Informe de Actividades, Ciberamenazas y Tendencias

2017

GENERALITAT VALENCIANA
Conselleria d'Hisenda i Model Econòmic

CSIRT-CV
Centre Seguretat TIC de la Comunitat Valenciana

Unió Europea
Fons Europeu de Desenvolupament Regional
Una manera de fer Europa

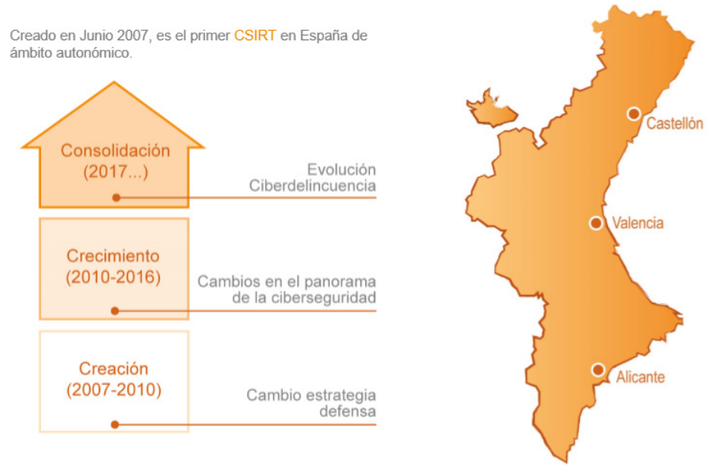
ÍNDICE

1	**CSIRT-CV**	**3**
2	**Servicios ofrecidos. Algunos datos**	**5**
2.1	Gestión de incidentes de seguridad	6
2.2	Activación del Gabinete de crisis. Wannacry	7
3	**Ciberamenazas y tendencias**	**9**
3.1	Campañas masivas de distribución de malware	10
3.2	Tendencias malware	11
4	**Plan Valenciano de Capacitación**	**12**
4.1	Cursos online y formación presencial	13
4.2	Portal principal. Material publicado	14
5	**Observatorio de ciberseguridad**	**15**
5.1	Shadow Brokers	16
5.2	Wikileaks	17
5.3	Internet de las Cosas	18
5.4	El correo electrónico como fuente de amenazas	18
5.5	Récord de filtraciones de datos	19
5.6	Auge de la criptomoneda	20
5.7	Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal	20
5.8	Aprobada la Estrategia de Seguridad Nacional 2017	21
5.9	Operación Cataluña	21
5.10	Evolución y prospectiva	22
6	**Relaciones y acuerdos institucionales**	**23**
7	**Cultura de ciberseguridad**	**25**

1 CSIRT-CV

CSIRT-CV es el Centro de Seguridad TIC de la Comunitat Valenciana.

Nace en junio del año 2007, como una apuesta de la Generalitat de la Comunitat Valenciana por la seguridad en la red.

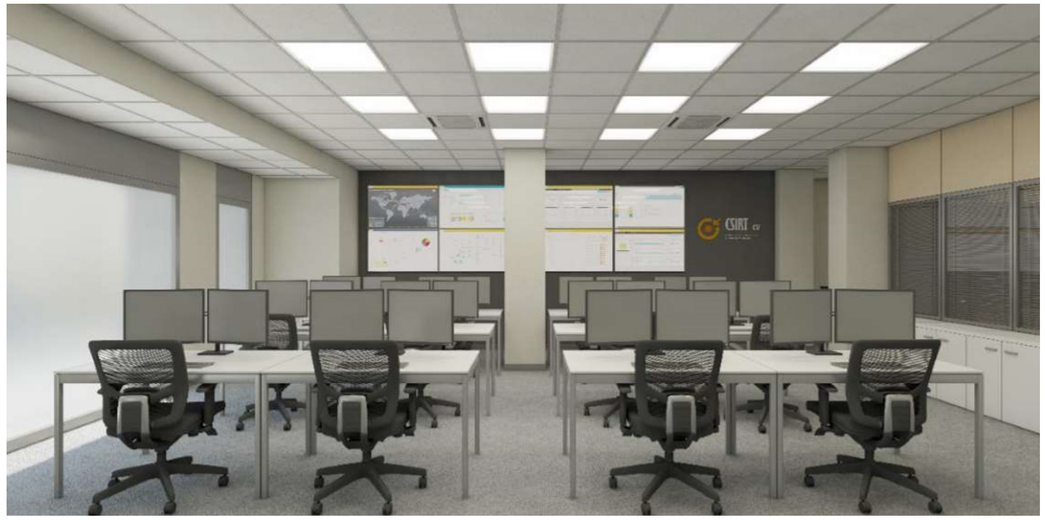


Se trata de una iniciativa pionera al ser el primer centro de estas características que se crea en España para un ámbito autonómico. Actualmente **CSIRT-CV** está adscrito a la Dirección General de Tecnologías de la Información y las Comunicaciones dentro de la Consellería de Hacienda y Modelo Económico.

CSIRT-CV ofrece servicios dentro de la Comunitat Valenciana (Alicante, Castellón y Valencia), con vocación de servicio público y sin ánimo de lucro, por lo que sus servicios se ofrecen gratuitamente.

Los colectivos destinatarios de estos servicios son:

- Los ciudadanos de la Comunidad Valenciana.
- Los profesionales y empresas privadas, especialmente las de menor tamaño.
- La Administración Pública, tanto local como autonómica. Principalmente esta última por la ubicación del centro.



Sala de operaciones de CSIRT-CV

El principal objetivo de **CSIRT-CV** es contribuir a la mejora de la seguridad de los sistemas de información dentro de su ámbito, así como promover una cultura de seguridad y buenas prácticas en el uso de las nuevas tecnologías de forma que se minimicen los incidentes de seguridad y permita afrontar de forma activa las nuevas amenazas que pudieran surgir.

2 Servicios ofrecidos: algunos datos

CSIRT-CV dispone de un amplio abanico de servicios ofrecidos en su ámbito que abarcan la amplitud todos los posibles escenarios dados dentro del ecosistema de la ciberseguridad.

Prevención	Detección	Respuesta
Auditorías de seguridad	Sistemas de decepción	Gestión de incidentes de seguridad
Test de intrusión	Securización de entornos	Grupo de intervención rápida
Informes y alertas. Observatorio de seguridad	Auditoría de seguridad semántica	Gabinete de crisis
Consultoría técnica y legal	Informe forense pericial	
Plan Valenciano de Capacitación	Detección de intrusos	
Intercambio de información	Detección de APT	
Cuadro de mando de seguridad	Test de intrusión	
I+D+i		
Laboratorio de malware		
Monitorización de servicios Web		
Normalización		
Auditoría ENS		
Validación de código		
Consultoría sobre las ISO 27001:2013		
Análisis de riesgos		
Auditoría LOPD		
Ciberseguridad industrial		
Planes de mejora de la seguridad		

Entre los servicios ofertados, los cuales son ofrecidos bien de manera proactiva o bien bajo petición, podemos destacar que en 2017 se han obtenido los siguientes datos:

Servicios ofrecidos	Total 2017
Test de intrusión	50
Auditorías de seguridad	95
Auditorías LOPD	4
Consultoría técnica, organizativa y legal	76
Emisión notas de alerta temprana	42

Entre las consultas que **CSIRT-CV** ha atendido predominan las relacionadas con el intento de fraude a través de correo electrónico tras la recepción de correos maliciosos, consultas sobre ataques de ingeniería social a través del telefóno, o sobre cuestiones legales, entre otros.

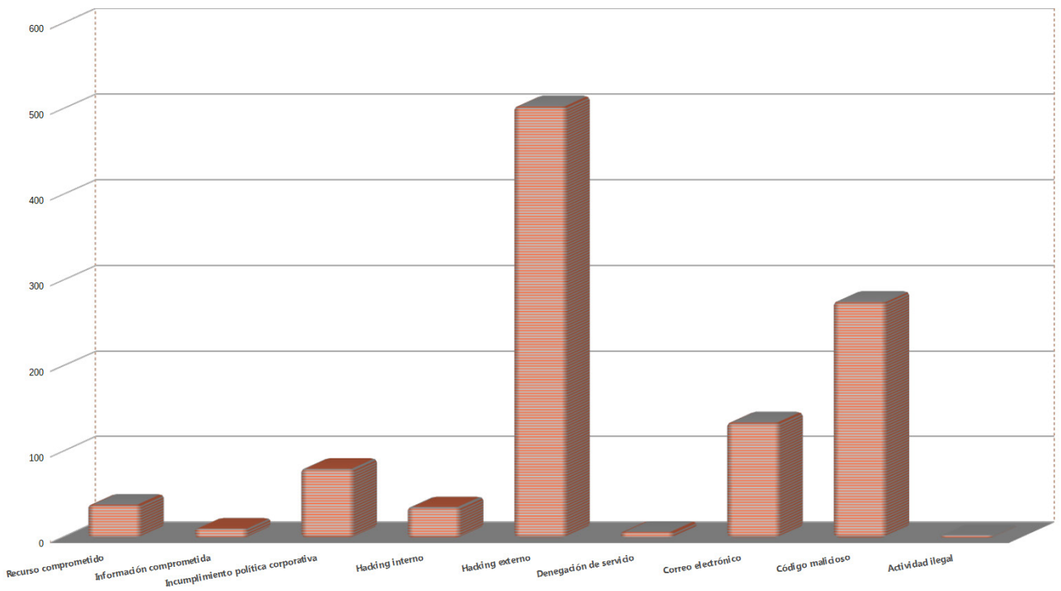
Por otro lado comentar que para la emisión de las 42 alertas tempranas emitidas se han analizado cerca de 1313 vulnerabilidades/alertas de ciberseguridad de diferentes fabricantes en nuestro ámbito, y que 30 de esas alertas han sido de caracter privado.

2.1 Gestión de incidentes de seguridad

La actividad principal de **CSIRT-CV** se centra, como todo **CSIRT**, en la **gestión de incidentes de seguridad. CSIRT-CV** proporciona una solución integral a cualquier incidente de seguridad de la información que se pueda producir, incluyendo entre ellos incidentes tales como: intento de fraude electrónico, phishing, malware en el equipo, detección de comportamiento sospechoso en el equipo o cuentas digitales, robo de información, etc.

Durante 2017 el equipo de analistas del centro han gestionado un total de 1223 incidentes de seguridad de los que 11 han sido de caracter crítico.

Como se observa en el gráfico a continuación, según la tipología de los incidentes de seguridad gestionados, los que más volumen han generado han sido los de tipo “Código Malicioso” y los de “Hacking externo”, entendiéndose éstos por todos aquellos intentos de intrusión en los sistemas. En vista también del volumen de incidentes gestionados por intentos de propagación de malware o fraude a través del correo electrónico, se pone de manifiesto que esta vía de entrada por parte de los atacantes está en auge.



2.2 Activación del Gabinete de crisis. Wannacry

CSIRT-CV ofrece en su ámbito un **Grupo de Intervención Rápida (GIR)** ante incidentes de seguridad especialmente relevantes, prestando apoyo técnico y organizativo para ante cualquier problema, recuperar los servicios en el menor tiempo posible. En este servicio también se contempla la gestión de crisis. Una crisis es un tipo especial de incidente que requiere, además del proceso de gestión de incidentes, la reunión de un comité de crisis para la toma rápida y efectiva de decisiones que permitan superar dicha crisis.

A lo largo de este año cabe destacar la activación del Gabinete de Crisis con motivo de *Wannacry*[1], una nueva amenaza que el pasado 12 de mayo puso en jaque la seguridad de varias empresas grandes y organismos (hasta 16 hospitales británicos) a nivel internacional y particularmente con un alto impacto en España. Muchos de los afectados fueron obligados a desactivar sus sistemas informáticos.

(1) Comunicado sobre malware Wannacry/Wannacrypt: https://www.csirtcv.gva.es/es/noticias/comunicado-sobre-malware-wannacrywannacrypt.html

Antel la magnitud de la situación, CSIRT-CV hizo un análisis de esta nueva amenaza para valorar su impacto en nuestro ámbito y propuso una serie de medidas de protección que lo mitigara en caso de que dicha amenaza impactara contra los sistemas corporativos. Puesto que el impacto de un ciberataque de esta magnitud en nuestros sistemas hubiera sido crítico, y podría haber afectado a la disponibilidad de los sistemas, se activó el Gabinete de crisis que CSIRT-CV lideró.

Deloitte por su parte, en un reciente informe que publicó el pasado julio muestra cifras mas escalofriantes y habla de hasta 15 millones de equipos infectados y reinfectados. Según varios estudios WannaCry *habría ocasionado cerca de 200 millones de pérdidas directas en todo el mundo.*[2]

Tan solo un mes después volvimos a estar en alerta -con un nivel mas inferior- por la amenaza de *Petya.A*[3], y en octubre llevamos a cabo un seguimiento intensivo de la campaña de distribución del malware *Bad Rabbit.*[4]

(2) Tras la sangría de 200 M de Wannacry, esta es la factura que nos dejará Petya
https://www.elconfidencial.com/tecnologia/2017-07-18/wannacry-petya-notpetya-deloitte-bra_1408510/

(3) Comunicado sobre el nuevo virus similar a Wannacry: Petya
https://www.csirtcv.gva.es/es/noticias/petya-el-nuevo-virus-similar-wannacry.html

(4) Comunicado sobre el nuevo ransomware: Bad Rabbit
https://www.csirtcv.gva.es/es/noticias/nuevo-ransomware-bad-rabbit.html

3 Ciberamenazas y tendencias

Durante todo 2017 se ha detectado una tendencia acusada de intentar explotar una vulnerabilidad crítica hacia ciertos servicios Web, concretamente los que utilizan la tecnología **Apache Struts**, que fue publicada junto con un exploit en marzo.

Sobre todo durante el segundo semestre de 2017, el tipo de ataque que mas nos hemos encontrado ha sido el de aprovechar vulnerabilidades de tipo **"Java Serialized"** para comprometer servidores inyectando malware de tipo **Minador**, que está en auge gracias a la subida del valor de las criptomonedas en este año, y también malware de tipo backdoor con capacidad de llevar a cabo ataques de Denegación de Servicio.

Otra tendencia que continua en alza y que llevamos detectando desde 2014, es el intento de explotación de diversas vulnerabilidades en el **protocolo SSL.** Aunque se trata de vulnerabilidades que deberían estar solucionadas, los atacantes aún continúan intentando aprovecharse de ellas.

En nuestro ámbito de actuación no nos vimos afectados por la nueva amenaza **Wannacry**, pero no podemos dejar de mencionar la situación de alerta vivida por este ransomware con capacidad de gusano que provocó el pánico en medio mundo.

En marzo de este año fueron publicadas diversas vulnerabilidades en el protocolo del servicio *Samba*[5], utilizado por Wannacry para extenderse, y como era de esperar los ataques hacia este protocolo han aumentado considerablemente como queda registrado en los datos de nuestra HoneyNet de investigación.

En líneas generales seguimos detectando numerosos escaneos e intentos por fuerza bruta de acceder a servicios como SSH y FTP así como ataques continuados de **iSQL** para extraer información de bases de datos internas o de Remote File Inclusion para comprometer servidores abriendo puertas traseras en ellos por ejemplo.

Remarcable también mencionar un incremento de intentos de ataque contra el gestor de contenidos **Wordpress**, sobre todo en el intento de explotar plugins, y contra **Drupal** intentado explotar vulnerabilidades de tipo iSQL.

(5) Vulnerabilidades en el protocolo del servicio Samba
www.samba.org/samba/history/security.html

CSIRT-CV también dispone de un **laboratorio de malware** donde los analistas pueden analizar artefactos para medir de un modo preciso el impacto y consecuencias reales de posibles códigos maliciosos activos en nuestro ámbito, y de este modo diseñar las medidas de contención y erradicación más adecuadas en cada caso.

Durante 2017 mas de un 25% de los incidentes de seguridad gestionados estaban relacionados con código dañino.

Se ha detectado un aumento del uso de **Exploit Kits** en la propagación de malware, esto hace que los navegadores y sus complementos se conviertan en uno de los principales objetivos a batir por parte de los atacantes.

Por otro lado cabe comentar que tras la nueva proliferación de publicaciones de vulnerabilidades muy recientes prácticamente para todas las versiones de Windows, y la tendencia en alza que están haciendo los ciberdelincuentes de cara a utilizarlas para la propagación masiva de malware de tipo ransomware -como es el caso de Wannacry-, de tipo **minador** de bitcoins como es Adylkuzz, o cualquier otro tipo de RAT, cabe la necesidad de proteger al máximo los puestos de trabajo con medidas más rigurosas de aplicación de las actualizaciones de seguridad, instalación y verificación de antivirus actualizado y concienciación del usuario.

En cuanto a los sectores mas expuestos según nuestros datos, el **sector Sanitatorio** es el que más está en el punto de mira de los atacantes.

3.1 Campañas masivas de distribución de malware

Durante este año se han detectado intentos de distribución masiva de malware a través de correo electrónicos con especial virulencia en el mes de *marzo*[6] en el que CSIRT-CV detectó en su ámbito cerca de 15.000 correos que intentaban distribuir un determinado tipo de ransomware.

(6) CSIRT-CV se enfrenta a tres campañas de ransomware el pasado mes de marzo
http://www.csirtcv.gva.es/es/noticias/csirt-cv-se-enfrenta-tres-campañas-de-ransomware-el-pasado-marzo.html

A estas campañas hay que sumarle la ya habitual campaña de phishing que utiliza como gancho el inicio de la campaña de la declaración de la renta, que tuvo lugar en *abril.*[7]

Tal y como se ha mencionado anteriormente, el malware de tipo minador está en auge y cada vez, de forma mas extendida, se detectan nuevos métodos de propagación bien sea a través de software instalado en los equipos, como cualquier otra aplicación legítima o bien a través de scripts instalados en páginas Web.

3.2 Tendencias malware

Según nuestros datos entre los *Exploit Kits*[8] más activos hemos observado Neutrino, BleedingLife, RIG y Astrum.

Algunos ciberdelincuentes utilizan los *Traffic Director System (TDS)*[9]para un uso fraudulento y facilitar así la distribución de malware a través de Internet. En este sentido, hemos detectado gran actividad de TDS Sutra y TDS Keitaro.

Según los informes públicos de tendencias mensuales del laboratorio de S2 Grupo las amenazas más en auge durante este año han sido las siguientes:

• Phishings a través del correo electrónico usando adjuntos maliciosos HTML o PDF entre otros. En el caso de HTML se utiliza una redirección fraudulenta a sitios clonados falsos que ejecutan el robo de credenciales (Google Drive, Dropbox, etc)

• Ransomware: Spora, Cerber, Locky, CryptoMix, Torrentlocker, Revenge, Matrix, Wannacry, NotPetya,

• Malware para Android: bancario, WireX

• Bankers: GootKit, Zeus, Zbot/Zloader, Trickbot, Diamond Fox/Gorynych, IcedID, Dridex

• Exploit Kits: RIG, Sundown, Nebula, Terror, ElTest, Disdain, Magnitude, Neptune

• RATs: Remcos, Godzilla, Bunitu, Ramnit, Chthonic, Emotet

• Malware IoT: Hajime, Mirai

• Malware de tipo minador

• Otros: Dreambot, SmokeLoader, LatentBot, Kovter, Necurs

(7) Phishing con motivo del inicio de la campaña de la renta 2016
http://www.csirtcv.gva.es/es/noticias/nueva-campaña-de-phising-con-motivo-del-inicio-de-la-campaña-de-la-renta-2016.html

(8) Los EK son herramientas que contienen códigos ejecutables o datos que se aprovechan de las vulnerabilidades del software instalando en un equipo. La finalidad de los mismos es abrir una vía de infección hacia el equipo víctima.

(9) Qué es un TDS (Traffic Director System)
https://www.securityartwork.es/2017/03/31/tds-traffic-director-system/

4 Plan Valenciano de Capacitación

Conseguir una gestión eficaz de la ciberseguridad no depende sólo de la implantación d e medidas técnicas o de la definición de procedimientos: es fundamental la implicación de las personas. Esta circunstancia queda claramente reflejada en la Agenda Digital de la Comunidad Valenciana, estableciéndose líneas de trabajo destinadas a mejorar la cultura en ciberseguridad de ciudadanos y empresas. De la misma forma lo incluyen la estrategia nacional y europea en ciberseguridad.

Por ello, y porque la divulgación y concienciación es algo consustancial a la manera de entender la ciberseguridad en **CSIRT-CV,** el centro ha puesto en marcha el servicio de Plan Valenciano de Capacitación que sitúa a las personas en uno de sus principales ejes de actuación.

Este servicio tiene como uno de sus objetivos principales incrementar la cultura en ciberseguridad de la Comunidad Valenciana, aumentando el nivel global de la seguridad y disminuyendo por tanto el riesgo de incidentes relacionados directamente con uno de los componentes clave en esta materia: las personas.

Para abordar el Plan Valenciano de Capacitación de la mejor forma posible, se ha definido un calendario donde se contemplan acciones concretas dirigidas a los colectivos identificados: Ciudadanos, Generalitat, PYMEs y otras Administraciones Públicas. Entre estas acciones podemos destacar Jornadas Familiares de Seguridad, conferencias, guías, estudios.

Este año desde **CSIRT-CV** se han llevado a cabo dos campañas de concienciación difundidas íntegramente en nuestras redes sociales. La primera, centrada en llevar a los ciudadanos los conceptos básicos de la LOPD. “LOPD para ciudadanos” (hashtag: #ciudadanosLOPD). En septiembre, y aprovechando el inicio del curso escolar, se llevó a cabo la publicación de la segunda campaña de concienciación, con el título “Inicio el curso seguro” (hashtag: #InicioElCursoSeguro). Estuvo enfocada al uso seguro que deberían hacer los menores y jóvenes con las tecnologías.

4.1 Cursos online y formación presencial

El Centro sigue potenciando su oferta formativa para ciudadanos con cursos y microcursos online que se imparten a través de la plataforma *SAPs?*[10] y de los que periódicamente se van abriendo nuevas ediciones para poder incrementar el número de alumnos formados. El material está elaborado íntegramente por el equipo de analistas del Centro.

Los cursos online son de más larga duración ya que profundizan en la materia un poco más que los microcursos, éstos últimos más orientados a dar una visión mas genérica del tema:

Cursos online ofertados por CSIRT-CV
Uso seguro en iOS
Uso seguro en Android
Curso LOPD
Introducción a la G.S.I
Herramienta Nmap

Entre dichos servicios, los cuales son ofrecidos, bien de manera proactiva o bien bajo petición, podemos destacar algunos datos que en el primer semestre de 2017 se han obtenido:

MicroCursos online ofertados por CSIRT-CV
Seguridad informática
Introducción al malware
Seguridad en redes sociales
Seguridad en redes inalámbricas
Seguridad en Internet para menores
Seguridad en redes P2P
Navegación segura
Seguridad en dispositivos portátiles
Seguridad en juegos online
Seguridad en el correo electrónico
Seguridad en móviles, PDAs y smartphones
Delitos tecnológicos
Compras online seguras

(10) *Plataforma SAPS http://www.saps.gva.es/*

En cuanto a formación presencial, desde **CSIRT-CV** se han realizado diferentes cursos de carácter interno para personal especializado dentro de nuestro ámbito. Por un lado, se ha impartido cursos relacionados con ciberespionaje y toolset de herramientas más usadas por algunos actores, por otro lado cursos de carácter técnico relacionados con el análisis de malware. De igual forma, se han organizado diferentes charlas divulgativas destinadas a concienciación para familias, y en determinados colectivos desprotegidos.

Nuestros análistas tampoco han dejado de formarse, y han recibido formación especializada sobre diferentes productos, técnicas de análisis de Big Data, Blockchain o Esquema Nacional de Seguridad, entre otros.

4.2 Portal principal. Material publicado

El portal www.csirtcv.gva.es donde se publican diariamente noticias de seguridad y se alerta sobre las vulnerabilidades más imporatntes, es la imagen principal del centro de cara al exterior. Este año el portal ha recibido cerca de 300.000 visitas y se han publicado mas de 350 publicaciones.

CSIRT-CV también pone a disposición una serie de guías/informes y otro tipo de material sobre ciberseguridad en su portal principal. En 2017 este contenido ha tenido casi 95.000 descargas.

Como novedad de este año, el centro ha publicado un estudio sobre algunas de las herramientas open source más utilizadas en mensajería instantánea, de cara a valorar sobre todo su usabilidad y seguridad y un informe sobre un breve análisis técnico del código dañino de tipo gusano denominado Forbix.

En la sección de Informes de nuestro portal pueden encontrar todo el material *disponible para su descarga.*[11]

(11) Enlace de desacarga del informe
https://www.csirtcv.gva.es/es/paginas/descargas-informes-csirt-cv.html

5 Observatorio de ciberseguridad

En el ecosistema de la tecnología en el que nos encontramos actualmente se están viviendo actualmente ciertas circunstancias que aumentan exponencialmente el riesgo al que las corporaciones se exponen.

Estas circunstancias vienen marcadas principalmente por una serie de elementos que han crispado el entorno de la ciberseguridad a nivel global en los últimos seis meses; por un lado, el grupo *Shadow Brokers*,[12] por otro las filtraciones *"Vault7"*[13] de Wikileaks. Ambos grupos han liberado información que ha sido o podría ser aprovechada por los delincuentes para perpetrar ataques de gran impacto, entre esa información destacan vulnerabilidades y exploits que afectan a la mayor parte de la tecnología usada en la mayoría de organizaciones y empresas.

Una de las vulnerabilidades reportadas en esta línea data del mes de Marzo y , corresponde a una actualización de software de Microsoft, que solucionaba dicha vulnerabilidad -de caracter crítico- en el protocolo Samba, concretamente la actualización MS17-010. Esta vulnerabilidad tuvo repercusión en el mes de mayo, ya que fue utilizada para propagar un nuevo malware, Wannacry que provocó un gran impacto en muchas empresas y organismos a nivel internacional.

NAME	TYPE	TARGET	NOTES	SERVICE	AUTH	VERSIONS	NT	XP	VISTA	7	8	10	2000	2003	2008	2012
EARLYSHOVEL	EXPLOIT	REDHAT 7.0/7.1	SENDMAIL			8.11.x										
EASYBEE	EXPLOIT	MDAEMON	WEBADMIN	HTTP/HTTPS		9.5.2-10.1.2 (except 10.0.0)										
EASYPI	EXPLOIT	LOTUS MAIL	LOTUS MAIL	(TCP) 3264			y	y					y	y		
EBBISLAND/EBBSHAVE	EXPLOIT	SOLARIS 6-10	RPC XDR			6-10										
ECHOWRECKER	EXPLOIT	LINUX	SAMBA 3.0.x			3.0.x										
ECLIPSEDWING	EXPLOIT	SERVER SERVICE	MS08-067	(TCP 445) SMB/ (TCP 139) NBT			y	y					y	y		
EDUCATEDSCHOLAR	EXPLOIT	SMB	MS09-050	(TCP 445) SMB					y						y	
EMERALDTHREAD	EXPLOIT	SMB	MS10-061	(TCP 445) SMB/ (TCP 139) NBT	y?			y						y		
EMPHASISMINE	EXPLOIT	LOTUS DOMINO		(TCP 143) IMAP	y	6.5.4-6.5.5FP1, 7.0-8.5.2										
ENGLISHMANSDENTIST	EXPLOIT	OUTLOOK EXCHANGE WEBACCESS		(TCP 25) SMTP		< exchange 2010?										
EPICHERO	EXPLOIT	AVAYA CALL SERVER														
ERRATICGOPHER	EXPLOIT	SMBv1		(TCP 445) SMB				y						y		
ESKIMOROLL	EXPLOIT	KERBEROS SERVICE	MS14-068	(TCP 88) KERBEROS	y								y	y	y	
ESTEEMAUDIT	EXPLOIT	RDP		(TCP 3389) RDP				y						y		
ETERNALBLUE	EXPLOIT	SMBv2/NBT	MS17-010	(TCP 445) SMB				y	y	y	y	y	y	y	y	y
ETERNALCHAMPION	EXPLOIT	SMBv1/SMBv2?	MS17-010	(TCP 445) SMB												
ETERNALROMANCE	EXPLOIT	SMBv1	MS17-010	(TCP 445) SMB				y	y	y	y?	y?	y?	y	y	y?
ETERNALSYNERGY	EXPLOIT	SMBv3	MS17-010	(TCP 445) SMB							y					y
ETRE	EXPLOIT	IMAIL				8.10-8.22										
EWOKFRENZY	EXPLOIT	LOTUS DOMINO		(TCP 143) IMAP		6.5.4, 7.0.2										
EXPLODINGCAN	EXPLOIT	IIS5.0?/6.0 (WEBDAV)		(TCP 80) HTTP/HTTPS		5.0?,6.0								y		
FUZZBUNCH	TOOL		FRAMEWORK (PYTHON)													
ODDJOB	TOOL		IMPLANT BUILDER													
ZIPPYBEER	EXPLOIT	SMB	DCs	(TCP 445) SMB	y											

Detalle vulnerabilidades publicadas por Shadow Brokers

Segun nuestras investigaciones, otro hecho que marca desfavorablemente el entorno de la ciberseguridad actual es la falta de concienciación sobre un uso adecuado tanto de dispositivos extraíbles como de **dispositivos móviles**. La creciente tendencia BYOD, pocas restricciones de seguridad en cuanto al uso de dispositivos no corporativos y el aumento de malware dirigido a dispositivos móviles conforma un entorno apropiado para aumentar el número de incidentes de seguridad ligados con este tipo de dispositivos.

Otra circunstancia externa que está afectando al ámbito de la ciberseguridad en general es el auge del precio de las **criptomonedas**. Este hecho provoca que el minado de criptomonedas sea un nuevo nicho que explotar por parte de los ciberdelincuentes y se están detectando un gran número de ataques en ese sentido.

Existen además otros factores que desde nuestro observatorio de seguridad hemos querido tener en cuenta de cara a fortalecer nuestra vigilancia, serán comentados a continuación.

5.1 Shadow Brokers

En agosto de 2016 un grupo autodenominado Shadow Brokers publicó parte de archivos que decían haber extraído de la NSA. Dichos archivos contenían información sobre supuestas herramientas de espionaje utilizadas por la agencia gubernamental norteamericana, incluyendo exploits de 0-day e información sobre vulnerabilidades de diferentes dispositivos tecnológicos y sistemas operativos.

Tras intentar vender esta información, liberaron parte de ella al público, en la que se incluía una serie de herramientas utilizadas para comprometer Windows. Estas herramientas traían varías vulnerabilidades de 0-día que comprometerían prácticamente todas las versiones de Windows, a destacar una vulnerabilidad crítica en la implementación del protocolo de red SMB realizada por Microsoft, vulnerabilidad que el fabricante solucionó un mes despues con el parche MS17-010 y que fue aprovechada para propagar el conocido Wannacry.

El alcance y la maginitud de los exploits publicados y los millones de máquinas vulnerables existentes actualmente provocaron que el nivel de riesgo global aumentara considerablemente.

Este grupo ya amenazó de nuevo con publicar más exploits *en los próximos meses*[12] y aseguran que cuentan información sobre vulnerabilidades relacionadas con navegadores Web, routers, smartphones, sistemas operativos y sistemas informáticos relativos a entidades bancarias.

Con todo ello, hay que tener en cuenta que podrían darse nuevos ataques de mayores dimensiones que WannaCry, afectando quizá a móviles, routers y otros dispositivos.

(12) Shadow Brokers anuncia una suscripción mensual de exploits
http://www.csirtcv.gva.es/es/noticias/shadow-brokers-anuncia-una-suscripción-mensual-de-exploits.html

5.2 Wikileaks

Durante este semestre Wikileaks también ha estado difundiendo información sobre el programa de hacking de otra agencia gubernarmental norteamericana, en este caso de la CIA. Se ha tratado de una de las mayores filtraciones de información de la historia de la CIA, extraída de un centro de ciberinteligencia de Langley.

Detalle Wikileaks filtración Vault 7 (Herramientas CIA)

Dicha información incluye datos sobre la mayor parte de su arsenal de hacking incluyendo malware, herramientas para ciberespionaje o vulnerabilidades desconocidas en una gran variedad de dispositivos y tecnologías. En dicha documentación pueden encontrarse millones de instrucciones destinadas a convertir casi cualquier dispositivo TI en una herramienta de espionaje bajo su control, incluyendo smartphones/PC (parecen ser capaces de comprometer cualquier tipo de sistema operativo) , smart TV o incluso coches.

En la actualidad Wikileaks periódicamente continua liberando *esta información.*[13]

(13) Wikileaks publica documentos internos del programa de hacking de la CIA
http://www.csirtcv.gva.es/es/noticias/wikileaks-publica-documentos-internos-del-programa-de-hacking-de-la-cia.html

5.3 Internet de las Cosas

El IoT sigue siendo un objeto vulnerable y es utilizado para lanzar ataques contra todo Internet. Durante este semestre hemos visto la proliferación de botnets orientadas a ainfectar estet ipo de dispositivos – sobre todo cámaras de videovigilancia- como la botnet *Pershing*[14] o la mediática *Mirai*.[15] La finalidad de estas botnet ha sido la de llevar a cabo mayormente ataques de Denegación de Servicio.

5.4 El correo electrónico como fuente de amenazas

Si bien es un factor importante en nuestro ámbito como via de entrada de amenazas, desde fuentes externas coinciden con nuestras investigaciones y nos alertan de que el correo electrónico es una de las principales puertas para los delincuentes.

Según el informe anual de *Symantec* [16] publicado en abril, 1 de cada 131 emails contiene un enlace o adjunto malicioso. España – según el informe – se situaría en el 22º puesto del ranking mundial de países objetivo de ciberamenazas, la mayoría relacionadas con el malware o el phishing. La construcción, el comercio mayorista, la banca y los seguros son los sectores a los que más se dirigen los ataques de malware, mientras que los ataques de phishing se dirigen más al sector financiero.

Un dato interesante del informe de Symantec es el aumento del uso de PowerShell, un lenguaje de programación común instalado en los PC con Windows y los ficheros de Microsoft Office como arma para los ciberdelincuentes, sobre todo par ala elaboración de adjuntos maliciosos que se usan en correos phishing. Esta información es reforzada por Kaspersky Lab, los cuales publicaron en febrero que habían descubierto una serie de ataques “invisibles” dirigidos que utilizaban que el código Meterpreter se había combinado con un número de scripts PowerShell y con otras utilidades y se había transformado en código malicioso que podía ocultarse en la memoria y , de forma invisible, recopilar las contraseñas de los administradores de sistemas. De esta manera, los atacantes podían controlar los sistemas de sus víctimas en remoto y conseguir su objetivo final: el acceso a los procesos financieros.

El uso del código de explotación de fuente abierta, funcionalidades Windows habituales y dominios desconocidos, hace casi imposible determinar el grupo responsable o si son varios los que comparten las mismas herramientas.

También es interesante que, de acuerdo con el informe, los CIO han perdido la capacidad de dar seguimiento al número de aplicaciones cloud que se usan en su corporación, la mayoría asume que sus organizaciones se utilizan muchas menos de las que en realidad son utilizadas.

(14) *100000 cámaras de vigilancia lanzando ciberataques*
http://www.csirtcv.gva.es/es/noticias/100000-cámaras-de-vigilancia-lanzando-cyberataques.html

(15) *El troyano Mirai regresa*
http://www.csirtcv.gva.es/es/noticias/el-troyano-mirai-regresa.html

(16) *El correo electrónico como fuente de amenazas*
http://www.csirtcv.gva.es/es/noticias/el-correo-electrónico-fuente-de-amenazas.html

5.5 Récord de filtraciones de datos

Según el informe realizado por IBM security titulado “IBM X-Force Threat Intelligence Index 2017”[17] sobre los datos recogidos durante 2016, se ha producido un incremento alarmante del número de “datos” comprometidos respecto al año anterior. Ampliándose los ataques al robo de documentos de correos electrónicos, documentos empresariales y espionaje industrial. Los datos han sido extraídos por IBM security a través de los sensores que monitorizan la seguridad de sus clientes, así como de sensores de spam y honeypots desplegados en diferentes ubicaciones.

Los datos recogidos indican más de ocho millones de ataques de spam y phishing diarios, datos que refuerzan que el correo electrónico es una vía de infección masivamente utilizada por los delincuentes.

(17) *IBM X-Force Threat Intelligence Index 2017*
https://www-01.ibm.com/marketing/iwm/dre/signup?source=urx-13655&S_PKG=ov57325

5.6 Auge de la criptomoneda

Es evidente que las criptomonedas están de moda. El incremento del precio de, por ejemplo, el Bitcoin con respecto al año pasado es exponencial, tal y como se aprecia en la siguiente gráfica de Coinbase:

En general, todo el mundo, incluidos los ciberdelincuentes, quieren sacar tajada de esta tendencia y los ataques en relación a la distribución de malware de tipo minador se han incrementado de manera exponencial.

No solo **CSIRT-CV** ha detectado un aumento de estos ciberataques sino que a nivel global está siendo una tendencia en auge y de actualidad debido a las numerosas técnicas que están usando los atacantes para distribuir este tipo de malware. Se pronostica que seguirá en auge esta tendencia.

5.7 Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal

El Consejo de Ministros, a propuesta del ministro de Justicia, Rafael Catalá, aprobó *el pasado 10 de noviembre* [18] el Proyecto de Ley Orgánica de Protección de Datos que adaptará nuestra legislación a las disposiciones del Reglamento UE 2016/679, introduciendo novedades y mejoras en la regulación de este derecho fundamental en nuestro país.

Este Reglamento Europeo que se aplicará a partir del próximo 25 de mayo de 2018, recoge como uno de sus principales objetivos acabar con la fragmentación existente en las distintas normativas de los países comunitarios. Además, persigue la adaptación de las normas de protección de datos a la rápida evolución tecnológica y los fenómenos derivados del desarrollo de la sociedad de la información y la globalización.

(18) *Propuesta del proyecto de Ley Organica de Protección de Datos*
http://www.lamoncloa.gob.es/consejodeministros/Paginas/enlaces/101117enlacedatos.aspx

En el caso de España, donde la protección de datos es un derecho fundamental protegido por el artículo 18.4 de la Constitución, se recogen novedades tanto en el régimen de consentimiento como en los tratamientos y en la introducción de nuevas figuras y procedimientos.

5.8 Aprobada la Estrategia de Seguridad Nacional 2017

El Consejo de Ministros aprobó el viernes, 1 de diciembre, *la nueva Estrategia de Seguridad Nacional 2017*,[19] que previamente había recibido el visto bueno en la reunión del Consejo de Seguridad Nacional, presidida por el presidente del Gobierno.

La Estrategia 2017 revisa su predecesora de 2013 y subraya, entre las amenazas y los desafíos identificados, el terrorismo internacional, las amenazas a las infraestructuras críticas y las amenazas y desafíos en los espacios comunes globales: ciberespacio, espacio marítimo y espacio aéreo y ultraterrestre. Pone énfasis, además, en la naturaleza híbrida de los conflictos actuales, entendida como la combinación de acciones que pueden incluir, junto al uso de métodos militares tradicionales, ciberataques, operaciones de manipulación de la información o elementos de presión económica.

El Gobierno de España situá las ciberamenazas como una de sus principales amenazas como se evidencia en dicha Estrategia de Seguridad Nacional. Una muestra de la importancia de esta amenaza ha sido el anuncio de la vicepresidenta del Gobierno durante las jornadas organizadas por el **CCN-CERT** el pasado diciembre de que en 2018 está prevista la creación de un **Centro de Operaciones de Seguridad de la Administración General del Estado** que permita ofrecer una respuesta “más eficaz” ante las ciberamenazas.

5.9 Operación Cataluña

Durante los últimos meses del año a raíz del referendum que puso en marcha el Gobierno catalán sobre la independencia de Cataluña, la siguiente aplicación del artículo 155 por parte del Gobierno Central y las elecciones autonómicas catalanas a posteri, se ha vivido un ambiente de hacktivismo y protesta en el que numerosas entidades públicas y privadas del ámbito nacional han sido objeto de ataques.

(19) *Nueva Estrategia de Seguridad Nacional 2017*
http://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/presidenciadelgobierno/Documents/2017-1824_Estrategia_de_Seguridad_Nacional_ESN_doble_pag.pdf

5.10 Evolución y prospectiva

A tenor de los últimos acontecimientos acaecidos por la liberación de vulnerabilidades y exploits de día 0 de carácter crítico por parte de ciertos grupos, cabe esperar que en los próximos meses se continúen no solo liberando más vulnerabilidades de este tipo, como ya han amenazado, sino que se desarrolle malware u otro tipo de herramientas que aprovechen este tipo de vulnerabilidades y exploits publicados, mas sofisticados y más discretos, que pudieran expandirse en el ciberespacio. Conviene monitorizar cada publicación de estos grupos de interés y valorar el impacto de cada una de ellas sin menospreciar su credibilidad, puesto que ya han demostrado la veracidad de la información que manejan. De igual forma, es conveniente evaluar las vulnerabilidades y parches de seguridad que los distintos fabricantes van publicando y que pudieran ser susceptibles de ser explotadas para propagar malware o llevar a cabo intrusiones, principalmente las que afectan a SO Windows y a navegadores Web.

El pasado enero tuvo lugar en Valencia el *50th TF-CSIRT meeting and FIRST Regional Symposium for Europe*[20], uno de los mayores eventos de ciberseguridad a nivel mundial en el que CSIRT-CV colaboró y asistió. En dicho evento se pronosticaron como retos que nos depara el futuro inmediato en cuanto a ciberseguridad los ciberataques relacionados con el IoT, dispositivos médicos y con sistemas de control industrial. Además, se prevé que continúen en auge el ataques basados en ransomware y robo de información.

Los ciberataques continuarán en auge, tanto los menos sofisticados como los intentos de distribución de minadores de criptomonedas o ransomware, como los mas avanzados dirigidos al robo de información para monetizarla, extorsionar o llevar a cabo funciones de espionaje. Es por ello que los Estados también se están reforzando para hacer frente a dichos ciberataques, prueba de ello no solo es el Proyecto de Ley Orgánica de Protección de Datos que adaptará nuestra legislación a las disposiciones del Reglamento UE 2016/679 sino también la aprobación de la Estrategia de Seguridad Nacional de 2017 que considera la ciberseguridad como un pilar fundamental en la defensa de un Estado.

(20) 50th TF-CSIRT meeting and First Reginal Symposium for Europe
https://www.csirtcv.gva.es/es/noticias/50th-tf-csirt-meeting-y-first-regional-symposium-para-europa-registro-abierto.html

6 Relaciones y acuerdos

El servicio de Intercambio de información que presta **CSIRT-CV** tiene como objetivo que el centro se transfore en el principal instrumento de intercambio de información relativa a ciberseguridad, tanto en la Generalitat como en empresas de la Comunitat Valenciana, estableciendo canales de comunicación y alerta tanto internos como con organismos, grupos de interés de seguridad, autoridades, empresas, etc. Que permitan, con las restricciones necesarias ara ganarntizar la legalidad vigente y la protección de información corporativa, un intercambio de información ágil, seguro y directo.

En 2017 se han gestionado 139 casos relacionados con el intercambio de información con otros CERTs. Entre los organismos que más información se ha intercambiado ha sido el CCN-CERT, centro con el que **CSIRT-CV** tiene un convenio vigente desde 2008 a través de Generalitat en materia de ciberseguridad y que *ha sido renovado el paso julio por tres años más*.[21] **CSIRT-CV** además de **CARMEN,** este año ha implantado la herramienta del CCN-CERT para intercambio de información sobre incidentes de seguridad, **LUCIA**. Además **CSIRT-CV** ha integrado completamente su plataforma con **REYES**,[22] otra herramienta desarrollada por CCN-CERT para agilizar la labor de análisis de ciberincidentes y compartir información de ciberamenazas.

Durante este año también se ha revitalizado el foro **CSIRT.es**[23] a través de varias reuniones en las que se han propuesto y llevado a cabo diferentes iniciativas entre las que destacan la revisión de los estatutos del foro, la puesta en marcha de un sistema de mensajería instantánea privado, la actualización de contactos o la puesta en marcha de un MISP. A partir de 2018 CSIRT-CV y S2 Grupo – CERT liderarán dicho foro en el que convergen tanto iniciativas públicas como privadas.

(21) *El Consell aprueba la renovación por tres años del convenio...*
https://www.csirtcv.gva.es/es/noticias/el-consell-aprueba-la-renovaci%C3%B3n-por-tres-a%C3%B1os-m%C3%A1s-del-convenio-vigente-desde-2008-entre-la

(22) *Reyes*
https://www.ccn-cert.cni.es/herramientas-de-ciberseguridad/reyes.html

(23) *Foro Csirt.es*
https://twitter.com/CSIRTCV

7 Cultura de ciberseguridad

CSIRT-CV está presente en las redes sociales de Facebook y Twitter, canales de comunicación que utiliza - junto a otros – para crear una cultura de ciberseguridad entre sus seguidores a través de la emisión diarias de noticias diarias, recomendaciones, alertas y consejos sobre ciberseguridad.

Otro de los servicios que **CSIRT-CV** ofrece es el de Comunicación del centro, que persigue fundamentalmente convertir al centro en el referente de la Comunidad Valenciana en temas de ciberseguridad y fomentar una sociedad segura e informada. Este servicio está ligado al servicio ofrecido en el Plan Valenciano de Capacitación como apoyo al mismo en las acciones programadas. Al hilo de ésto, una de las actividades que el centro ha realizado durante este 2017 ha sido la presencia como ponentes en diferentes eventos y jornadas: en el mes de enero **CSIRT-CV** participó en la organización del 50º Congreso TFCSIRT-CV en el que además dió una ponencia, "**CSIRT-CV** Team Update and Plan for 2017-2020, en la Universitat Politécnica de Valencia el centro dió una charla sobre Ciberseguridad en el ámbito de IoT, misma temática que abordamos como ponentes en *PaellaCON*.[24] También fuimos ponentes en *RootedCON*[25] Valencia con una charla sobre análisis de documentos maliciosos, entre muchos otros eventos en los que hemos participado tanto como ponentes como asistentes.

(24) *PaellaCON*
http://www.paellacon.com/

(25) *RootedCON*
https://www.rootedcon.com/inicio

CSIRT-CV

Centre Seguretat TIC
de la Comunitat Valenciana