REAL INSTITUTO elcano ROYAL INSTITUTE

FEBRERO 2018
Nº 33

CIBERelcano

Informe mensual de ciberseguridad

Desarrollado por: THIBER

Copyright y derechos:

Fundación Real Instituto Elcano de Estudios Internacionales y Estratégicos-THIBER, the Cyber Security Think Tank

Todos los derechos de esta Obra están reservados a Fundación Real Instituto Elcano de Estudios Internacionales y Estratégicos y a THIBER, the Cyber Security Think Tank. Los titulares reconocen el derecho a utilizar la Obra en el ámbito de la propia actividad profesional con las siguientes condiciones:

a) Que se reconozca la propiedad de la Obra indicando expresamente los titulares del Copyright.
b) No se utilice con fines comerciales.
c) No se creen obras derivadas por alteración, trasformación y/o desarrollo de esta Obra.

Los titulares del Copyright no garantizan que la Obra esté ausente de errores. En los límites de lo posible se procederá a corregir en las ediciones sucesivas los errores señalados.

Eventuales denominaciones de productos y/o empresas y/o marcas y/o signos distintivos citados en la Obra son de propiedad exclusiva de los titulares correspondientes.

Informe editado en Madrid.

Más información:

Fundación Real Instituto Elcano de Estudios Internacionales y Estratégicos.

THIBER, The Cyber Security Think Tank.

Índice

1 Comentario Ciberelcano 04

2 Análisis de actualidad internacional 06

3 Ciberpolítica: análisis de actualidad 10

4 Informes y análisis sobre ciberseguridad publicados en enero 13

5 Herramientas del analista 14

6 Análisis de los ciberataques del mes de enero 17

7 Recomendaciones

7.1 Libros y películas 22

7.2 Webs recomendadas 24

7.3 Cuentas de Twitter.....24

8 Eventos.....25

1 COMENTARIO CIBERELCANO:
La importancia de la narrativa tecnológica

AUTOR: Enrique Fojón Chamorro. Subdirector de THIBER, the cybersecurity think tank.

Fuente: www.neoesperience.com

Inteligencia Artificial, robótica, nanotecnología, biotecnología, internet de las cosas o computación cuántica son solo algunas de las áreas de investigación que hasta pocos años parecían ciencia ficción; sin embargo, en un futuro no muy lejano, estas tecnologías – en su mayoría procedentes de centros de investigación, start ups y grandes empresas- serán la base de muchos productos y servicios que transformarán profundamente el modo en el que vivimos, trabajamos y nos relacionamos, sino lo son ya.

Sobra decir que vivimos en un mundo cada vez más interconectado lo que propicia que la velocidad de la transformación tecnológica sea exponencial. Una transformación que no solo afecta al "que" y "como" se hacen las cosas sino también a "quienes somos". Una transformación que en palabras de Marc Benioff – CEO de SalesForce - está cambiando el significado de ser "humano".

Sin embargo, esta realidad contrasta con el hecho de que la inmensa mayoría de los deciso-

res empresariales y políticos –sobre todo estos últimos- siguen instalados en un pensamiento analógico, lineal y cortoplacista que les impide evolucionar hacia un pensamiento estratégico y prospectivo que les permita inferir las implicaciones que la innovación tecnológica tiene hoy en día y tendrá en un futuro cercano. Por tanto, aunque parezca una obviedad, resulta necesario – y no lo estamos haciendo- que todos los sectores de la sociedad – gobierno, empresa, academia y sociedad civil- comprendan y asimilen las implicaciones de la continua transformación tecnológica ya que debemos prepararnos e interiorizar que las futuras generaciones vivirán - de manera inevitable- en un contexto social, económico, cultural y político totalmente condicionado por los avances tecnológicos presentes y futuros.

En este sentido, y como hemos comentado anteriormente los gobiernos deberían comenzar a trabajar –algunos ya lo hacen, pero de manera desigual- en la evolución desde el mencionado pensamiento analógico, lineal y cortoplacista a uno más estratégico y tecnológico. Para ello, como primer paso, **será necesario construir una narrativa consistente, comprensible, positiva y común** que sirva de base a un conjunto de líderes de opinión y/o grupos de presión para evangelizar a estos decisores políticos y empresariales –así como a la sociedad civil en general- creando así una base de pensamiento sobre los principales retos y oportunidades que ofrece la revolución tecnológica. De este modo, se podrán generar respuestas óptimas – o al menos intentarlo- a estos retos y oportunidades evitando una pérdida de control sobre los efectos que la transformación tecnológica pueda tener sobre el modelo de sociedad que queremos. Si no trabajamos en este sentido, corremos el serio riesgo de que la transformación tecnológica imponga el “que“ y “como” se hacen las cosas y el “quienes somos”. Aún estamos a tiempo.

“Es necesaria una narrativa tecnológica consistente,comprensible, positiva y común”

2 ANÁLISIS DE ACTUALIDAD INTERNACIONAL:

Camboya: ¿hacia un autoritarismo 2.0?

AUTORA: Clara Chirino. Analista de THIBER, the cybersecurity think tank.

La intrusión de las redes sociales en la política está resultando clave a la hora de decidir el futuro de algunos países. En el siguiente artículo, se toma como estudio de caso Camboya, donde tanto el Primer Ministro, Hun Sen, como la oposición están recurriendo, principalmente, a Facebook para recabar votos entre la población y, sobre todo, llegar a un público más joven. De hecho, alrededor del 90% de la población camboyana que usa Facebook tiene entre 18 y 34 años.

Según un informe de 2016, esta plataforma social se ha convertido en la primera fuente de noticias para los camboyanos. Las nuevas generaciones han tendido a alejarse de las fuentes tradicionales de información, que, aparte de carecer de la inmediatez que ofrece Internet, están fuertemente controladas por el Gobierno. A esto hay que sumarle la posibilidad que ofrecen las redes sociales de interactuar entre usuarios mediante comentarios y la difusión de noticias, lo que promueve el debate. También, cabe señalar que este cambio en la forma de consumir información diaria se ha visto favorecido por el incremento en el número de dispositivos electrónicos con conexión a la red, tales como ordenadores y *smartphones,* al alcance de la población camboyana.

"Ciudadanos camboyanos que han publicado en Facebook críticas contra el Gobierno han sido multados o arrestados."

Para el régimen de Hun Sen –en el poder desde 1993, primero mediante una coalición con el Funcinpec y, desde 1997, gobernando su partido, el Partido Popular de Camboya (CPP), en solitario tras dar un golpe de Estado– Facebook supone una amenaza. El principal partido en la oposición, el Partido de Rescate Nacional de Camboya[1] (CNRP), siendo consciente de la influencia del Ejecutivo sobre los medios de comunicación tradicionales, lleva años persiguiendo una estrategia virtual para acercarse a la población camboyana. Desde 2013 el CNRP está obteniendo cada vez más apoyos, lo que le ha permitido igualar, prácticamente, resultados en los comicios con el CPP. En las elecciones generales celebradas el 28 de julio de 2013, en las que hubo un 70% de participación, el CPP consiguió 68 escaños de 123, siendo los 55 restantes para el CNRP. No obstante, este último rechazó los resultados al considerar que más de un millón de personas habían sido excluidas del censo electoral y que el CPP había introducido falsas papeletas en las urnas para lograr la victoria. Durante las siguientes semanas a los comicios se convocaron distintas protestas multitudinarias en Phnom Penh contra el Gobierno,

[1] El CNRP surgió en 2012 de la fusión del Partido Sam Rainsy (SRP) y el Partido de Derechos Humanos (HRP).

lo que motivó que este movilizase al ejército para disuadir a la población de convocar nuevas manifestaciones. El 7 de agosto de 2013, distintos grupos de la sociedad civil denunciaron la imposibilidad de acceder a Facebook durante varias horas y exigieron al Gobierno una explicación. El bloqueo de la red social fue interpretado por la población como un intento por parte del Ejecutivo de controlar e incluso censurar esta red social –lo que ya había ocurrido con otras plataformas virtuales como KI Media, una web crítica con la gestión de Hun Sen.

Desde las elecciones de 2013, el Gobierno está llevando a cabo una política represiva contra la oposición, consistente en arrestos, amenazas, seguimientos, agresiones, etc., con el fin de evitar que le arrebaten el poder en los comicios de julio de 2018. De hecho, Hun Sen ha declarado, en reiteradas ocasiones, que se desatará una guerra civil si el CNRP logra la victoria en las elecciones generales del próximo verano[2]. El acoso a la oposición por parte del Ejecutivo camboyano ha propiciado que muchos parlamentarios del CNRP hayan optado por presentar un perfil bajo o se hayan exiliado, entre ellos su antiguo líder Sam Rainsy, quien será arrestado si regresa al país. En julio de 2016, Kem Ley, conocido opositor al régimen, fue asesinado en una gasolinera. Ante este acontecimiento, Rainsy acusó al Gobierno de la muerte de Ley a través de Facebook, lo que le valió una condena de más de un año de cárcel y una multa por difamaciones. Los medios de comunicación no retransmitieron el multitudinario funeral por Kem Ley que se celebró en la capital, por lo que los camboyanos emplearon las redes sociales para averiguar el recorrido del mismo y unirse a él.

[2] Además, distintas personalidades del Gobierno han amenazado públicamente a la población en los últimos meses. A modo de ejemplo, el ministro de defensa, Samdech Tea Banh, amenazó con “romper los dientes” a todo aquel que protestase tras las elecciones locales de 2017, y el ministro de asuntos sociales, Vong Sauth, anunció que el Gobierno golpearía con varas de bambú a aquellos que rechazasen los resultados de las elecciones generales de 2018.

Diversas cuentas en redes sociales y de correo electrónico de activistas y defensores de derechos humanos han sido hackeadas en los últimos años. Asimismo, varios civiles que han publicado en Facebook críticas contra el Gobierno han sido multados o incluso arrestados. A modo de ejemplo, en noviembre de 2016, Rainsy fue multado por acusar a Hun Sen de haber, supuestamente, inflado el número de seguidores en su perfil de Facebook. De acuerdo con la plataforma virtual Socialbakers, esta cuenta tiene más de nueve millones de seguidores en la actualidad. Un artículo publicado en el periódico The Phnom Penh Post en marzo de 2016 señaló que la mitad de los seguidores de Hun Sen en Facebook son de otros países, principalmente, Filipinas e India, lo que pone en duda su legitimidad. Por el contrario, la mayoría de los apoyos que Rainsy está obteniendo a través de Facebook provienen de Camboya.

"El Primer Ministro está intentando acercarse a las nuevas generaciones a través de Facebook."

El hecho de que la continuación del régimen de Hun Sen esté en peligro ha motivado que el Primer Ministro intente acercarse a las nuevas generaciones a través de Facebook, en vez de adoptar una estrategia de censura, como ha seguido con los medios de comunicación tradicionales[3]. Su objetivo es desbancar en popularidad a la oposición en Internet, a la que acusa de promover la tensión política mediante comentarios que publica en Facebook contra el Ejecutivo. En esta plataforma social, el Primer Ministro trata de dar una imagen familiar y amena, compartiendo fotografías y videos de su vida personal. Además, según Hun Sen, su partido está abogando por un e-government, en el que los ciudadanos interactúen con los funcionarios de forma virtual a través de Facebook. En consecuencia, el sector público debe atender las peticiones de la población en esta plataforma social, para lo que, supuestamente, se han establecido grupos de trabajo que monitoricen los comentarios de los usuarios. No obstante, la policía camboyana controla las publicaciones en Facebook para detectar contenido contrario al CPP con el presunto fin de salvaguardar la unidad nacional, aludiendo, incluso, a que en esta red social se podría estar gestando un movimiento rebelde contra el Gobierno.

En junio de 2017, se celebraron las elecciones locales en el país. El CNRP logró tres millones de votos, mientras que el CPP consiguió tres millones y medio. Sin duda, estos resultados pueden considerarse como una antesala de lo que podría ocurrir en los comicios generales de 2018. Ante la posibilidad de que el CNRP acabe venciendo próximamente, el Gobierno ha intensificado su campaña de acoso a la oposición. Ya en febrero de 2017, Rainsy dimitió de su puesto tras la aprobación por parte del Ejecutivo de una Ley que permite disolver partidos políticos cuyos líderes han sido condenados. Desde entonces, el cargo lo ocupa Kem Sokha, que fue enviado

[3] El pasado septiembre, el periódico Cambodia Daily fue obligado a cerrar, mientras que otros fueron acusados de infringir la reglamentación en materia de impuestos y licencias, lo que hace sospechar que el Gobierno aboga por la finalización de su actividad.

a prisión en septiembre acusado de traición. En noviembre de 2017, el Tribunal Supremo de Camboya –cuyo principal juez está vinculado al CPP– disolvió de manera oficial el CNRP, prohibiendo a 118 de sus integrantes dedicarse a la política durante los próximos cinco años. Asimismo, desde el pasado junio, 200 de los 6.000 políticos en la oposición se han unido al CPP ante la amenaza de que su asiento en el Parlamento sea revocado.

La comunidad internacional ha denunciado la vertiente autoritaria que está adoptando Camboya. En este contexto, Estados Unidos ha expresado su negativa a proveer de ayuda al país asiático para que financie las elecciones y ha anunciado restricciones de visado para algunos líderes camboyanos. Por su parte, Hun Sen ha declarado que las elecciones del próximo verano se celebrarán a pesar de que no sean reconocidas por la comunidad internacional, ya que quienes deben aceptarlas deben ser los propios camboyanos.

"El Gobierno aboga por un e-government, en el que los ciudadanos interactúen con los funcionarios a través de Facebook."

3 CIBERPOLÍTICA: ANÁLISIS DE ACTUALIDAD

El GDPR desde la perspectiva de la ciberseguridad

AUTOR: Javier Alonso Lecuit. Miembro Grupo de Trabajo sobre Ciberpolítica del Real Instituto Elcano.

El 25 de mayo de 2018 entrará en vigor del Reglamento de la UE para la protección de las personas físicas en el tratamiento de datos personales (RGPD). Representa un salto cualitativo en las exigencias sobre la seguridad y la gestión del riesgo de la información para empresas y administraciones públicas en aras de la salvaguarda del derecho fundamental de la privacidad de los ciudadanos, así como en el progreso hacia un Mercado Único Digital, potenciando las oportunidades ofrecidas por la economía digital[1].

EL REGLAMENTO RGPD

El RGPD será de aplicación a toda organización (controlador y/o procesador de datos) que ofrezca servicios a ciudadanos europeos, con independencia del emplazamiento de la empresa que realice procesado de los datos. Implicará cambios significativos en relación a la *Ley orgánica para la Protección de Datos de Carácter Personal (LOPD).*

El Reglamento se apoya en tres principios fundamentales: el de responsabilidad (accountability), el de protección de datos por defecto y desde diseño (privacy by design) del producto o servicio y el de transparencia a los usuarios[2]. Establece nuevas obligaciones tales como la designación de un Delegado de Protección de Datos (DPO), la de evaluar el impacto de los riesgos, la de adoptar las medidas adecuadas para mitigarlos, la de designar un establecimiento principal a las empresas multinacionales que ofrecen sus servicios a ciudadanos europeos o la de comunicar las brechas de seguridad a las autoridades de control y, en casos graves, a los afectados, tan pronto sean conocidas, estableciéndose el plazo máximo de 72 horas.

En relación con los incidentes de seguridad – extravío, robo o acceso no autorizado a los datos de carácter personal - los controladores de los datos deberán detectar, registrar y decidir si procede comunicar el incidente a la autoridad de protección de datos, así como facilitar la información sobre el mismo ante la solicitud de la autoridad competente, para lo que precisan sistemas de detección, investigación, actuación y reporte internos confiables y ágiles.

EL RGPD DESDE LA PERSPECTIVA DE LA GESTIÓN DE RIESGOS

El RGPD no prescribe procedimientos o medios técnicos específicos para la protección de datos personales, por el contrario establece un modelo de regulación basado en la *gestión de riesgos.* Este enfoque supone que las compañías tendrán la flexibilidad de adoptar aquellas

[1] Este comentario es un resumen del ARI del mismo título y autor, Javier Alonso Lecuit, para el Real Instituto Elcano.
[2] ENISA ha publicado sendas guías para facilitar la implantación del principio de privacidad por *diseño a proveedores* y a empresas de *big data.*

medidas técnicas y organizativas que consideren apropiadas para garantizar la integridad y confidencialidad de los datos de carácter personal y demostrar el cumplimiento de los principios establecidos en el RGPD. El enfoque de riesgos tendrá que evitar todo tratamiento no autorizado o ilícito de los datos de carácter personal, su pérdida, destrucción o daño accidental. Habida cuenta la necesaria adaptación de estas medidas a lo largo del tiempo, las organizaciones tendrán que revisar la evolución tecnológica, los costes de aplicación de las medidas, la naturaleza, alcance, contexto y finalidades del tratamiento, así como la probabilidad y gravedad de los potenciales incidentes para los derechos y libertades de las personas. Una vez que entre en vigor el RGDP, las medidas de seguridad regladas en la LOPD pasaran a ser opcionales.

"la notificación de una brecha de seguridad (no siempre evitable incluso adoptando estrictas medidas de seguridad) puede exponer a la organización a sanciones en el curso de la investigación por incumplimiento o mala praxis a pesar de que no guarden relación directa con el incidente notificado."

RETOS PARA LAS ORGANIZACIONES EN EL CURSO DE LA IMPLANTACIÓN DEL RGPD

En las fases iniciales de la adaptación de las empresas al nuevo RGPD, éstas habrán tenido que realizar y documentar una pormenorizada evaluación de la organización en relación a los riesgos que se derivan del tratamiento de los datos personales tales como la destrucción, pérdida o alteración accidental o ilícita de datos personales, la comunicación o el acceso no autorizados a dichos datos que pudieran ocasionar daños y perjuicios físicos, materiales o inmateriales junto a la evaluación de los riesgos tecnológicos concretos, las potenciales vulnerabilidades de los procesos y sistemas así como el impacto potencial sobre la integridad y disponibilidad de los datos.

Entre las medidas de seguridad a aplicar en este contexto caben que destacar:

- Tecnologías para la mejora de la privacidad *(Privacy-Enhancing Technologies, PET)* tales como el cifrado y la (seudo) *anonimización*, teniendo en cuenta la difusa frontera que existe entre los datos de carácter personal anonimizados y aquellos cuya anonimización puede ser reversible (o seudo-anonimizados) gracias a la evolución con la tecnología y la disponibilidad de información adicional.

- Capacidades organizativas, tecnológicas y de inteligencia implantadas por la organización que faciliten garantizar la confidencialidad, integridad, disponibilidad y resiliencia de la información.

- Capacidades para restaurar la disponibilidad y acceso a datos tras un incidente.

- Procesos y tecnologías de monitorización para la verificación, evaluación y valoración continua de la eficacia de las medidas (detectar brechas y demostrar el cumplimiento de la norma).

Las medidas de seguridad adoptadas por las organizaciones en cumplimiento del RGPD serán verificadas por la autoridad regulatoria cuando la organización notifique una brecha de seguridad o cuando se detecte una brecha desde el exterior sin notificación previa de la organización a pesar de su notoriedad.

El nuevo Reglamento aumenta notablemente la exposición de las organizaciones a elevadas sanciones y a daños reputacionales. En este sentido, la notificación de una brecha de seguridad (no siempre evitable incluso adoptando estrictas medidas de seguridad) puede exponer a la organización a sanciones en el curso de la investigación por incumplimiento o mala praxis a pesar de que no guarden relación directa con el incidente notificado. También las organizaciones tendrán que asegurarse por la vía contractual de que las empresas subcontratadas cumplen el RGPD y estar preparadas a responder ante las autoridades judiciales si se denuncia alguna brecha de seguridad ante ellas por los afectados.

Para ayudar a su implantación, la AEPD ha elaborado varias guías y orientaciones dirigidas a profesionales, empresas y *administraciones públicas* así como una herramienta *(FACILITA)* para la adecuación al RGPD de empresas y profesionales responsables o encargados de tratamientos que procesen datos personales de escaso riesgo. En el ámbito nacional, la aplicación del principio de gestión de riesgos en las Administraciones Públicas españolas tendrá en consideración los criterios establecidos para el tratamiento de los datos por el *Esquema Nacional de Seguridad*, las metodologías de análisis de riesgos utilizadas por las Administraciones y las directrices establecidas por la Agencia de Protección de Datos *(Orientaciones sobre el nuevo RGPD para Administraciones Públicas y para Entidades Locales).*

"la AEPD ha elaborado varias guías y orientaciones dirigidas a profesionales, empresas y administraciones públicas así como una herramienta (FACILITA) para la adecuación al RGPD de empresas y profesionales responsables o encargados de tratamientos que procesen datos personales de escaso riesgo.

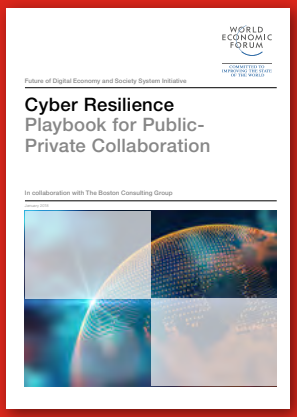
4 Informes y análisis sobre ciberseguridad publicados en enero de 2017

Cyber: The stakes have changed for the C-suite (Marsh&McLennan -- Fireeye)

The Global Risks 2018 (World Economic Forum)

ENISA Threat Landscape 2017 (ENISA)

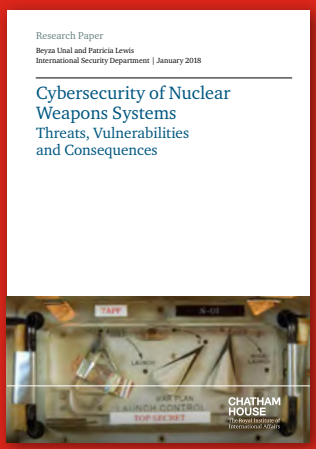
Cyber Resilience: Playbook for Public-Private Collaboration (World Economic Forum)



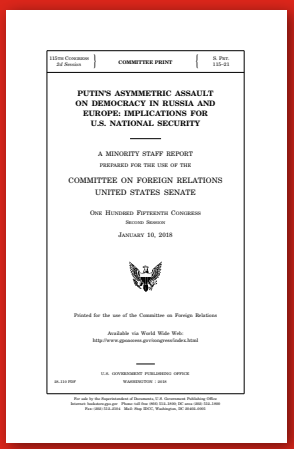
Privacy and Data protection in mobile applications (ENISA)

Iran´s cyber threat (Carnegie Endowment)

Cybersecurity of Nuclear Weapons Systems (Chatham House)



Putin's asymmetric assault on democracy in Russia and Europe: Implication for U.S National Security (U.S Congress)



5 HERRAMIENTAS DEL ANALISTA:
Stackhackr

Stackhackr es una herramienta gratuita de simulación de malware diseñada para probar la seguridad de los endpoints (PCs, servidores, etc).

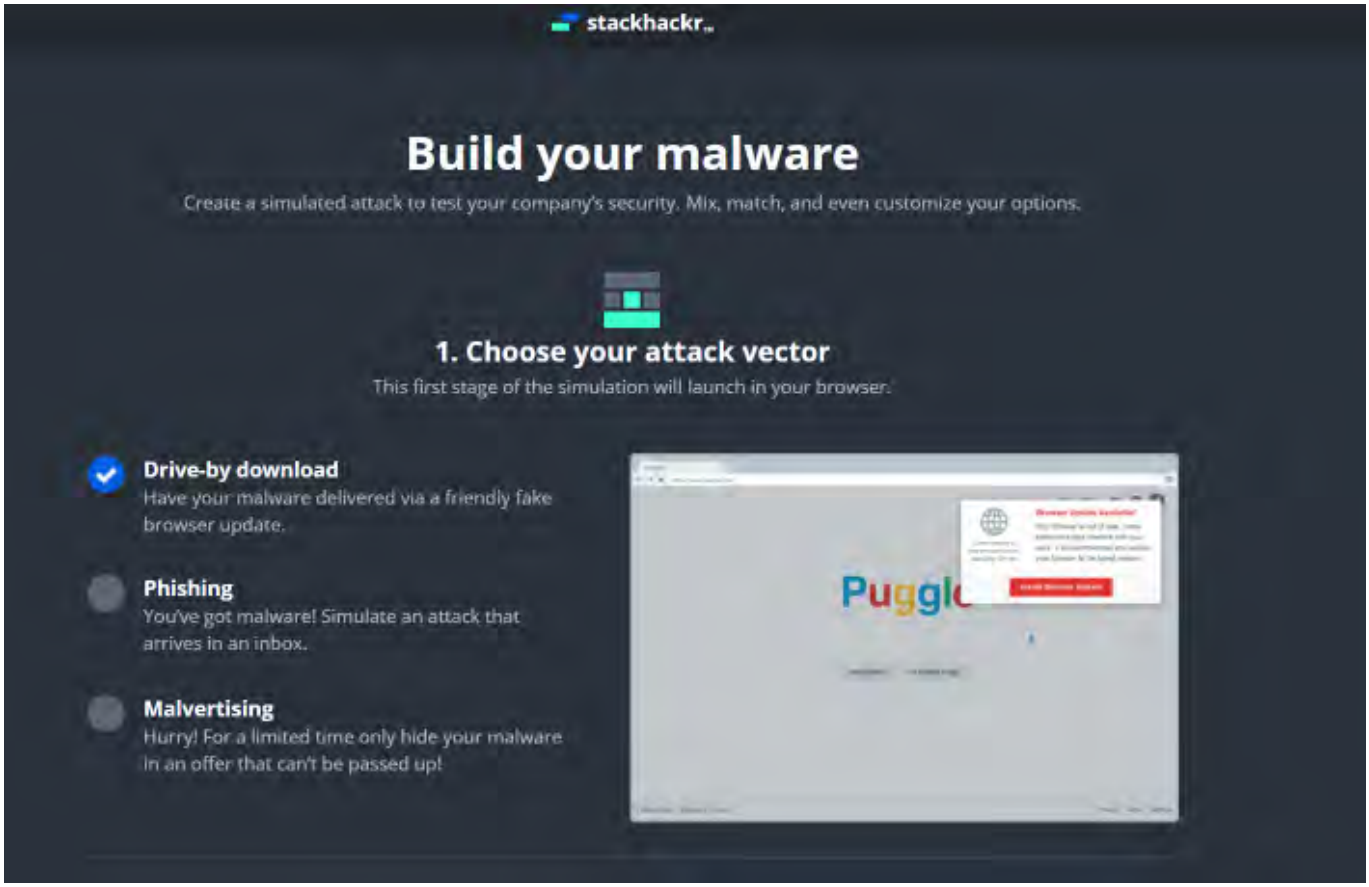
Stackhackr permite crear y personalizar un malware que simula el comportamiento malicioso de un atacante, sin dañar realmente su máquina. Es una forma rápida y segura de descubrir qué máquinas de una organización son vulnerables a ataques reales.

En solo dos minutos puede construir y personalizar su propio malware y ver cómo va a funcionar su seguridad cibernética: ransomware y robo de credenciales.

En la actualidad, probar un antivirus para verificar que esté actualizado con las últimas firmas de malware no es suficiente. Esto se debe a que gran parte del malware de hoy está modificado para evitar la detección mediante el escaneo de archivos. De hecho, está diseñado para ser distribuido y / o ejecutado sin archivos (conocido como *fileless*).

Stackhackr permite probar las capacidades de detección y bloqueo ante dos de los ataques más comunes: el ransomware y robo de credenciales.

Actualmente la plataforma funciona sobre Windows 7, 8.1 y 10.

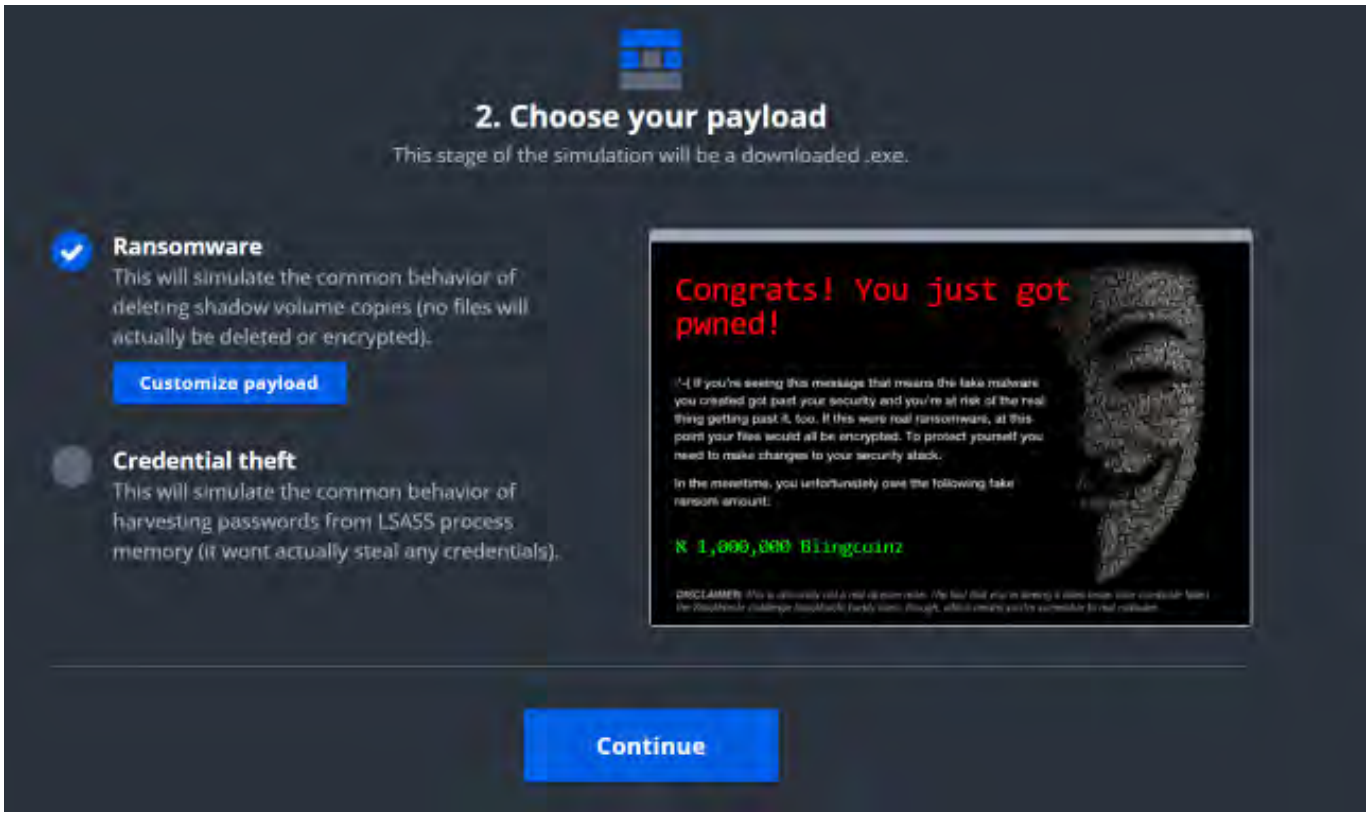


El primer paso es elegir un vector de ataque. Esta es realmente solo una de las formas de probar los endpoints.

Hay tres opciones de vector de ataque para elegir:

1. Drive-by download
2. phishing
3. publicidad maliciosa

En este caso, se selecciona malvertising. Eso significa que cuando se lance la prueba, lo primero que se verá es un sitio web falso ("The Funyun") con un anuncio falso simulado que transporta nuestra carga útil.



El payload determinará qué tipo de comportamiento de malware simulado se intentará en la máquina a probar.

Actualmente, las dos opciones son:

Ransomware: este payload simula eliminar el volumen oculto creando un script oculto en su directorio temporal. A continuación, esa secuencia de comandos inicia un ejecutable para simular la eliminación del volumen oculto. Esta es una cadena de comportamientos sospechosos común en el ransomware, diseñado para evitar que las víctimas usen copias de volúmenes ocultos para recuperar archivos encriptados.

Robo de credenciales: este payload simula otro comportamiento malicioso común, la extracción de contraseñas almacenadas en máquinas con Windows en el subsistema de servicio de la autoridad de seguridad local (LSASS.exe).

También tenemos la opción de personalizar nuestra carga para cambiar la pantalla del rescate.

3. Test your malware vs. your security

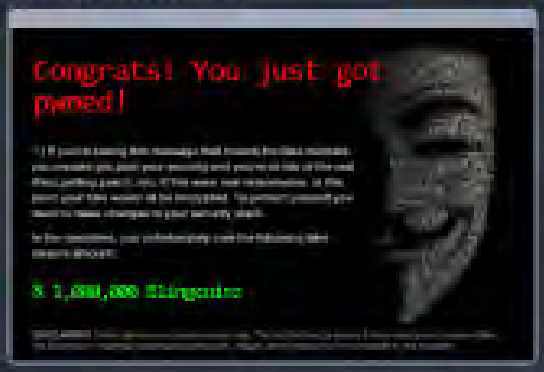
Ready to launch your simulated attack?

Attack vector

Drive-by download Edit

Payload

Ransomware Edit



How the test will work:

1. The attack vector you chose will launch in your browser.
2. From there, you'll need to download launcher.exe and run it.
3. Click 'Start test' in the launcher window to test your mock malware vs. your security stack.

Important: If your AV blocks launcher.exe, that's a false positive

Tests are only run when you click 'Start test' in the launcher window, previewed above. launcher.exe is a benign user interface to help you start and see results of your test with minimal configuration.

6 Análisis de los Ciberataques del mes de enero de 2017

AUTOR: Adolfo Hernández, subdirector de THIBER, the cybersecurity think tank.

CIBERCRIMEN

A comienzos del mes de enero, investigadores de *Quick Heal Security Labs* detectaron un troyano bancario en Android que afectaba aproximadamente a 232 aplicaciones en GooglePlay.

El troyano se distribuye a través de una aplicación Flash Player falsa ubicada en markets de aplicaciones de terceros. Tras la instalación de la aplicación, solicita al usuario que habilite los derechos administrativos. Una vez habilitados, el troyano busca 232 aplicaciones en el dispositivo, principalmente aplicaciones bancarias y de criptomonedas.

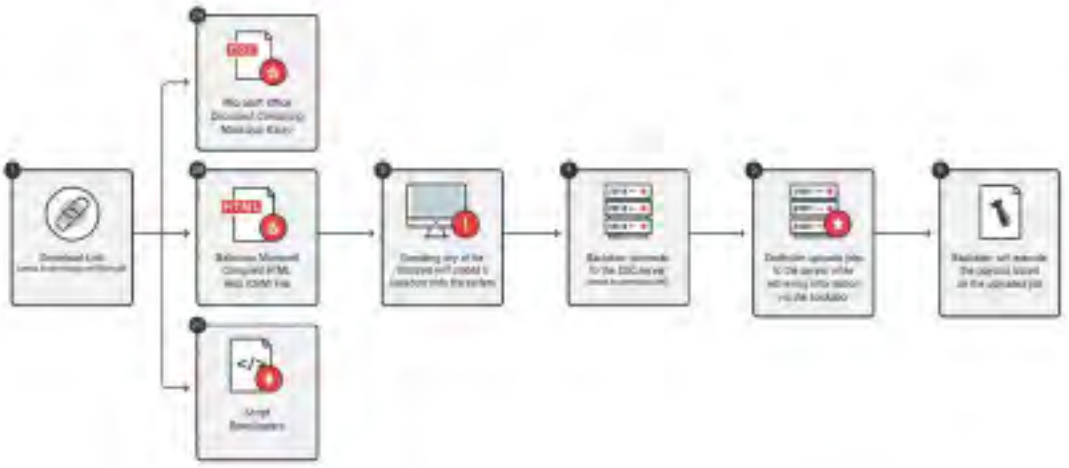
Si se encuentra una aplicación específica en el dispositivo, se muestra una notificación y si el usuario hace clic en ella, se muestra una página de inicio de sesión falso que muestra las credenciales del usuario. El troyano también puede filtrar contactos, ubicaciones y mensajes SMS desde el dispositivo.

Detalle de la app requiriendo permisos de administrador

El 24 de enero, el actor conocido como "Lazarus Group", asociado a diversos Advanced Persistent Threats (APTs) ha estado llevando a cabo una nueva campaña con el objetivo de robar criptomonedas *según los investigadores de Trend Micro.* Las criptomonedas específicas objetivo del ataque del grupo Lazarus son Bitcoin (BTC) y Ant Share (NEO).

Para hacerse con las criptomonedas, el grupo distribuye documentos de Microsoft Office con macros maliciosas, archivos de ayuda compilada en HTML de Microsoft (CHM) y descargadores (downloaders) de scripts para infectar a los usuarios con una nueva versión del backdoor "RATANKBA". RATANKBA puede recibir y ejecutar comandos y robar datos

de una máquina infectada. Se ha observado que RATANKBA está transfiriendo acciones de NEO a un ewallet diferente en una máquina infectada. Esta versión de RATANKBA está escrita en PowerShell para que sea más difícil de detectar.



Vector de infección de RATANKBA

A mediados de mes, según diversos informes gubernamentales, el banco de exportación dirigido por el gobierno mexicano, llamado Bancomext, fue blanco de un ataque infructuoso para robar dinero de diversas cuentas del banco. El banco ha indicado que los atacantes focalizaron su actividad sobre la plataforma SWIFT, un servicio de mensajería global utilizado por las instituciones financieras para transferir dinero.

El mismo método se ha utilizado contra otras instituciones financieras en América Latina. La plataforma SWIFT fue previamente atacada en diversas campañas atribuidas al Grupo Lazarus, un grupo criminal supuestamente asociado con Corea del Norte.

Aunque no hay evidencia que vincule a Lazarus Group con el incidente de Bancomext, el 8 de enero de 2018, el malware asociado a Lazarus Group se dirigió a una empresa mexicana de telecomunicaciones. Debido a la naturaleza y el perfil de los ataques originales en la plataforma SWIFT, cuyo impacto económico se cifra en 81 millones de dólares hasta la fecha, es probable que aumente esta cifra en unos meses.

CIBERESPIONAJE

En el plano del ciberespionaje, se ha detectado una campaña de phishing avanzado focalizado sobre multitud de organizaciones usando como gancho las Olimpiadas de Pyeongchang, *según detallan investigadores de la firma de seguridad McAfee.*

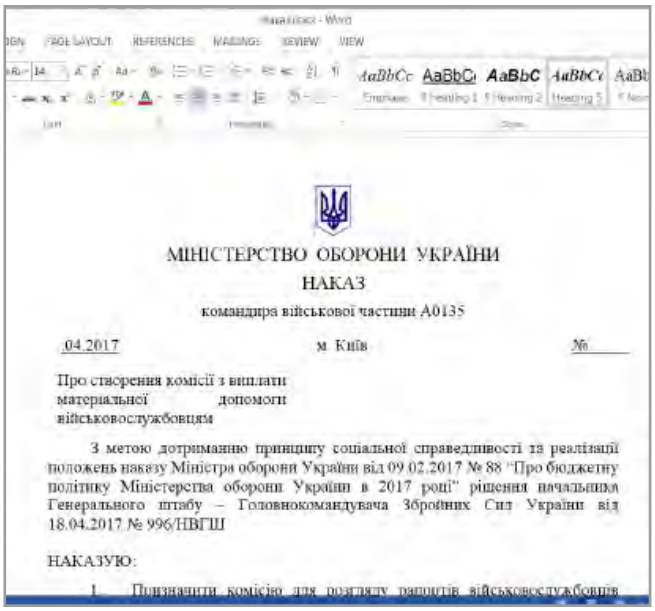
Los autores de esta campaña distribuyen documentos maliciosos de Microsoft Word que tienen como nombre original "Organizado por el Ministerio de Agricultura y pesca de los Juegos Olímpicos de Invierno de Pyeongchang". Esta campaña se dirige principalmente a organizaciones de Corea del Sur. Con la apertura del documento Word, se solicita "Habilitar contenido" de forma que, si se habilita, iniciará un script ofuscado de PowerShell. La secuencia de comandos configura la comunicación a un servidor de comando y control (C2) para obtener instrucciones adicionales a fin de exfiltrar información.

Imagen que contiene el código powershell malicioso oculto

VERMIN: Quasar RAT and Custom Malware Used In Ukraine (January 29, 2018).

A finales de mes, se han identificado diferentes actores empleando una nueva herramienta de acceso remoto / troyano (RAT) denominada "Vermin" en combinación con otro RAT llamado "Quasar", en lo que parece ser una campaña que se remonta a finales de 2015, *según investigadores de la Unidad 42 de Palo Alto.*

La herramienta « Vermin » se distribuye a través de ejecutables autoextraíbles (SFX), algunos de los cuales serán utilizados por el Ministerio de Defensa de Ucrania como Vermin antes de continuar ejecutando el RAT. Vermin es capaz de robar información diversa índole de una máquina infectada, como la arquitectura, el nombre del sistema operativo, la dirección IP local, el nombre de la máquina y el nombre de usuario.



МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ
НАКАЗ
командира військової частини А0135

04.2017 м. Київ №

Про створення комісії з виплати матеріальної допомоги військовослужбовцям

З метою дотримання принципу соціальної справедливості та реалізації положень наказу Міністра оборони України від 09.02.2017 № 88 "Про бюджетну політику Міністерства оборони України в 2017 році" рішення начальника Генерального штабу – Головнокомандувача Збройних Сил України від 18.04.2017 № 996/НВГШ

НАКАЗУЮ:

Documento que contiene el payload malicioso inicial

Los investigadores han indicado que Vermin también es capaz de instalar un keylogger si el malware no detecta un software antivirus en la máquina infectada.

El 6 de enero, el usuario de Twitter AnonXeljomudoX afirmaba haber realizado un ataque de denegación de servicio (DDoS) contra la web del Grupo Parlamentario Popular (gppopular.com) y la web de Instituciones Penitenciarias (institucionpenitenciaria.Es). Ambos ataques se realizaron como parte de la campaña hacktivista OpCatalunya.

El método empleado para impedir el tráfico legítimo a esas webs es todavía desconocido. La actividad de OpCatalunya ha fluctuado desde septiembre de 2017 en respuesta a la situación geopolítica en la región.

Finalmente, el 30 de enero, la facción de Anonymous conocida como AnonPlus anunció una nueva fase de OpCatalunya, la operación en apoyo de la independencia catalana.

Es probable que #OpCatalunyaNew sea una respuesta a la decisión del Tribunal Constitucional español de que el Carles Puigdemont no sería elegible para la reelección como líder del parlamento regional el pasado 27 de enero. Desde esa sentencia, el parlamento catalán ha anunciado que pospondrá la sesión de investidura, pero ha seguido afirmando que Puigdemont es el líder legítimo después de la victoria del bloque independentista en las elecciones del pasado diciembre.

Aunque inicialmente la campaña se centró en organizaciones conectadas al gobierno español, dada la orientación oportunista y la motivación publicitaria de Anonymous, es probable que los ataques continúen ampliándose para afectar a otros sectores.

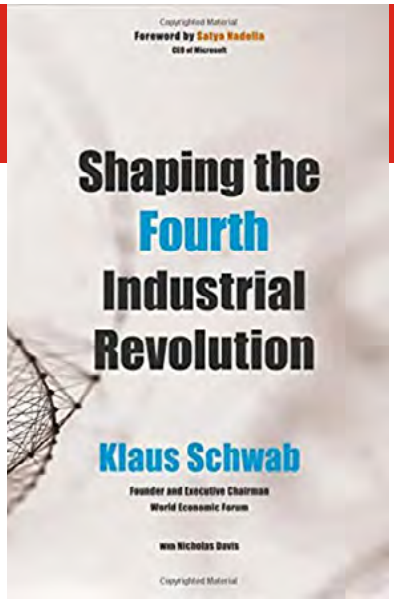
En los últimos días, diversos actores reclamaron la autoría de diversos ataques de DDoS contra una serie de objetivos, entre ellos; Alerta Digital del Ministerio de Defensa español, Casa Real, Diarioya, Corporación Alba y DineroCat. Es probable que los ataques adicionales se limiten a la denegación de servicio distribuida (DDoS) y ataques de defacement.

Los miembros del colectivo Anonymous siguen estando influenciados por eventos geopolítico. Además, y aunque la operación OpCatalunya anteriormente se limitaba en gran medida al gobierno español, desde entonces se ha ampliado para incluir entidades españolas que han ganado notoriedad en la operación. Como tal, es probable que las empresas españolas de diversos sectores, incluidos los medios de comunicación, el sector financiero, sector industrial, y las telecomunicaciones, sean blanco de ataques.

También es notable que varias cuentas anónimas afiliadas a OpCatalunya, incluyendo Anon909, CCALegion y Anoncatalonia, solo han estado activas desde octubre de 2017. Otras facciones anónimas como AnonPlus y NamaTikure, anteriormente estaban separadas del colectivo. Sin embargo, en la segunda mitad de 2017 volvieron a confluir, en lo que parece un retorno a los valores centrales de Anonymous. Es probable que dichos grupos estén utilizando OpCatalunya como un movimiento político dentro del colectivo para ganar notoriedad e influencia. Como tal, las tasas de ataques DDoS y de defacement probablemente serán más altas y más persistentes a medida que estas facciones intenten obtener publicidad.

7 Recomendaciones

7.1 Libros y películas



Libro:
SHAPING THE FOURTH INDUSTRIAL REVOLUTIONER

Autor: Klaus Schwab
Num. Páginas: 287
Editorial: World Economic Forum
Año: 2018
Precio: 13,50 Euros
Sinopsis: Para las empresas, la estrategia más importante es experimentar más, mientras simultáneamente se invierte en las personas. La Cuarta Revolución Industrial aún se encuentra en sus primeras etapas, y el potencial de las nuevas tecnologías está lejos de ser completamente comprendido. Sin embargo, podemos anticipar algunas de las dinámicas de la revolución, incluido el hecho de que cada vez más, la disrupción emana de la periferia de industrias y organizaciones. Solo al experimentar directamente con las tecnologías, las organizaciones pueden conocer su potencial. Dado que la mejor experimentación es la que realizan los profesionales del sector, esto también significa hacer esfuerzos concertados para mejorar el capital humano y adoptar una mentalidad empresarial. En este sentido, el autor defiende que todos deberíamos ser parte de la construcción de estas aspiraciones y visiones de futuro, que influyen en cómo se desarrollan y adoptan las tecnologías. A medida que cambiamos la manera en que hablamos, cambiamos la manera en que pensamos y creamos nuevas oportunidades para actuar.

Libro:
MACHINE, PLATFORM, CROWD

Autor: Andrew McAfee y Erik Brynjolfsson
Num. Páginas: 416
Editorial: W.W.Norton and Company
Año: 2017
Precio: 20,00 Euros
Sinopsis: Andrew McAfee y Erik Brynjolfsson conocen lo que se necesita para dominar el cambio de poder digital en que estamos inmersos: debemos repensar la integración de mentes y máquinas, de productos y plataformas y del núcleo y la multitud. A dia de hoy, el saldo favorece al segundo elemento de cada una de estas parejas, lo que tiene profundas y trascendentales implicaciones para nuestras vidas. Los autores ofrecen un análisis profundo de un mundo nuevo y un conjunto de herramientas para prosperar en él. No cabe duda de que Machine Platform crowd es una obra esencial para entender las implicaciones de la Industria 4.0

Libro:
LA SOCIEDAD QUE SEREMOS

Autor: Belén Barreiro
Num. Páginas: 288
Editorial: Planeta
Año: 2017
Precio: 18,50 Euros
Sinopsis: La sociedad sale de la recesión y entra en la revolución digital dividida en cuatro grandes grupos: digitales acomodados, digitales empobrecidos, analógicos salvados y analógicos hundidos. Pasó la crisis, pero casi nada es ni será igual. El futuro ha llegado ya. ¿Realmente van a vivir peor nuestros hijos? ¿Las nuevas formas de trabajar, comunicarse e informarse conducen, de verdad, a una sociedad menos grata? Estas y otras muchas preguntas encuentran respuesta en este interesantísimo libro que nos ayudará, a través de multitud de reflexiones, historias personales, anécdotas y estudios de campo, a prepararnos como sociedad para el futuro que viene, a prepararnos para la sociedad que seremos.

7.2 Webs recomendadas

https://www.politico.com/newsletters/morning-cybersecurity
Sitio web del daily briefing de POLITICO en materia de ciberseguridad.

https://www.intelligence.gov
Sitio web de la comunidad de inteligencia del gobierno de los Estados Unidos.

https://www.nato.int/cps/en/natohq/topics_78170.htm
Nuevo sitio web de OTAN dedicado a la ciberdefensa.

https://rootedcon.com/
Sitio web del Congreso de Seguridad Informatica ROOTEDCON.

https://www.acorn.gov.au/
Sitio web del Australian CyberCrime Online Reporting Network (ACORN)

http://www.export.gov.il/eng/Branches/Technologies/CyberSectorEng/CyberSectorEngAboutUs/
Sitio web del Israel Export Institute dedicado al ámbito ciber.

7.3 Cuentas de Twitter

@politico

@CDTIoficial

@CyberNews4you

@jlcyberwarfare

@inteldotgov

8 Eventos

FECHA	LUGAR	ORGANIZADOR	TÍTULO	URL
6 Febrero	Copenhague	Cylance	The Underworld Tour Copenhagen	https://pages.cylance.com/UWTCopenhagen2018.html?_ ga=2.162677436.1461805514.1516883492- 2138961369.1516883492/?utm_source=infosec-confereces-com&utm_medium=directory&utm_campaign=free-listing
8 febrero	Madrid	ISACA	JuevesISACA	http://www.redseguridad.com/eventos/agenda-del-sector/juevesisaca
8 febrero	Madrid	Computerworld	Ciberseguridad 2018	http://eventos.computerworld.es/ciberseguridad/ciberseguridad-2018
9 febrero	Tenerife	Hackron	Hackron 2018	https://hackron.com/
14- 15 febrero	Oslo	HackCon	HackCon	https://www.hackcon.org/english//?utm_source=infosec-conferences-com&utm_medium=directory&utm_campaign=free-listing
15 febrero	Marousi, Grecia	EITS	5th Information Security Conference	http://eits.boussiasconferences.gr//?utm_source=infosec-conferences-com&utm_medium=directory&utm_campaign=free-listing
20 febrero	Londres	TEISS	The European Information Security Summit	https://biztechevents.co.uk/teiss/?utm_source=infosec-conferences-com&utm_medium=directory&utm_campaign=free-listing
20 -23 febrero	Madrid	SICUR	SICUR Cyber	http://www.ifema.es/sicur_01/
20 febrero	Madrid	IDC	IDC Ciberseguridad 2018.	http://www.cvent.com/events/idc-ciberseguridad-2018/event-summary-9041da0d4d504826acf10bc5d500d16c.aspx
26 febrero- 1 Marzo	Barcelona	MWC	Mobile World Congress 2018	https://www.mobileworldcongress.com/
1- 3 Marzo	Madrid	Rooted	RootedCON Madrid 2018	https://www.rootedcon.com/

Patrocinadores

Consejo Asesor Empresarial

Empresas Colaboradoras

www.realinstitutoelcano.org

www.blog.rielcano.org

www.globalpresence.realinstitutoelcano.org

www.thiber.org

twitter.com/thiber_esp

www.linkedin.com/groups/7404269