Informe de Amenazas
CCN-CERT IA-04/17

Hacktivismo y Ciberyihadismo
Informe Resumen 2016

Marzo de 2017

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC,
ou=sello electrónico, serialNumber=S2800155J,
o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO
CRIPTOLOGICO NACIONAL, c=ES
2017.03.25 08:18:01 +01'00'

ÍNDICE

1. SOBRE CCN-CERT

El CCN-CERT (www.ccn-cert.cni.es) es la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN (www.ccn.cni.es). Este servicio se creó en el año 2006 como el **CERT Gubernamental/Nacional** español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el RD 421/2004 regulador 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.

De acuerdo a todas ellas, es competencia del CCN-CERT la gestión de ciberincidentes que afecten a **sistemas del Sector Público**, a **empresas y organizaciones de interés estratégico** para el país y a cualquier sistema clasificado. 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.

2. RESUMEN EJECUTIVO

El hacktivismo de raíz española en 2016 ha sido prácticamente inexistente en términos operacionales de ciberataque salvando la actividad ofensiva desplegada por La 9ª Compañía', que ha comprometido algunos sitios web de algún Ayuntamiento, un par de medios de comunicación, algunas empresas y cámaras de comercio.

Además de 'La 9ª Compañía' y al margen de alguna acción ocasional de identidades hacktivistas aisladas, el colectivo 'Anonymous' autóctono puede considerarse tanto inactivo operativamente como carente de impacto en términos de propaganda en España.

Al igual que numerosos países del mundo y en un nivel comparable al de otros Estados de la Unión Europea como Italia, Francia o Reino Unido, sitios web con direcciones IP localizadas en España han sido objeto en 2016 de ataques por desfiguración por parte de identidades hacktivistas que han mostrado rasgos identificativos del Norte de África, Oriente Medio, Iberoamérica y Asia.

Estos ataques hacktivistas desde el exterior de España han mostrado características de amenaza de bajo perfil, con débil capacitación técnica, desplegando ciberataques que han explotado vulnerabilidades comunes, principalmente en sistemas de gestión de contenidos de distribución libre, en sitios web correspondientes a negocios de profesionales individuales, a colectivos o a pequeñas empresas.

En Iberoamérica 2016 ha mostrado un debilitamiento general de las entidades hacktivistas en la órbita de 'Anonymous', dejando preeminencia a identidad hacktivistas con marca propia. Estas identidades, no obstante, decayeron en sus acciones hacia finales de año.

El debilitamiento de 'Anonymous' se ha traducido en un menor número y recorrido de marcos narrativos hacktivistas planteados en los países de la región en 2016, muchos de los cuales han resultado en un bajo volumen de ciberataques y con bajo impacto.

A nivel internacional el hacktivismo en 2016 ha puesto de manifiesto que, aunque se producen varios miles de ciberataques hacktivistas al día en todo el mundo ejecutados por varias decenas de identidades, no hay más de media decena de ellas que pueden considerarse una ciberamenaza de nivel medio, capaces no sólo de explotar las vulnerabilidades más comunes para comprometer sitios web sino de aplicar varios tipos de técnicas para lograr acceso a sus servidores y contenidos en objetivos.

Como novedad respecto de años anteriores, en 2016 se han detectado un par de casos de identidades mostrando rasgos de Indonesia que han insertado mecanismos de distribución de malware de bajo impacto (adware) en servidores web atacados por desfiguración. Adicionalmente, una identidad hacktivista en Brasil profirió amenazas, no cumplidas, de realizar un ciberataque mediante ransomware.

Esta intersección entre hacktivismo y técnicas cibercriminales convencionales (distribución de malware) se considera de momento ocasional y no representa un patrón en el modus operandi hacktivista.

En cuanto al ciberyihadismo, 2016 ha continuado confirmando que la amenaza cibernética procedente de entidades terroristas de orientación yihadista es, de momento, una conceptualización teórica que no se ha traducido en ciberataques específicos.

No obstante, 2016 ha puesto de manifiesto que la presencia de esta conceptualización teórica sobre una posibilidad de amenaza está siendo aprovechada e instrumentada por identidades hacktivistas para llevar a cabo ciberataques por desfiguración de sitios web de alta vulnerabilidad en los que se inyecta contenido islamista proyihadista.

La propaganda de estos contenidos y la denominación que utilizan estas identidades hacktivistas de orientación islamista a veces conducen a que se realicen evaluaciones de amenaza de estas identidades que no solo sobreestiman marcadamente sus débiles capacidades técnicas, sino que realizan atribuciones erróneas sobre su vinculación real a organizaciones yihadistas como el 'Daesh', vinculación que no es apoyada por ninguna evidencia.

3. HACKTIVISMO EN ESPAÑA

3.1 Estructura hacktivista en España

En 2016 ha continuado el patrón observado desde 2014 consistente en la no articulación de un tejido hacktivista operativo con carácter insurgente en España, ni alrededor del movimiento conocido como 'Anonymous' ni a través de otras identidades con intenciones de generar y constituir un colectivo hacktivista de raíz española.

Desde 2012 'Anonymous' ha sido incapaz de establecer una infraestructura estable en España, ni desde la perspectiva de la propaganda ni mucho menos desde el ámbito de las capacidades de ciberataque.

La única excepción a la ausencia de un tejido hacktivista insurgente con capacidad ciberoperativa ofensiva en España en 2016 ha sido la misma que en los años previos: 'La 9ª Compañía', entidad hacktivista que continúa identificándose con el colectivo 'Anonymous' pero que mantiene sus propias señas de identidad y no está conectada ni integrada en un tejido 'Anonymous' nacional ni internacional.

'La 9ª Compañía' es una identidad hacktivista insurgente con los siguientes probables rasgos identificativos: ideología anarquista de izquierda anticapitalista; una o dos personas, siendo la principal un individuo en el rango de los 40 años de edad; educación universitaria; dedicación laboral a la administración de sistemas informáticos donde podrían estar próximos o afiliados a un órgano sindical de orientación anarquista.

3.2 Operaciones hacktivistas en España

En 2016 se mantiene la ausencia desde 2014 de operaciones hacktivistas de ciberataque generadas en España o centradas sobre España desde el exterior.

Los ciberataques de raíz hacktivista en España han estado protagonizado por identidad conocida como 'La 9ª Compañía' y, ocasionalmente, por identidades generalmente mostrando rasgos árabes que han ejecutado ataques puntuales por desfiguración contra sitios web en España habitualmente en el contexto de oleadas de desfiguraciones contra webs en varios países del mundo y empleando narrativas sin centrar hostilidad sobre España.

Esta ausencia de actividad hacktivista organizada contra España correlaciona con la mencionada inexistencia de un tejido hacktivista articulado en el país.

El panorama de baja densidad hacktivista ofensiva en España durante 2016, además de la aludida presencia de 'La 9ª Compañía' y de identidades atacando ocasionalmente sitios web con direcciones IP localizadas en España, ha visto algunos momentos muy puntuales de ciberataques de baja amplitud por identidades probablemente españolas.

Entre estas acciones puntuales consta la desfiguración de la web de la Asociación Vallisoletana de Empresarios del por la identidad '**AN0N3SCRACH3**'; la ejecución de una inyección SQL sobre la web del Ayuntamiento de Tordesillas en el contexto anual de rechazo a las fiestas populares del Toro de la Vega, acción desarrollada por la identidad '**Spain Squad**'; o varios ataques por la identidad '**N1ght1ng4l3**' contra la web de la Diputación de Toledo, un par de webs de marketing de las empresas Endesa e Iberdrola, y la web del Partido Socialista en Álava.

3.2.1 Marcos narrativos hacktivistas

En la línea de inexistencia de un tejido hacktivista articulado en España durante 2016 y de una baja densidad de ciberataques por identidades ciberinsurgentes radicadas en España, así mismo durante el año se ha registrado una práctica ausencia de elaboración de marcos narrativos hacktivistas destinados bien a producir propaganda antisistema en el ciberespacio bien a generar acciones coordinadas de ciberataque desde identidades hacktivistas en España.

De hecho, en 2016 se observa una sola propuesta nueva de narrativa hacktivista, la denominada **#Op_Save_Spain** u **#Op_Viva_La_República** una retórica contra la corrupción que no obstante estaba literalmente extraída de Wikipedia. La propuesta con orientación hacktivista la realizó en mayo de 2016 la identidad '**JuandeLemos**', proponiendo tras la retórica activación de ataques por denegación de servicio (DDoS) contra un conjunto de direcciones IP correspondientes a varios organismos de la Administración Pública, conjunto de direcciones que la misma identidad ya propuso en diciembre de 2015 para la entonces denominada #Op20D en el contexto del proceso para las elecciones legislativas en aquel momento en España.

La **#Op_Save_Spain** no tuvo ningún recorrido ni se tradujo en ninguna acción de ciberataque, ni generó ninguna colectivización hacktivista alrededor de su narrativa.

3.2.2 'La 9ª Compañía'

Al igual que el año previo, durante 2016 'La 9ª Compañía' ha desarrollado un ritmo regular de ciberataques, consistente en un rango promedio de entre una y dos acciones mensuales, con un lapso de inactividad de un trimestre completo.

El modus operandi de la 'La 9ª Compañía' se ha mantenido así mismo centrado en la ejecución de inyecciones SQL sobre bases de datos de servidores web explotando vulnerabilidades bien a la propia inyección SQL o bien de configuración de los propios servidores. La identidad hacktivista ha combinado las inyecciones SQL con alguna desfiguración ocasional sobre las webs comprometidas, insertando narrativa antisistema y anticapitalista.

En el primer trimestre de 2016, 'La 9ª Compañía' ejecutaba una inyección SQL contra la web del Centro para el Desarrollo Tecnológico Industrial del Ministerio de Economía, Industria y Competitividad, desfiguraciones menores sobre una web informativa del pantano de Flix en Tarragona y sobre el portal Infodefensa, y un acceso ilegal con desfiguración y exfiltración de información sobre un par de sitios web de la empresa El Corte Inglés.

Adicionalmente y en el ámbito de propaganda, en marzo de 2016 un miembro de 'La 9ª Compañía' intervenía en directo por IRC en una sesión de la conferencia de ciberseguridad RootedCON que se estaba celebrando en Madrid, respondiendo a preguntas de los asistentes.

Durante el segundo trimestre de 2016, 'La 9ª Compañía' lograba acceso ilícito a una aplicación web de compras del Ayuntamiento de Albacete, exfiltrando parcialmente contenido del servidor. Así mismo, desfiguraban las webs de la Asociación de Usuarios de Banca AUSBANC y del medio de prensa 'La Nueva España'.

En el tercer trimestre de 2016, 'La 9ª Compañía' no muestra actividad operativa ni comunicaciones de propaganda en abierto, silencio del que sale en octubre de 2016 para advertir de que sus acciones "serán más limitadas", "intentando ser más estrategas" y "manteniendo y ampliando el plano ideológico". Ya en los últimos dos meses del año produce una desfiguración en la web del Ayuntamiento de Valencia y otra vez en 'La Nueva España', para acabar 2016 con accesos ilícitos a los sitios web de las Cámaras de Comercio en Madrid, Valencia, Cantabria y Alicante, vulnerables a inyecciones SQL.

3.2.3 Ciberataques por entidades externas a España

Del mismo modo que en los dos años precedentes, en 2016 ha proseguido un ritmo regular de ciberataques por desfiguración llevados a cabo por identidades hacktivistas fuera de España contra sitios web residentes en direcciones IP de España.

La mayoría de estos ataques se han dirigido contra sitios web de bajo perfil correspondiéndose con pequeñas empresas o webs informativas personales o de colectivos.

En los ciberataques, que, aunque han mantenido un patrón irregular mes a mes han mostrado baja volumen en términos cuantitativos, han participado principalmente como autoras identidades hacktivistas definidas con rasgos culturales árabes, en su mayor parte identificándose con Marruecos o Argelia.

En el conjunto de acciones llevadas a cabo en este contexto no se ha detectado durante 2016 ninguna campaña hacktivista desarrollada en el extranjero con narrativa específicamente dirigida contra España, sino que los ataques contra sitios web en España se han producido generalmente en el marco de oleadas de acciones involucrando decenas de webs como objetivo de desfiguración en varios países.

En promedio, identidades hacktivistas presumiblemente desde el exterior de España han atacado a 73 webs mensuales con dirección IP en el país, siendo julio y diciembre los meses con mayor incidencia (Figura 1).

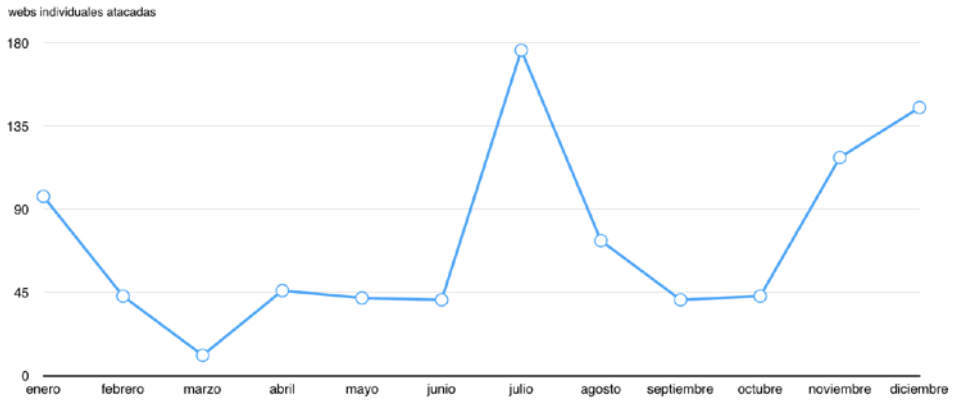

Figura 1.- Webs atacadas por meses.

De las webs residentes con dirección IP en España atacadas principalmente por desfiguración de su contenido por identidades hacktivistas presumiblemente actuando desde el exterior de España, alrededor de un 70% estaban desarrolladas sobre gestores preconfigurados de contenidos de distribución gratuita (Figura 2).

Entre estos gestores de contenidos, los sitios web dotados de Wordpress acumulan un 64% de los ataques, seguidos de Joomla con un 22%, y Drupal y Prestashop cada uno con un 6% de incidencia.

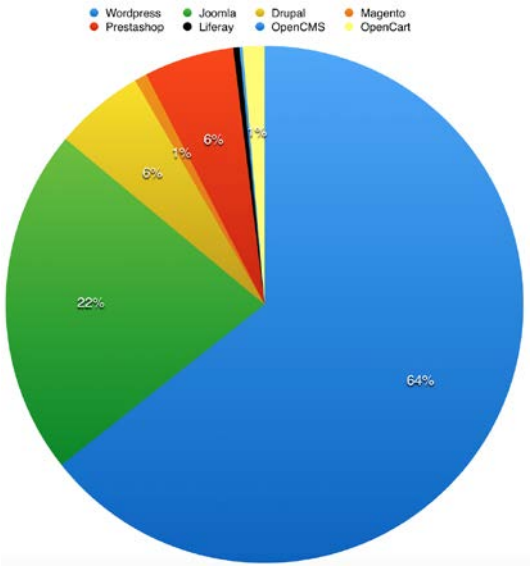

Figura 2.- Gestores de contenidos objetos de ataque.

Los tipos de web más comprometidas en las acciones de ciberataque han sido los correspondientes con negocios de pequeñas empresas y con webs informativas personales o de colectivos. Ocasionalmente se han producido ataques puntuales contra webs de las Administraciones Públicas (Ayuntamientos de Tarragona o Vigo, Diputación de Toledo, Ministerio de Educación) y de universidades (Salamanca, Zaragoza, Cartagena o Vigo).

Las identidades con los rasgos mencionados en este epígrafe que más han retornado a desfigurar webs con direcciones IP localizadas en España durante 2016 han sido el egipcio '**Dr.Silnt HilL**', explotando vulnerabilidades en plataformas basadas en Wordpress; los tunecinos de '**Fallaga Team**', en ocasiones inyectando mensajes proyihadistas en inglés sobre webs operando con Prestashop o Drupal; '**MuhmadEmad**' y '**Bala Sniper**' inyectando ambos contenidos prokurdos en idioma inglés sobre webs operando con Wordpress o Joomla; '**aDriv4**', inyectando contenido sin especificidad principalmente sobre webs con Joomla; '**Anonymous Arabe**', inyectando contenido en inglés reivindicativo sobre Palestina generalmente sobre webs operando con Wordpress; '**Peruvian Hackers**', inyectando su logotipo hacktivista; o el argelino '**ERORDZ**' inyectando contenido en inglés con alusiones a Argelia sobre webs principalmente con Wordpress.

Por otro lado, la inyección en ataques por desfiguración de contenidos alusivos a la propaganda proyihadista o al 'Daesh' no se ha producido estadísticamente en España, con algún caso individual de iconografía general islamista.

Las únicas acciones hacktivistas ofensivas realizadas presumiblemente desde el exterior de España (o diseñadas para parecerlo) que han tenido una intención dirigida específicamente contra objetivos en el país durante 2016 han sido cuatro (4):

1. El 17.05.2016 los canales del Sindicato de Mossos d'Esquadra (SME) en web [sme-mossos.cat] y en Twitter [@smemossos] fueron objeto de una vulneración mediante la cual se desfiguraba parcialmente la web inyectando un texto

reivindicativo donde se afirmaba en catalán que se "refundaba el sindicato a Sindicato de los Mossos d'Esquadra para los Derechos Humanos" y "dejaban de ser la fuerza bruta como soldados rasos del capitalismo".

También se secuestraba el canal en Twitter del SME, cambiándole la imagen de portada por una composición gráfica reivindicativa, y enviando varios mensajes con retórica militante, uno de los cuales adjuntaba un link a un paste conteniendo un fichero con datos de 5.600 afiliados al SME (nombre, teléfonos, direcciones y números de cuenta corriente) supuestamente procedentes de una iSQL sobre la web vulnerada.

Menos de 48 horas después del ciberataque, la identidad '**Phineas Fisher**' reivindicaba la acción y justificaba el ciberataque a SME como una iniciativa para "evidenciar que están espiando a activistas y a movimientos sociales y libertarios".

2. El 01.06.2016 se producía una exfiltración sobre la web de la Mutualidad de Previsión Social de la Policía de España [mupol.es], realizando un volcado en el dominio público de contenido de base de datos. La información exfiltrada contenía 5446 registros con datos personales de nombres, DNI, correo electrónico y contraseña de los miembros de la mutualidad.

   En la exfiltración, el autor atribuía a Marketinet, el desarrollador de la web afectada, las posibilidades de comprometer la web (probablemente por explotación de alguna vulnerabilidad).

   El mismo día de la exfiltración, una nueva identidad hacktivista con perfil recién constituido en Twitter, sin actuar nuevamente con posterioridad, y denominación '**F**kPoliceAnonOps**' reivindicaba la acción. Por su ausencia de actividad posterior a este ataque, es probable que 'F**kPoliceAnonOps' sea un alias de conveniencia para otra identidad hacktivista.

3. El 22.06.2016 '**Moroccan Revolution**' desfiguraba dos subdominios de la web cierco.es, inyectando un mensaje reivindicativo del Sáhara "marroquí" y escribiendo en español "aquí estamos otra vez; demostrando que tan buena es vuestra seguridad; protege su sistema o volveremos a hackearlo".

4. El 27.08.2016 la identidad '**OurMine**', conocida por comprometer perfiles personales en Quora, Twitter y Youtube de figuras destacadas de empresas principalmente estadounidenses de tecnología y/o redes sociales, secuestraba el acceso del perfil en Twitter de 'El Rubius' (@Rubiu5), identidad considerada "el primer youtuber español" en popularidad y que tiene más de 7 millones de seguidores en Twitter.

   Durante el secuestro del perfil en Twitter, 'OurMine' modificó la declaración de bio de 'El Rubius' y transmitió una serie de mensajes reivindicativos de la acción a través del timeline del perfil.

Por otro lado, como único ataque hacktivista detectado en España durante 2016 que combina la desfiguración con una intención maliciosa de diseminación de malware consta el llevado a cabo el 10.10.2016 por '**FORBIDD3N**', que comprometía las webs en

Cataluña cbsripolles.cat y calsort.cat inyectando ficheros indonesian.htm y hax.php conteniendo una composición gráfica con el logotipo de 'Indonesian Intelegent Security'. Así mismo comprometía las webs en Alemania das-tischtennisturnier.de o mrb-frankenschweiz.de.

Al cliquear el usuario en el contenido inyectado, la web mostraba aleatoriamente redireccionamientos para la descarga de software como 'Media Player' o 'Adobe Flash Player', que en realidad descargan ficheros de instalación de malware, en concreto, un adware de la familia 'Bundlore'.

4. HACKTIVISMO EN IBEROAMÉRICA

4.1 Panorama hacktivista en Iberoamérica

El panorama del hacktivismo en Iberoamérica durante 2016 ha descendido en general en volumen de acciones con respecto a 2015, aunque se han realizado más planteamientos narrativos hacktivistas, la mayoría de ellos con débil traducción operativa y bajo impacto real en ciberataques.

Las características comunes del hacktivismo actuando contra países de Iberoamérica en 2016 se resumen en:

- Práctica desaparición de los canales IRC como medio de comunicación entre células hacktivistas, patrón que es común internacionalmente.
- Mantenimiento de la caída de actividad observada en 2015 de células hacktivistas que habían mostrado en 2014 alta capacidad ofensiva en varios países, como 'Lulz Security Perú', 'Chilean Hackers', 'Colombian Hackers'. Algunas de estas células han tenido una recuperación de actividad entre diciembre de 2016 y enero de 2017.

  Una interrupción prácticamente común de acciones de varias de estas identidades, en concreto 'Mexican Hackers', 'Chilean Hackers', 'Peruvian Hackers' y 'Colombian Hackers' en octubre de 2016 coincidió con el arresto policial en Colombia de la identidad conocida como '**Oroboruo**': de esta coincidencia cronológica se infiere la hipótesis de que 'Oroboruo' estuviera integrado, colaborara estrechamente o él mismo fuera el componente de 'Mexican Hackers', 'Peruvian Hackers', 'Chilean Hackers' y 'Colombian Hackers'.
- Inactividad, excepto alguna propuesta trivial de bajo impacto, del conglomerado 'Anonymous Iberoamérica', en paralelo a un declive general de las operaciones del movimiento 'Anonymous' en el continente.

  Con la excepción de 'Anonymous Venezuela' y 'Anonymous Brasil', que también han decrecido no obstante en actividad, la capacidad ofensiva de facciones en otros años con mayor presencia ofensiva como 'Anonymous Chile' o 'Anonymous Perú' prácticamente ha desaparecido en 2016, dando carta de naturaleza a la hipótesis de que varias de las facciones 'Anonymous' en el continente habían sido creadas a partir de 'Anonymous Iberoamérica' y, por tanto, han decaído con ella.

Hasta su arresto policial en octubre de 2016, la identidad hacktivista atacante probablemente más activa de Iberoamérica era '**Oroboruo**', aunque centrada geográficamente casi en exclusiva en Colombia, con decenas de acciones continuadas por desfiguración contra webs de Gobierno en el país.

Entre las identidades que más protagonismo han tenido en ataques en Iberoamérica durante 2016 continuó, al igual que el año precedente, '**Anonymous CCL**' con desfiguraciones de webs de Gobierno local y regional en Colombia, Venezuela y México entre enero y abril de 2017, para posteriormente cesar su actividad a lo largo del resto de año excepto un par de acciones en julio y septiembre y otras asumidas por una identidad paralela, '**Esp1A_c1bern3tic0**'.

La identidad probablemente más activa en ataques en Iberoamérica fue '**aDriv4**', atacante que tiene un ritmo hiperactivo de acciones por desfiguración contra webs de todo el mundo, en general explotando vulnerabilidades en webs desarrolladas bajo el gestor de contenidos Joomla, y que no suele utilizar una narrativa motivadora elaborada en sus desfiguraciones, inyectando por lo habitual el texto "hacked by aDriv4". Esta identidad, que en ocasiones ha utilizado contenido en árabe para inyectarlo en sus ataques por desfiguración, podría emplear también el alias de 'Abo Al-EoS'.

En Brasil las identidades predominantemente más ofensivas han sido '**Asor Hack Team**' y '**ProtoWave Reloaded**', que han comprometido principalmente servidores web de Gobierno, de entidades políticas y de universidades en el país desfigurando las webs y exfiltrando su contenido en el dominio público. 'ProtoWave', que también podría emplear el alias de '**Tsunami Faction**', desfiguraba además la web de la Embajada de EE.UU. en Brasil en noviembre de 2016.

También en Brasil se observó en 2016 una táctica generalmente ajena a identidades hacktivistas que desarrollan sus ciberataques sobre motivaciones ideológicas y no cibercriminales. En julio de 2016 'Anonymous Brasil' amenazaba con infectar con ransomware ordenadores de la Agencia de Telecomunicaciones de Brasil ANATEL. Se trata de la primera ocasión que se tienen constancia de que una identidad puramente hacktivista emplea o amenaza con el empleo de ransomware por motivos ideológicos. Finalmente, la amenaza no llegó a materializarse.

'**Chilean Hackers**', '**Chilean Crew**', '**Peruvian Hackers**' y '**Mexican Hackers**' tuvieron un par de meses de actividad más o menos constante a principios del año, para posteriormente decaer como ya se ha mencionado, con acciones ocasionales mantenidas de 'Peruvian Hackers' contra webs tanto en Iberoamérica como en varios países del mundo a lo largo del año.

Por otro lado, fuera de los focos principales de hacktivismo de Venezuela, Brasil, Chile o Colombia, durante 2016 han sido atacadas webs de Gobierno en otros países no habitualmente blanco central del hacktivismo (República Dominicana, Bolivia, Ecuador, Paraguay), en acciones llevadas a cabo por identidades presumiblemente en exterior de Iberoamérica y con rasgos árabes, como '**Nofawkx-al**', '**Fallaga Team**', '**Team System DZ**' o '**Hani Xavi**'.

Identidades que en Iberoamérica han permanecido con menor actividad que el año precedente han sido '**Hanom1960**', con acciones durante el primer mes del año para luego probablemente mutar en 'PureEliteTeam', que desarrolló algunos ataques en la segunda mitad del año; '**AnonymousOIC**' en Brasil, con ataques la primera mitad del año para posteriormente detenerse; y la argentina '**Libero**', muy activa los años previos y en 2016 prácticamente sin acciones.

En cuanto a nuevas identidades hacktivistas que en 2016 han aparecido con ciberataques ocasionales en el panorama iberoamericano cabe nombrar a '**Bolivian Hackers**', con ataques ocasionales en Venezuela; '**Brazilian Cyber Army**' y '**La Firma Sec**' con acciones por desfiguración al principio del año contra webs de Gobierno en Brasil.

4.2 Operaciones hacktivistas en Iberoamérica

Durante 2016 identidades hacktivistas, la mayoría en la órbita de 'Anonymous', promovieron varios marcos narrativos insurgentes que en buena parte se utilizaron como base ideológica para desarrollar campañas de ciberataque.

En general el conjunto de estas campañas de ciberataque fue de baja intensidad y limitadas en el tiempo; los dos únicos marcos hacktivistas que prolongaron su actividad con ciberataques adscritos más o menos a lo largo de todo 2016 fueron la #OpVenezuela, mantenida desde el año previo y la #OpOperadoras en Brasil.

La lista de marcos narrativos hacktivistas con intenciones de ciberataque aparecidos en Iberoamérica en 2016 son, por orden cronológico:

MARCOS NARRATIVOS HACKTIVISTAS EN IBEROAMÉRICA 2016					
PAÍS	**OPERACIÓN**	**PROMOTOR**	**TIPO DE OBJETIVO**	**ACCIÓN**	**RESULTADO**
VE	#OpVenezuela	Anonymous Venezuela	Instituciones públicas de Venezuela	DDoS Desfiguración Exfiltración	Varias decenas de webs afectadas
MEX	#OpNiUnaMas	Mexican Hackers Anonymous Venezuela	Instituciones públicas de México	Desfiguración	Algunas decenas de webs afectadas
CR	#OpPuraVida	Anonymous Costa Rica	Instituciones públicas de Costa Rica	Desfiguración Exfiltración	Menos de una decena de webs afectadas
CO	#OpParoNacional	Anonymous Iberoamérica	Instituciones públicas en Colombia	Desfiguración	Varios ataques a webs de Gobierno municipal

MARCOS NARRATIVOS HACKTIVISTAS EN IBEROAMÉRICA 2016					
BR	#OpOlympicHacking	Anonymous Brasil	Instituciones públicas en Brasil	Desfiguración Exfiltración	Una par de decenas de webs afectadas
PE	#OpParoRegional	Anonymous CCL	Instituciones públicas del Departamento de Ucayali	Exfiltración	Ataques ocasionales
MX	#OpJusticia43Mx	Anonymous CCL	Instituciones públicas regionales en México	Desfiguración	Ataques ocasionales
AR	#OpMendoza	Anonymous CCL	Empresas en Mendoza, Argentina	DDoS	Un par de acciones
BR	#OpOperadoras	Anonymous Brasil	Instituciones públicas y empresas de telecomunicaciones en Brasil	Desfiguración Exfiltración	Una docena de ataques
BR	#OpStopBlocking	Anonymous Brasil	Instituciones públicas en el Estado de Río de Janeiro	DDoS Desfiguración	Menos de media docena de ataques
CO	#OpFalsa Independencia	Peruvian Hackers	Instituciones públicas en Colombia	DDoS Desfiguración	Una decena de ataques
MX	#OpFalsa Independencia	Anonymous Iberoamérica	Instituciones públicas en México	DDoS	Menos de media docena de ataques
IB	#OpLibertad dePrensa	Anonymous CCL	Instituciones públicas en varios países	Desfiguración	Menos de media docena de ataques
GT	#OpFalsas Promesas	Anonymous Guatemala	Gobierno de Guatemala	Sin definir	No se activó
INT	#OpCambio Climático	Anonymous Iberoamérica	Objetivos internacionales	Desfiguración	Un par de webs atacadas
CH	#OpSodimac	Anonymous Chile	Empresa Sodimac	DDoS	Un objetivo atacado

5. HACKTIVISMO INTERNACIONAL

5.1 Panorama hacktivista internacional

En 2016 el hacktivismo a nivel internacional ha estado dominado por identidades fuera de la órbita de 'Anonymous'. A pesar de que 'Anonymous' ha mantenido y desarrollado campañas de ciberataque en varios países y zonas (África, China, Japón) y de que tal vez la presencia de 'Anonymous' sea cuantitativamente mayor en el panorama, cualitativamente esas campañas han tenido bajo impacto en general por la débil capacidad técnica de los atacantes y la menor adhesión que la causa de 'Anonymous' ha aglutinado en 2016 con respecto a los años previos.

La excepción, tanto técnica como de impacto, en la actividad internacional de 'Anonymous' no ha sido global sino localizada en una geografía concreta, centrada en la actividad de 'Anonymous Italia' que ha mantenido un ritmo más o menos estable de ciberataques sobre sitios web de medio/alto perfil principalmente contra instituciones públicas y empresas en Italia.

'Anonymous Italia' ha permanecido en 2016 como única marca con denominación específica 'Anonymous' en la Unión Europea que ha mantenido capacidades ciberofensivas de nivel medio de amenaza, a pesar de que dos de sus principales activos, las identidades 'Aken' y 'Otherwise' fueron arrestados policialmente a mediados de 2015.

Las campañas internacionales de 'Anonymous' en 2016 se han caracterizado, en general, por un sobredimensionamiento narrativo con falta de correspondencia operativa: es decir, primar la propaganda amenazante intentando "hacer ruido" en redes sociales para posteriormente ejecutar acciones de ciberataque con mínimo impacto.

Un ejemplo de este patrón en el modus operandi de 'Anonymous' ha sido la **#OpIcarus** en 2016, definida como para ciberatacar a los Bancos Centrales nacionales en todo el mundo y que se tradujo en ataques por denegación de servicio (DDoS) programados contra webs de Bancos Nacionales en numerosos países, ataques que tuvieron muy bajo seguimiento internacional en cuanto a participación de identidades 'Anonymous' y nulo impacto sobre los objetivos atacados.

Una característica de la estructura del colectivo 'Anonymous' a nivel internacional en 2016, ya mencionada para Iberoamérica, es la retirada a un plano anecdótico de la coordinación de campañas hacktivistas a través de comunicaciones en canales IRC. Estos canales, considerados inseguros por la mayoría de facciones 'Anonymous', continúan sobreviviendo en operaciones de bajo impacto en las que se pretende (aunque no se consigue) una colectivización global. El servidor más empleado para los canales IRC aún existentes es **Cyberguerrilla.org**, que prácticamente funciona como la única plataforma de comunicaciones representativa de 'Anonymous' a nivel internacional junto con el canal en Twitter **'YourAnonNews'**.

Al margen de 'Anonymous', entre las identidades hacktivistas más activas durante 2016, que han logrado producir impacto internacional por la técnica empleada en sus ciberataques o por la naturaleza de los objetivos atacados, se encuentran '**OurMine**',

un alias al que se ha venido atribuyendo origen saudí y que a partir de mediados de 2016 ha comprometido perfiles en redes sociales (Twitter, Quora, Vine) de ejecutivos de empresas ligadas a redes sociales o tecnológicas principalmente en EE.UU.

Entre los objetivos alcanzados por 'OurMine' están el Director General de Google (Sundar Pichai), el Director General de Twitter (Jack Dorsey), el portal de noticias tecnológicas BuzzFeed, la revista Variety o las empresas de entretenimiento global Netflix o Marvel.

Otra identidad que, aunque con baja proliferación de ataques, se ha revelado como una ciberamenaza que ha demostrado una elevada capacidad técnica para comprometer objetivos de alto perfil en el plano internacional ha sido '**Phineas Fisher**', también conocida como **'Hack Back!'**.

Esta identidad, que ha reivindicado vulnerar los sistemas de información de las empresas de ciberseguridad ofensiva Gamma Group en 2014 y Hacking Team en 2015, en 2016 comprometía los canales web y en redes sociales del Sindicato de la Policía Autonómica de Cataluña en España, atribuyéndose también haber donado bitcoins a la insurgencia independentista de Rojava en el Kurdistán, dinero supuestamente sustraídos a una entidad bancaria (sin determinar). El 20.07.2016 producía la exfiltración de ficheros y correos electrónicos del partido gobernante turco AKP.

También internacionalmente, aunque sin impacto global, ha destacado en 2016 una acción de la identidad hacktivista turca '**RedHack**', que en octubre situaba en una dirección de Tor una exfiltración de correos electrónicos que alegaba habían sido obtenidos por el hackeo del Ministro de Energía del país (y yerno del Presidente de Turquía) Berat Albayrak.

Tras la acción, supuestamente las autoridades turcas habrían bloqueado el acceso a plataformas de almacenamiento masivo en red, como Google Drive, Github, Archive.org o Dropbox para evitar la redifusión de la información por parte de 'RedHack'. No obstante, en diciembre '**Wikileaks**' divulgaba más de 57 mil mensajes de correo electrónico supuestamente originarios de Berat Albayrak, cuya obtención ilícita era atribuida al colectivo hacktivista 'RedHack'.

Otra identidad cuya evaluación como amenaza todavía es prematura y que ha emergido en el último tercio de 2016 es '**Kapustkiy**', que ha mostrado especialización en la ejecución de ataques sobre servidores web explotando vulnerabilidades SQL, extrayendo contenido de base de datos y exfiltrándolo al dominio público. Esta identidad ha atacado webs de alto perfil de Gobierno en India y hacia el final del año cambió su foco de atención hacia webs de Gobierno en algunos países de Iberoamérica.

En un ámbito de baja amenaza pero de significativa repercusión informativa, en 2016 identidades como '**Lizard Squad**', '**PoodleCorp**' o '**New World Hackers**' han continuado una práctica observada en años previos consistente en simular ser identidades hacktivistas que llevan a cabo campañas de ataques DDoS contra objetivos que tienen determinado impacto mediático (principalmente plataformas web de juegos online con alcance global, o medios de comunicación internacionales), cuando en realidad estaban poniendo en práctica una estrategia de

marketing de visibilidad para proporcionar el alquiler de sus propias plataformas para llevar a cabo ataques DDoS (por ejemplo, la denominada BangStresser).

En marzo de 2016, la Agencia Federal de Investigación (FBI) de EE.UU. añadía a dos presuntos miembros del '**Syrian Electronic Army**' a su lista de los "más buscados". Esta identidad hacktivista ha tenido nula actividad en 2016, si bien en años previos se atribuía la probable vinculación con el Gobierno de Siria.

Además de 'Anonymous' y las identidades que se han mencionado como destacadas, el *volumen de hacktivismo internacional de bajo perfil* está cifrado en cientos de identidades hacktivistas individuales que producen alrededor de *tres mil ataques al día*, sólo en la modalidad de desfiguración, contra sitios web de todo el mundo. Alrededor de dos tercios de esos ataques por desfiguración se producen contra sitios web cuyo desarrollo está basado en sistemas de gestión de contenidos (siglas CMS en inglés) de libre distribución.

5.2 Operaciones hacktivistas internacionales

Las narrativas hacktivistas más significativas que se tradujeron en campañas de ciberataques en países distintos de España o del subcontinente iberoamericano durante 2016 se sintetizan en la siguiente tabla, por orden cronológico:

MARCOS NARRATIVOS HACKTIVISTAS EN AMBITO INTERNACIONAL 2016					
PAÍS	**OPERACIÓN**	**PROMOTOR**	**TIPO DE OBJETIVO**	**ACCIÓN**	**RESULTADO**
INT	#OpFrance	Caliphate Cyber Army	Todo tipo de webs en Israel, EE.UU. y Francia, principalmente	Desfiguración	Algunas decenas de webs afectadas
CN	#OpHongKong	Anonymous	Partido Comunista y Policía de China	No desarrollada	Sin ataques
JP	#OpKillingBay	Anonymous	Instituciones públicas y empresas en Japón	Desfiguración DDoS	Menos de media docena de webs
TH	#BoycottThailand	Anonymous	Policía de Tailandia	DDoS Exfiltración	Una par de ataques
NG	#OpNigeria	Anonymous	Gobierno de Nigeria	Exfiltración	Tres ataques
SA KE ET	#OpAfrica	Anonymous	Instituciones públicas y empresas en Sudáfrica, Kenia Etiopía, Uganda y Zimbabue	Desfiguración Exfiltración	Alrededor de dos centenares de objetivos alcanzados
IT	#OpHomes	Anonymous Italia	Instituciones policiales en Italia	Exfiltración Desfiguración DDoS	Tres objetivos atacados

MARCOS NARRATIVOS HACKTIVISTAS EN AMBITO INTERNACIONAL 2016					
IT	#OpGreenRights	Anonymous Italia	Instituciones de Gobierno regional en Italia	Desfiguración DDoS	Tres objetivos atacados
USA	#OpTrump	Anonymous	Empresas relacionadas con Donald Trump	DDoS Desfiguración	Una docena de objetivos atacados
CA	#OpCanary	Anonymous	Empresas energéticas en Canadá y Kenia	Desfiguración	Menos de media docena de ataques
AO	#OpAngola	Anonymous Portugal	Instituciones de Gobierno en Angola	DDoS	Una docena de objetivos atacados
IT	#OpNessum Dorma	Anonymous Italia	Empresas de trabajo temporal en Italia	Desfiguración Exfiltración	Medio centenar de objetivos afectados
IL	#OpIsrael	AnonGhost	Todo tipo de sitios web en Israel	Desfiguración Exfiltración	Varios centenares de webs atacadas
INT	#OpPharma	Anonymous	Objetivos en industria farmacéutica internacional	No desarrollada	Sin ataques
INT	#OpSilence	Ghost Squad Hackers	Medios de comunicación internacionales	DDoS	Menos de media docena de webs en varios países
INT	#OpIcarus	Anonymous	Bancos Centrales en varios países	DDoS Exfiltración	Varias decenas de objetivos atacados
TK	#OpTurkey	Anonymous	Empresas, Partidos Políticos e Instituciones Públicas en Turquía	Exfiltración DDoS	Una decena de objetivos alcanzados
DE	#OpAnarchist	Anonymous	Deutsche Bank en Alemania	Desfiguración Exfiltración	Un objetivo atacado
INT	#OpOlympics	Fancy Bear	Agencia Mundial Antidopaje	Desfiguración	Un objetivo atacado
USA	#OpClosedMedia	Powerful Greek Cyberarmy	Medios de comunicación en varios países.	DDoS	Una docena de objetivos atacados
IT	#OpSafePharma	Anonymous Italia	Empresas farmacéuticas en Italia	Exfiltración DDoS	Menos de media docena de objetivos atacados

MARCOS NARRATIVOS HACKTIVISTAS EN AMBITO INTERNACIONAL 2016					
USA	#OpNoDAPL-2	Varias identidades y colectivos sociales	Instituciones de Gobierno y empresas en Dakota del Norte	No desarrollada	Sin ataques
IT	#OpArbitrium	Anonymous a Italia	Partidos Políticos e Instituciones en Italia	Desfiguración	Media docena de ataques
TH	#OpSingle GateWay	Anonymous	Instituciones públicas de Tailandia	DDoS Desfiguración Exfiltración	Una docena de objetivos atacados

6. CIBERYIHADISMO Y HACKTIVISMO PROYIHADISTA

6.1 Panorama ciberyihadista

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

- Mientras el **yihadismo** emplea la violencia física (asaltos armados, atentados con bomba, despliegue de fuerzas armadas sobre el terreno) para actuar sobre objetivos en 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 (generación del terror en la sociedad, advertencia a las instituciones estatales).

Durante 2016 puede afirmarse que el ciberyihadismo estrictamente como tal es una amenaza teórica que todavía no se ha manifestado. En las evaluaciones de ciberseguridad, el ciberyihadismo ha venido estando asociado al desarrollo de capacidades ciberterroristas por parte de grupos terroristas como 'Al Qaeda' o el 'Daesh', pero ese escenario todavía no se ha producido más allá del plano de las hipótesis.

6.2 Hacktivismo proyihadista

El término '**Cibercalifato**' ha venido siendo empleado desde principios de 2015 en diversos ciberataques por desfiguración de sitios web en donde los autores del ataque han inyectado con narrativa de apoyo al 'Daesh', 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.

La información recogida durante 2016 confirma la inexistencia de evidencias que sugieran que el 'Daesh' haya desarrollado una división ciberarmada específica destinada a la comisión de atentados terroristas por medios cibernéticos.

Así mismo se confirma que la denominación "cibercalifato" no se corresponde con una entidad única asociada directamente al 'Daesh', sino con un conjunto borroso de identidades hacktivistas no vinculadas orgánicamente al 'Daesh', sino simpatizantes de su simbología e ideología, que llevan a cabo cibertataques por desfiguración contra sitios webs de bajo perfil insertando consignas concretas de propaganda del 'Daesh' o más generales de apoyo a ideologías proyihadistas.

Es decir, el 'Cibercalifato' no existiría como una estructura orgánica del 'Daesh' sino como un concepto instrumentado en el hacktivismo para difundir simbología simpatizante con el islamismo proyihadista.

Por tanto, el 'Cibercalifato' como tal no sería conceptualizado en el ámbito del ciberyihadismo sino del hacktivismo, un tipo de hacktivismo que por emplear una narrativa islamista y proyihadista como sustento ideológico podría caracterizarse como "hacktivismo proyihadista".

En 2016 el panorama del 'hacktivismo ciberyihadista' en torno a la denominación de 'Cibercalifato' ha pivotado alrededor de lo que se conoce como '**United Cyber Caliphate**', a su vez una amalgama borrosa de denominaciones integrando 'Ghost Caliphate Section', 'Sons Caliphate Army', 'Caliphate Cyber Army', 'Cyber Kahilafah' o 'Kalachnikv E-Security Team'. Probablemente todas ellas identidades de oportunidad para una única marca: el colectivo '**AnonGhost**', una ya conocida entidad hacktivista operando en árabe a la que están adscritas un número indeterminado de entidades individuales y que lleva activa al menos desde 2013 con campañas hacktivistas continuadas como #OpIsrael u #OpUSA.

En realidad, en un vídeo situado el 11.01.2016 en Youtube[1] se dejaba claro que la supuesta alianza bajo 'United Cyber Caliphate' (UCA) trata de miembros de 'AnonGhost' renombrándose como 'Ghost Caliphate' para continuar con sus acciones de ciberataque bajo una narrativa islamista con iconografía proyihadista.

De hecho, la UCA no es la primera denominación conjunta por la que optó este conjunto de identidades que pretendían comunicar su afiliación al 'Daesh'. El 10.09.2015 se distribuía en redes sociales un comunicado de constitución del '**Islamic Cyber Army**', con la misma narrativa e intención unificadora que el UCA y con el propósito declarado de "ser el frente de acción contra los americanos y sus seguidores para apoyar al Califato del Estado Islámico con todas sus fuerzas en el campo de la yihad electrónica".

En 2016 volvía a repetirse esa práctica del "primer comunicado de unificación" de identidades alrededor del UCA cuando el 08.10.2016 la identidad '**AhmadHaxor**'

[1] https://www.youtube.com/watch?v=0ycOwhJvUFc

difundía[2] lo que calificaba como el "primer comunicado oficial" del '**United Cyber Caliphate**' (UCC). El perfil en Twitter desde el que se difundió el comunicado está recién creado con el nombre de '**Abu Nubia**', pero el alias de la identidad del usuario coincidía con el empleado por un hacktivista islamista que ha venido actuando en cooperación con 'Mexican Hackers'; de hecho uno de los perfiles a los que sigue la nueva cuenta en Twitter se corresponde con el de 'Mexican Hackers'[3].

El comunicado de UCC estaba estructurado de la siguiente forma: en un primer párrafo exponían su compromiso de "vencer a los infieles en una guerra técnica y militar" y prometían lealtad al "Estado" para establecer el Califato. En un segundo párrafo informaban de la creación de su Ejército (el UCC), apelando a que Allah quiere la unión para el beneficio de los necesitados, la "Unión de Hackers de Califato" formado por "Caliphate Cyber Army", "Kalashnikov" y "Sons Caliphate Army" para finalizar informando que no disponen de ninguna cuenta en redes sociales salvo el canal oficial que dicen anunciar, aunque en el documento no aparecía ningún canal.

Operando ya sea como cualquiera de las marcas bajo el paraguas de '**United Cyber Army**', '**United Cyber Caliphate**' o de '**AnonGhost**' (incluso en enero de 2016 ambas denominaciones anunciaron una "alianza" bajo el nombre de '**Ghost Caliphate**'), la actividad de estas identidades, en tanto ciberamenaza, se ha mantenido durante 2016 en los límites del hacktivismo y, además, con ataques que han revelado consistentemente baja capacitación técnica en su ejecución por los procedimientos empleados de explotación de vulnerabilidades muy comunes sobre sitios web de muy bajo perfil.

6.2.1 Infraestructura hacktivista proyihadista

'United Cyber Caliphate' o cualquiera de sus supuestos grupos constituyentes no han mostrado estabilidad en la permanencia de canales en redes sociales, principalmente debido a la elevada tasa de clausuras de perfiles por parte de Facebook y Twitter al utilizar iconografía o narrativa proyihadistas.

Por ejemplo, el 02.02.2016 se constituía una entidad con la denominación de 'CyberCaliphate', con el nombre en Twitter de '**Sons Caliphate Army**'[4] y en Facebook de '**Caliphate Cyber Army**'[5] sin ni siquiera tiempo para llevar a cabo acciones de propaganda pues fueron suspendidas en ambas redes sociales.

Esta acción de limitación de la propaganda proyihadista en Twitter y Facebook ha empujado a identidades de esta orientación a trasladarse a Telegram, limitando considerablemente su capacidad de difusión de mensajes. No obstante, también en Telegram las identidades alrededor del 'Cyber Caliphate' han venido mutando durante 2016 tanto de denominaciones como de localizaciones.

Por otro lado, el 07.07.2016 la identidad '**s1ege**', que es parte del colectivo 'GhostSquadHackers' que desarrolla, entre otras, las #OpSilence, #OpIcarus y que

[2] https://twitter.com/abu_maghrib1437/status/784894966308802560
[3] https://twitter.com/HackersMx01
[4] https://twitter.com/suod_131
[5] https://www.facebook.com/Caliphate-cyber-army-989487851097031/

lleva a cabo ciberataques contra identidades que considera afiliadas al 'Daesh' en la denominada **#OpReverseCaliphate**, situaba en Twitter el nombre del que atribuye ser uno de los miembros del colectivo hacktivista 'United Cyber Caliphate' (UCC), al que identifica como Harith Al-Muhajir, con Facebook ya clausurado[6].

El 11.07.2016 's1ege' identificaba al argelino Ouali Bouziad como cofundador de UCC y miembro del conocido 'AnonGhost', con Facebook[7] y difundiendo sus supuestos datos identificativos en el dominio público[8]. También atribuían a Moulaye Ahmed Ould Ahmed Semane, residente en Nuakchot (Mauritania), con número de teléfono +22234656555 ser la identidad '**Mauritania Attacker**', líder de 'AnonGhost'.

Respecto de la identidad '**AhmadHaxor**' que difundía el "primer comunicado" del UCC, tenía perfil en Twitter[9] ya clausurado, y cuentas en Vimeo[10] y en la web de la entidad hacktivista 'Gantengers Crew'[11]. Durante 2014 podría haber utilizado los alias de 'TerryBits' y de 'Anon543k'. En LinkedIn aparece un perfil con el nombre de Ahmed Haxor localizado en el área de San Nicolás de los Garzas (México) y que afirma ser "autónomo" y "profesional del software"[12]. Adicionalmente en Google+[13] y en Twitter[14] se observan dos perfiles sin contenido y con iconografía proyihadista que podrían corresponderse con el sujeto, quien ha venido firmando sus ataques por desfiguración sobre sitios web con iconografía islamista y proyihadista, aunque adscritos a 'Mexican Hackers Team'.

6.2.2 Ciberataques de orientación hacktivista proyihadista

Aparte de la intensa propaganda desplegada en redes sociales, promocionada indirectamente por análisis de empresas de ciberseguridad que sobreestiman la amenaza que representan, los procedimientos más utilizados de ciberacción por las identidades alrededor de 'United Cyber Caliphate' o de 'AnonGhost' han venido siendo:

- Desfiguraciones contra webs de bajo perfil a lo largo del mundo, pero principalmente sobre direcciones IP localizadas en Israel y EE.UU.
- Divulgación de las denominadas "kill-lists" (listas de objetivos a abatir), compuestas por listados de nombres y direcciones, generalmente en EE.UU., de personas a las que se atribuye ser integrantes de las Fuerzas Armadas o de las Fuerzas de Seguridad de EE.UU. Otras listas son de ciudadanos de alguna ciudad o Estado (Tennessee, Texas, Nueva York).

[6] facebook.com/harith.abumuhajir
[7] facebook.com/Extazy005
[8] https://justpaste.it/w2e0
[9] www.twitter.com/AhmadHax0r
[10] https://vimeo.com/ahmadhax0r
[11] https://forum.gantengers-crew.org/user-1586.html
[12] https://www.linkedin.com/in/ahmad-haxor-755bb8b8
[13] https://plus.google.com/+AhmadHaxor
[14] www.twitter.com/ahmad_hax0r

La evidencia disponible no es sólida en sustentar que las listas hayan sido obtenidas por el pirateo de sistemas de información y no por otros medios (incluso compuestas a través de consultas sobre bases de datos públicas[15]).

En cuanto a la desfiguración de webs menores durante 2016, por ejemplo el 29.02.2016 y empleando la denominación '**ISIS Cyber Army**' fueron desfiguradas algunas webs de bajo perfil en EE.UU.[16] y Reino Unido, inyectando el mensaje "hacked by Islamic State"[17].

El 10.04.2016 se situaba un paste[18] donde se listaban 32 sitios webs de bajo perfil, en varios países (principalmente Argentina, también Chile o India) desfigurados por el denominado '**United Cyber Caliphate**, que inyectó en las webs atacadas una composición gráfica con el nombre del grupo y como trasfondo una imagen de la bandera estadounidense ardiendo sobre la Casa Blanca.

El 26.04.2016 la web de la Iglesia Reformista Cristiana de Lamont en Michigan[19] (EEUU) fue desfigurada inyectando una composición gráfica firmada por el '**United Cyber Army**', con un vídeo embebido del yihadista Abu Muhammad Al-Adnani.

El 21.04.2016 circuló en un paste ya clausurado[20] una amenaza supuestamente proveniente del 'Caliphate Cyber Army' conteniendo un listado de lo que se identificaba como "lista de ciudadanos importantes de Nueva York, Brooklyn y otras ciudades", con un listado de tres mil nombres acompañados del llamamiento "We Want Them #Dead" (los queremos muertos).

El 28.06.2016 la identidad '**United Cyber Caliphate**' distribuía una lista (no disponible) de doce mil ciudadanos canadienses, sin información sensible sino limitándose a circular sus nombres y ciudades de residencia, con un mensaje en inglés apelando a "lobos solitarios en Canadá a "matarlos inmediatamente".

El 18.08.2016 era desfigurada en España la web de la agencia de empleo empleacastillalamancha.es inyectando el texto "hacked by United Cyber Caliphate". En la misma acción fueron comprometidas las webs de bajo perfil almanar.ps en Palestina y prolog-logistics.co.il en Israel. La web comprometida en España empleaba un gestor de contenidos Drupal 7, mientras la israelí un Joomla 1.5.

En cuanto a 'AhmadHaxor', también sería conocido como '**Ahmad al Maghribi**' y habría venido ejecutando en 2016 ataques por desfiguración contra sitios web en varios países del mundo inyectando contenido con retórica e iconografía proyihadistas, incluso de apoyo al 'Daesh'. El 08.01.2016 firmó tres desfiguraciones sobre webs con direcciones IP en España[21] en todas las cuales inyecto un fichero x.php con el texto "hacked by AhmadHax0r", sin más composición gráfica.

[15] http://sitemultimedia.org/docs/SITE_Analysis_of_Islamic_State_Kill_Lists.pdf
[16] como prarrow.com
[17] townandcountrybedrooms.co.uk
[18] https://justpaste.it/t5nx
[19] lamontcrc.org
[20] paste.c99.nl/7316c4cef0e09bbe757f544b4792d669.html
[21] webinmersiva.com, paginaanticrisis.com y subastastenerife.com

Entre el 11 y el 13.10.2016 'AhmadHaxor' desfiguraba varias webs[22] con direcciones IP en España, entre ellas un subdominio de la Universidad de Vigo[23], en el contexto de ataques contra webs en otros países, inyectando un fichero 1912.gif con el texto "hacked by AhmadHax0r".

Respecto a las supuestas identidades aglutinadas bajo las presuntas alianzas UCA o UCC ('Ghost Caliphate Section', 'Sons Caliphate Army', 'Caliphate Cyber Army', 'Cyber Kahilafah' o 'Kalachnikv E-Security Team'), la evidencia disponible no sugiere que tengan más entidad que ser denominaciones de conveniencia empleadas instrumentalmente para ejecutar desfiguraciones puntuales, por parte de identidades hacktivistas tunecinas o argelinas principalmente adscritas asimismo a otras denominaciones hacktivistas sobre sitios web de bajo perfil y alta vulnerabilidad inyectando contenido proislamista.

[22] distintofilms.com, viajeslavicky.com

[23] mitpa.uvigo.es