Eleven Paths

Informe de Tendencias: Ciberamenazas Hacktivistas 2019

Telefónica CYBER SECURITY UNIT

elevenpaths.com

Índice

1. Introducción

El Informe de Ciberamenazas Hacktivistas es un informe analítico que recoge el escaneo periódico del comportamiento de la amenaza hacktivista en cinco anillos de observación: Europa y Reino Unido, Norteamérica, Latinoamérica, MENA/Asia, y África, donde se realiza una descripción de las operaciones hacktivistas y ciberataques más significativos, la caracterización selectiva de las identidades hacktivistas a las que se atribuye la autoría de las acciones, y un análisis enfocado de las estructuras, infraestructuras, intenciones y capacidades de las identidades hacktivistas.

El informe pretende ser un documento generalista y sin profundidad, pensado para ser completado por un análisis especializado que podría ser solicitado al servicio CyberThreats de Telefónica sobre una base caso_por_caso.

2. Europa

La ciberamenaza hacktivista en Europa durante 2019 se ha mantenido, al igual que en resto del mundo, concentrada en **ataques por desfiguración sobre webs provistas de gestores de contenidos vulnerables o de *software* desactualizado**. Puede afirmarse que esta es la tendencia dominante globalmente con respecto a la ciberamenaza hacktivista en todos los países.

En algunos países de Europa, atacantes específicos han desarrollado ciberataques más ideológicamente motivados en la naturaleza militante del hacktivismo, adscribiendo esos ciberataques a marcos narrativos específicos desarrollados para justificar ideológicamente las acciones. En esta línea de ciberacciones ofensivas más dirigidas han destacado marcos narrativos específicos en Italia y España.

En Italia, **'LulzSecITA' continuaba reactivando narrativas de la antigua 'Anonymous Italia'**, desarrollando ataques durante varios meses de 2019 con una pauta de continuidad en el marco de las **#OpNoTAV** y **#OpGreenRights**; las acciones han consistido principalmente en inyecciones SQL sobre webs vulnerables de pequeñas empresas, de asociaciones gremiales, o de gobiernos locales y regionales.

En España, por su parte, ha destacado la **#OpCataluña** u **#OpCatalonia**, un marco narrativo reactivo a la situación de conflictividad social y política en Cataluña principalmente a raíz del encausamiento judicial de dirigentes políticos y sociales de la región por la comisión de delitos de sedición. En este contexto, en marzo se producían algunas exfiltraciones de baja entidad y una oleada de **ataques puntuales por denegación de servicio contra webs del Ministerio de Justicia**. En junio, una identidad que habitualmente ejerce labores de propaganda y desinformación hacktivistas reivindicaba haber tenido **acceso al servicio web de correos electrónicos corporativos de Microsoft Outlook del Poder Judicial en España**, divulgando contenido parcial del buzón de correo del juez del Tribunal Supremo Manuel Marchena; no se obtuvo evidencia de que se tratara de una acción de ciberataque de la misma identidad que divulgaba la información, sino que el canal de divulgación podría haber sido instrumentado por un atacante distinto que llegó nunca a reivindicarla y que podría haber accedido a los correos aplicando algún tipo de técnica por compromiso de credenciales de usuario.

En septiembre de 2019 y en el contexto de la **precampaña electoral para la convocatoria de elecciones generales en España** una identidad interviniente en la #OpCatalunya divulgaba información privada del teléfono móvil del **presidente del partido político Ciudadanos**, información que a tenor de la denuncia policial interpuesta por la víctima se obtuvo ilícitamente mediante un ataque tipo phishing. No hay constancia de que la identidad hacktivista difusora de la información al dominio público fuera la autora directa del ataque por *phishing*; más bien, a tenor del histórico conocido de **esa identidad, la hipótesis es que esa identidad ('Anonymous Catalonia') podido haber ejercido de canal de difusión de información obtenida por otro atacante que no se ha revelado.**

En la primera mitad de octubre de 2019 se **reactivaba tímidamente la #OpCatalonia** como reacción a la publicación de la sentencia condenatoria a líderes independentistas catalanes acusados de sedición. No obstante, y al igual que ya ocurriera en el reciente escenario de protestas en Hong-Kong (con la #OpHongKong), la dimensión de protesta hacktivista es ínfima en comparación con la intensidad de protestas en las calles: el hacktivismo concentrado en la #OpCatalonia no llegaba a lograr en 2019, colectivizarse ni atraer identidades hacktivistas de otros países; y depende de identidades con nula o baja capacitación técnica para llevar a cabo ciberataques que, como corresponde a esa capacitación, están siendo ocasionales, de ejecución deficiente, apuntando a webs irrelevantes para el contexto narrativo de que se trata. En general, la #OpCatalonia ha mostrado muy **baja peligrosidad y anecdótico volumen de participación** durante 2019.

Por otro lado y más en el ámbito europeo, en marzo de 2019 se convocaba la **#OpCopyWrong**, un marco hacktivista de protesta contra la votación en el Parlamento Europeo de legislación de protección de derechos de copia, que desarrollaba algunos **ataques por denegación de servicio** contra webs de organizaciones europeas y de partidos políticos alemanes; el marco narrativo no obtuvo colectivización ni alcance.

Adicionalmente, en julio, agosto y octubre de 2019 destacó la **vulneración de acceso de varios perfiles en Twitter correspondientes a cinco ayuntamientos en España, correlacionando con el mismo tipo de acciones sobre instituciones gubernamentales en Ecuador y República Dominicana**: durante su secuestro momentáneo todos los perfiles en Twitter emitieron mensajes en idioma español sobre "corrupción política" y en algunos casos amenazas contra funcionarios o personas de gobierno, modificándose en ocasiones las declaraciones biográficas de los perfiles con frases sobre la corrupción. El autor de la oleada de ciberataques no ha firmado ninguna reivindicación específica o difundido una narrativa militante que no sean los propios mensajes atribuyendo corrupción a ayuntamientos y órganos gubernamentales. El **vector de ciberataque en estas acciones fue el *phishing***, y la ejecución estuvo basada en la divulgación de mensajes insultantes y amenazantes a través del perfil comprometido mientras permanece secuestrado.

Finalmente, en noviembre de 2019 **'La 9ª Compañía'** penetraba la web de la **agencia internacional de noticias EFE**, sin producir en esta ocasión ninguna exfiltración de contenidos al dominio público.

2.1. Reino Unido

En el Reino Unido se ha reproducido el patrón ya descrito para Europa de **desfiguraciones principalmente sobre webs privadas probablemente explotando vulnerabilidades comunes de *software***, principalmente en gestores comerciales de contenidos.

Al margen de la habitualidad de ese patrón específico, en abril de 2019 identidades hacktivistas principalmente desde fuera del país respondían al arresto policial del activista Julian Assange con la **#OpUK**, **una variante del marco narrativo #OpAssange** que llamaba a realizar ataques contra webs en ese país y en Ecuador. En el Reino Unido, se desarrollaban **ataques por denegación de servicio** sobre webs del gobierno nacional así como **inyecciones SQL** sobre webs de gobiernos locales. En general, la #OpUK tuvo muy bajo alcance y, aparte algunos ataques ocasionales por desfiguración sobre webs privadas, **la variante #OpUK de la #OpAssange produjo acciones de baja intensidad**, con algunos ataques por denegación de servicio sobre webs de instituciones de gobierno y algunas desfiguraciones afectando principalmente a subdominios de universidades y webs privadas, sobre las que se inyectó contenido alusivo a Julian Assange.

3. Norteamérica

Las ofensivas hacktivistas en Norteamérica han estado igualmente caracterizadas durante 2019 por desfiguraciones sobre webs dotadas de software desactualizado y vulnerable, en un volumen en general menor que en otras regiones.

Entre las acciones llevadas a cabo para ilustrar este patrón pueden mencionarse la llevada a cabo en enero cuando **'zHypnogaja'** desfiguraba dos subdominios[1] del Massachusetts Institute of Technology, que estaban programados con el gestor de contenidos Wordpress desactualizado; o en julio, la desfiguración por **'G4mm4'** con un fichero nervo.html y su alias la web del gobierno de la ciudad de Wappingers Falls[2] en el Estado de Nueva York, que estaba desarrollada con una versión vulnerable de Drupal; o la inyección por **'M3sicth'** del fichero relaz.html con su alias en webs de otras tres ciudades estadounidenses[3], que están equipadas con un gestor de contenidos DotNetNuke vulnerable; en noviembre **'unbid'** utilizaba su alias sobre dos subdominios[4] alojados en la Universidad de Yale, que estaban programados con el gestor de contenidos Drupal.

[1] ling-phil.mit.edu, haiti.mit.edu

[2] wappingersfallsny.gov

[3] wyomingmi.gov, ride.ri.gov, nconemap.gov

[4] cbey.research.yale.edu, envirocenter.research.yale.edu

Fuera de este patrón típico, ha destacado la aparición en abril de una identidad (**'PokemonGo Team'**) que vulneró la web de una asociación de funcionarios de policía en EEUU; de la observación de sus características se hipotetiza que probablemente se trate de una **ciberamenaza con intenciones cibercriminales o incluso desinformativas** que utilizó tácticas hacktivistas para buscar notoriedad en medios de comunicación, pero siendo en realidad una ciberamenaza de corte más hacker que hacktivista; no volvió a realizar ningún ataque posterior reivindicado.

Por otro lado, en agosto se producía **la vulneración del perfil en Twitter de su CEO y fundador Jack Dorsey**, empleándose por los atacantes una táctica no vista previamente en acciones hacktivistas (es probable que el atacante no sea una identidad hacktivista, sino otro tipo de ciberamenaza): la vulneración de un servicio asociado a Twitter a través de la aplicación de **SIM Card Swap**, un procedimiento de fraude mediante el cual el atacante obtendría un duplicado de la tarjeta SIM de una víctima a atacar. Esta acción sobre Twitter no tiene relación con las informadas sobre España y también observadas en Latinoamérica.

4. Latinoamérica

Durante 2019 en Latinoamerica se han concentrado principalmente ciberataques vulnerando webs de instituciones de gobierno local y regional en varios países equipadas con software desactualizado y vulnerable, principalmente gestores comerciales de contenidos. Aparte esta pauta general, dos marcos narrativos de distinto ritmo se han sucedido ciberataques concentrados brevemente en Ecuador y en mayor medida en Chile como reacción hacktivista a climas de protesta social en ambos países, con un conato de resucitar ataques en Nicaragua que no resultó materializado en ningún escenario sostenido.

En marzo de 2019 se hacía un **llamamiento para reanudar la #OpNicaragua**, que no acabó por traducirse en ciberataques efectivos.

En Ecuador, en abril de 2019 la variante **#OpEcuador de la mencionada #OpAssange** se inició con la misma fisonomía que en Reino Unido: se lanzaron ataques por denegación de servicio, realizado iSQL sobre webs de gobierno local y de universidades, y probablemente se comprometía el acceso a la web del Ministerio de Medio Ambiente. A finales de mismo abril decaían los ciberataques en este marco narrativo, produciéndose durante la última mitad del mes varios ataques por denegación de servicio contra webs de gobierno; el ataque más relevante del período fue la **vulneración de la web de la Corte Constitucional de Ecuador**, desfigurada con una imagen de Assange probablemente explotándose alguna vulnerabilidad en el gestor de contenidos Joomla.

En cuanto a Chile, el contexto de inestabilidad social en Chile ha tenido un correlato hacktivista en la **#OpChile**, un marco narrativo que llamaba a ciberataques contra webs gubernamentales en el país. A pesar de que la #OpChile ha tenido en general una baja colectivización y las identidades que a ella se han adherido muestran baja capacitación técnica como ciberamenazas, **una acción de ciberataque sobre el Cuerpo de Carabineros de Chile**, con posterior exfiltración de información sensible en el dominio público, resultaba en una **considerable visibilización de la #OpChile**. En esa acción de ciberataque con exfiltración, denominada por sus atacantes **#PacoLeaks**, es probable que participara una secuencia operativa hacktivista compuesta por: 1) una identidad atacante que se mantiene anónima; 2) una identidad

instrumental bajo tipología 'Anonymous' que reivindica el ataque en redes sociales; 3) otra u otras identidades distintas que proporcionan una infraestructura de exfiltración a través de un dominio web.

En noviembre y diciembre la #OpChile era objeto de un **llamamiento a una segunda fase de ciberataques**, que se traducía principalmente en denegaciones de servicio sobre webs gubernamentales y de partidos políticos, además de alguna exfiltración menor en el dominio público. De nuevo se producía una exfiltración de datos al dominio público, que bajo la denominación de **#MilicoLeaks** divulgaba **contenido de correos electrónicos de varias cuentas corporativas del Ejército de Chile**. Esta exfiltración se sucedía en diciembre con ataques por denegación de servicio sobre webs gubernamentales en el país, algunas desfiguraciones, y varias series de inyecciones SQL sobre diversas webs, produciendo exfiltraciones de usuarios con contraseñas en diversos casos, así como reutilizando datos ya comprometidos en anteriores ciberataques.

Por lo que respecta a Venezuela, en marzo de 2019 y en paralelo al calentamiento de la situación política en el país, varias identidades realizaban **ciberataques afectando con desfiguraciones e inyecciones SQL a varias webs de segundo y tercer nivel de gobierno**, y a universidades; las acciones no acumulaban colectivización sustantiva ni un revitalización del marco narrativo hacktivista de la **#OpVenezuela**, sino que se limitaba a ataques puntuales.

En agosto de 2019 la situación medioambiental en la Amazonia tenía respuesta hacktivista en la propuesta de una **#OpAmazonia**, un marco narrativo que sugería ataques contra webs de gobierno en Brasil, pero también los insinuaba contra países y empresas que se "aprovechen" de la Amazonia. La propuesta apenas fue materializada, con algunas acciones de bajas peligrosidad e intensidad, principalmente a través de la ejecución de inyecciones SQL, la mayor parte defectuosas o fallidas, sobre webs de instituciones públicas, además de algún ataque individual por denegación de servicio sobre webs de gobierno en el país.

En el mismo mes de agosto, se reproducían en algunos países de Latinoamérica la vulneración de perfiles en Twitter de instituciones públicas en algunos países (Ecuador, República Dominicana, Chile, Colombia o México) ya reportados en este informe para España. Esos ataques tuvieron su **epicentro originario de victimización en El Salvador**, donde fueron realizados los primeros ataques con las mismas características que el resto, y en una ocasión **reivindicado por una desconocida identidad 'Lullz DL'**, probablemente un alias de oportunidad.

5. MENA y Asia

Durante 2019 la operativa hacktivista en ambas regiones se ha caracterizado, al igual en la mayoría de países afectados en otras regiones, por ataques por desfiguración sobre webs exponiendo vulnerabilidades comunes en *software* generalmente desactualizado.

No se han propusieron marcos narrativos hacktivista estables en ambas regiones con la excepción de la **#OpIsrael**, tradicional llamamiento a ciberataques contra Israel que se produce todos los años durante el mes de abril y que en los últimos cinco años ha registrado un curso descendente tanto en peligrosidad, en adherencia de identidades atacantes,

o en volumen de ciberataques. En este contexto, en marzo de 2019 se observaban algunos ataques preliminares por desfiguración sobre webs privadas menores en Israel. En abril, y continuando la tendencia instalada desde años previos, la convocatoria de la **#OpIsrael** resultó en una **muy baja colectivización y en acciones de baja peligrosidad contra webs menores**, causando un impacto residual a pesar de algún intento de reivindicar acciones falsas a efectos de buscar notoriedad para identidades hacktivistas.

En cuanto a países concretos, en Egipto coincidiendo con **el aniversario de la revuelta popular de 2011, se lograban desfiguraciones sobre webs de primer nivel de la Administración Pública y de universidades**, entre ellas la Universidad de El Cairo, el Ministerio de Salud o la agencia de registro de dominios de Internet, inyectando sobre ellas contenido conmemorativo.

Durante el primer trimestre del año en Argelia una identidad producía desfiguraciones en **varias webs de segundo nivel de gobierno**, sin mostrar narrativa hostil sobre ellas sino probablemente instrumentando vulnerabilidades en los gestores de contenidos Joomla y Wordpress; igualmente se producían diversos desfiguraciones en la web de un partido político y de varias gobernaciones locales, probablemente en el contexto del rechazo a la reelección del presidente del gobierno de país.

En marzo en Líbano se alteraba la web del **Ministerio de Industria**, que está dotada de varios componentes vulnerables de *software*. En abril se comprometía **la web del ente gubernamental dedicado a la ciberseguridad** en Libia, que equipaba un gestor de contenidos Wordpress.

Por su parte en Asia fue comprometido el **Ministerio de Industria** de Myanmar, que tiene numeroso software descatolizado y vulnerable; y así mismo eran desfigurados el Ministerio de Asuntos Exteriores de Laos, el Ministerio de Medio Ambiente de Filipinas, y el Parlamento Asiático, que tienen webs dotadas de ***software* vulnerable**.

En octubre, la ofensiva militar turca en Siria provocaba una **tímida reacción hacktivista reactivando la #OpTurkey** para, igual que en el caso de la #OpCatalonia en España, producir ataques ocasionales, la mayor parte por denegación de servicio sobre webs en general con baja relevancia.

Por otro lado, en agosto se observaba por primera vez la **intersección**, o al menos la concatenación, entre **prácticas hacktivistas y cibercriminales**, después de que durante al menos el último año se hayan venido reportando conexiones entre el hacktivismo y la inyección de contenido SEO Spam (esto último que podría ser considerado pequeña cibercriminalidad); en esta ocasión, se trata de un paso cibercriminal más allá, inyectándose **una falsa web de aterrizaje de *phishing* para robo de credenciales de American Express**, tras una desfiguración hacktivista: ha ocurrido contra el Ministerio de Planificación de Libia, y al menos el atacante hacktivista, que actúa bajo el alias de 'Mr.Donut's', se identifica como **atacante indonesio** bajo el pseudónimo de **'Krayzie Haxor'**.

6. África

África al igual que en Latinoamérica el patrón principal de ataques hacktivistas viene dominado por acciones de desfiguración sobre webs que exponen vulnerabilidades comunes en software desactualizado, con la diferencia en África de que en vez de ser principalmente afectadas webs de gobiernos locales y regionales (como en Latinoamérica) lo son webs ministeriales de primera línea de gobierno.

De este modo, en el primer trimestre de 2019 eran comprometidas la web del Ministerio de Defensa de Kenia, o ministerios en Ghana, Burkina-Faso y Etiopía, en todos los casos sobre webs desarrolladas con software vulnerable. En abril en Gambia quedaba afectada una web del Ministerio de Agricultura, en Eritrea el banco central del país, y de nuevo en Kenia un subdominio del Ministerio de Comunicaciones. En mayo en Zimbabwe otro atacante afectaba a otra web con gestor comercial de contenidos del Ministerio del Interior, mientras en Rwanda y Sudán se comprometían webs -también con software vulnerable- de gobiernos regionales.

En el contexto de conflictividad en Sudán, un leve marco narrativo hacktivista bajo la denominación de #OpSudan producía durante el año principalmente ataques por denegación de servicio muy ocasionales sobre webs en el país, en acciones de muy baja peligrosidad.

7. Elementos globales

Durante todo 2019 ha sido evidente el patrón hacktivista compuesto por desfiguraciones de sitios web que exponían software desactualizado y vulnerable, seguidas esas desfiguraciones por inyecciones de contenido **SEO Spam contingentes a los ataques hacktivistas por desfiguración**. Este patrón ha sido protagonizado principalmente por identidades **atacantes con rasgos turcos**. En menor porcentaje que los contenidos SEO Spam, contingentes a las desfiguraciones también eran inyectados *script* en Javascript que conducen a los visitantes de las webs comprometidas a **redes de distribución de contenidos maliciosos**.

Por otro lado, en el segundo trimestre de 2019 se observaba un predominio, superior cuantitativamente al patrón habitual de desfiguraciones sobre webs basadas en gestores comerciales de contenidos, de **webs afectadas equipando el gestor Wordpress**; es probable que ello se debiera a **tres vulnerabilidades** descubiertas durante 2019 (CVE-2019-8942, CVE-2019-8943 y CVE-2019-9787, así como otra que lleva cinco años activa en Wordpress 5.0.0) y no parcheadas todavía en numerosas webs.

Así mismo, durante la segunda mitad de mayo de 2019 en varias regiones del mundo se apreciaba un incremento, por encima de lo habitual, de **desfiguraciones vulnerando sitios webs dotados del gestor de contenidos Drupal.**

Posteriormente, en julio de 2019, varios incidentes destacaban **correlaciones entre desfiguraciones de webs y utilización del gestor de contenidos DotNetNuke y del software ASP.net**, ambos de Microsoft. Aunque en el primer caso

la última vulnerabilidad crítica es de 2017 y en el segundo de 2011, pueden estarse explotando en webs no actualizadas: de hecho en el segundo caso se comprobaba que las webs desfiguradas equipaban predominantemente la versión vulnerable 4.0.30319.

En la ejecución de esos ataques a webs equipadas con ASP.net, DotNetNuke y SharePoint de Microsoft en países de todo el mundo ha destacado durante 2019 la identidad **'VandaTheGod'**, que tenía una **doble dedicación al hacktivismo y a la pequeña cibercriminalidad**, esta última manifestada en la venta de shells inyectadas en sitios web. En diciembre de 2019 un joven de 23 años, natural de la localidad brasileña de Uberlandia, era arrestado por la Policía del Estado de Minas Gerais en Brasil como presunto responsable de estar detrás del alias 'VandaTheGod'.

Por otro lado, en marzo de 2019, la conocida identidad **'Phineas Fisher'**, que hace varios años tuvo considerable visibilidad por atacar a empresas de ciberseguridad ofensiva, ha reaparecido con un mensaje en redes sociales advirtiendo de que **"volverá a hackear" en 2019**, sin más datos. En la segunda mitad de noviembre de 2019 cumplía su advertencia **comprometiendo la web de un banco en la Isla de Man**, penetrando alguno de sus servidores web mediante la explotación de al menos dos vulnerabilidades no parcheadas, instalando en su red un **troyano tipo puerta trasera, y afirmando haber realizado algunas transferencias SWIFT**. La acción de 'Phineas Fisher' era un ciberataque individual que no presupone la derivación desde ella de un marco narrativo hacktivista específico en forma de ciberamenaza más allá de la que ya representa desde hace al menos cinco años de actividad el propio 'Phineas Fisher', que por otro lado es la única ciberamenaza de naturaleza puramente hacktivista (ideológica) a escala internacional que opera técnicamente como una ciberamenaza avanzada, mediante el uso de exploits, malware y técnicas de penetración; 'La 9ª Compañía' en España estaría, por ejemplo, en un nivel menor, con similar habilidad de operaciones pero sin el uso (conocido) de malware.

Por último, en lo que tiene que ver con la reunión anual de simpatizantes de 'Anonymous' cada 5 de noviembre bajo la denominación **'Million Mask March'**, continuando con un patrón de declive observado en los últimos años 2019 se saldó con un **seguimiento testimonial y sin incidentes en algunas ciudades del mundo**; los únicos ciberataques coincidentes con la temática del encuentro fueron llevados a cabo por **'LulzSecITA'** en Italia, que siguiendo su modus habitual de comportamiento comprometió principalmente mediante inyecciones SQL webs de varias corporaciones locales y regionales en el país, además de al operador de telecomunicaciones Lyca Mobile, exfiltrando datos personales identificativos de clientes de esta empresa en el país.

Sobre ElevenPaths

En ElevenPaths, la unidad global de ciberseguridad del Grupo Telefónica, creemos que es posible un mundo digital más seguro. Apoyamos a nuestros clientes en su transformación digital, creando innovación disruptiva, aportando la privacidad y la confianza necesaria en nuestra vida digital diaria.

Combinamos la frescura y energía de una start-up con la potencia, conocimiento y robustez de Telefónica, contribuyendo con soluciones que posibilitan la prevención, detección y respuesta ante amenazas diarias en nuestro mundo digital.

Generamos alianzas estratégicas que permiten ampliar la seguridad de nuestros clientes y además, colaboramos con organismos y entidades como la Comisión Europea, CyberThreat Alliance, ECSO, EuroPol, Incibe, y la la Organización de los Estados Americanos (OEA).

Más información

elevenpaths.com

@ElevenPaths

blog.elevenpaths.com