GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

CCN-CERT centro criptológico nacional

CCN-CERT IA-07/18

Informe Anual 2017
Hacktivismo y Ciberyihadismo

Mayo 2018

Edita:

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA DEL GOBIERNO
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

CCN Centro Criptológico Nacional

Fecha de Edición: mayo de 2018

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

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

ÍNDICE

1. SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL

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

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

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

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

2. RESUMEN EJECUTIVO

El año 2017 no solo ha servido para dar continuidad a la situación observada desde 2014 de inexistencia de una infraestructura hacktivista estable en España, sino que ha constatado que el hacktivismo en general, en tanto fenómeno social, o 'Anonymous' en particular, como una de sus articulaciones, son expresiones que se quedaron en el pasado. Durante 2017 no se han constituido identidades hacktivistas con vocación de colectivo militante en España. No obstante, 'La 9ª Compañía' continúa siendo la única identidad activa, que desarrolla ciberataques, adscrita a lo que podría considerarse un ideario hacktivista.

La #OpCatalunya constituye el mejor ejemplo del hacktivismo en España: un escenario de conflictividad social definido por factores políticos, teóricamente ideal para militancias hacktivistas. En su caso, no solo no ha encontrado una infraestructura de desarrollo en España, sino que se ha articulado en una campaña de muy baja intensidad, promovida por identidades hacktivistas desde el exterior de España, sin cohesión colectiva. Sus habilidades técnicas de nivel principiante y su incapacidad para lograr la adhesión de un tejido hacktivista internacional, al igual que el español, denota que se encuentra falto de mentalidad común, de columna vertebral y de musculatura.

El caso de España, no obstante, no es más que el reflejo de lo que sucede a nivel europeo, iberoamericano o internacional. La evidencia demuestra que el hacktivismo asociado a 'Anonymous' está agotado o a la espera de ser reinventado. Las escasas campañas con narrativa hacktivista han recibido bajo apoyo, baja socialización, y la participación de identidades de nivel técnico principiante que no han sido capaces de suponer una ciberamenaza. Por el contrario, la mayoría de identidades hacktivistas que han atacado internacionalmente se dedican al "**hacktivismo oportunista**".

En definitiva, el **hacktivismo** se ha desconectado de escenarios de protesta social para convertirse en un fenómeno oportunista, centrado en ataques de identidades individuales ajenas a cualquier ideología que no sea inyectar su alias, logotipo o reivindicación personal en webs con alta vulnerabilidad de fácil explotación. En cuanto a **ciberyihadismo**, al igual que en años previos, durante 2017 se ha confirmado que no existen evidencias directas ni indicadores indirectos que sugieran que el 'Daesh' haya desarrollado una división específica destinada al desarrollo de acciones ciberofensivas contra servidores web u otros medios tecnológicos.

Asimismo, se ha constatado que la denominación "cibercalifato" no se corresponde con una identidad única, sino con un conjunto borroso de identidades hacktivistas parásitas no vinculadas orgánicamente al 'Daesh. Probablemente, ni siquiera simpaticen con su ideología, sino que utilizan instrumentalmente sus referencias a modo de provocación o para dar una falsa impresión sobredimensionada de su propia capacidad de amenaza. Todo ello con el fin de llevar a cabo cibertataques

por desfiguración contra sitios webs vulnerables de bajo perfil, insertando consignas islamistas generales o más concretas que simulan apoyar al 'Daesh'.

Es decir, el "cibercalifato" no existiría como una estructura orgánica del 'Daesh' sino como un concepto parasitado desde identidades hacktivistas individuales como táctica de provocación, principalmente.

3. HACKTIVISMO EN ESPAÑA

3.1 Estructura hacktivista en España

El año 2017 no sólo ha servido para dar continuidad a la situación observada desde 2014 de inexistencia de una infraestructura hacktivista estable en España, sino que ha constatado que el hacktivismo en general, en tanto fenómeno social, o 'Anonymous' en particular, como una de sus articulaciones, son expresiones que se quedaron en el pasado.

En efecto, durante 2017 no se han constituido identidades hacktivistas con vocación de colectivo militante en España. 'La 9ª Compañía' continúa siendo la única identidad activa, que desarrolla ciberataques, adscrita a lo que podría considerarse un ideario hacktivista: ejecución de acciones criminales sobre sistemas tecnológicos web justificadas con narrativas de sesgo social o político.

En este panorama de desertización hacktivista en España, ocasionalmente aparecen y desaparecen identidades que muestran alguna intencionalidad ofensiva, con mayor o menor capacidad técnica y con errático potencial de continuidad. El mejor ejemplo de este tipo de identidades fluctuantes es '**ACAB Gang**', que en 2017 ha mostrado capacidad técnica para desarrollar algunas acciones, para las que emplea una estética 'Anonymous' bajo una marcada narrativa antisistema. Esta identidad apareció en 2016 y constituyó perfiles en redes sociales (actualmente presente en Facebook y Twitter[1]) e incluso una web de vida breve[2], realizando algunos ataques puntuales. Alguna otra identidad con presumible radicación en España, como '**c0g0ll0**', ha actuado individual y casi imperceptiblemente con algún ataque personalista de bajo perfil sin rubro ideológico hacktivista.

Sin embargo, la #OpCatalunya es el mejor ejemplo del que podría calificarse como "*estado comatoso*" del hacktivismo en España en 2017: un escenario de conflictividad social definido por factores políticos, teóricamente ideal para militancias hacktivistas.

En su caso, no solo no ha encontrado una infraestructura de desarrollo en España, sino que se ha articulado en una campaña de muy baja intensidad, promovida por identidades hacktivistas desde el exterior de España sin cohesión colectiva. Sus habilidades técnicas de nivel principiante en general, y su incapacidad para lograr la adhesión de un tejido hacktivista internacional que, al igual que el español, denota que se encuentra falto de mentalidad común, de columna vertebral y de musculatura.

[1] https://www.facebook.com/AnonymousACAB/, https://twitter.com/ACABGvng
[2] acab.team

En torno a la #OpCatalunya aparecieron identidades oportunistas generalmente para cumplir funciones de propaganda, lanzar ataques individuales por denegación de servicio de baja capacidad o usar herramientas automáticas como SQLmap para realizar, con poca pericia, escaneos de vulnerabilidad sobre webs de menor significación. Una de estas identidades en España fue '**XeljomudoX**', que actuaba hasta su arresto policial.

3.2 Operaciones hacktivistas en España

En cuanto al desarrollo de narrativas hacktivistas para sustanciar ciberataques específicamente centrados sobre España, durante 2017 se ha mantenido la ausencia de este tipo de justificaciones ideológicas, que ha venido observándose desde 2014 –con la excepción del último trimestre de 2017–.

Es en ese último periodo de 2017, cuando se inicia la **#OpCatalunya**, un llamamiento reivindicativo a desarrollar ataques hacktivistas, que se establece como reacción al conflicto secesionista en torno al referéndum proindependentista organizado en Cataluña en octubre de 2017.

Aparte de ese marco en Cataluña, se han repetido propuestas realizadas por identidades individuales de propaganda hacktivista que ni estaban mínimamente desarrolladas en el plano narrativo para ofrecer un marco hacktivista motivador, ni promovidas por identidades que tuvieran habilidades técnicas como ciberamenaza o capacidad para socializar sus propuestas. Ejemplos de estas propuestas, que por sus débiles características estructurales más que iniciativas colectivas podrían ser calificadas de "ocurrencias" de individuos aislados, han sido la **#OpSaveSpain,** en enero, y **#OpLexnetACascarla,** en septiembre de 2017.

Además, al igual que en años previos, el hacktivismo operativo con raíz en España –es decir, desarrollado por identidades con supuesto origen y asentamiento en el país- ha estado protagonizado casi en exclusiva por la '**La 9ª Compañía**'. No obstante, la identidad '**ACAB Gang**' ha llevado a cabo algunas acciones puntuales sin mostrar vocación de permanencia militante.

En términos cuantitativos, el panorama hacktivista en España durante 2017 ha continuado dominado por ciberataques por desfiguración llevados a cabo por identidades externas a España en el contexto de acciones de oportunidad, explotando vulnerabilidades en gestores comerciales de contenidos y afectando simultáneamente a varios países. Es decir, no han sido ataques con centralidad geográfica, sino con centralidad tecnológica –vulnerabilidades web–, que se han desarrollado en oleadas en las que las IPs de la víctima han sido un factor accesorio y ocasional.

3.2.1 'La 9ª Compañía'

Del mismo modo que en los dos años previos, durante 2017, 'La 9ª Compañía' ha mantenido una pauta mensual de ciberataques, con un receso en agosto y septiembre.

Asimismo, la tipología de ciberataques continúa sin variar, desarrollando principalmente acciones por penetración sobre servidores web, explotando diversas vulnerabilidades. Estos ataques han mostrado, en su ejecución, estar en disposición de aplicar habilidades técnicas y conocimientos suficientes en tecnologías de red, de servidores, de desarrollo web o en la operación de software de penetración incluido en la suite Metasploit.

Durante el primer trimestre vulneró la web informativa que el grupo Prensa Ibérica[3] dedica a los premios cinematográficos Oscar y Goya, inyectando un texto con retórica militante antisistema y descalificatorio con la política. Adicionalmente, ´La 9ª Compañía´ divulgó en Twitter supuestas contraseñas de acceso a otras webs del grupo Prensa Ibérica. Amenazó también con "intervenir" en el contexto de la huelga de estibadores portuarios, en curso en ese momento, sin traducir esa amenaza en ningún ciberataque reivindicado.

En el segundo trimestre, 'La 9ª Compañía' inyectó contenido en la web de la empresa tecnológica de soluciones de conectividad en red, Zyxel[4]; y logró acceso ilícito al servidor web de CEDRO[5], el órgano que en España gestiona los derechos de copia de publicaciones con propiedad intelectual.

También reivindicó el acceso ilegítimo a la web de la Asociación de Empresarios de Sada e As Mariñas (AESADA) en Galicia[6] y aplicó una inyección SQL sobre la web de la franquicia de clínicas dentales iDental[7], acusándola de "fraude a clientes" y "mala praxis", entre otras insinuaciones.

A pesar de que en el tercer trimestre el atacante permaneció mayormente inactivo, en este periodo accedió a un subdominio de gestión interna del servidor de la web de grupo de comunicación español Vocento[8], sin exfiltrar información en el dominio público. Además, realizó una desfiguración parcial en la web del Ayuntamiento de Guadalajara, inyectando en ella[9] una composición gráfica reivindicativa en el contexto informativo de la exhumación de Timoteo Mendieta −miembro del sindicato UGT, fusilado durante la Guerra Civil española de 1939−.

[3] premios-cine.com
[4] zyxel.com
[5] cedro.org
[6] aesada.com
[7] asistenciadentalsocial.com
[8] support.vocento.com
[9] guadalajara.es

'La 9ª Compañía' iniciaba el último trimestre del año comprometiendo los servidores web del Sindicato Unificado de Policía[10], produciendo una desfiguración y mostrando en Twitter contenidos que sugerían que habían accedido al conjunto de su base de datos de alumnos de cursos, aunque no se exfiltraron esos datos al dominio público.

Posteriormente, inyectó varios contenidos irónicos en la web de la Plataforma Sindical de Policías Locales[11], como si Policía Municipal de Madrid (España) "defendiera un ideario fascista". Esta acción fue enmarcada en la polémica creada por la filtración en prensa del contenido de Whatsapp de un grupo de Policías Municipales de Madrid. Finalmente, al acabar el año, 'La 9ª Compañía' penetró en un servidor de la compañía española Indra, comprometiendo una de sus instancias en los servidores cloud de Azure[12] creando un subdominio[13] e inyectando sobre él una composición gráfica reivindicativa con el logotipo del atacante.

3.2.2 Marcos narrativos hacktivistas

La **#OpCatalunya** ha representado durante 2017 el único marco narrativo de naturaleza hacktivista originado en España, que ha servido para poner de manifiesto la falta de organización de un tejido hacktivista operativo en el país; la relegación del movimiento 'Anonymous' a débiles perfiles de propaganda sin iniciativa, dedicados a redifundir información en redes sociales; y en línea con lo que sucede internacionalmente, la desconexión del hacktivismo de escenarios de protesta social para convertirse en un fenómeno oportunista, centrado en ataques de identidades individuales ajenas a cualquier ideología que no sea inyectar su alias, logotipo o reivindicación personal en webs con alta vulnerabilidad de fácil explotación.

Las acciones preliminares de la #OpCatalunya comenzaron el 24/9/2017 cuando se publicó en Pastebin un "Comunicado de Anonymous España sobre la Situación en Cataluña"[14], en español, que no contenía semántica de amenaza, sino que se limitaba a repetir consignas-clichés contra el Partido Popular y el Gobierno de España, y se mostraba a favor del diálogo con Cataluña.

Ese mismo día, en igual línea narrativa ideológica y sin amenaza, las identidades de propaganda '**Anonymous Video**' y '**Team Poison**' compartieron en Youtube[15] un vídeo de 1'13" de duración con el título "Operation Free Catalonia". Esta pieza, que tenía una portada en idioma español con **#OpCatalunya**, exponía con una voz digitalizada una retórica típica a favor del derecho de autodeterminación para Cataluña, atribuyendo

[10] sup.es, supformacion.es
[11] pspl.es
[12] azurewebsites.net
[13] la9deanon.azurewebsites.net
[14] https://pastebin.com/vkbG8Wcc
https://www.youtube.com/watch?v=f4cAkfTYDrA,https://www.youtube.com/watch?v=aC00AxQ_U64

"raíces históricas" a los deseos catalanes de autogobierno y "represión" a un gobierno en España "heredero del neofranquismo"; más allá de esta narrativa, no contenía elemento de amenaza explícita.

También en el mes de septiembre, se publicó un texto no firmado en Pastebin[16], titulado "#OpEspana JTSEC target#1 (Ministry of Education)", que listaba varias IPs del Ministerio de Educación de España. El formato sugería que se había realizado un escaneo simple para obtener IPs relacionadas con el Ministerio de Educación. Además, el 1/10/2017, la identidad italiana '**AnonPlus**' inyectó, sobre una URL de la web de la Comunidad de Madrid[17], contenido reivindicativo generalista en inglés sin alusiones al referéndum, aunque posteriormente fue etiquetado como #OpCatalonia en mensajes en Twitter.

Durante el mes de octubre de 2017 y principalmente con el impulso de identidades hacktivistas externas a España – como '**Nama Tikure**' ligada a Grecia y operando como 'Anonymous Greece'; o '**AnonPlus**', a Italia− se ejecutaron alrededor de 80 acciones repartidas entre ataques individuales por denegación de servicio−con muy baja socialización contra webs gubernamentales en España−, e inyecciones SQL defectuosas o de alcance mínimo. Estas acciones revelaron la débil capacidad técnica por parte de los atacantes sobre webs que mostraban vulnerabilidades convencionales ante escaneos simples con la herramienta SQLmap.

En noviembre se llevaron a cabo algo más de una veintena de acciones de la misma tipología, decayendo la cifra en diciembre, sin aumentar la peligrosidad de los ataques. Adicionalmente, en estas acciones tomarían parte identidades presumiblemente externas a España como '**Giant's PS**', '**Gaben Security**' o '**FSecurity**'. En este mes también comenzó a operar la identidad española

Alrededor de las identidades que articulaban la mayor parte de las acciones ofensivas de muy baja intensidad, aparecían y desaparecían alias oportunistas de propaganda con nulo efecto operativo y baja capacidad de propaganda reales: 'CatCia', 'Anonymous Catalonia', 'UnitedSecAnon', 'Anonymous_Opt' o 'Catalonia Cyber Army'.

También en noviembre de 2017 comenzó a operar la identidad española '**XeljomudoX**' con ataques iSQL de baja habilidad técnica sobre algunas webs de Ayuntamientos y universidades, o ataques individuales por denegación de servicio contra webs gubernamentales. En febrero de 2018 la Guardia Civil procedería al arresto de un varón de 30 años de edad, residente en Tarragona, supuestamente responsable de las acciones de este alias hacktivista.

[16] https://pastebin.com/nSqG24CT
[17] madrid.org/legislatura-ignacio-gonzalez/cache/

En definitiva, y a pesar de tener todas las características “sobre el papel” para poder convertirse en una “operación ciberactivista” con atractivo global (típico escenario social que habría convocado la reactividad ‘Anonymous’ en los años 2014 o 2015), la #OpCatalunya se caracterizó, en el último trimestre de 2017, por ser un marco hacktivista muy limitado por su escasa colectivización de la propuesta y por el bajo nivel tanto de intensidad y de peligrosidad, debido a una muy débil capacitación técnica de las identidades ciberactivistas atacantes.

3.2.3 Acciones no adscritas

El 4 de abril de 2017, ‘**ACAB Gang**’ desfiguró subdominios de la web del colectivo ‘Hazte Oír’[18] inyectando un texto en el que se reivindicaba la acción por los “derechos del colectivo LGBT (lesbianas, gays, bisexuales, transexuales), Figura 3-2-3-1. El primero de los subdominios vulnerados empleaba Wordpress; y el segundo, un gestor de contenidos de código abierto para comercio electrónico, CubeCart.

Al día siguiente, la identidad amenazó a ‘Hazte Oír’ con “publicar todos sus archivos” y difundió, en una cuenta de Twitter[19] ya clausurada, capturas de pantalla que sugerían que podría haber obtenido acceso ilegítimo al buzón de correo electrónico en Gmail del presidente de ‘Hazte Oír’, Ignacio Arsuaga. Igualmente, secuestró algunos perfiles de redes sociales relacionados con ‘Hazte Oír’ − en Instagram, @derechoavivir; en Twitter, @WCFMadrid2012, @familiasociedad; y en Youtube, de ‘CitizenGO’−, e inyectó en ellos iconografía ciberactivista.

Figura 3-2-3-1.

[18] blogs.hazteoir.org, tienda.hazteoir.org
[19] https://twitter.com/ACABGang/status/849613115507576832

El 17 de mayo de 2017 '**ACAB Gang**' reclamó haber desfigurado un subdominio de la web del Cuerpo Nacional de Policía de España, inyectando, presumiblemente en una URL[20], el contenido "encryptCp no rule", probablemente refiriéndose a que la página alterada empleaba protocolo https. Una muestra del contenido inyectado fue situada en el repositorio Archive.is[21] (Figura 3-2-3-2).

Figura 3-2-3-2.

En julio, '**ACAB Gang**' secuestró el perfil en Twitter de Bolsa.com[22] –canal informativo sobre mercados financieros con 21.500 seguidores– modificando la descripción púbica de la cuenta y sustituyéndola por el mensaje "hacked by #ACABGang". Publicó además un mensaje con el texto "todos los archivos de la bolsa están en nuestro poder" (Figura 3-2-3-3). No obstante, la acción no afectó a la web del canal[23], de lo que se infería que el ataque podría haberse limitado al perfil en Twitter.

Figura 3-2-3-3.

3.2.4 Ciberataques por entidades externas a España

Continuando con el patrón de años previos, durante 2017, el desarrollo de ciberataques por desfiguración contra sitios web con IP en España ha permanecido como escenario predominante y definitorio de la amenaza hacktivista en España. Los ataques se han llevado a cabo principalmente por identidades que, en los contenidos

[20] webpol.policia.es/e-hotel/index.html
[21] http://archive.is/BvHhg
[22] @Bolsacom
[23] Bolsa.com

inyectados en las desfiguraciones, han mostrado rasgos culturales norteafricanos, turcos e indonesios.

Los sitios web atacados pertenecían a pequeñas empresas o negocios de baja visibilidad y sin relación con un sector específico. La afectación a estas webs se ha producido en general en el contexto de oleadas de desfiguraciones contra webs en varios países. Esta circunstancia, junto al hecho de que los ciberataques por desfiguración contra webs en España no se hayan apoyado en narrativas negativas mencionando al país o a lo español, sugiere de forma consistente que las acciones hacktivistas no se han desarrollado sobre motivadores que tengan centralidad en España, sino sobre razones de oportunidad comunes a los ciberataques a cualquier otro país.

En conjunto, durante 2017, fueron atacados por desfiguración 6.356 sitios web con IP en España. Los meses de agosto y septiembre acumularon los mayores picos (más de 1.300 acciones por mes); y febrero y mayo, los menores (por debajo de 100 cada mes), Figura 3-2-4-1. Estos picos no suelen ser definitorios de un patrón, puesto que se configuran principalmente por la existencia de algunas oleadas de desfiguraciones masivas en varios países explotando una vulnerabilidad activa, generalmente en gestores comerciales de contenidos y común a una misma tipología de web. Esta explotación dispara coyunturalmente la volumetría de webs afectadas; es decir, son picos de coyuntura y, por tanto, raramente son útiles para hacer comparaciones interanuales.

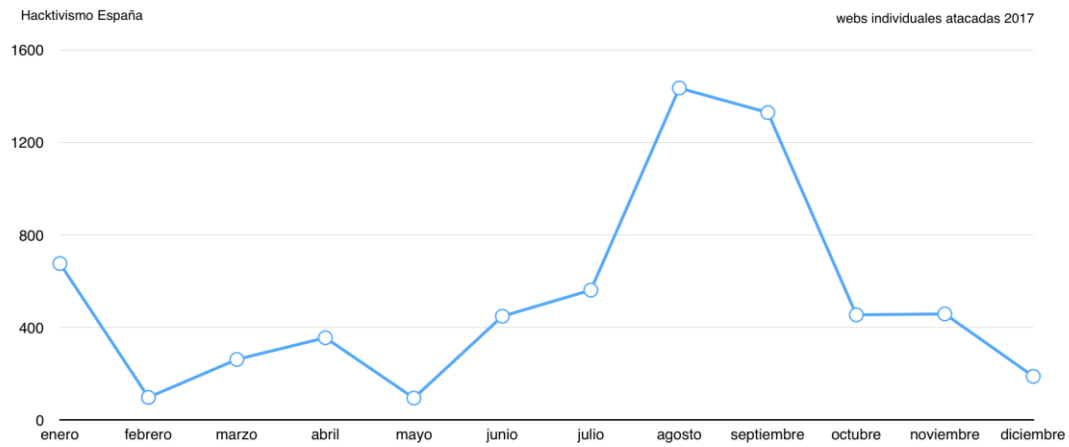


Figura 3-2-4-1.

En términos comparativos, este volumen anual de ciberataques sitúa a España aproximadamente en el 11% de impacto a nivel mundial. Se calcula que mensualmente se reivindican entre cuatro y cinco mil acciones por desfiguración a escala mundial, de manera que **los ciberataques hacktivistas recibidos en España en todo un año**

equivaldrían cuantitativa y aproximadamente a los que se llevan a cabo en sólo un mes a nivel global.

El patrón observado en años precedentes permite establecer una relación directa entre la probabilidad de que una web sea objetivo de un ataque hacktivista de desfiguración y que esta haya sido desarrollada con un gestor de contenidos. Este patrón es cierto y consistente tanto en España como en Europa o el resto del mundo.

En España, un 96% de las webs desfiguradas en cibertaques hacktivistas están desarrolladas tomando como base un gestor comercial de contenidos; siendo Wordpress, con un 74%, y Joomla, con un 14%, los gestores cuyas versiones han mostrado mayor vulnerabilidad de ser deformados por un ciberataque. Entre los gestores de comercio electrónico, Prestashop ha recibido el mayor volumen de ataques (8%), con Magento en una lejana segunda posición con menos del 0'1% de acciones

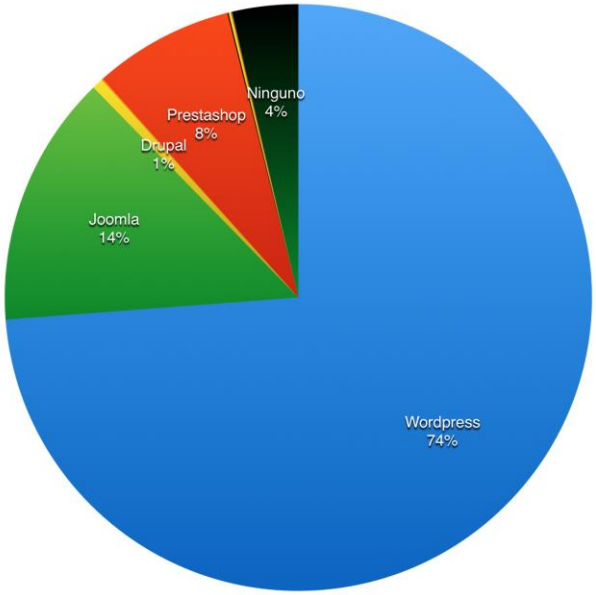


Figura 3-2-4-2.

recibidas. (Figura 3-2-4-2)

La dominante posición interanual en la volumetría de victimología hacktivista de webs desarrolladas con gestores comerciales de contenidos, unido a la ausencia de centralidad nacional de los ciberataques y el desarrollo de las acciones sin una narrativa atacante reivindicativa concreta de carácter político o social, sugiere que el hacktivismo en España, al igual que el resto del mundo, ha sido durante 2017 un **hacktivismo oportunista**.

Las identidades que más habitualmente han desfigurado webs en España, explotando probablemente vulnerabilidades en gestores comerciales de contenidos, se representan en la siguiente tabla:

Identidad	Origen	Gestor comercial empleado por la web atacada
'Attacker Gaza' / 'Anonymous Ghost Gaza'	Argelia	Wordpress y Joomla
'MuhmadEmad' / 'SA3D'	Prokurdo	Prestashop y Wordpress
'ERORDZ'	Argelia	Wordpress, Liferay, Drupal
'RxR'	Indonesio / turco (sin confirmar)	Wordpress
'Dr.Silnt HilL'	Egipcio	Wordpress
'Chinafans' o 'VandaTheGod'	Brasil (sin confirmar)	Wordpress y Joomla
'Anonymous Fox'	Norteafricano	Prestashop y Wordpress
'Mr.Spy' o 'Et04'	Norteafricano (sin confirmar)	Wordpress y Joomla
GeNErAL	Desconocido	Wordpress
'Alarg53'	Desconocido	Prestashop y Wordpress
'Ayyildiz Tim' o 'TheWayEnd'	Turco	Wordpress y Joomla
'CyBeRIZM', 'ZoRRoKiN' o 'KingsKrupellos'	Desconocido	Open Journal System y Drupal
'Zedan-Mrx'	Desconocido	Wordpress
'BD_LEVEL_7'	Bangladesh	Wordpress
'magelang6etar'	Desconocido	Joomla
'LUN4T1C0'	Desconocido	Wordpress
'Tobitow'	Argelia	Joomla

Los ciberataques hacktivistas sobre sitios web con IP en España no han mostrado elementos que sugieran que alguna de las acciones estuviera dirigida contra estas webs por ser españolas o representar a España.

Ni siquiera en el incidente de agosto de 2017 de '**OurMine**'[24], cuando esta identidad comprometió el perfil de Twitter del F.C. Barcelona[25] –@FCBarcelona, con más de 23 millones de seguidores (Figura 3-2-4-3)– con mensajes de naturaleza reivindicativa y sin contenido político, aparecían indicadores de amenaza centrados en España. La elección de objetivos representativos españoles fue coyuntural en el histórico de las acciones de visibilidad que perseguía esa identidad atacante en su actividad.

[24] Identidad conocida por realizar ciberataques que conllevan al acceso ilícito y al secuestro coyuntural de perfiles de alta influencia en redes sociales –principalmente cuentas de responsables de empresas tecnológicas, de redes sociales o de medios de comunicación en EE.UU.–

[25] El grupo cyberhacktivista 'Syrian Electronic Army' ya vulneró, en febrero de 2014, el perfil en Twitter del FC Barcelona publicando mensajes reivindicativos.

En alguno de los mensajes de **'OurMIne'** se utilizaba el contexto de fichajes del club deportivo y se proponía la etiqueta #FBCHack para ser compartida en redes sociales.

Figura 3-2-4-3.

Asimismo, 'OurMine' repitió la operación vulnerando, también en el mes de agosto, el perfil de Twitter del equipo de fútbol del Real Madrid (@RealMadrid, con más de 25'6 millones de seguidores de la cuenta), emitiendo varios mensajes irónicos sobre fichajes de futbolistas (Figura 3-2-4-4).

Figura 3-2-4-4.

3.2.5 Acciones con narrativas islamistas o proyihadistas

Durante 2017 no se han producido ciberataques de naturaleza hacktivista sobre webs en España que fueran motivados o canalizados a través de narrativas islamistas, proyihadistas, o que mostraran algún tipo de simpatía por el 'Daesh'.

No obstante, han incidido acciones por desfiguración sobre webs con IP en España, en el contexto de ataques sobre varios países, en las que los autores han inyectado contenido que aludía al islam o a su profeta Mahoma, sin concretar simbología ideológica ni mostrar intencionalidad geopolítica.

En julio de 2017, '**King almafia**' desfiguró webs en España[26] inyectando contenido en inglés y en árabe con alabanzas al profeta Mahoma y a los musulmanes (Figura 3-2-5-1); contenido que también fue utilizado en acciones contra webs en Emiratos Árabes o Alemania.

También ese mismo día, '**SOK**', identidad que menciona a 'King almafia' en el contenido inyectado en sus ataques, desfiguró 16 webs[27], la mayoría basadas en Wordpress. En ellas inyectó contenido alusivo al islam en inglés ("Islam will win soon very soon[28]") e iconografía propia de la Intifada palestina.

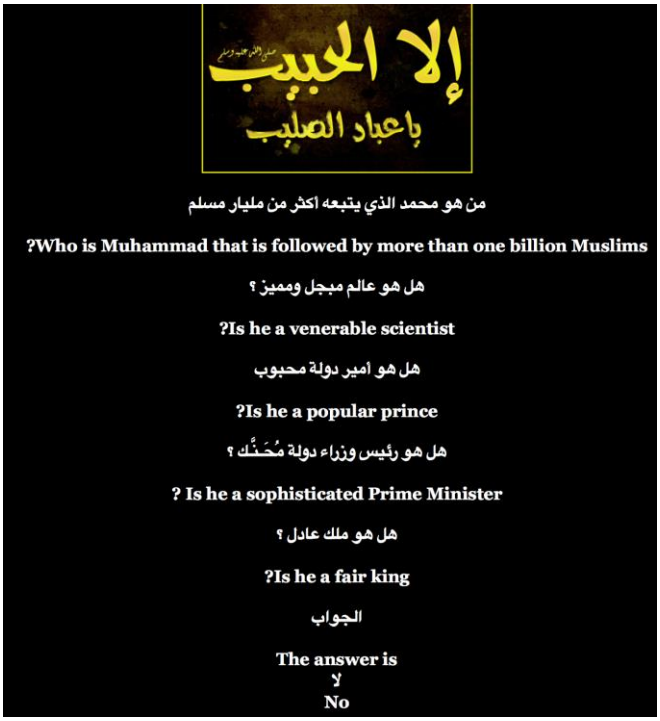


Figura 3-2-5-1.

[26] solidaridadconcuba.com, aixia.es, damasdeblanco.com, traveltocubainfo.com
[27] entre ellas parischic.es, fincaspemar.es, revistatodo.com
[28] "El islam ganará pronto, muy pronto"

Los días 11 y 12 de agosto de 2017, '**Team CC**' alteró una decena de webs en España[29] y otras tantas en Polonia, basadas en el gestor de contenidos Wordpress. En ellas, alternó la inyección de contenido general con el que combinaba el texto "hacked by Po!sonous… Muhamad is the Messenger of Allah" con imágenes alusivas al Islam (Figura 3-2-5-2).

Figura 3-2-5-2.

4. HACKTIVISMO EN IBEROAMÉRICA

4.1 Panorámica hacktivista en Iberoamérica

La actividad hacktivista en Iberoamérica disminuyó sensiblemente en 2017 con respecto a años precedentes. Las operaciones o campañas denominadas habitualmente con el símbolo "#" se redujeron a un cuarto de los propuestos durante 2016.

Los elementos a destacar del hacktivismo centrado en Iberoamérica durante 2017 son:

- Confirmación de la desactivación de 'Anonymous Iberoamérica' como clúster hacktivista en la región.
- Ausencia de tejidos hacktivistas estables tanto a nivel regional como nacional, con carencia de infraestructuras estables de comunicación y de propaganda más allá de perfiles individuales en Twitter y Facebook. En países donde en años previos se observó una intencionalidad más o menos estable de identidades hacktivistas alrededor del fenómeno 'Anonymous' –como Brasil, México, Colombia, Perú o Chile– se aprecia un paulatino declive de la colectivización hacktivista –más marcado en Brasil o México– donde se ha pasado de 'Anonymous' como fenómeno a 'Anonymous' como ausencia. Además, se ha observado en Chile y en Perú una progresiva inactividad de los 'Chilean' y 'Peruvian Hackers'.

[29] entre ellas todoenmamparas.com, congresoed.org, blogune.org

- Bajo apoyo y colectivización de las narrativas hacktivistas propuestas como campañas de ciberataque ante determinados escenarios sociales en algunos países de Iberoamérica.
- Predominio general de acciones coyunturales y ocasionales de identidades individuales, muy activas y sin demasiada centralidad geográfica, como ocurre con varios atacantes hacktivistas brasileños.

A pesar de que en prácticamente todos los países de Iberoamérica no ha habido campañas coordinadas con potencial de colectivización, en Brasil y, en menor medida, en México han destacado oleadas de ataques contra webs del Gobierno local o federal[30]. No obstante, en Brasil también han sido objetivos preferentes webs de universidades federales y regionales.

En la mayoría de los casos, estos ataques se han llevado a cabo explotando probables vulnerabilidades en gestores comerciales de contenidos. Los atacantes que han sobresalido en esta práctica han sido '**Protowave Reloaded**', en Brasil al igual que en 2016, y también '**Tsunami Faction**', '**TeaMGh0st**', '**Yunkers Crew**', '**Anarchy Ghost**' o '**Umbrella Gang**'; o '**ByteDesc**' con 'Mexican Hackers', en México, principalmente durante la primera mitad de 2017 en México.

En Perú, 'Peruvian Hackers' y su atacante '**Sie7e**' han actuado contra webs del Gobierno bajo dominio gob.pe y contra algunos pequeños negocios o webs de empresas, empleando en general narrativas antigubernamentales.

Por otro lado, Venezuela ha representado durante 2017 el escenario prototípico para poner de manifiesto la debilidad del movimiento hacktivista en la región. A pesar de la continuidad del marco narrativo de **#OpVenezuela** −reactivo a la inestabilidad política y social en el país−, los ataques han sido ocasionales, descoordinados, de baja intensidad y sin establecerse una campaña que haya hecho notar una adhesión hacktivista real al escenario. En ellos han participado diversas identidades con acciones puntuales, principalmente ataques por denegación de servicio o desfiguraciones sobre webs bajo dominio de Gobierno gob.ve.

La República Dominicana ha sido objeto durante este año de una veintena de ataques contra webs bajo dominio gov.do (entre ellos, la desfiguración de las webs de la Policía Nacional, de la Defensa Civil o de la Superintendencia de Valores), llevados a cabo por identidades externas al país, como la de rasgos albaneses '**Nofawkx Al**', '**Mamad Warning**' o '**Shade**'.

[30] bajo dominio gob.mx en México y gov.br en Brasil.

En Argentina, hasta su arresto policial, estuvo operando la identidad '**Libero**' con acciones sobre varias webs de Gobierno, durante la primera mitad de 2017, y ocasionalmente '**niño orsino**', también desactivado policialmente.

Además, se han llevado a cabo ataques ocasionales contra webs de visibilidad en Guatemala, país en el que desfiguraron la web del Congreso; en Ecuador, donde se vio afectada la Defensoría del Pueblo y el Servicio Integrado de Seguridad; en Bolivia, con ciberataques al Ministerio de Ciencia y Tecnología; y en Colombia o Panamá, países en los que las identidades '**GeNErAL**' y '**Moroccan Islamic Union**' desfiguraron sitios web de marcas automovilísticas.

Sin embargo, identidades como '**Anonymous CCL**' o '**aDriv4**', que durante el año precedente fueron muy activas, redujeron drásticamente su actividad en 2017.

4.2 Operaciones hacktivistas en Iberoamérica

El conjunto de propuestas narrativas de llamamiento a ciberataques hacktivistas en Iberoamérica durante 2017 se ha compuesto de las siguientes iniciativas:

MARCOS NARRATIVOS HACKTIVISTAS EN IBEROAMÉRICA 2017					
PAÍS	**OPERACIÓN**	**PROMOTOR**	**TIPO DE OBJETIVO**	**TIPO DE ACCIÓN**	**RESULTADO**
VE	#OpVenezuela	Anonymous Venezuela	Instituciones públicas de Venezuela	DDoS Desfiguración Exfiltración	Varias decenas de webs afectadas
BR	#OpOperadoras	Anonymous Brasil	Empresas de telecomunicaciones en Brasil	DDoS DoX	Algún ataque DDoS de baja intensidad y alguna difusión de información pública (DoX) no sensible.
PE	#OpPNP	Peruvian Hackers	Policía Nacional del Perú	Desfiguración Exfiltración	Dos webs deformadas e información no sensible exfiltrada
VE	#OpBlackBanco	Anonymous	Sistema bancario de Venezuela	Exfiltración	Falsa reivindicación sin resultado real. Una web menor no bancaria desfigurada

5. HACKTIVISMO INTERNACIONAL

5.1 Panorama hacktivista internacional

Al margen de España o de los países incluidos en la región iberoamericana, se ha producido durante 2017 un significativo descenso de las acciones hacktivistas impulsadas por narrativas ideológicas, ganando terreno el hacktivismo oportunista de atacantes individuales cuyo objetivo es situar su alias o logotipo en la desfiguración de un sitio web con visibilidad.

Asimismo, al igual que en el resto de territorios, en 2017 el fenómeno 'Anonymous' ha demostrado llevar varios años en crisis de identidad, con ausencia de sentido colectivo y con incapacidad casi crónica para producir campañas mínimamente organizadas. Del mismo modo, ha mostrado falta de afiliación de identidades con habilidades técnicas suficientes como para representar una ciberamenaza que se identifique con el ideario 'Anonymous'.

Por el contrario, el panorama hacktivista internacional en 2017 ha estado articulado a partir de identidades atacantes aisladas que respondían a pautas de ese hacktivismo oportunista, caracterizado por un individualismo sin trasfondo narrativo militante en lo ideológico y por el aprovechamiento de vulnerabilidades tecnológicas comunes en los objetivos a atacar en lo operativo. Sus acciones perseguían el egocentrismo (identidades *egofag* en la propia terminología de 'Anonymous') y el protagonismo del atacante.

A falta de operaciones hacktivistas de renombre, en 2017 se han realizado ciberataques individuales subrayables por su complejidad técnica de ejecución o por la visibilidad de los objetivos victimizados. Ejemplo de ello fueron el secuestro de canales secundarios en redes sociales de la cadena británica de noticias *BBC* o de *The New York Times* por parte de '**OurMine**' –acción que repetiría en agosto con la productora de televisión HBO o con PlayStation-.

Con la misma naturaleza de ataque del ejemplo anterior, se llevó a cabo la desfiguración de varios subdominios alojados en la web del Gobierno Federal de Bélgica[31] por '**Don-2**', en enero de 2017; la deformación de webs de Unicef en Croacia y Malasia, en febrero; o el secuestro, en marzo, de perfiles en Twitter de varias organizaciones internacionales −como Amnistía Internacional, Forbes o Unicef US− para inyectar contenidos proturcos. Esta última acción, aunque no fue reivindicada, coincide con el modus operandi posteriormente observado en la identidad turca '**Ayyildiz Tim**'.

Además, otros ejemplos subrayables en el panorama internacional han sido la exfiltración, en abril, de datos de la web de la Asociación Internacional de Federaciones

[31] fgov.be

de Atletismo, atribuida a la ciberamenaza rusa 'Fancy Bear' en el contexto de la **#OpOlympics**; el compromiso de una veintena de webs de gobiernos locales en el Estado de Michigan en EE.UU. por parte de '**Mamad Warning**', en junio; el ciberataque de '**TheRebelz**', que comprometió el subdominio whois del registrador nacional de dominios de Arabia Saudí; o las acciones de la identidad brasileña 'Anarchy Ghost' que comprometió la web del registrador de dominios domain.ma de Marruecos y alteró también la web de la empresa Coca-Cola en este país.

En Europa, aparte de las oleadas de ataques por desfiguración que reproducían las mismas pautas que en España en cuanto a la explotación de vulnerabilidades en gestores comerciales de contenidos, cabe mencionar la actividad de '**AnonGhost Portugal**' y de '**Anonymous Italia**'. Ambas identidades deformaron webs, de manera puntual, en ambos países; pero, en el caso de **Anonymous Italia**', también se produjo una exfiltración de las webs del Ministerio de Asuntos Exteriores y del Arma de Carabineros, en junio de 2017.

Los ataques en países del Norte de África se han basado en desfiguraciones contra webs menores, llevadas a cabo por identidades que explotaban vulnerabilidades comunes en gestores comerciales de contenidos. No se han detectado identidades centradas en esa región, exceptuando el caso de '**Moroccan Revolution**' y sus ataques contra webs de pequeñas empresas en Marruecos; o el de '**LGH**/Ly_Kermit' en Libia, en cuyos ataques contra webs, como la del Ministerio de Exteriores, no empleó una narrativa hostil.

En Argelia, y en menor medida en Egipto, se ha apreciado una determinada cantidad de acciones sobre webs de universidades; no tanto porque hayan constituido un foco sectorial de ataques, sino probablemente porque exponen webs con vulnerabilidades en gestores de contenidos. En Egipto, a pesar de la situación oscilante de conflictividad social contra el Gobierno, el hacktivismo no se ha erigido como un fenómeno de contestación a considerar.

En Turquía tampoco se ha apreciado una infraestructura hacktivista que opere de modo regular, sino identidades que atacaban de forma ocasional y con poco criterio. Aunque los atacantes de probable origen turco se encuentran entre las identidades hacktivistas más activas a nivel internacional, su foco contestatario sobre Turquía es entre bajo y moderado, dependiendo de las coyunturas.

Entre esas identidades, '**ifactoryx**' ha atacado con asiduidad al Gobierno del país. Por ejemplo, comprometiendo dominios de la web del Ministerio de Educación. Además, diversas identidades alrededor de '**Ayyildiz Tim**' o '**Akincilar**' han actuado contra webs de diversos países inyectando siempre contenido de simbología nacionalista proturca y de apoyo al régimen turco.

También las turcas '**Jonturk75 & RootDevilz & Bozkurt97**' se han caracterizado por ser capaces de llevar a cabo ataques de mayor complejidad técnica de lo habitual. Alteraron en julio subdominios de webs[32] internacionales de cierta visibilidad y de varios sectores −con especial incidencia en la industria del entretenimiento con base en EEUU−; y en noviembre de 2017 alteraron webs de alta visibilidad en Vietnam mediante el compromiso de sistemas de nombres de dominio (DNS) en el país.

En diversos países de África, como Kenia o Uganda, identidades hacktivistas han aprovechado vulnerabilidades en webs, principalmente del gobierno, desarrolladas con gestores comerciales de contenidos para llevar a cabo su desfiguración. Se trata, además, de webs con visibilidad, como las del Ministerio de Defensa de Kenia, del Ministerio del Tesoro en Costa de Marfil, la web de la Autoridad de Energía en Etiopía, las de las embajadas de Uganda en el exterior o el Parlamento del mismo país, la del Servicio de Policía de Botswana, la web de la Unidad de Cibercrimen de la Policía de Ghana o la de la operadora Orange en Isla Mauricio, entre otras.

En Asia son constantes las oleadas de desfiguraciones en países como Indonesia, China y Tailandia, donde el hacktivismo oportunista de raíz individual explota vulnerabilidades en webs con gestores comerciales de contenidos y desarrolla una actividad mensual continuada.

No obstante, '**Moroccan Islamic Union**', identidad que destaca por ser capaz de comprometer webs de alto perfil que no exponen vulnerabilidades comunes en gestores de contenidos, comprometió en el primer trimestre del año webs de varios ministerios en Bangladesh o de las Aduanas de Birmania. En julio, '**w4l3XzY3**' desfiguró la web del Tribunal Supremo de Camboya; y '**r00t d3str0y3r**' alteró en agosto webs del Ministerio de Defensa de Pakistán.

Como elemento novedoso en el escenario hacktivista internacional, en abril de 2017 −mes en el que anualmente se convoca una oleada de ciberataques contra webs en Israel en el contexto de la **#OpIsrael**−, se informó de que diversos perfiles en Twitter, sin características definitorias específicas y probablemente creados para la ocasión, estaban difundiendo links de descarga a una supuesta app para dispositivos Android con la que participar en ataques DDoS en el marco de #OpIsrael.

El contenido del fichero descargable se correspondía con archivos .apk (instaladores de Android), infectados con un troyano de acceso remoto (RAT). La hipótesis tras el hallazgo indicaba que un actor, de momento sin atribuciones de identidad, estaría tratando de infectar a participantes potenciales en la #OpIsrael con un RAT a fin de tener acceso remoto a sus dispositivos Android.

[32] solutions.reuters.com, modelos.honda.com, twentytwenty.justintimberlake.com, flawless.beyonce.com

Las acciones de '**zanakifre**', en octubre de 2017, se consideran también de una cierta novedad táctica en el ámbito del hacktivismo, aunque sin peligrosidad operativa añadida. Esta identidad desfiguró medio centenar de webs menores basadas en Wordpress, con domino en Irán e IP en EE.UU.[33], inyectando en alguna de ellas referencias generales al Kurdistán y en otras, una composición gráfica que simulaba que la web había sido (falsamente) cifrada por un ransomware. En estos ataques se amenazaba con el borrado de ficheros, que solo podía evitarse con un pago en bitcoins a una dirección electrónica (Figura 5-1-1). En la acción se simuló el empleo de malware para obtener un pago en bitcoin.

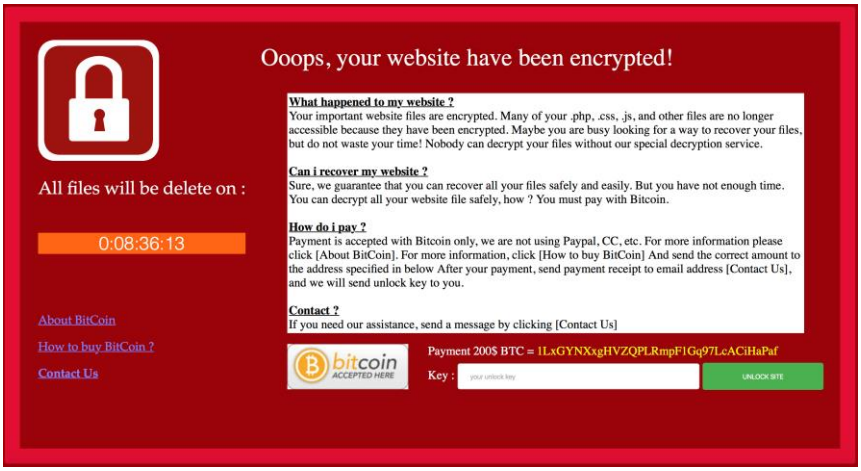


Figura 5-1-1.

5.2 Operaciones hacktivistas internacionales

Las campañas hacktivistas dotadas de algún tipo de narrativa justificadora específica que durante 2017 han dirigido algún ciberataque en países distintos de España o del subcontinente iberoamericano han sido:

MARCOS NARRATIVOS HACKTIVISTAS EN AMBITO INTERNACIONAL 2017					
PAÍS	**OPERACIÓN**	**PROMOTOR**	**TIPO DE OBJETIVO**	**TIPO DE ACCIÓN**	**RESULTADO**
TH	#OpSingle GateWay	Anonymous	Instituciones públicas de Tailandia	DDoS Desfiguración Exfiltración	Una veintena de objetivos atacados
PT	#OpAlgarveSaudavel	AnonGhost Portugal	Empresas de gas y petróleo en Algarve	No desarrollada	Sin ataques

[33] entre otras dr-amirpour.ir, drasgarloo.ir, elmju.ir

MARCOS NARRATIVOS HACKTIVISTAS EN AMBITO INTERNACIONAL 2017					
PT	#Op25Abril	CyberTeam	Instituciones públicas de Portugal	Desfiguración DDoS	Dos ataques sobre webs de bajo perfil y un DDoS sobre Policía de Portugal
IL	#OpIsrael #OpAlAqsa	Anonymous	Webs en Israel	DDoS Exfiltración Desfiguración	Alguna oleada de desfiguración sobre webs de bajo perfil. Sin relevancia.
INT	#OpIcarus	Minion Ghost	Bancos Centrales Nacionales y bolsas de valores	DDoS Exfiltración	Siete ataques DDoS
SA	#OpSaudi	Anonymous Arabe	Instituciones públicas y empresas en Arabia Saudí	Desfiguración DDoS	Menos de media docena de DDoS y tres deformaciones de webs menores
INT	#OpLeakThe Analyst	Desconocido	Analistas de empresas de ciberseguridad	Exfiltración	Sin activar
USA	#OpDomestic Terrorism	Anonymous	Colectivos calificados como de extrema derecha o neonazis	Desfiguración DDoS	Una decena de objetivos atacados
MY	#OpRohingya	Anonymous	Instituciones de gobierno en Birmania	DDoS Desfiguración	Una veintena de DDoS sobre webs de Gobierno y medio centenar de webs menores desfiguradas

MARCOS NARRATIVOS HACKTIVISTAS EN AMBITO INTERNACIONAL 2017					
INT	#OpOlympics	Fancy Bear	Organismos gestores del deporte internacional	Exfiltración	Una web atacada
INT	#OpVendetta	Anonymous	Objetivos diversos	Desfiguración	Sin ataques relevantes
GR	#OpGreece	Anonymous	Parlamento, Bolsa de Valores y Ministerio de Finanzas de Grecia	DDoS	Un ataque aislado
INT	#OpHermes	Anonymous	Empresas internacionales	Exfiltración	Sin activar

6. CIBERYIHADISMO Y HACKTIVISMO PROYIHADISTA

6.1 Panorama ciberyihadista

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

- El **yihadismo** emplea la violencia física (asaltos armados, atentados con bomba, despliegue de fuerzas armadas sobre el terreno) para actuar sobre objetivos en el plano físico: instalaciones de Gobierno o de empresas, personas, infraestructuras críticas, poblaciones.
- El **ciberyihadismo** recurre a armas cibernéticas (malware, exploits, remote access tools, remote control systems) para intentar producir un perjuicio o daño en los sistemas de información 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, como la generación del terror en la sociedad o la advertencia a las instituciones estatales.

Con este espacio terminológico de partida como criterio de observación, durante 2017 no se ha detectado ningún incidente que pueda ser calificado de ciberyihadismo.

6.2 Hacktivismo parásito de simbología proyihadista

El término '**Cibercalifato**' ha sido empleado desde principios de 2015 en diversos ciberataques por desfiguración de sitios web. Los autores de dichos ataques han inyectado narrativa de apoyo al 'Daesh' (Estado Islámico), emulando con esta denominación el objetivo estratégico del 'Daesh' de instaurar un "califato islámico" que abarque mundialmente todos los territorios donde se profesa culto al islam.

Al igual que en 2016, durante 2017 se confirma que no existen evidencias directas ni indicadores indirectos que sugieran que el 'Daesh' haya desarrollado una división específica destinada al desarrollo de acciones ciberofensivas contra servidores web u otros medios tecnológicos.

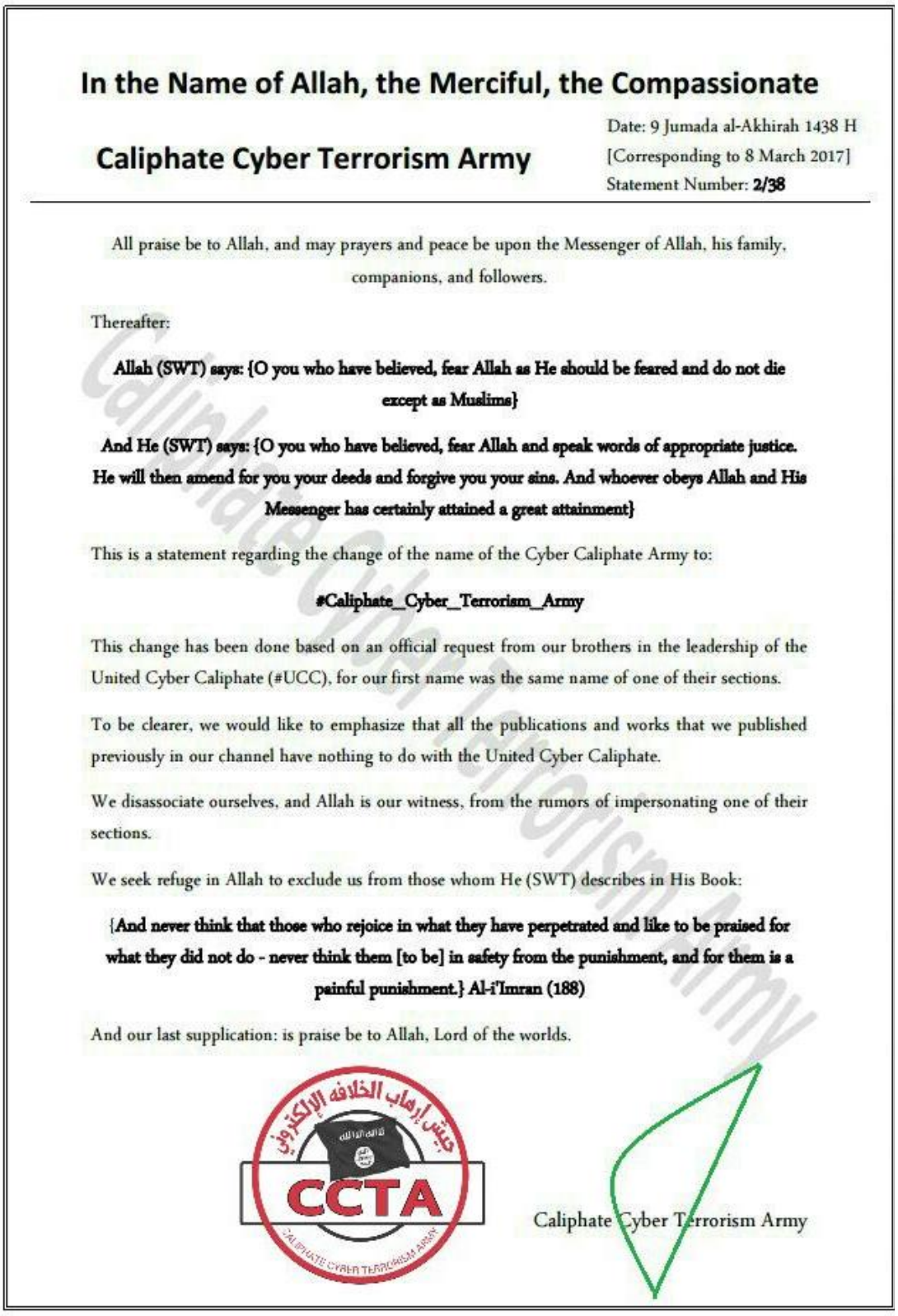
Asimismo, se constata que la denominación "cibercalifato" no se corresponde con una identidad única, sino con un conjunto borroso de identidades hacktivistas no vinculadas orgánicamente al 'Daesh'. Probablemente, estas identidades ni siquiera sean simpatizantes de su ideología, sino que utilizan instrumentalmente sus referencias a modo de provocación o para dar una falsa impresión sobredimensionada de su propia capacidad de amenaza, a fin de llevar a cabo cibertataques por desfiguración contra sitios webs vulnerables de bajo perfil insertando consignas islamistas generales o más concretas que simulan apoyar al 'Daesh'.

Es decir, **el 'Cibercalifato' no existiría como una estructura orgánica del 'Daesh' sino como un concepto parasitado desde identidades hacktivistas individuales principalmente como táctica de provocación**.

6.2.1 Infraestructura hacktivista proyihadista.

Durante 2017 no se han detectado nuevas identidades hacktivistas operando en la órbita del denominado 'Cibercalifato', sin contar el universo de identidades digitales en redes sociales dedicadas a labores de reclutamiento y propaganda proyihadista, y cuya observación y análisis no son objeto de este informe.

En este epígrafe cabe mencionar que el 8 de marzo de 2017 la entidad hacktivista '**Caliphate Cyber Army**', de retórica proyihadista, comunicó en inglés (Figura 6-2-1-1) su cambio de denominación a '**Caliphate Cyber Terrorism Army**', sin aparejar ninguna acción ciberofensiva en lo que parecía ser una "acción de marketing".



In the Name of Allah, the Merciful, the Compassionate

Caliphate Cyber Terrorism Army

Date: 9 Jumada al-Akhirah 1438 H
[Corresponding to 8 March 2017]
Statement Number: **2/38**

All praise be to Allah, and may prayers and peace be upon the Messenger of Allah, his family, companions, and followers.

Thereafter:

Allah (SWT) says: {O you who have believed, fear Allah as He should be feared and do not die except as Muslims}

And He (SWT) says: {O you who have believed, fear Allah and speak words of appropriate justice. He will then amend for you your deeds and forgive you your sins. And whoever obeys Allah and His Messenger has certainly attained a great attainment}

This is a statement regarding the change of the name of the Cyber Caliphate Army to:

#Caliphate_Cyber_Terrorism_Army

This change has been done based on an official request from our brothers in the leadership of the United Cyber Caliphate (#UCC), for our first name was the same name of one of their sections.

To be clearer, we would like to emphasize that all the publications and works that we published previously in our channel have nothing to do with the United Cyber Caliphate.

We disassociate ourselves, and Allah is our witness, from the rumors of impersonating one of their sections.

We seek refuge in Allah to exclude us from those whom He (SWT) describes in His Book:

{And never think that those who rejoice in what they have perpetrated and like to be praised for what they did not do - never think them [to be] in safety from the punishment, and for them is a painful punishment.} Al-i'Imran (188)

And our last supplication: is praise be to Allah, Lord of the worlds.

جيش إرهاب الخلافه الإلكتروني
CCTA
CALIPHATE CYBER TERRORISM ARMY

Caliphate Cyber Terrorism Army

Figura 6-2-1-1.

En otro orden, en marzo de 2017 un Tribunal en Iraq, aplicando la legislación antiterrorista, condenó a muerte a '**Abu Haresh**', que fue arrestado en Baghdad (Iraq) en 2016 por desfigurar sitios web inyectando retórica proyihadista. Tras completar estudios universitarios de ingeniería informática en Iraq, aparentemente se habría aproximado a círculos proyihadistas bajo promesa de que le ayudarían a buscar asilo en Europa vía Turquía. Comenzó creando perfiles en Twitter para la difusión de propaganda proyihadista y supuestamente habría confesado ser miembro del '**Cyber Caliphate Army**'.

Por otro lado, Samata Ullah, de 34 años de edad y residente en Cardiff (Reino Unido), fue arrestado en marzo por la Policía británica atribuyéndosele cargos de apoyo al terrorismo. El arrestado, que gestionaría por sí mismo un blog de retórica proyihadista bajo la denominación de "Ansar al Khilafah", se habría ofrecido para poner sus conocimientos de técnico informático al servicio de la entidad hacktivista proyihadista '**Cyber Caliphate Army**' (CCA). Supuestamente habría afirmado estar planeando desarrollar software para "derribar drones enemigos". El sujeto está diagnosticado de autismo.

En abril de 2017, '**United Cyber Caliphate**' continuaba la retórica de propaganda ya observada en años previos, centrada en generar una percepción sobredimensionada de su estructura y emitiendo comunicados de "alianzas" con otras supuestas identidades ciberhacktivistas afines –se trataría de '**Anon Terror**' y de '**Fighter Muslim Cyber Caliphate**', la primera de ellas operando bajo el alias de 'Shadow Caliphate'– (Figura 6-2-1-2).

بسم الله الرحمن الرحيم

بيعة مجموعتي Anon Terror and FMCC لاتحاد قراصنة الخلافة الالكتروني

Anon Terror" and "Fighter Muslim Cyber Caliphate" (FMCC) Pledges Allegiance to United Cyber Caliphate"

على خلفية وقائع لائحة القتل التي نشرها الاتحاد UCC في الآونة الاخيرة والتي اجتاح صيتها ربوع الارض فإن الله قد من على الاتحاد ببيعة مباركة لاخواننا بمجموعة Anon Terror بقيادة الأخ الفاضل Shadow Caliphate التي كانت ولازالت تحتل الصدارة في ارهاب امم الكفر قاطبة فقد نجحت بامتياز في اختراق مواقع روسية مهمّة ساهمت في دب الرعب فيهم وهاهي الآن بفضل الله ومنه تنضم لاتحاد قراصنة الخلافة بقائدهم الجديد خلفا للأخ أسيد تقبله الله وايضا بانضمام فريق FMCC بقيادة الاخ xozer z4yn7x

Based on the latest events surrounding the widely propagated and circulated killing lists that UCC had recently posted which swept the earth, Allah has blessed UCC with a new pledge of allegiance by "Anon Terror" under the leadership of brother "Shadow Caliphate" and "Fighter Muslim Cyber Caliphate" under the leadership of brother "xozer z4yn7x". "Anon Terror" was and remains in the forefront in terrorizing infidel nations and was successful in hacking into prominent Russian sites instilling fear in them here they are now with Allah's blessing joining UCC with its new leadership after the killing of Osed-may Allah accept him

ان هذه البيعة لا تتوقف فقط على تلاحم مجموعات بل هي صدق في تلبية النداء والاجتماع تحت لواء واحد وتكوين الصف المنظم الذي يقهر الكفار ويغيظهم

This pledge is not merely the union of groups, but is true in meeting the appeal and meeting under one banner and be one organized union that conquers the infidels and enrages them

إن من نعم الله على الاتحاد توحيد الصفوف الذي شد من عزمهم وقوى مهجهم وثبت أقدامهم في هذه الحرب، إلى جانب ما يحصدونه كل يوم من الغنائم، والرعب الذي يلقيه الله في صدور الكفار من هول ما ينالونه منهم فالحرب بيننا ما كانت فقط فوزا عليهم بالاختراقات بل إنا نحاربهم لاظهار الحق وهكذا يحصل الخير برص الصفوف وانضمام الانصار إلينا، وهذه وإن لم تكن دعوة للانضمام فهي بحد ذاتها دليل على أن الذي يصدق الله يجازيه وينصره

One of Allah's blessing on UCC is to unite the ranks, intensify their determination and strengthening them in this war in addition to what they harvest every day from spoils and the horror that Allah instills in the hearts of the infidels. Our war with them was not only to hack them but we also fight them by showing the truth resulting in strengthening the ranks and having supporters joining us. If this was a call to join us, it is proof that whoever believes Allah, He will reward him and support him

Figura 6-2-1-2.

Con la misma intencionalidad de proyectar al exterior una imagen sobredimensionada de capacidades, ha sido habitual que las distintas denominaciones asociadas al "cibercalifato" realizaran actividades en redes sociales para "mantener presencia". Ejemplos de esta práctica son la supuesta generación de perfiles en Twitter o Facebook, la puesta en marcha de iniciativas como #Op_Rising_Vengeance a través de la que se difundían datos personales pero públicos de ciudadanos en EEUU (Figura 6-2-1-3) o la promoción de pretendidas campañas de reclutamiento de "hackers" (Figura 6-2-1-4).

Figura 6-2-1-3.

Figura 6-2-1-4.

Por otro lado, en agosto de 2017, la empresa de ciberseguridad rusa Group IB difundió una nota[34] en la que revelaba la identidad de los ciberactivistas que operaban tras el alias '**United Islamic Cyber Force**', empleada en la órbita del 'United Cyber Caliphate' (UCC) y denominaciones similares.

[34] https://www.group-ib.com/blog/uicf

A partir del análisis de redes sociales, dicha nota atribuyó la identidad para los alias '**AnoaGhost**' −Chakra Bernaty, estudiante de informática residente en Indonesia−; '**Gunz_Berry**' −Guntur R, residente en Indonesia−; '**W3bh4x0r**' −Habiblahi Adeleke, residente en Nigeria−; '**Lakhdar Dz**' −Lakhar B, varón de 21 años residente en Argelia−; '**Zishan Rider**' −Zishan S, residente en India−.

De este análisis de los perfiles de los individuos identificados no se ha podido establecer ninguna conexión ni adhesión formal a ideologías proyihadistas o a estructuras que las promuevan, más allá de las menciones que emplean en los contenidos inyectados en sus ciberataques por desfiguración.

Por otro lado, en lo que podría ser calificado como un artículo de prensa carente de fundamento, el diario británico Express publicó[35] el 31 de diciembre de 2017 un artículo infundado en el que especulaba con la posibilidad de que el 'Daesh' "evolucionara hacia un Ciber Califato", que atacaría a las infraestructuras críticas. Dicho artículo planteaba además que empresas aseguradoras del país estarían "preparando" pólizas para hacer frente "a este tipo de escenarios", donde otras amenazas cibernéticas como las "rusas" estaban siendo contempladas.

6.2.2 Ciberataques de hacktivismo oportunista

En el contexto de identidades individuales hacktivistas que llevan a cabo acciones por desfiguración, instrumentando simbología proislamista o proyihadista, cabe mencionar la actividad de '**Shadow Caliphate**'. Esta identidad desfiguró, en abril de 2017, la web gubernamental del Museo de la Ciudad de Rosario en Argentina [museodelaciudad.gob.ar], inyectando una composición gráfica con iconografía proyihadista y el nombre 'United Cyber Caliphate' (Figura 6-2-2-1). Con anterioridad, **Shadow Caliphate**' había inyectado el mismo contenido en tres webs de muy baja entidad en Rusia[36], todas desarrolladas con Wordpress.

Figura 6-2-2-1.

[35] https://www.express.co.uk/news/uk/898270/isis-terrorist-attack-cyber-crime-uk-security
[36] qingdao.su, sonykpk.com, mirrobo.ru

Además, 'comprometió una veintena de sitios web en el Líbano con IP principalmente en EE.UU., y en Francia[37] inyectando el mismo contenido ya mencionado. Las webs vulneradas no empleaban ninguno de los gestores de contenidos habitualmente considerados vulnerables; tenían en común estar provisionadas por la francesa OVH, alojadas en servidores Nginx, programados en ASP.NET, y con contenidos desarrollados en unos casos con XHTML1 y otros con HTML5 y Javascript.

En Turquía, en mayo de 2017, fue desfigurada la web del mercado del municipio de Kütahya [pazarlar.bel.tr] inyectando una composición general con iconografía del '**United Cyber Caliphate**'. Junto a ella, los mensajes "islamic state rules" y "obey islamic state" (Figura 6-2-2-2).

Figura 6-2-2-2.

Asimismo, la identidad '**NcPro-Dz**', de probable origen argelino y miembro del colectivo 'Team System Dz', efectuó a lo largo de 2017 distintos ataques por desfiguración, inyectando la ya conocida composición gráfica (Figura 6-2-2-3) con iconografía alusiva al islam. A dicha imagen añadía los textos "I love Islamic State" y "security stupidity", denotando en esta última expresión la probabilidad de que la motivación de la acción no fuese ideológica-religiosa sino el hacktivismo propiamente dicho.

En esta práctica se vieron afectadas webs del gobierno local en Italia[38]; de la Junta Federal del Estado de Oklahoma, en EEUU[39]; un centenar en Croacia[40] y varios centenares de pequeños negocios en EEUU, Francia, Ucrania, China y Alemania, en julio de 2017.

[37] entre ellas carmelsaintjoseph.edu.lb, lebanoninapicture.com, mesp-lb.com
[38] comune.nusco.gov.it
[39] oklahoma.feb.gov, ok.feb.gov
[40] incluyendo la Infraestructura Nacional de Datos [nipp.hr], la marca automovilística Mitsubishi en el país [mitsubishi-motors.hr] o el aeropuerto de Pula [airport-pula.hr]

En noviembre lanzó una oleada de ataques, de alrededor de medio millar de desfiguraciones, por más de diez países (EEUU, Eslovenia, Irán, Suecia, Noruega, Canadá, Holanda, Kazastán, Reino Unido, Nueva Zelanda, Sudáfrica y Alemania), inyectando en la mayoría de los casos el texto "hacked by Team System DZ. I Love Islamic State". Sin embargo, en webs de EE.UU. y de Eslovenia se incluía además una imagen del expresidente de Iraq Sadam Hussein y la iconografía de la profesión de fe islámica.

En diciembre la identidad '**NcPro-Dz**' actuó sobre una veintena de webs en Holanda[41] y una treintena en Irán[42], que operaban con el gestor de contenidos DotNetNuke.

Figura 6-2-2-3.

Por su parte, '**Anonymous Ghost Gaza**' comprometió, en junio de 2017, unas 20 webs de bajo perfil en Holanda[43] inyectando un fichero Pal.html con una imagen de un individuo sujetando una bandera negra con la inscripción de la Shahada, la profesión de fe islámica (Figura 6-2-2-4); información que por sí sola no se podía identificar netamente con el proyihadismo. Al mes siguiente realizó la misma operación contra webs en Noruega, Francia e Israel; y en octubre, contra objetivos en Dinamarca y Polonia.

Figura 6-2-2-4.

[41] entre ellas parochiedgh.nl, mijntuinen.nl
[42] entre ellas sjb.co.ir, kardan.ir
[43] entre ellas tikvis.nl, suberp.nl, golfq.nl

La web del Ejército de Argentina [ejercito.mil.ar] fue comprometida en junio de 2017 con la inyección de una composición gráfica encabezada por el mensaje en español "somos el Estado Islámico Allahu Akbar. Esto es una amenaza. ISIS está en Argentina y muy pronto van a saber de nosotros. Allahu Akbar Allahu Akbar". Debajo del texto se incrustaba una imagen general mostrando a milicianos yihadistas portando las habituales banderas e indumentarias del 'Daesh' (Figura 6-2-2-5).

La web comprometida no empleaba ningún gestor de contenidos de los habitualmente considerados vulnerables, sino que se alojaba en un servidor Microsoft IIS y operaba con Windows programado en ASP.net, con contenidos desarrollados en HTML5 y Javascript. La acción no fue firmada o reivindicada por ninguna identidad específica lo que, unido al idioma español, al estilo narrativo y a la falta de información, sugiere la hipótesis de un ataque de "falsa bandera" o de provocación.

Figura 6-2-2-5.

'**Moroccan Wolf**[44]' alteró, en julio, las webs basadas en el gestor de contenidos Joomla 1.5 del Ministerio de Educación [education.gov.vc] y del Parlamento [assembly.gov.vc] de San Vicente y las Granadinas, isla en las Antillas del Caribe. En estas inyectó una composición gráfica en inglés que contenía el texto "hacked by Morroccanwolf – Islamic State", la imagen de un militante yihadista disparando una ametralladora desde un vehículo, y dos párrafos en inglés mezclando una diatriba contra EE.UU., la OTAN e Israel y en (pretendida) defensa de los países árabes (Figura 6-2-2-6).

[44] 'Moroccan Wolf' es una identidad conocida al menos desde 2014. Desde entonces ha empleado ocasionalmente contenido proislamista en sus desfiguraciones, con menciones al "Islamic State".

Figura 6-2-2-6.

'Moroccan Wolf' no realizaba ningún ataque por desfiguración desde mayo de 2017. En estas acciones empleaba contenido con menciones al islam, pero sin alusiones explícitas al "Daesh" (Figura 6-2-2-7). No obstante, el análisis de su trayectoria y de los contenidos que inyecta en sus ataques sugiere que es un sujeto con "consciencia islámica" y probablemente con una visión "islamista" de la política, pero sin adscripción ni siquiera periférica al ecosistema de apoyo al 'Daesh' en redes sociales.

Figura 6-2-2-7.

En concreto, sus mensajes en inglés contienen una semántica muy centrada en la ira contra EE.UU. y sus aliados, donde utiliza el término "Islamic State" y su iconografía relacionada como una especie de verbalización agresiva, pero sin elaborar una semántica islamista específica de apoyo explícito, de proselitismo o de afiliación al 'Daesh'.

Por tanto, de momento se infiere que 'Moroccan Wolf' no representa una ciberamenaza proyihadista, sino que se trata de un atacante ciberactivista que hace alusiones proyihadistas como táctica de provocación y para imprimir una connotación más agresiva a sus mensajes.

En lo que respecta a identidades oportunistas que emplean contenido pretendidamente proyihadista como modo de provocación y sin afiliación aparente a ese tipo de actividades o incluso a su ideología, destaca la identidad '**MDR01**'.

En septiembre de 2017 desfiguró una treintena de webs[45] con IP en EE.UU., basadas en el gestor de contenidos Wordpress y destinadas en su mayor parte a divulgar contenidos de ocio o incluso de spam. Empleaban, probablemente de forma indebida, marcas de conocidos fabricantes de software en las que se inyectaba contenido con el texto "Islamic Cyber" y en indonesio "Jayalah Indonesiaku" (Figura 6-2-2-8).

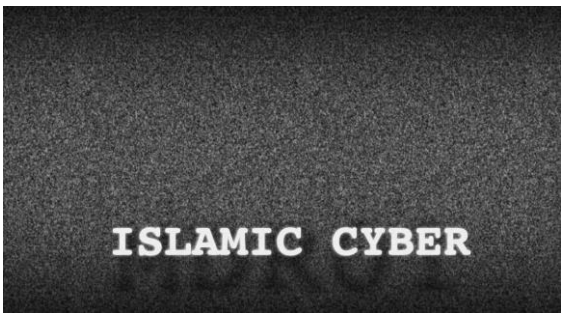


Figura 6-2-2-8.

Por otro lado, el a finales de octubre de 2017, varios sitios web menores de información deportiva en Rusia[46] fueron deformados con contenido amenazante en árabe, inglés y ruso contra la Copa Mundial de Fútbol −organizada en Rusia en 2018−, advirtiendo que "arderá en el infierno con bombas y cinturones explosivos" (Figura 6-2-2-9).

[45] entre ellas norton.setuphelp.club, office.setup-help.club, windowssecurity1.club
[46] elsys.ru, clearrunet.ru

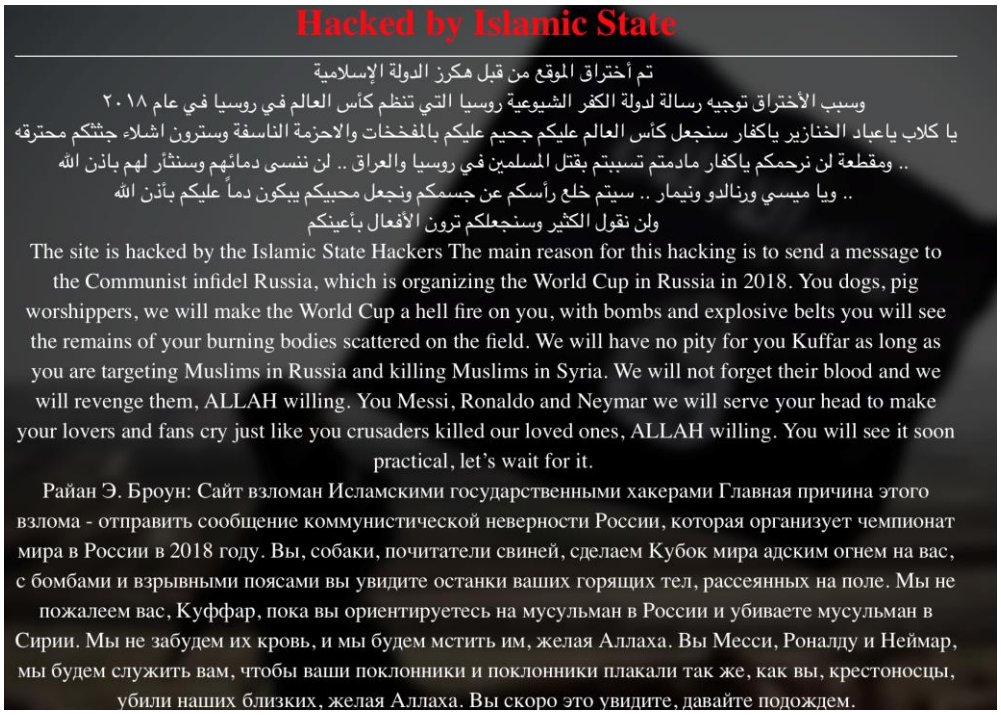


Figura 6-2-2-9.

El contenido encabezado por la frase "hacked by Islamic State" y firmado la identidad '**Islamic State Cyber Team**' incluía una composición gráfica en la que simulaban que dos jugadores del Fútbol Club Barcelona eran rehenes del 'Daesh' (Figura 6-2-2-10). A pesar de que el contenido gráfico inyectado estaba muy elaborado, el carácter secundario de las webs atacadas y la nueva denominación de 'Islamic State Cyber Team' utilizada sugerían que se trataba de un "ataque oportunista" sin indicadores de estar vinculado al 'Daesh'.

Figura 6-2-2-10.

A final de 2017 y con el anagrama de '**Caliphate Cyber Ghosts**' se difundió un vídeo[47] (Figura 6-2-2-11) en el que una voz electrónica, que hablaba en árabe y se identificaba genéricamente como "los hackers del Estado Islámico", amenazaba con "penetrar servidores de gobiernos, ministerios de defensa, empresas a nivel global". Además, declaraba "la guerra electrónica a todos los pilares de infidelidad y apostasía", siendo EE.UU. su primer objetivo; y el 8 de diciembre de 2017, la fecha de lanzamiento de ciberataques.

Más allá del ejercicio de propaganda, la amenaza era otro de tantos productos audiovisuales con iconografía pretendidamente proyihadista diseñados, precisamente, para lograr circulación en redes sociales. El ataque no se concretó en la fecha marcada.

Figura 6-2-2-11.

En diciembre de 2017 la misma identidad 'Caliphate Cyber Ghosts' volvió a difundir un vídeo de amenaza[48] de 1:37 minutos, relatado en árabe y subtitulado en inglés, en el que tras la consabida retórica proyihadista dedicaba los últimos 15 segundos a asegurar que habían "hackeado webs sensibles del Ejército de EEUU, de su Ministerio del Interior y del Departamento de Estado… y que habían capturado miles de informaciones confidenciales… que enviarían a lobos solitarios para que cometiesen asesinatos". De nuevo, aparte del contenido de propaganda, ningún elemento sugería credibilidad sobre la amenaza.

Por otro lado, también en diciembre de 2017, '**AnonGhost**' desfiguró tres webs en Suecia[49] inyectando una composición que combinaba iconografía de 'Anonymous' con alusiones a Alá y la imagen, habitualmente empleada por colectivos proyihadistas, del jinete que representa a un muyahidin con una bandera mostrando la profesión de fe islámica (Figura 6-2-2-12).

[47] http://video.dailymail.co.uk/video/mol/2017/12/07/708745938192646490/1024x576_MP4_708745938192646490.mp4
[48] http://video.dailymail.co.uk/video/mol/2017/12/18/3946047963737141869/1024x576_MP4_3946047963737141869.mp4
[49] karriärtorget.se, alltomledigalokaler.se, energijobb.eu

Figura 6-2-2-12.

'AnonGhost' es un atacante que, en su trayectoria de varios años, nunca ha mostrado una inclinación proyihadista en el plano ideológico, aunque alguna de las identidades que orbita a ese alias ha llevado a cabo iniciativas "desinformativas" con el fin de provocar y de confundir al auditorio sobre sus intenciones. En dichas iniciativas se cuenta la supuesta alianza con el 'Caliphate Cyber Army', anunciada a principios de 2016 con el sobrenombre de 'Ghost Caliphate'.

Dicha unión fue asumida por algunos analistas como una acción de apoyo ciberactivista al 'Daesh' cuando no fue más, como el tiempo ha demostrado, que una acción desinformativa de propaganda con el propósito de "lucir" una determinada estética desafiante. Se entiende que este nuevo contenido inyectado va en la misma línea de "pose" sin base ideológica real.