Bitcoin.

El primero de esta secuencia de incidentes se produjo el 12/12/2021, cuando la cuenta personal en Twitter[109] del primer ministro de la India, Narendra Modi, en ese momento con 73,5 millones de seguidores, fue comprometida por un atacante no identificado que transmitió desde ella un mensaje en inglés (Figura 6-3-2-1) afirmando que <<India ha adoptado el bitcoin como moneda de curso legal>> y que el gobierno había comprado <<500 BTC para distribuirlos entre los residentes del país>>, facilitando un hipervínculo a un blog[110] ya eliminado.


Narendra Modi
@narendramodi

India has officially adopted bitcoin as legal tender.

The government has officially bought 500 BTC and is distributing them to all residents of the country.

Hurry up 👉 INDIA-OFFICIAL.BLOGSPOT.COM/ #BITCOIN-GIVEA...

The future has come today!

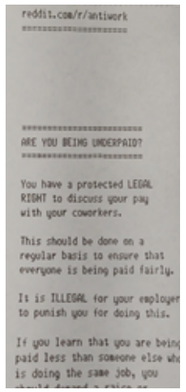
2:11 AM · 12/12/21 · Twitter Web App

Figura 6-3-2-1

[109] @narendramodiw
[110] india-official.blogspot.com

6.3.3. Reivindicación de condiciones laborales a través de impresoras

A partir de primeros de diciembre de 2021, un hilo[111] en la plataforma Reddit servía para reportar la recepción en impresoras, generalmente parte de infraestructuras informáticas de empresas y conectadas a Internet en Estados Unidos de América, de órdenes de impresión en papel con textos reivindicativos en idioma inglés haciendo un llamamiento a los trabajadores para reivindicar mejoras en las condiciones laborales (Figura 6-3-3-1).


reddit.com/r/antiwork

==========

ARE YOU BEING UNDERPAID?

==========

You have a protected LEGAL RIGHT to discuss your pay with your coworkers.

This should be done on a regular basis to ensure that everyone is being paid fairly.

It is ILLEGAL for your employer to punish you for doing this.

If you learn that you are being paid less than someone else who is doing the same job, you

Figura 6-3-3-1

Aunque no se produjeron reivindicaciones públicas de la acción, de sus procedimientos o de sus motivaciones, se especula[112] con que, técnicamente, se podría estar realizando mediante escaneos en Internet buscando impresoras con puertos TCP-9100 visibles y sin protección, a través de los cuales forzar las órdenes de impresión.

Por otro lado, si bien por su retórica sociopolítica la acción podría encuadrarse a priori en el marco del hacktivismo, no es la primera vez que un ciberataque de esta naturaleza se produce sin que tenga una motivación ideológica. En enero de 2019 ya se reportaba que las identidades '**Hacker Giraffe**' y '**j3ws3r**' habían comprometido dispositivos en línea basados en Chromecast e impresoras HP vulnerables a inyección remota de código para mostrar en ellos mensajes e impresiones en papel que promocionaban el canal de YouTube PewDiePie.

[111] https://www.reddit.com/r/antiwork/
[112] https://www.vice.com/en/article/qjbb9d/hackers-are-spamming-businesses-receipt-printers-with-antiwork-manifestos

07 HACKTIVISMO DE FALSA BANDERA PROISLAMISTA O PROYIHADISTA

7.1. Apunte terminológico sobre ciberyihadismo

Abundando en lo que viene subrayándose en la edición anual de este informe de ciberamenazas en el ámbito del hacktivismo y del ciberyihadismo, se entendería por ciberyihadismo la utilización de medios cibernéticos para desarrollar ataques ("atentados cibernéticos" podrían denominarse) sobre la base de una motivación ideológica yihadista. Por tanto, el ciberyihadismo se diferenciaría del yihadismo propiamente dicho únicamente en los medios a utilizar para el ejercicio de la violencia:

- mientras el **yihadismo** emplea la violencia física (asaltos armados, atentados con bomba, despliegue de fuerzas armadas sobre el terreno) para actuar sobre objetivos en un plano físico predominantemente analógico: instalaciones de Gobierno o de empresas, personas, infraestructuras críticas, poblaciones.

- el **ciberyihadismo** recurriría potencialmente a armas cibernéticas (malware, exploits, remote access tools, remote control systems, ransomware) para intentar producir un perjuicio o daño en los sistemas cibernéticos de un objetivo a atacar.

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

Con este espacio terminológico de partida como criterio de observación, al igual que ocurrió en 2018, 2019 y 2020, durante 2021 no se ha documentado ningún incidente que sea calificable de ciberyihadismo.

Así mismo, la información de incidentes cibernéticos durante 2021 confirma la **inexistencia de evidencias que sugieran que el 'Daesh' (Estado Islámico) o cualquier otro agrupamiento yihadista hayan desarrollado una división ciberarmada específica** destinada a la comisión de atentados terroristas por medios cibernéticos.

7.2. Hacktivismo de falsa bandera proislamista

Ausente, por el momento, del panorama de ciberamenazas el desarrollo de un escenario de ciberyihadismo, lo que viene constatándose desde 2015 es la instrumentación de la denominación '**Cibercalifato**', o de alguna de sus variantes, por parte de atacantes 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.

Esta instrumentación de contenidos alusivos al 'Cibercalifato' ha seguido inscribiéndose en la misma tónica del hacktivismo mundial actual, la cual es la ausencia de motivaciones ideológicas en una práctica provocativa y vandálica de ciberataques por desfiguración que sirve para dejar en ellos la firma del atacante.

Los incidentes en 2021 suman para continuar confirmando la hipótesis 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. 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 vandálico que por emplear conceptos e iconografías proislamistas a modo de provocación de un potencial auditorio podría calificarse como "**hacktivismo de falsa bandera proislamista**".

En este contexto, durante 2021 se ha mantenido la tendencia de volumetría a la baja de incidentes, documentada desde 2018, para acciones por desfiguración empleando contenidos alusivos al "Cibercalifato" o al "Estado Islámico".

Además, las acciones por desfiguración en esta categoría han sido ocasionales, pero ejemplifican con nitidez el progresivo solapamiento entre hacktivismo vandálico y tácticas subsidiarias de ciberamenazas para la propagación de contenidos maliciosos que se viene reseñando para el hacktivismo generalista. Las únicas desfiguraciones de hacktivismo de falsa bandera proislamista acaecidas en 2021 han correlacionado con la inserción de envenenamiento SEO o de scripts redirectores en las webs victimizadas.

Así, el 4/8/2021 una nueva identidad bajo la denominación '**Hackers of the Islamic State**'[113] desfiguraba con contenido alusivo al Califato Islámico (Figura 7-2-1) un subdominio[114] del Ministerio de Sanidad de Moldavia, la web[115] de una empresa de ingeniería en Irán, y un foro informático[116] también en Irán, todas programadas con WordPress. En la última de las webs comprometidas inyectaba contenido de intoxicación SEO en idioma japonés.

Figura 7-2-1

Entre el 6 y 9/8/2021 '**mukafihun7**' desfiguraba media docena de webs privadas programadas con software WordPress en Irán[117], Emiratos[118] o Turquía[119], además de un gobierno municipal en Filipinas[120], infectándolas con contenidos de envenenamiento SEO en idioma japonés, y con scripts de redirección hacia webs[121] (Figura 7-2-2) con estructura de tienda de comercio electrónico, también en idioma japonés, que podrían ser trampas para phishing. En alguna de ellas inyectaba contenido alusivo al "califato islámico", junto a un grafismo con el texto de la profesión de fe islámica, y un párrafo de amenaza genérica en árabe contra <<los infieles que actúan contra los musulmanes>>, advirtiéndose que no se <<abandonará un grano de tierra de los países musulmanes>> e imprecando a los gobiernos <<tiránicos>> (Figura 7-2-3).

Figura 7-2-2

Figura 7-2-3

Al igual que las desfiguraciones de 'Hackers of the Islamic State', la utilización de SEO Spam y scripts redirectores sugiere que '**mukafihun7**' está más próximo a la pequeña cibercriminalidad que al hacktivismo ideológico de corte islamista. Por si esto no fuera suficiente muestra de su motivación, la identidad 'mukafihun7' también utiliza el alias **'Alkhoure Bshar**', que mantenía un perfil en Facebook[122] cuya descripción biográfica, escrita en árabe, puede traducirse como <<las religiones han sido corrompidas por el judaísmo, ratificado por el cristianismo, y adoptado por el Islam, y sólo nosotros somos las víctimas>>, declaración que desacredita a la identidad como afiliado a ideologías islamistas.

[113] https://t.me/islamcyber
[114] cnddcm.msmps.gov.md
[115] sat-iran.com
[116] nablearning.ir
[117] hicomed.ir
[118] farahphoto.qa, rt-uae.com
[119] turkeli.bel.tr
[120] tacloban.gov.ph
[121] Por ejemplo, endnarrow.top
[122] https://www.facebook.com/profile.php?id=100002098569171

Adicionalmente, se comprueba que 'mukafihun7' ha utilizado en algunas de sus desfiguraciones[123] el contenido inyectado por 'Hackers of the Islamic State' con un prototípico error ortográfico ("Cailphate"), lo que abre la posibilidad a conjeturar que ambas identidades se correspondan con la misma persona tras el sobrenombre 'Alkhoure Bshar'.

Por si estos incidentes no fueran suficientes para acreditar la naturaleza de falsa bandera proislamista para lo que no son más que ataques oportunistas por desfiguración para la propagación de código software malicioso, 2021 era el año en el que desplegaba mayor actividad uno de los agrupamientos de identidades atacantes más prolíficos en la desfiguración de sitios web con propósitos de servir a la diseminación de código malicioso: se trata de un conjunto de identidades alrededor de '**KrdSec**', que durante el año han actuado principalmente a través de los alias '**0x1998**' y '**b44t**' con un elevado ritmo mensual de desfiguraciones por todo el mundo.

'KrdSec' representa el prototipo de ese hacktivismo de eje vandálico desdoblado para derivar hacia tácticas de ciberamenazas para la propagación de malware, instrumentando además desfiguraciones de falsa bandera proislamista. Por ejemplo, el 11/9/2021 se inyectaba el alias '**KrdSec**' y el símbolo (Figura 7-2-4) de la profesión de fe islámica (Shahada) sobre la web[124] de la Comisión de Naciones Unidas para los Refugiados en Turquía, que estaba desarrollada con WordPress, alterando así mismo un centenar de webs[125] privadas en ese país. 'KrdSec' podría corresponderse con un atacante de origen turco presente en varios foros[126] de ciberamenazas operando en ese idioma e involucrado en distinto tipo de actividades ilícitas de venta de datos y de código informático malicioso.

Figura 7-2-4

[123] Por ejemplo, contra hicomed.ir
[124] unhcr.org.tr/ks.html
[125] Entre ellas, promoshop.com.tr/ks.html, mekmim.com/ks.html
[126] https://spyhackerz.org/forum/members/krdsec.126779/, https://crackturkey.com/konular/dev-tuerk-hack-arsivi-hersey-icinde.311/#post-554663

08 PREVISIONES 2022-2023

8.1. ¿Mutación de 'Anonymous' en 2022?

Con ocasión de la invasión militar de Ucrania por parte de Rusia a finales de febrero de 2022, se originó una campaña hacktivista de respuesta en forma de ciberataques principalmente sobre sistemas informáticos conectados a Internet de empresas e instituciones de Rusia.

Durante el primer trimestre de 2022 esta campaña, identificada principalmente con las etiquetas **#OpRussia** u **#OpRedScare**, ha venido teniendo al menos cuatro vertientes:

1. Filtraciones de información, provista de distinto grado de sensibilidad, supuestamente proveniente de sistemas informáticos conectados a Internet y vulnerados en ciberataques de empresas o instituciones de Rusia, ciberataques reivindicados por actores no identificados, que se presentan a sí mismos como "próximos a Anonymous" y que llevan a cabo sus reivindicaciones y volcados de información a través de canales dedicados a la propaganda hacktivista e iconografía de 'Anonymous', con amplio seguimiento en redes sociales, como '**YourAnonTV**' o '**YourAnonNews**'.

2. Filtraciones de información contra Rusia, en el mismo sentido que las anteriores, pero reivindicadas por actores de ciberamenaza que principalmente, y hasta el contexto bélico en Ucrania, se habían venido dedicado a operar en foros de compraventa de información sensible o de tráfico de credenciales de acceso a servicios digitales, pero que, a partir de ese conflicto, intervienen también reivindicando acciones de comprometimiento de sistemas informáticos en Rusia con consiguiente divulgación de información comprometida en el dominio público. Ejemplos de esta categoría podrían ser actores como 'Ke**lvin Security**' o '**Against The West**'.

3. Filtraciones de información, combinadas con ataques por denegación de servicio contra sistemas informáticos en Rusia o Bielorrusia, conducidas por nuevas identidades con intenciones hacktivistas que se constituyen a raíz de la situación de conflicto militar en Ucrania, como '**IT Army of Ukraine**', '**Belarusian Cyber-Partisans**', '**Pwn-Bär International Hack Team**', o '**The Black Rabbit World**'.

4. Unas pocas identidades hacktivistas con un historial ya de adhesión al movimiento 'Anonymous' y de intervención en campañas hacktivistas previas durante años anteriores en otros países, que no participan de las grandes y mediáticas exfiltraciones y que llevan a cabo algunos ataques por denegación de servicio y algunas acciones ocasiones por desfiguración sobre sitios web en Rusia.

En las diferentes vertientes de esta campaña hacktivista contra Rusia, presentada como respuesta a la invasión militar de Ucrania, la visibilidad que ha tomado la denominación 'Anonymous' ha sido preponderante desde el principio.

Algo antes del día en que Rusia iniciara sus operaciones militares a gran escala en Ucrania, pero cuando estaba escalando el conflicto con claros signos de escenario militar, el 15 de febrero de 2022 el que había venido siendo un canal principalmente de propaganda hacktivista en Twitter en lengua inglesa, 'YourAnonTV' (o '**Anonymous TV**'), divulgaba[127] un vídeo con iconografía del movimiento hacktivista 'Anonymous' en donde, en algo más de dos minutos de duración, se pedía en inglés la <<creación de una zona neutral internacional en Ucrania>> y de un "referéndum de autodeterminación", administrado por Naciones Unidas, en su región de Dombás, advirtiendo de que <<si las tensiones continúan empeorando en Ucrania, tomaremos rehenes… sistemas de control industrial>>.

El 24 de febrero de 2022 de nuevo 'Anonymous TV' proclamaba[128] <<ciberataques a gran escala sobre websites de gobierno en Rusia en represalia por la invasión de Ucrania>> (Figura 8-1-1), al tiempo que se llevaban a cabo ataques de denegación de servicio sobre varias webs gubernamentales[129]. Al anuncio se unían también los canales de propaganda hacktivista '**YourAnonOne**'[130], con 1'2 millones de seguidores, y '**YourAnonNews**'[131] con 7'5 millones, mientras la cadena de noticias rusa RT[132] era objeto de un ataque por denegación de servicio. 'YourAnonNews' añadía[133] <<Anonymous está actualmente involucrado en operaciones contra la Federación Rusa>>. El mismo 24 de febrero de 2022, identidades con histórico hacktivista, como 'Powerful Greek Army' o 'LiteMods', lanzaban ataques por denegación de servicio sobre el Ministerio de Educación[134] de Rusia o la web de la empresa energética Gazprom[135].

Figura 8-1-1

El 26 de febrero de 2022 el recién constituido '**IT Army of Ukraine**' hacía un llamamiento[136] a <<todo el mundo a actuar como uno solo>>, advirtiendo de que si <<esta guerra no se gana con armas, se ganará con ciberarmas>> (Figura 8-1-2). El mismo día, se situaba en el dominio público[137] un listado de sitios webs del gobierno ruso como objetivos para ataques por denegación de servicio, que continuaban produciéndose también sobre webs en Chechenia[138] o Bielorrusia[139]. Respecto de este último país, la también nueva identidad 'Belarusian Cyber-Partisans' aseguraba[140] que sus ataques sobre el sistema de ferrocarriles habrían obligado a sus operadores a pasar a "control manual".

Figura 8-1-2

[127] https://twitter.com/YourAnonTV/status/1493718462207832065
[128] https://twitter.com/YourAnonTV/status/1496891433843888134
[129] kremlin.ru, government.ru, mil.ru
[130] https://twitter.com/YourAnonOne/status/1496965766435926039
[131] https://twitter.com/YourAnonNews/status/1496954233492541444
[132] RT.com
[133] https://twitter.com/YourAnonNews/status/1496954233492541444
[134] edu.gov.ru
[135] Gazprom.com
[136] https://twitter.com/ITarmyUA/status/1497707706286678016
[137] https://pst.klgrth.io/paste/bxyjyo43ggetn2ubhh55j5mf
[138] Por ejemplo, Chechnya.gov.ru
[139] Por ejemplo, sobre la web de los ferrocarriles del país en portal.rw.by
[140] https://twitter.com/cpartisans/status/1497930273425661958

En las mismas fechas, actores de nueva constitución, como los alias '**Pwn-Bär International Hack Team**' o '**Network Battalion 65**' (NB65), producían exfiltraciones a partir del supuesto comprometimiento de sistemas informáticos en Rusia, como el Instituto de Seguridad Nuclear de Rusia o el fabricante de armas Tetraedr de Bielorrusia. A partir de primeros de marzo de 2022, actores de ciberamenaza hasta entonces tangenciales al hacktivismo, como '**Kelvin Security**' o '**Against the West**', participaban así mismo en exfiltraciones de información sobre sistemas informáticos de Rusia, comenzándose a observar cierta convergencia entre comunicaciones llevadas a cabo por canales de propaganda de 'Anonymous' y estos actores.

Por ejemplo, el 20 de marzo de 2022, **'Anonymous TV'** amenazaba a través de Twitter[141] a <<todas las empresas que continúan operando en Rusia y pagando impuestos al régimen criminal del Kremlin>> con convertirse en <<objetivos>> de ciberataques sin no abandonaban el país en el plazo de <<48 horas>> (Figura 8-1-3). El mismo 20/3/2022 '**BlueHornet**', identidad del alias colectivo 'AgainstTheWest', anunciaba en Twitter[142] que se <<vendrían cosas grandes muy pronto>>, adjuntando el logo de la compañía alimentaria Nestlé y advirtiendo de la próxima exfiltración de una <<pequeña base de datos de empleados>>, mostrando en la plataforma Breached.co[143] un volcado de datos identificativos de contacto (nombre, correo electrónico, dirección física en Estados Unidos) de quienes parecen ser una decena de usuarios registrados en la web de Nestlé.

Figura 8-1-3

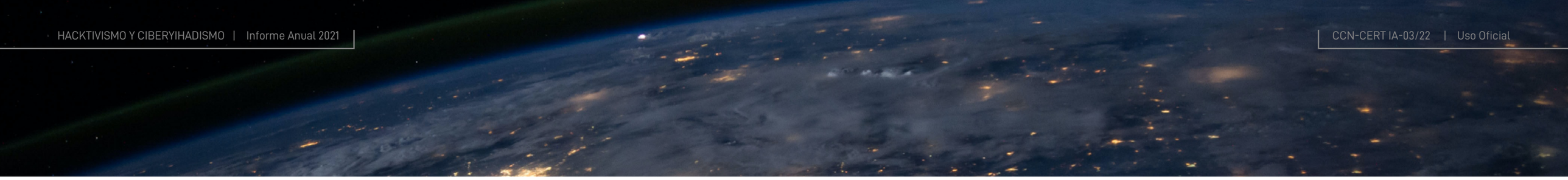
Un día después, '**Kelvin Security**' reivindicaba[144] una exfiltración de 10GB de datos identificativos de clientes y de autenticación de administradores probablemente procedentes de una base MySQL de un repositorio en Azure de Nestlé, detallando una muestra de 5MB del contenido el dominio público[145], muestra que el 22 de marzo de 2022 era replicada en otras plataformas de exfiltración[146] No obstante, un día después, el 23 de marzo, TheRecord citaba[147] fuentes de la propia Nestlé para negar que se haya producido un comprometimiento de sistemas informáticos de la compañía, alegando que los datos diseminados ahora se corresponden con los expuestos en una brecha de seguridad en febrero de 2022, cuando un entorno de pruebas de la empresa con datos de proveedores y clientes corporativos fue accidentalmente visible en línea durante un breve período de tiempo.

El 11 de marzo de 2022 la plataforma web identificada con '**Anonymous Alemania**' AnonLeaks.net, desde 2020 dedicada fundamentalmente a tareas de propaganda hacktivista y al marco narrativo de la #OpTinfoil, éste centrado en "contrarrestar las teorías conspiranoicas", publicaba una nota reivindicativa[148] atribuyendo a 'Anonymous Alemania' el comprometimiento de <<servidores web>> de la filial en Alemania de la petrolera rusa Rosneft. A modo de evidencia de la acción, divulgaban varias capturas de pantalla identificativas de consolas de administración de distintos dispositivos de control industrial o de máquinas virtuales, la mayoría conectadas en el rango de IP 10.100.XXX.XX (red de infraestructura privada); o consolas de VMware Workspace ONE UEM.

A esta muestra de ciberataques que se reseña se les sumarían otros de similar tipología durante marzo y abril de 2022. De entre las tácticas, técnicas y procedimientos de esta campaña #OpRussia predominan las filtraciones de información, presuntamente obtenida por ciberataques sobre sistemas informáticos en Rusia.

Tal como se menciona, algunos de esos actores han surgido específicamente en el contexto de la invasión rusa de Ucrania, mientras otros son ciberamenazas que han venido operando hasta el momento más en el ámbito de los foros de compraventa de exfiltraciones (leaks) que parecen haberse sumado por cuestiones de oportunidad al incremento de la temperatura cibernética a partir del escenario ucraniano.

[141] https://twitter.com/YourAnonTV/status/1505679705797713927
[142] https://twitter.com/_Blue_hornet/status/1505657400610721796
[143] https://breached.co/showthread.php?tid=813
[144] https://twitter.com/Ksecureteamlab/status/1505715248472465411
[145] https://kelvinsecteamcyber.wixsite.com/my-site/post/nestle-databreach, https://anonfiles.com/17QcmcQbx4/admin_user_csv, https://anonfiles.com/r0T1m7Q7x8/response_sql
[146] https://gofile.io/d/kyFj0A, https://anonfiles.com/f9W5KbP5xf/Nestle_zip
[147] https://therecord.media/nestle-denies-cyberattack-says-stolen-data-came-from-business-test-website/
[148] https://anonleaks.net/en/2022/anonymous-germany/20-terabytes-anonymous-germany-hijacks-data-from-rosneft-germany/



Además, y precisamente aprovechándose del momento, están surgiendo plataformas de exfiltraciones nuevas que ya sea más pretendidamente hacktivistas (como anonymousleaks.xyz) o dedicadas al cibercrimen (breached.co), se unen a las más clásicas (DDoSecrets) para replicar de una a otra los contenidos difundidos por los actores. Sea como fuere, en términos hacktivistas éste de la invasión rusa sobre Ucrania es un escenario donde las exfiltraciones de información de las que, en su mayor parte, queda dudosa constancia de sus mecanismos de obtención o de la naturaleza de las identidades atacantes, son las protagonistas. En su mayoría, estas exfiltraciones son atribuidas genéricamente a un colectivo 'Anonymous' o a actores "afiliados a Anonymous".

En cierto modo, todo este escenario de atribución a un genérico colectivo 'Anonymous' de ciberataques con resultado de filtración pública de información sensible contiene una paradoja. En realidad, el procedimiento de ciberataque de muchas de las acciones de filtración de información que divulgan canales en nombre del colectivo 'Anonymous' podría corresponderse con lo que se entendería, precisamente, por el uso de una "máscara" para mantener el anonimato hacktivista: atacantes, supuestamente movidos por una causa política o social (activismo) comprometen sistemas informáticos (hackeo) para reivindicar esa causa, actuando anónimamente (Anonymous) y reivindicando los ciberataques únicamente con único interés de visibilizar esa causa (hacktivismo). Sin embargo, ese escenario ideal no encaja del todo con la evolución histórica de 'Anonymous', pero sí muestra puntos de convergencia con la degradación del hacktivismo hacia una práctica oportunista a la que ciberamenazas, con otras motivaciones distintas del idealismo hacktivista originario, se acogen para disfrazar otras intenciones e intereses.

Al contrario de lo que ocurría prácticamente hasta la primera mitad de la década de 2010, en la actualidad no existe un colectivo 'Anonymous' como tal. Es cierto que sus partidarios siempre han pretendido que fuera sólo una idea, una causa de libre adhesión por cualquiera que compartiera unos principios, pero, aun así, 'Anonymous' se correspondía con una suerte de infraestructura distribuida más o menos estable, compuesta por configuraciones nacionales de hacktivistas que hacían parte de 'Anonymous' en Colombia, en Perú, en España o en Italia.

El hacktivismo que se gesta a partir de 2008 con 'Anonymous', que a su vez es heredero de otro hacktivismo previo, ponía el énfasis en actuar anónimamente, mediante ofensivas cibernéticas, en base a una causa reivindicativa, pero reuniéndose en grupos de identidades que desplegaban un conjunto de técnicas ciberofensivas y una campaña de comunicación. Entre esas técnicas, los ataques distribuidos por denegación de servicio eran predominantes, seguidos de las desfiguraciones de sitios web con contenido militante y de filtraciones de información, generalmente, aunque no sólo, obtenidas por inyecciones sobre bases de datos SQL. Esas acciones solían arroparse en una narrativa que se elaboraba en común por los participantes en las campañas hacktivistas, y la motivación, salvando excepciones, solía ser ideológica, con un cierto sesgo de idealismo.

Aquel **hacktivismo idealista** de principios de la década de 2010 se estructuraba principalmente en torno a esa "idea de Anonymous", en configuraciones que preservaban el anonimato, pero sin dejar de mostrarse como una estructura activista, dedicada a una causa y sin más propósito que visibilizar esa causa, habitualmente de tinte social o político. Dejando aparte algunas singularidades, la peligrosidad de esos activistas era moderada y, aunque los ciberataques producían intrusiones en sistemas informáticos y filtraciones de información, en acento estaba menos puesto en perjudicar sistemas que en hacer que las acciones transmitieran un mensaje reivindicativo.

Tal como estos informes anuales vienen reflejando a lo largo de varias ediciones, aquel hacktivismo idealista ha ido declinando en dos direcciones: 1) las configuraciones tipo 'Anonymous' en los distintos países han ido desapareciendo en términos operativos, manteniéndose canales de propaganda hacktivista en redes sociales pero disminuyendo la militancia de actores y la colectivización de campañas; 2) en paralelo a ese declive operativo de 'Anonymous', el hacktivismo ha ido confluyendo con ciberataques en donde los actores ya no están movidos por el idealismo de una causa social o política, sino por participar en secuencias preparatorias de la actividad de ciberamenazas avanzadas, movidas por intereses oportunistas, muchas veces con ánimo de lucro; esta segunda línea de hacktivismo conlleva mayor peligrosidad para los sistemas informáticos.

Con el decaimiento del hacktivismo idealista, 'Anonymous' había llegado a 2021 convertido, principalmente, en iconografía y propaganda en redes sociales, con ocasionales campañas que no llegaban a configurarse por falta de colectivización y adhesión de actores.

La paradoja que presenta para el hacktivismo el escenario de la invasión rusa de Ucrania es que esa idea clásica de 'Anonymous' que pretendidamente cualquiera puede arrogarse para llevar a cabo ciberataques en defensa de una causa, puede ser así mismo empleada para vestir con apariencia hacktivista ciberataques que son llevados a cabo con intenciones más lejos del activismo sociopolítico y más cerca de intereses geopolíticos.

No es que esos ciberataques mediados por "interés de parte" y, tal vez, desprovistos de "idealismo meramente ideológico" no puedan llevar el sello de 'Anonymous', siendo como es 'Anonymous', por definición, una idea abstracta no propietaria que cualquiera podría adjudicarse. Lo que parece evidente, al contrario, es que ese 'Anonymous' utilizado como canal de filtración de información sensible en un escenario de guerra híbrida como el de Ucrania en 2022 es una mutación del hacktivismo de la década de 2010: del **hacktivismo ideológico al hacktivismo oportunista**. Eso sin contar con la posibilidad de que el hacktivismo en general y la etiqueta 'Anonymous' en particular puedan ser instrumentados, en cualquier momento, como falsa bandera en circunstancias desinformativas de guerra híbrida.

Esta sospecha de un hacktivismo que puede ser contenedor de otros vectores de guerra híbrida ya está latente, incluso, en las comunicaciones de una de las plataformas web de filtraciones que se está haciendo popular en entornos hacktivistas: en las filtraciones de información que le son comunicadas a DDoSecrets como parte de acciones de 'Anonymous' o de otras identidades afiliadas a 'Anonymous', la plataforma está incluyendo en la divulgación de la información el siguiente aviso[149]: <<este conjunto de datos>> (el que se está divulgando al dominio público) <<se publica en el transcurso o en la continuación de una ciberguerra o guerra híbrida. Por tanto, hay probabilidades incrementadas de malware, motivaciones ocultas, datos alterados o implantados, o falsas banderas/personas>>.

[149] Por ejemplo, https://ddosecrets.com/wiki/VGTRK para una filtración atribuida a NG65, o https://ddosecrets.com/wiki/Capital_Legal_Services a 'Anonymous', entre otras.

En ese contexto de hacktivismo oportunista o de conveniencia puede conceptualmente encajar que, en torno a la invasión militar de Ucrania, haya ciberamenazas que lleven a cabo ciberataques con resultado de filtración de información al dominio público, firmen esos ciberataques como 'Anonymous' o como "actores afiliados a Anonymous", pero en realidad sean actores apoyados, o incluso constituidos, por alguno de los intereses en conflicto, sin que la mención de esa posibilidad en este informe suponga prejuzgar la legitimidad o no de cualquiera de esos intereses en conflicto.

Esta suposición no excluye que haya o pueda haber identidades con un histórico y/o motivadores más netamente del hacktivismo idealista tradicional que están participando o se sumen con ciberataques a la #OpRussia, sino que apunta la eventualidad de que la dinamización del escenario se esté dando mediante una instrumentación de la bandera 'Anonymous', que puede servir tanto para enmascarar motivaciones de guerra híbrida como para arrancar una campaña por parte de nuevas identidades militantes que adoptan un enfoque hacktivista, de primeras, ante la emergencia de un conflicto en Ucrania. Igualmente puede darse que, inicialmente empleada la etiqueta 'Anonymous' por partes interesadas en un escenario de guerra híbrida, la visibilidad de esa etiqueta sirva para atraer la implicación de identidades hacktivistas movidas por el idealismo de una causa.

En cualquiera de los casos, el escenario es de una amplia volatilidad, y tiene elasticidad suficiente como para que cualquier tipo de ciberataque, tenga la gravedad y el alcance que tenga, pueda ser reivindicado como **'Anonymous' en tanto bandera** de conveniencia; y, al mismo tiempo, también caben los escenarios combinados en donde alguna identidad hacktivista con mayor capacitación técnica decida sumarse a ciberataques en el contexto de la #OpRussia en función de sus propias motivaciones, y/o que los ciberataques que se están llevando a cabo sirvan como atractor para una campaña colectivizada en la que participen más actores de la escena hacktivista internacional. Lo que parece probable, si el conflicto continúa con la dinámica observada, es que el hacktivismo, sea como bandera de conveniencia o sea como catalizador ideológico primario, forme parte de las tácticas, técnicas y procedimientos de la guerra híbrida en el contexto de enfrentamiento militar entre Ucrania y Rusia.

8.2. Despedida de 'La 9ª Compañía de Anonymous'

El domingo 17 de abril de 2022, 'La 9ª Compañía de Anonymous' ('La 9 de Anon') publica un texto[150] en su habitual perfil en Tumblr en donde, titulando <<Hasta Siempre>>, afirman despedirse <<habiendo cumplido una década… en el hacktivismo>>. La nota de despedida está acompañada de un vídeo de 1:45 minutos de duración, situado por el propio actor en Vimeo[151] en 2015, donde se muestra una narrativa visual con simbología antisistema (Figura 8-2-1).

La nota de despedida menciona que 'La 9' considera llegado el momento de <<decir adiós>>, esperando que <<muy pronto otras tomen el testigo… bajo otras performatividades adaptadas al nuevo panorama cibernético>>. El texto refiere, así mismo, que, durante su trayectoria, 'La 9' ha <<perdido a algunas compañeras por el camino y de las tres que estuvieron en la idea primigenia, dos nos han dejado definitivamente. Sin vuelta de hoja>>, lo que podría haber influido en su evaluación de que actualmente no se considera capaz de <<cubrir nuestras múltiples y diversas facetas que nos han hecho tan particulares>>.

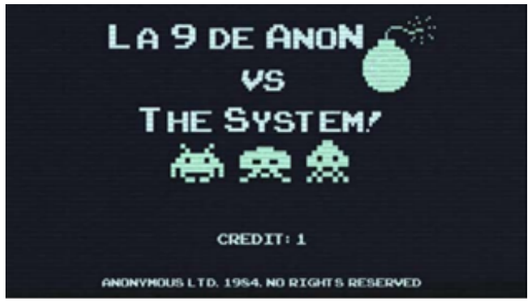
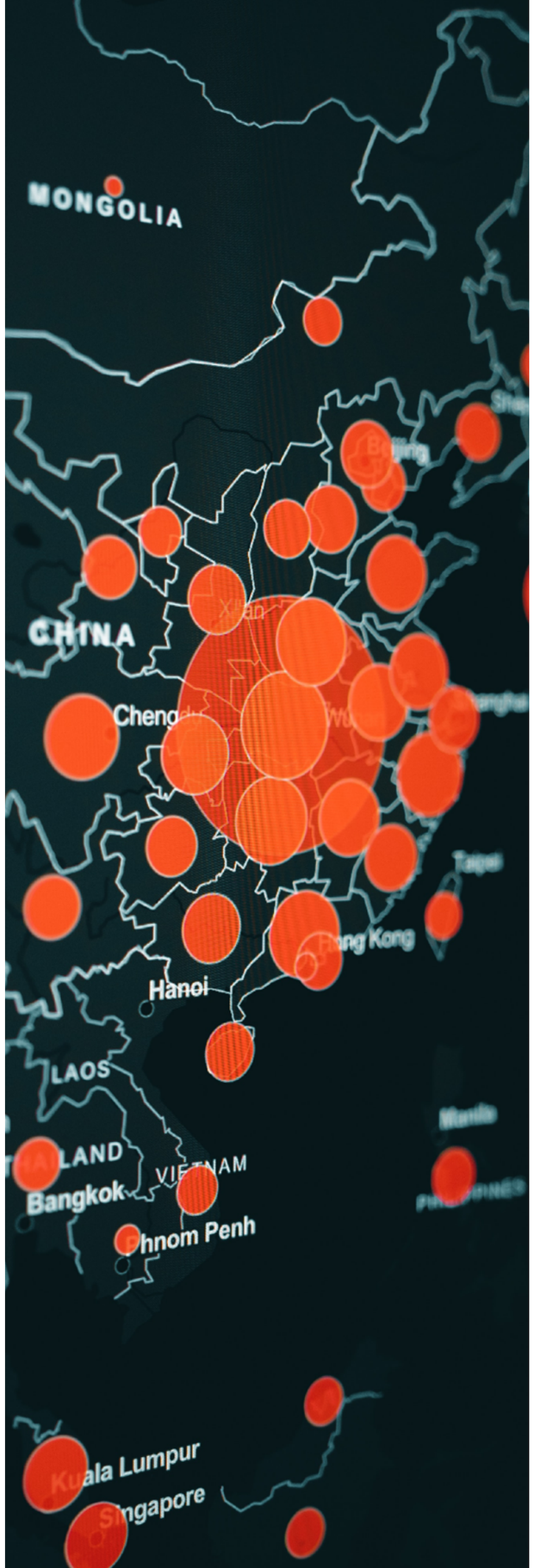


Figura 8-2-1

Dicha nota no contiene ninguna ciberamenaza explícita, así como tampoco proporciona elementos identificativos adicionales útiles. En síntesis, presenta la retirada de 'La 9ª Compañía de Anonymous' como actor hacktivista operativo con intenciones y capacidades ciberofensivas. El texto no descarta, por sí mismo, que alguno de los hasta ahora integrantes (o integrante) pueda continuar ejerciendo actividad hacktivista bajo otro alias, sino que se centra en el cese de operaciones de 'La 9' en tanto actor específico de ciberamenaza.

[150] https://la9deanon.tumblr.com/post/681801857785528320/hasta-siempre
[151] https://vimeo.com/146160054



8.3. Tendencias más probables en 2022-2023

• Continuando con una tendencia instalada desde hace más de media década, derivación del **hacktivismo** ideológico hacia **ciberataques vandálicos de baja/moderada peligrosidad explotando fallos comunes de código informático** en sitios web. Esta tendencia está alimentada por un paulatino desmembramiento interanual de configuraciones hacktivistas colectivas respondiendo a motivadores hacktivistas ideológicos, dando paso a un conjunto muy atomizado de identidades individuales desideologizadas con baja motivación para adherirse a los llamamientos militantes antaño propios del hacktivismo y, actualmente, reducidos a escenarios puntuales y, en la práctica, meramente retóricos.

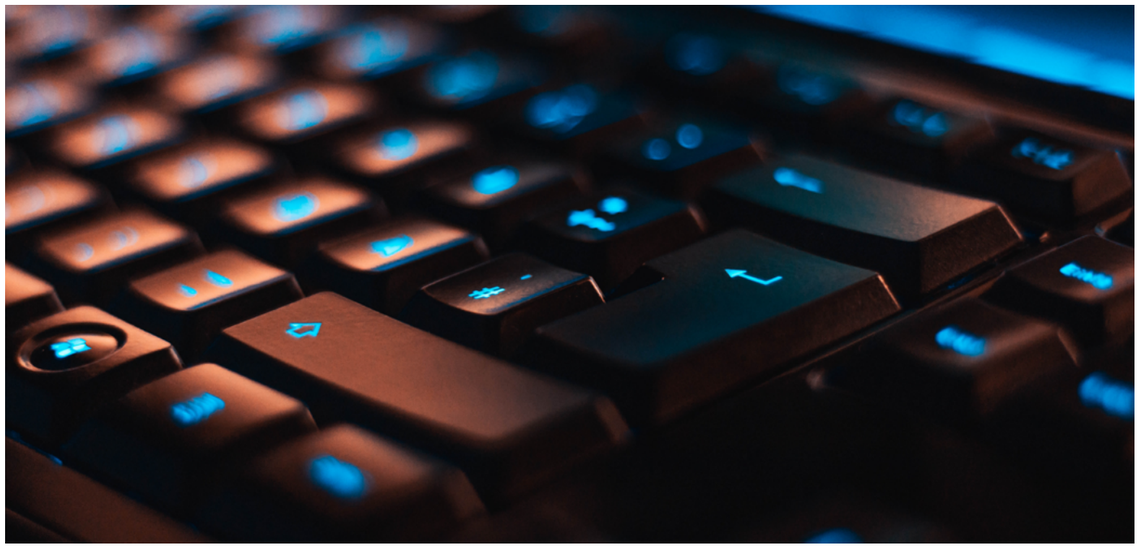
• La actividad de **identidades individuales de peligrosidad moderada o alta, movidas por razones ideológicas antisistema**, y dotadas de suficientes capacidades técnicas como para llevar a cabo ciberataques por penetración sobre servidores web de significación nacional o internacional, con el propósito 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**.

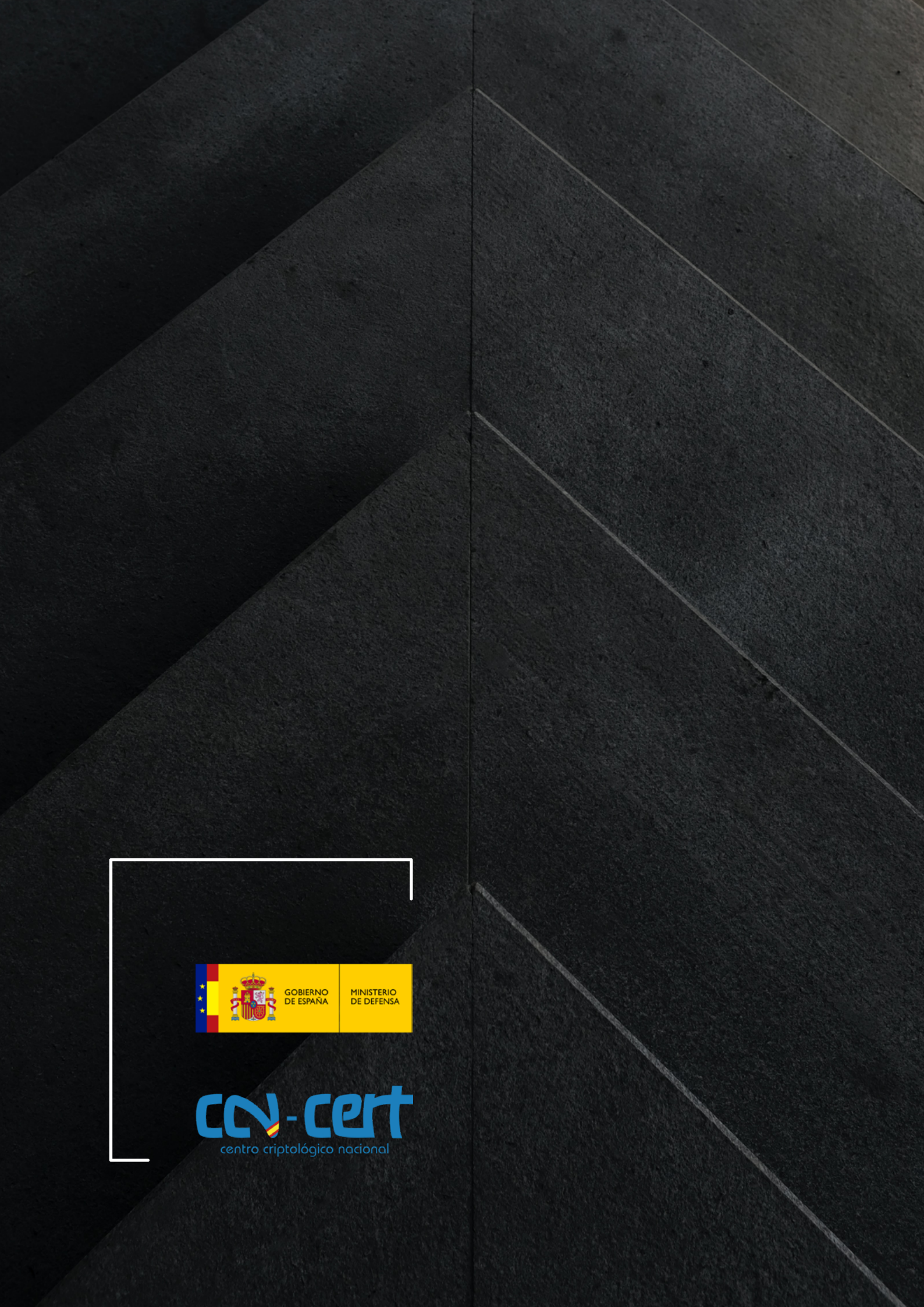
• Aumento de la **intersección entre los reductos vandálicos hacia los que ha desembocado el hacktivismo y la vulneración de sitios web como práctica instrumental para ciberamenazas de propagación de código informático malicioso**, entre las cuales están la intoxicación SEO y el redireccionamiento de tráfico mediante inserción de scripts maliciosos, estos últimos pudiendo conducir tanto a infraestructuras de difusión de contenidos no deseados, como a webs con apariencia de comercio electrónico diseñadas como trampas de phishing, o a la propagación de varias familias de código informático dañino, como los troyanos o el software espía.

• Los ciberataques por desfiguración de sitios web continuarán teniendo en **la explotación de vulnerabilidades en sitios web provistos de software desactualizado** su principal **vector de ciberataque**.

• En paralelo a un declive de 'Anonymous' y del hacktivismo como fenómenos idealistas, ideológicamente motivados, podría darse un aumento paulatino en la instrumentación del **hacktivismo y de 'Anonymous' como banderas de conveniencia** en conflictos híbridos o en ciberataques donde confluyen varios intereses de parte por actores que pretenden una ganancia, ya sea geopolítica, militar, económica o de otra naturaleza. Este hacktivismo de conveniencia u oportunista, que posee mayor peligrosidad que el hacktivismo idealista clásico, podría dar más visibilidad a una suerte de colectivo 'Anonymous' mutado hacia una herramienta de guerra híbrida, una de cuyas características sería seguir presentándose ante la opinión pública como hacktivismo ideológico.

• El denominado "**ciberyihadismo**" tiene probabilidad de continuar siendo un **fenómeno empíricamente inexistente**, instrumentado en sus símbolos y narrativas proislamistas por identidades con **intenciones de falsa bandera**.




GOBIERNO
DE ESPAÑA
MINISTERIO
DE DEFENSA
CCN-CERT
centro criptológico nacional