CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

INFORME DE ACTIVIDADES, CIBERAMENAZAS Y TENDENCIAS

2018

GENERALITAT VALENCIANA
Conselleria d'Hisenda i Model Econòmic

CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

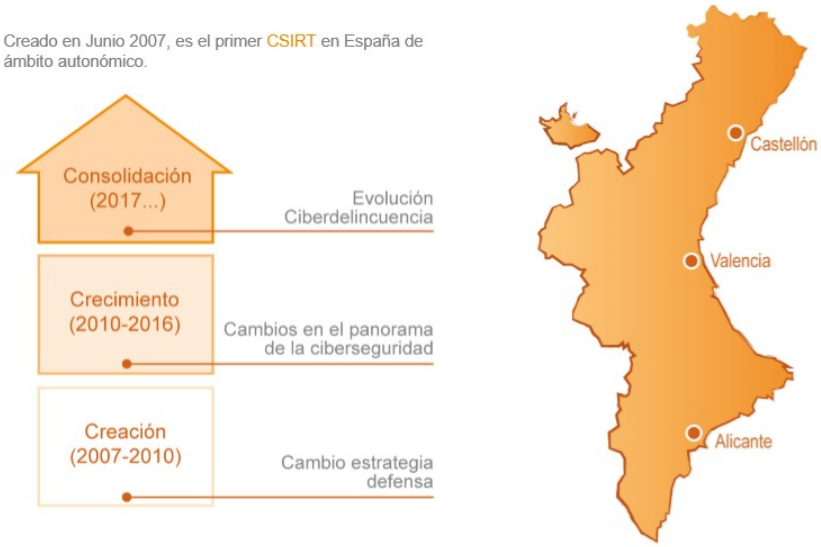
Fondo Europeo de Desarrollo Regional
Una manera de hacer Europa
UNIÓN EUROPEA

Índice

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.

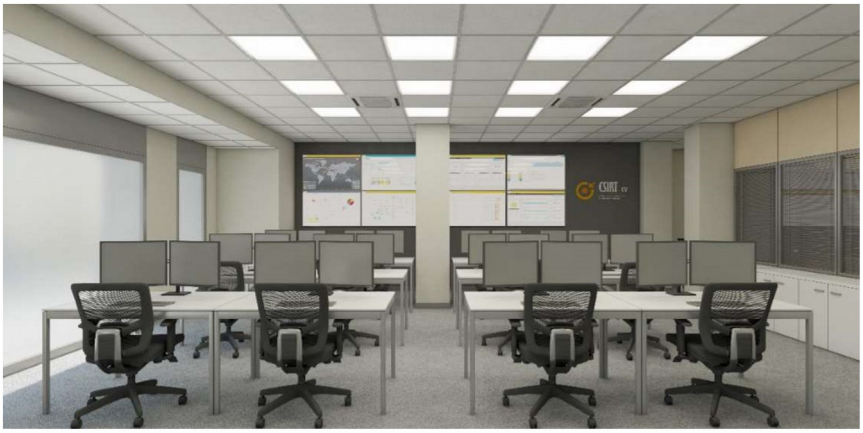


Se trata de una iniciativa pionera al ser el primer centro de estas características que se crea en España para un ámbito autonómico. Actualmente **CSIRT-CV** está adscrito a la Dirección General de Tecnologías de la Información y las Comunicaciones dentro de la Consellería de Hacienda y Modelo Económico.

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 PYMES.
- 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 con amplitud todos los posibles escenarios dados dentro del ecosistema de la ciberseguridad.

Prevención
Auditorías de seguridad
Test de intrusión
Informes y alertas. Observatorio de seguridad
Consultoría técnica y legal
Plan Valenciano de Capacitación
Intercambio de información
Cuadro de mando de seguridad
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

Detección
Sistemas de decepción
Securización de entornos
Auditoría de seguridad semántica
Informe forense pericial
Detección de intrusos
Detección de APT
Test de intrusión

Respuesta
Gestión de incidentes de seguridad
Grupo de intervención rápida
Gabinete de crisis

Los servicios ofertados por CSIRT-CV pueden ser ofrecidos de manera proactiva o bien bajo petición. A continuación se muestra una tabla con los datos de los servicios más relevantes realizados por CSIRT-CV en el año 2018.

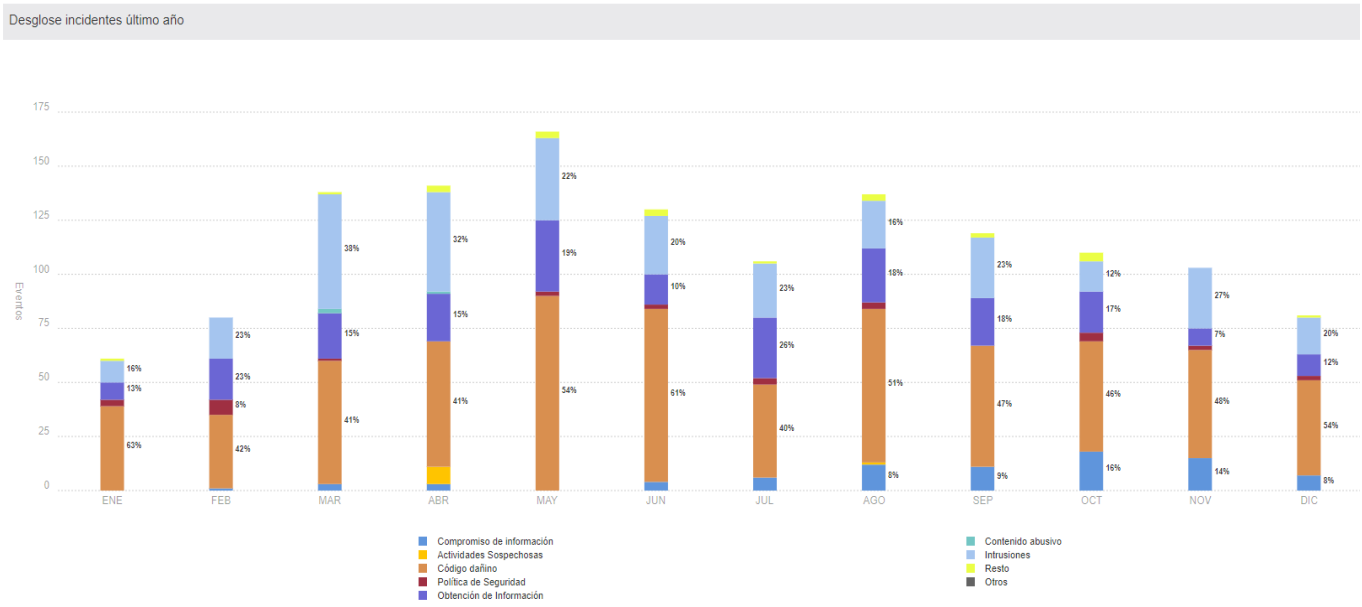
Servicio ofrecidos	Total 2018
Test de intrusión	86
Auditorías de seguridad	110
Consultoría técnica, organizativa y legal	116
Emisión notas de alerta temprana	17

Entre las consultas externas que CSIRT-CV ha atendido predominan las relacionadas con la adecuación al nuevo Reglamento General de Protección de Datos (RGPD), privacidad en redes sociales, securización de terminales móviles, vulnerabilidades de fabricantes o componentes certificados por el ENS, entre otros.

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 2018 el equipo de analistas del centro han gestionado un total de 1619 incidentes de seguridad. Ésta cifra es un 30% mayor que la que se obtuvo en 2017. A continuación una gráfica con la distribución de incidentes por tipología y evolución temporal:



Podemos deducir que los incidentes de tipo “Intrusiones” -se tratan de intentos de accesos no autorizados o intrusiones- y los de tipo “Código dañino” -relacionados con malware-

son los que más se han dado por volumen. También llama la atención el creciente número de incidentes gestionados de tipo "Obtención de información", relacionados principalmente con la detección de correos maliciosos.

3 Ciberamenazas y tendencias

Durante 2018 se ha detectado que el principal objetivo a explotar sobre nuestro ámbito es el de los **servicios Web,** principalmente a través del intento de **subida de ficheros** que permitan tomar el control del sitio o bien a través del intento de explotación de vulnerabilidades de **inyección SQL** con el objetivo de obtener información de las bases de datos que están tras esos servicios Web atacados. Además, se ha detectado un incremento de intentos de acceso a través de servicios directos a los equipos como el SSH, VNC o Escritorios Remotos.

Se ha detectado que a nivel de gestor de contenidos los más atacados han sido Drupal -de una forma muy agresiva- seguidos de Joomla y Wordpress. En el caso de Drupal este incremento de ataques se sustenta en el hecho de que recientemente se han publicado una serie de vulnerabilidades muy críticas (***Drupalgeddon2***) con exploit público que los atacantes no han dudado en intentar aprovechar.[1]

Como novedad con respecto al año pasado, se ha producido un aumento significativo de **ataques hacia routers y todo tipo de dispositivos de red;** se han detectado numerosos intentos de explotación de vulnerabilidades críticas de reciente publicación en routers, lo que pone en evidencia que los atacantes han situado este elemento de red en uno de sus principales objetivos. También es destacable que entre los servicios más atacados, comiencen a estar puertos expuestos de sistemas Android que principalmente son usados para introducir malware de tipo minero.

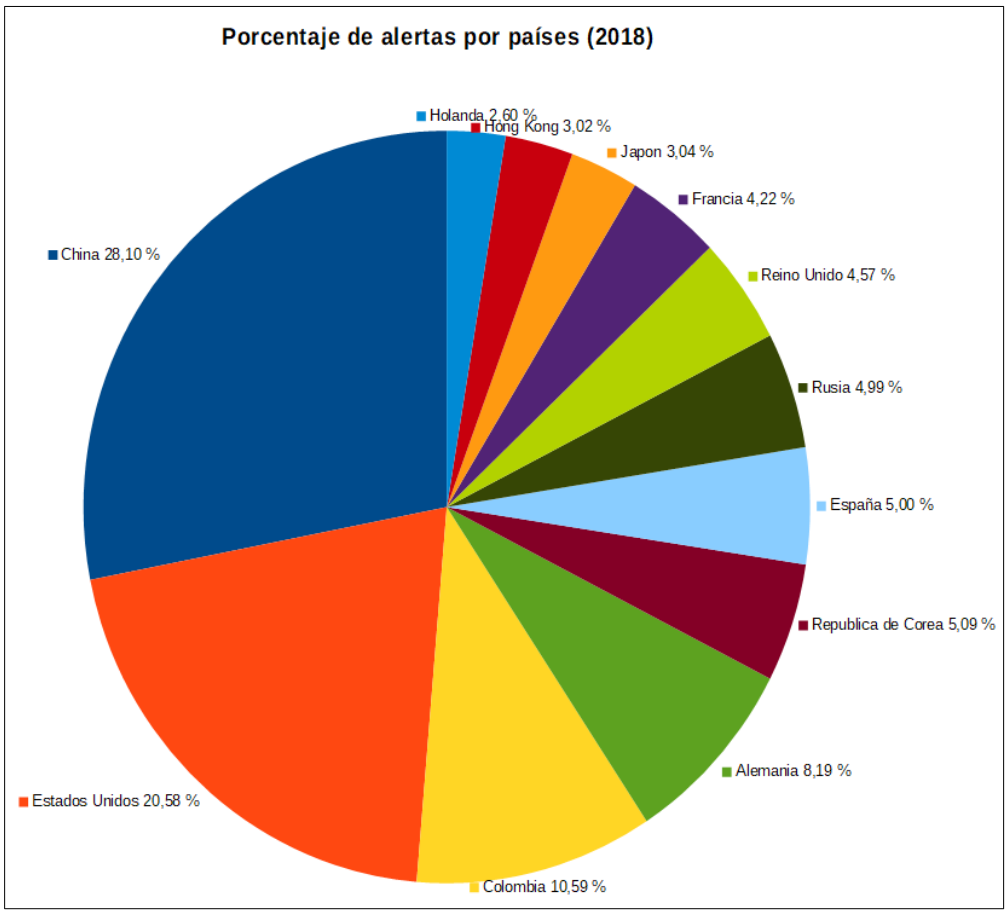
Al igual que ocurría durante todo el 2017 este año se ha vuelto a corroborar una tendencia que continúa en auge y es el intento de explotación de ciertas vulnerabilidades de reciente publicación en la tecnología **Apache Struts**, servidores de aplicaciones **JBoss**, así como la explotación de vulnerabilidades de tipo "**Java Serialized**", en la mayoría de los casos principalmente con el objetivo de comprometer los servidores con malware de tipo **minador de criptomonedas**. En este 2018 sumamos otras dos nuevas tendencias para distribuir malware minero, como es intento de explotación de vulnerabilidades recientes de ejecución de código remoto del servicio **WebDAV** o plataformas **Oracle Weblogic.**

Entre nuestros sectores más atacados destacamos el sector educativo y el sanitario.

En cuanto a países extranjeros de los que proceden los ciberataques podemos identificar que el top 5 sería China, USA, Colombia, Alemania y Corea. También hemos detectado que desde Rusia y Japón se han emitido más ataques de tipo reconocimiento, desde Brasil,

1 https://www.csirtcv.gva.es/es/noticias/una-gran-cantidad-de-sites-son-vulnerables-y-podrían-estar-infectados.html

USA y China se han detectado ataques más agresivos de intentos de explotación de vulnerabilidades.



A continuación se expondrán una serie de casos más reseñables dentro del tipo de ciberataques que han ocasionado incidentes de seguridad.

3.1 Gestores de contenidos. Caso Drupalgeddon

Los gestores de contenido (CMS) son un gran blanco para los atacantes ya que su uso es muy extendido. Los CMS además cuentan habitualmente con una gran variedad de módulos y/o extensiones que amplían sus funcionalidades pero que en ocasiones no están lo suficientemente securizados y se convierten en una potencial puerta de entrada de un atacante.

Durante 2018 se han detectado numerosos ataques de fuerza bruta a los paneles de administración de **WordPress y Joomla** principalmente. En el caso de Joomla además se ha detectado el intento de explotación de una vulnerabilidad que continúa en auge, la **CVE-2015-8562**[2] que permite a atacantes remotos llevar a cabo ataques de inyección de objetos PHP y **ejecutar código arbitrario**.

Si bien WordPress y Joomla han sido objeto de ataques, quedan muy lejos del número de ataques que se han detectado contra **Drupal**, en particular intentando explotar dos vulnerabilidadades recientes, **CVE-2018-7600**[3] **y CVE-2018-7602**. La primera de ellas (**Drupalgeddon2**) corresponde a una vulnerabilidad crítica en el core de Drupal que permitiría ejecución remota de código (RCE) y que fue publicada y parcheada en Marzo de 2018, miles de sitios podrían haberse visto afectados[4-5]. La segunda vulnerabilidad se publicó en abril y también se trataba de tipo RCE de carácter crítico.

Actualmente se siguen explotando activamente estas vulnerabilidades y existe una alta probabilidad de que lo continúen haciendo en los próximos meses.[5]

3.2 Intento de explotación Apache Struts (CVE-2017-5638)

El pasado marzo de 2017 se descubrió que se estaba explotando en Internet una vulnerabilidad de carácter crítico en Apache Struts[6], la cual permitiría a atacantes remotos la ejecución de comandos arbitrarios. Este año continuamos detectando este tipo de ataques que continúa en campañas activas para compromiso de datos o minado de criptomonedas.

3.3 Intento de explotación vulnerabilidades Java Serialized

A nivel mundial se ha visto incrementada la actividad de ataques en relación a la distribución de minadores que pretenden comprometer equipos.

La técnica de distribución de este malware que más hemos observado es la del uso de vulnerabilidades en los procesos inseguros de "deserialización" de objetos Java, para tras explotarlas, descargar y ejecutar el minador en el sitio comprometido. Estas

2 https://www.certsi.es/alerta-temprana/vulnerabilidades/cve-2015-8562
3 https://www.certsi.es/alerta-temprana/vulnerabilidades/cve-2018-7600
4 https://badpackets.net/over-100000-drupal-websites-vulnerable-to-drupalgeddon-2-cve-2018-7600/
5 https://researchcenter.paloaltonetworks.com/2018/05/unit42-exploit-wild-drupalgeddon2-analysis-cve-2018-7600/
6 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5638

vulnerabilidades no son nuevas pero los atacantes siguen utilizándolas en sus campañas.

En concreto este año se ha detectado un aumento de ataques contra el servidor de aplicaciones **JBoss**. Su uso es muy extendido por su carácter gratuito, multiplataforma y potencia, es por ello que los atacantes suelen tenerlo en su punto de mira. Particularmente se ha detectado un intento de explotación de la vulnerabilidad **CVE-2015-7501**[7] la cual permite ejecución de código remoto mediante un objeto Java serializado manipulado y de **CVE-2017-12149**[8] publicada a finales de 2017 y que también permite ejecución de código remoto mediante datos serializados manipulados.

3.4 Unauthenticated Weblogic RCE (CVE-2017-10271)

Durante este año hemos detectado el intento de explotación masivo de una vulnerabilidad que afecta al componente **Oracle WebLogic Server de Oracle Fusion Middleware**, **CVE-2017-10271**[9]. Se trata de una vulnerabilidad de tipo RCE muy fácil de explotar y con una gran alta tasa de éxito que salió publicada a finales de 2017.

Los atacantes están intendo utilizarla principalmente para distribuir CryptoMiners.[10]

3.5 WedDAV (CVE-2017-7269)

En marzo de 2017 salió publicada una vulnerabilidad crítica en la función *ScStoragePathFromUrl* en el servicio WebDAV en *Internet Information Services* en Microsoft Windows Server que permitía a un atacante remoto ejecutar código arbitrario, **CVE-2017-7269**[11]. El exploit público no tardó en aparecer y cientos de sitios con IIS 6.0 se fijaron como objetivo.[12]

Durante 2018 hemos detectado un gran volumen de alertas relacionadas con esta vulnerabilidad principalmente para distribuir malware de tipo minero.[13]

7 https://www.certsi.es/alerta-temprana/vulnerabilidades/cve-2015-7501
8 https://access.redhat.com/security/cve/cve-2017-12149
9 https://nvd.nist.gov/vuln/detail/CVE-2017-10271
10 https://www.fireeye.com/blog/threat-research/2018/02/cve-2017-10271-used-to-deliver-cryptominers.html
11 https://www.certsi.es/alerta-temprana/vulnerabilidades/cve-2017-7269
12 https://medium.com/@iraklis/number-of-internet-facing-vulnerable-iis-6-0-to-cve-2017-7269-8bd153ef5812
13 https://www.f5.com/labs/articles/threat-intelligence/windows-iis-60-cve-2017-7269-is-targeted-again-to-mine-electroneum

3.6 Routers y dispositivos IoT y SCADA

Si hay algo que ha destacado este año es el gran aumento de ataques detectados intentado explotar vulnerabilidades en routers. Un dato curioso es que prácticamente el 100% de este tipo de ataques tiene como origen Brasil. En concreto desde CSIRT-CV se han detectado los siguientes escenarios.

Por un lado el intento de explotación de las Vulnerabilidades **CVE-2018-10561**[14] y **CVE-2018-10562** [15](GPON).

Durante el pasado mayo se publicaron dos vulnerabilidades críticas de salto de restricciones e inyección de comandos en routers de fibra GPON (Gigabit-capable Passive Optical Network). Tras la publicación de los exploits comenzamos a detectar numerosos intentos de explotación sobre dichas vulnerabilidades. Investigadores de Netlab concluyeron que al menos 5 familias de botnets - Mettle, Muhstik, Mirai, Hajime y Satori- habían estado explotando activamente estas vulnerabilidades.[16]

Por otro lado se han detectado distintos ataques más genéricos contra los sistemas de administración remota de los routers Cisco, contra sistemas AsusWRT o contra dispositivos D-Link.

También se han detectado algunos intentos de explotación en dispositivos IoT, especialmente cámaras IP en las que principalmente los atacantes buscan saltarse la autenticación.

Respecto a dispositivos SCADA también se ha detectado un incremento de ataques relacionados con el protocolo DNP3[17] con alertas del tipo:

DNP3 Warm Restart

DNP3 Stop Application

DNP3 Enable Unsolicited Messages

DNP3 Cold Restart

3.7 Maldocs

Durante 2018 se han analizado miles de documentos maliciosos que hemos ido recolectando de nuestras fuentes y se han extraído algunas conclusiones de interés. Entre

14 https://www.certsi.es/alerta-temprana/vulnerabilidades/cve-2018-10561
15 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10562
16 http://blog.netlab.360.com/gpon-exploit-in-the-wild-i-muhstik-botnet-among-others-en/
17 https://es.wikipedia.org/wiki/DNP3

dichas conclusiones podemos destacar:

- Uso significativo de la vulnerabilidad **CVE-2017-11882**[18] para evitar el uso de macros en documentos ofimáticos.
- Aumento de malware relacionado con las botnet Pony y Lokibot.
- Aumento del uso de powershell para descarga de binarios o segunda fase de la infección
- Aumento de uso de documentos RTF con objetos Office embebidos conteniendo macros.
- Algunos documentos modificando claves de registro relacionadas con Microsoft Office para realizar evitar la detección.

A continuación nuestro análisis con algo más de detalle.

Las principales extensiones de los documentos maliciosos que hemos detectado son las siguientes: .doc/.docx, .xls/.xlsx, .pdf y .exe.

En la mayoría de casos la extensión del fichero adjunto no se corresponde con el formato del contenido del fichero, en la siguiente tabla podemos ver las extensiones más comunes:

Extensión utilizada en el fichero	Extensión asociada al formato real
.doc	.rtf
.xls	.oxml
.jpg	.exe
.bat	.exe
.wiz	.rtf

Además de los tipos de fichero usuales que se suelen utilizar, hemos detectado el uso de nuevos tipos de ficheros:

.xlam

Fichero Add-In Excel con macros utilizado para añadir nuevas funciones a Excel

.url

Similar a un fichero .lnk pero con un enlace externo a un sitio web

.hta

Fichero con código ejecutable desde un navegador, puede contener vbscript,

18 https://www.certsi.es/alerta-temprana/vulnerabilidades/cve-2017-11882

javascript

.iqy

Fichero que contiene una url y otros parámetros para realizar una consulta hacia internet

Respecto al malware distribuido por estos fichero maliciosos, estas son las principales familias detectadas dentro de este 2018:

- PONY (password stealer)
- JRAT (RAT)
- LOKIBOT (password stealer)
- Miners (cryptomining)
- GandCrab
- ADWIN JAR (RAT)
- Necurs

Detalle de algunas de las principales vulnerabilidades explotadas:

- **CVE-2017-11882** (Office - EQNEDT32.EXE) [19]
- **CVE-2018-4990** (Acrobat Reader)[20]
- **CVE-2017-8570** (Office)[21]
- **CVE-2012-0158** (Office)[22]

Así mismo hemos detectado que las técnicas más utilizadas para la descarga/instalación del contenido malicioso en el equipo de la víctima que hemos detectado son las siguientes:

- Utilización de Macros en los documentos ofimáticos para descarga o descifrado de objetos embebidos.
- Utilización de Macros para el descifrado de scripts embebidos en el documento, que realizan la descarga del ejecutable malicioso.
- Uso de la característica de incluir documentos remotos en documentos ofimáticos para enlazar con ficheros maliciosos durante la carga del documento.

19 https://www.certsi.es/alerta-temprana/vulnerabilidades/cve-2017-11882
20 https://helpx.adobe.com/es/security/products/acrobat/apsb18-09.html
21 https://nvd.nist.gov/vuln/detail/CVE-2017-8570
22 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0158

• Utilización de powershell para descargar el contenido malicioso.

• Uso de BITs para realizar la descarga de contenido malicioso. Y uso de varios objetos embebidos en un único documento, cada uno con una función durante la explotación de la vulnerabilidad y la instalación del malware.

3.8 Herramientas de reconocimiento

Como viene siendo habitual en los últimos años, durante 2018 también se han detectado numerosos escaneos con herramientas automáticas. En particular hemos detectado un aumento del uso de las siguientes herramientas:

ZmEu[23]: escáner de vulnerabilidades de tipo Web y también realiza ataques de fuerza bruta contra SSH.

GoScanSSH[24]: una tendencia en alza es esta familia de malware, activa principalmente desde junio de 2017, escrita en Go y cuyo vector de ataque inicial está basado en ataques de fuerza bruta contra servicios SSH.

Sqlmap[25]: conocidísima herramienta orientada a la búsqueda y explotación de vulnerabilidades de tipo iSQL.

Cisco-Torch[26]: herramienta muy potente de fingerprinting para descubrir dispositivos Cisco. Identifica los dispositivos y busca sus servicios: telnet, SSH, los servicios Web, NTP y SNMP. También permite realizar ataques de fuerza bruta.

FOCA[27]: herramienta utilizada principalmente para encontrar metadatos e información oculta en los documentos que examina.

3.9 Otros

De manera más general también podemos hacer mención al intento de explotación de otras vulnerabilidades que si bien no de forma masiva pero sí notable, se han detectado en nuestros sistemas.

Por un lado, se han detectado un número significativo de alertas relacionadas con la explotación de una vulnerabilidad en Windows DNS Server (**CVE-2017-0171**[28]) de mayo de 2017. Se trata de una vulnerabilidad de denegación de servicio cuando Microsoft Windows

23 https://en.wikipedia.org/wiki/ZmEu_(vulnerability_scanner)
24 https://www.ssh.com/attack/GoScanSSH
25 http://sqlmap.org/
26 https://tools.kali.org/information-gathering/cisco-torch
27 https://www.elevenpaths.com/es/labstools/foca-2/index.html
28 https://www.certsi.es/alerta-temprana/vulnerabilidades/cve-2017-0171

Server 2008 SP2 y R2 SP1, Windows Server 2012 Gold y R2 y Windows Server 2016 están configurados para responder a consultas de versiones, también conocido como "Windows DNS Server Denial of Service Vulnerability".

Durante este año también hemos detectado un incremento de alertas relacionadas con el intento de explotar la vulnerabilidad FREAK que afecta a OpenSSL aunque se trata de una vulnerabilidad de hace varios años (CVE-2015-0204).

4 Plan Valenciano de Capacitación

Conseguir una gestión eficaz de la ciberseguridad no depende sólo de la implantación de 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 en los centros educativos de secundaria de la Comunidad Valenciana, conferencias, guías, estudios.

Este año desde CSIRT-CV se han llevado diferentes acciones en el marco de este plan, a destacar:

- Lanzamiento de un nuevo portal por parte de CSIRT-CV dedicado en exclusiva a la concienciación en ciberseguridad: **https://concienciat.gva.es/**

Figura 1: Portal www.concienciat.gva.es

- Pruebas de Humsec a diferentes colectivos de nuestro ámbito.
- Campañas de concienciación online en redes sociales:
  - "Fraudes Digitales"[29]
  - "Pon a prueba la recuperación de datos"[30]

29 https://www.csirtcv.gva.es/es/paginas/fraudes-digitales.html
30 https://concienciat.gva.es/tips_de_seguridad/puedes-permitirte-perder-la-informacion-de-tu-negocio-te-traemos-10-consejos/

- Publicación de dos informes de carácter público:
  - Cryptomining Malware[31]
  - Informe actividades del centro del año 2017[32]
  - Informe actividades del centro del semestre 1 de 2018[33]

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 [34] 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

31 https://www.csirtcv.gva.es/es/descargas/informe-sobre-cryptomining-malware.html
32 https://www.csirtcv.gva.es/es/descargas/informe-actividades-csirt-cv-2017.html
33 https://www.csirtcv.gva.es/es/descargas/informe-actividad-csirt-cv-s12018.html
34 http://www.saps.gva.es/

En 2018 se han formado cerca de **5.000 alumnos**.

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

En cuanto a formación presencial, desde CSIRT-CV se han realizado diferentes cursos de carácter interno para personal especializado dentro de nuestro ámbito sobre análisis forense, gestión de incidentes de seguridad o análisis de malware, entre otros. Formando de forma presencial a mas de 100 empleados de Generalitat.

De igual forma, se han organizado diferentes charlas divulgativas destinadas a concienciación para familias, en centros educativos (se profundizará sobre ésto en puntos posteriores), en determinados colectivos desprotegidos como víctimas de violencia de género, dirigidas al sector sanitario o a altos cargos entre otros.

4.2 Jornadas concienciación a altos cargos

El objetivo de estas charlas son principalmente personas de tipo directivo, con acceso a información sensible, en los que los riesgos asociados no son los mismos que otros cargos con funciones y responsabilidades diferentes. La charla dispone de un lenguaje sencillo y sin tecnicismos y pretende concienciar sobre los riesgos de los usos no seguros de la tecnología y de la gestión de la información.

Este año se han impartido varias sesiones dirigidas a personal directivo de Hospitales, Magistrados, Jueces, Fiscales, Interventores, Investigadores, etc.

Figura 2: Sesión Concienciación personal médico en Hospital La Fe de Valencia

4.3 Jornadas de concienciacion a colectivos desprotegidos

Durante el año 2017, aprovechando que el día 25 de noviembre se celebra el "Día Internacional de la Eliminación de la Violencia contra la Mujer", CSIRT-CV se sumó a las iniciativas programadas aportando su conocimiento en algo tan necesario como es la concienciación en ciberseguridad y privacidad. Estas iniciativas han continuado durante 2018.

Para ello CSIRT-CV comenzó un plan de jornadas centradas en ayudar a mejorar la seguridad de la información de las víctimas de violencia de género, tratando temas como la prevención del ciberacoso, cómo hacerle frente al mismo, la importancia de la privacidad en las redes sociales, cómo configurar los perfiles en redes sociales de la forma más segura, la seguridad de los dispositivos móviles, la grabación y

difusión de imágenes sin consentimiento, o herramientas contra el maltrato y alejamiento digital, entre muchos otros temas de actualidad en el mundo de la ciberseguridad y privacidad.

4.4 Concienciación en centros educativos

En el marco del Plan Valenciano de Capacitación, los adolescentes han sido identificados como uno de los colectivos más vulnerables. Por este hecho se ha visto la necesidad de poner en marcha acciones específicas en este sector y su entorno más cercano, sus padres y sus profesores.

El alcance de la propuesta abarca todos los institutos públicos, concertados y privados de la Comunidad Valenciana, centrándose en los alumnos de 2º de la E.S.O. y su entorno más cercano, sus padres y sus profesores, para que puedan encontrar en las personas adultas respuestas en sus dudas del día a día.

Durante 2018 se han llevado a cabo Jornadas de Ciberseguridad en casi una treintena de institutos de la Comunitat, estimando una asistencia de unas 3500 personas entre alumnos, padres y docentes.

En este apartado de "Educación" mencionar que también se ha estado impartiendo un taller en el Congreso de Educación TIC organizado por la Consellería de Educación denominado "Protégete y Ayúdales a Protegerse".

4.5 Portales principales. Material publicado

El portal www.csirtcv.gva.es donde se publican diariamente noticias de seguridad y se alerta sobre las vulnerabilidades más importantes, es la imagen principal del centro de cara al exterior. Este año el portal ha recibido cerca de 400.000 visitas y se han realizado más de 500 publicaciones.

CSIRT-CV también pone a disposición una serie de guías/informes y otro tipo de material sobre ciberseguridad en su portal principal. En este 2018 este contenido ha tenido casi 200.000 descargas.

Como novedad, este año el centro ha publicado un estudio sobre las últimas técnicas de Cryptomining Malware que le invitamos a consultar.[35]

35 https://www.csirtcv.gva.es/es/descargas/informe-sobre-cryptomining-malware.html

En la sección de Informes de nuestro portal se puede encontrar todo el material disponible para su descarga.[36]

Este año se ha puesto en marcha también otro portal para el ciudadano, https://concienciat.gva.es/ En dicho portal se pueden consultar vídeos formativos y promocionales, infografías, información sobre nuestros cursos en SAPS, etc.

36 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, se están viviendo actualmente ciertas circunstancias externas que aumentan exponencialmente el riesgo al que las corporaciones se exponen.

A continuación, fruto de nuestra investigación, se exponen estas circunstacias externas:

Según 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 (Bring Your Own Device), 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 estén detectando un gran número de ataques en ese sentido.

Pero si hay una circunstancia externa que nos ha llamado la atención este semestre, ha sido el elevado número de vulnerabilidades y exploits publicados sobre dispositivos de tipo **IoT** y electrónica de red, fundamentalmente routers, los cuales han sido especialmente atacados en nuestro ámbito.

A continuación se enumeran una serie de hitos relevantes provenientes de análisis externos que se han detectado y que podrían afectar a nuestro ámbito.

5.1 Fraude al CEO

Durante 2018 hemos detectado un número creciente de casos del tipo conocido **"fraude al CEO".** Este timo consiste en que un empleado de la alta dirección, o empleados con capacidad para hacer transferencias o accesos a datos de cuentas, recibe un correo, supuestamente de su jefe ("CEO") en el que se le pide ayuda para una operación financiera confidencial y urgente. Evidentemente se trata de una suplantación de identidad y que desafortunadamente hemos observado un incremento significativo en nuestro ámbito. CSIRT-CV este año envió una alerta masiva para informar a todos los empleados de GVA sobre este tipo de fraudes.

5.2 Sector Sanitario

Un estudio de Kaspersky Lab[37] alertaba recientemente del alto nivel de desprotección que sufre la información médica y consecuentemente los datos de los pacientes almacenados en la infraestructura sanitaria conectada. Diferentes investigaciones concluyen la desprotección de la mayoría de los dispositivos y sistemas médicos ante posibles incidentes de seguridad, con lo que su situación se ha vuelto cada vez más preocupante. Está demostrado que el acceso no autorizado a estos dispositivos puede tener efectos muy graves: no sólo pone los datos personales al alcance de los ciberdelincuentes, sino que también podría afectar de forma directa la salud y hasta las vidas de los pacientes.

Desde Kaspersky alertan también de un incremento de ataques contra el sector sanitario en todo el 2018 y futuro. De hecho este primer semestre, desde Symantec se descubrió una nueva campaña APT denominada **Orangeworm**[38] dirigida a empresas y organizaciones de salud con el fin de realizar espionaje. Este campaña carga malware en dispositivos que alojan software empleado para controlar máquinas de rayos X, Resonancia Magnética Nuclear (RMN), así como dispositivos utilizados para ayudar a los pacientes a completar los formularios de consentimiento para procedimientos médicos.

5.3 Ataques a la cadena de suministro

Una tendencia aterradora que nos presenta Kaspersky Lab[39] es el uso de proveedores o terceros por grupos APT para inmiscuirse en el destino objetivo.

En ocasiones atacar a la cadena de suministro puede ser más efectivo que atacar a su objetivo de forma directa. Es probable incluso, que un objetivo cuyas redes están protegidas con las mejores defensas, use software de un tercero. El tercero podría ser un objetivo más fácil, este hecho se puede aprovechar para vulnerar la protección de la empresa objetivo. Ya durante el pasado 2017 se observaron casos similares como Shadowpad, CCleaner o NotPetya.

Es muy recomendable exigir de forma contractual a nuestros proveedores unos niveles de seguridad adecuados para evitar este tipo de riesgos.

37 http://www.europapress.es/portaltic/ciberseguridad/noticia-kaspersky-pronostica-aumento-numero-ataques-dirigidos-contra-dispositivos-sanitarios-conectados-2018-20180404172907.html
38 https://www.symantec.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia
39 http://www.itdigitalsecurity.es/vulnerabilidades/2017/11/los-ataques-a-la-cadena-de-suministro-seran-una-constante-en-2018

5.4 Regulación Internet of Things

"***Un dispositivo es tan fuerte como su enlace más débil***". Las palabras de Ondrej Vlcek, vicepresidente ejecutivo de Avast, sirven para explicar la situación que se está comenzando a vivir en la mayoría de escenarios TI. A pesar de que contemos con medidas de seguridad exhaustivas en nuestros servidores o dispongamos del mejor firewall del mundo, nuestras infraestructuras forman ecosistemas cada vez más complejos y mas interconectados. Si uno de los eslabones falla, puede fallar el resto.

"*A medida que el Internet de las Cosas conectadas innecesariamente se vuelve menos evitable, crece la superficie de ataque, con dispositivos en red y sensores integrados en elementos y contextos inesperados: desde routers hasta heladeras y medidores inteligentes, desde televisores hasta juguetes, desde centrales eléctricas hasta estaciones de servicio y marcapasos. Como todo se vuelve más inteligente, aumenta la cantidad de servicios que pueden verse afectados por el malware*", señalan en el último informe de ciberseguridad de la compañía We Live Security.[40]

En este mundo conectado cada vez más complejo aún existe una pregunta fundamental que responder: **¿quién debe asumir la responsabilidad?**

Los fabricantes se suben a la ola del **Internet de las Cosas**, pero muchas veces carecen de la experiencia y el conocimiento complejos para garantizar la seguridad de sus dispositivos. Los proveedores gestionan las redes y las mantienen seguras, pero es complicado que protejan el dispositivo final, en el extremo del usuario. Las autoridades y los reguladores todavía deben avanzar para diseñar estándares y protocolos seguros en el ecosistema del Internet of Things (IoT). Los proveedores de soluciones de seguridad cuentan con el conocimiento y la experiencia, pero dependen del resto para tener acceso a dispositivos y redes. **La respuesta, probablemente, englobe a todos**. La seguridad pasa por usuarios más conscientes, fabricantes más preparados, mejores regulaciones y redes y protocolos más fiables.

5.5 Sofisticación del spear-phishing

Según el CCN-CERT[41] las campañas de phishing han aumentado en el último año tanto en volumen como en sofisticación. Hecho que desde CSIRT-CV también hemos notado. Según el CCN-CERT este método constituye el vector de infección más exitoso, tanto en ataques

40 https://www.kasilh.com/index.php/noticias/100-noticias-iot-seguridad
41 https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2856-ccn-cert-ia-09-18-ciberamenazas-y-tendencias-2018-resumen-ejecutivo-2018/file.html

dirigidos como de distribución masiva de malware a través de correos spam. El Spear-Phishing se adapta al objetivo con lo que es díficil detectar su naturaleza dañina y por tanto más díficil de mitigar su impacto.

El principal método de lucha contra este tipo de ataques es sin duda la concienciación al usuario.

5.6 Minas de datos provocados por leaks de información

Desde Kaspersky nos alertan que las recientes fugas de datos a gran escala podrían ayudar a los atacantes a mejorar el éxito de los spear phishing, pues si logran realizar correos más personalizados con información del usuario, éste puede confiar en la legitimidad del origen.

5.7 Ciberseguridad industrial

Desde Forcepoint indican que tanto los dispositivos domóticos, como los que controlan aires acondicionados, sistemas de transporte de las compañías o plataformas industriales que manejan infraestructuras críticas como petróleo, gas, luz o agua estarán en 2019 en el punto de mira del cibercrimen. Estos sistemas suelen carecer de esquemas robustos de ciberseguridad y los delincuentes se aprovechan de ello.

5.8 Ataques contra redes sociales

Es presumible que en los próximos meses se desarrollen formas más asequibles para los atacantes gracias a las redes sociales, que pueden ser empleadas para sofisticadas actividades de ingeniería social y reconocimiento. Como señala Airbus Cybersecurity, para protegerse de estos ataques, las organizaciones deben implementar políticas de seguridad, como programas de formación para los empleados.

Desde el punto de vista de CSIRT-CV, no solo creemos que es muy interesante un programa de formación específico para el uso de redes sociales especialmente indicado para altos cargos, sino también fomentar el servicio de auditoría semántica por el que de forma proactiva se podría tomar como objetivo una persona y rastrear toda su actividad en Internet, en busca de información que pudiera ser usada en campañas de ingeniería social con el fin de alertarle y prevenirle, y sobre todo enseñarle a hacer un uso seguro de sus datos.

5.9 Auge de la criptomoneda

Es evidente que las criptomonedas están de moda. Todo el mundo, incluidos los ciberdelincuentes, quieren obtener beneficio de esta tendencia y los ataques en relación a la distribución de malware de tipo minador se han incrementado de manera exponencial.

No solo en Generalitat ha sido 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 (minado desde dispositivos IoT, compromiso de smartphones para minado, etc) que están usando los atacantes para distribuir este tipo de malware. Se pronostica que seguirá en auge esta tendencia.

5.10 Inteligencia Artificial

Con el objetivo de reducir el número de vulnerabilidades y ataques a los sistemas TI , la inversión en investigación sobre inteligencia artificial se va a triplicar para 2020, según señala la compañía Digiware. A través del machine learning se puede recolectar y almacenar información para identificar posibles comportamientos inusuales en los equipos y servidores y de esta forma lograr reaccionar de manera anticipada a posibles ataques. Esperemos que ésto consiga que los proveedores de servicios de ciberseguridad mejoren sus métodos de detección y protección en sus productos.

Es posible además, que la inteligencia artificial también sea utilizada por parte de los ciberdelincuentes para encontrar formas de aplicación e indroducir nuevos vectores de ataque en las organizaciones. [42]

5.11 Marco Estratégico y Legal

En España, en 2018, se han publicado dos nuevas Instrucciones Técnicas de Seguridad que se suman a las ITS de Conformidad con el ENS y del Informe de Estado de Seguridad publicadas con anterioridad:

• Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.

42 https://www.securityartwork.es/2019/01/18/inteligencia-artificial-y-ciberseguridad/

• Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.

En España, en 2018, se han publicado dos nuevas Instrucciones Técnicas de Seguridad que se suman a las ITS de Conformidad con el ENS y del Informe de Estado de Seguridad publicadas con anterioridad:

- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.

- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.

El 7 de septiembre se publica el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información (trasposición de la Directiva NIS) , cuyo objeto es regular la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y de los servicios digitales, y establecer un sistema de notificación de incidentes. Este real decreto determina:

• La forma y criterios de identificación de los servicios esenciales y de los operadores que los presten.
• Las medidas de seguridad que habrán de aplicar.
• Las Autoridades competentes.
• Identifica cuales son los CSIRTs de referencia.
• Asigna al CCN-CERT la coordinación y respuesta técnica en casos de especial gravedad.

A partir del 25 de mayo de 2018, es de plena aplicación Reglamento (UE) 2016/679 Reglamento General de Protección de Datos (RGPD) , el cual entró en vigor en mayo de 2016.

En julio de 2018 se publica el Real Decreto Ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos, el cual adapta aquellos preceptos en los que el RGPD remitía su desarrollo a los Estados miembros, y que no requieren rango de ley orgánica. Este Real Decreto Ley entra en vigor el 31 de julio de 2018.

Finalmente a principios de diciembre de 2018 se publica la Ley Orgánica 3/2018, de 5 de

diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
El objeto de la Ley entre otras cosas, es facilitar a los ciudadanos el ejercicio de sus derechos en materia de protección de datos personales, exigir que los medios para hacerlo sean fácilmente accesibles. Además de regular el modo en que debe informarse a las personas acerca del tratamiento de sus datos personales.

6 Presidencia del foro CSIRT.es

El Foro CSIRT.es es una plataforma independiente de confianza y sin ánimo de lucro compuesto por los equipos de respuesta a incidentes de seguridad CSIRT/CERT, cuyo ámbito de actuación o comunidad de usuarios en la que opera, se encuentra dentro del territorio español. Proteger el ciberespacio español, intercambiando información sobre ciberseguridad y actuar de forma rápida y coordinada ante cualquier incidente que pueda afectar simultáneamente a distintas entidades en nuestro país, es el principal objetivo del Foro CSIRT.es

Durante 2018 CSIRT-CV y S2 Grupo–CERT han liderado dicho foro en el que convergen tanto iniciativas públicas como privadas. Durante este año se han celebrado tres encuentros organizados por CSIRT.es y se ha gestionado la incorporacion de casi una quincena de organismos, llegando a una suma de 34 miembros que forman parte de CSIRT.es.

Ilustración 1: Detalle reunión foro CSIRT.es

Se han puesto en marcha también nuevas herramientas para compartir información, así como una plataforma interna de mensajería instantánea o una plataforma interna para compartición de IOCs.

Dicha labor de coordinación por parte de CSIRT-CV fue agradecida en las jornadas del CCN-CERT con la presencia de la dirección del centro en la recepción de bienvenida a Su Majestad el Rey, Don Felipe VI a dichas jornadas.

Figura 3: La Directora de CSIRT-CV junto al resto de autoridades acompañando a SAR Don Felipe VI

7 Relaciones y acuerdos institucionales

El servicio de Intercambio de información que presta CSIRT-CV tiene como objetivo que el centro se transforme 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 alerte tanto de forma interna como con organismos externos, grupos de interés de seguridad, autoridades, empresas, etc.

En 2018 se han gestionado 200 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 fue renovado el pasado julio por tres años más.[43] CSIRT-CV además de **CARMEN**, hace uso de la herramienta del CCN-CERT para intercambio de información sobre incidentes de seguridad, **LUCIA**. Además CSIRT-CV ha integrado completamente su plataforma con **REYES**,[44] otra herramienta desarrollada por CCN-CERT para agilizar la labor de análisis de ciberincidentes y compartir información de ciberamenazas.

Este año también CSIRT-CV se ha incorporado a Carnegie Mellon y FIRST.

Por primera vez este año CSIRT-CV participó en la última edición de los ciberejercicios Cyber Europe 2018 que organiza ENISA. CSIRT-CV participó de la mano del CCN-CERT y coordinados por el Departamento de Seguridad Nacional.

Los ciberejercicios tuvieron una duración de tres jornadas y en ellas se pudo poner en marcha toda la capacidad de reacción y coordinación ante un escenario de crisis a nivel internacional que tiene CSIRT-CV, siendo una experiencia muy enriquecedora y productiva.

8 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, 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

43 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

44 https://www.ccn-cert.cni.es/herramientas-de-ciberseguridad/reyes.html

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 2018 ha sido la presencia como ponentes en diferentes eventos y jornadas públicas:

Desde CSIRT-CV se han impartido las siguientes charlas:

- Ponencia sobre optimización de un IDS opensource para el encuentro del Trusted Introducer que se celebró en Hamburgo en febrero de 2018
- Charla en las jornadas del instituto de Cheste sobre "Rotten Phish - Maldoc Analysis Tricks" en enero de 2018
- Ponencia en las Jornadas SAT del CCN-CERT sobre GLORIA, el SIEM de CSIRT-CV
- Ponencia sobre GLORIA al Club de Exportadores e Inversores de INECO junto con el CCN-CERT
- Ponencia en la base de la ONU de Valencia sobre la actividad del CSIRT-CV
- Ponencia sobre "Diseccionando Emotet, un caso práctico" en el foro CSIRT.es
- Ponencia sobre "Auditando dispositivos médicos" en el foro CSIRT.es
- Ponencia sobre "Optimización de un IDS opensoruce" en el foro CSIRT.es
- Ponencia "Adquisición de evidencias forenses en la nube" en las Jornadas STIC del CCN-CERT

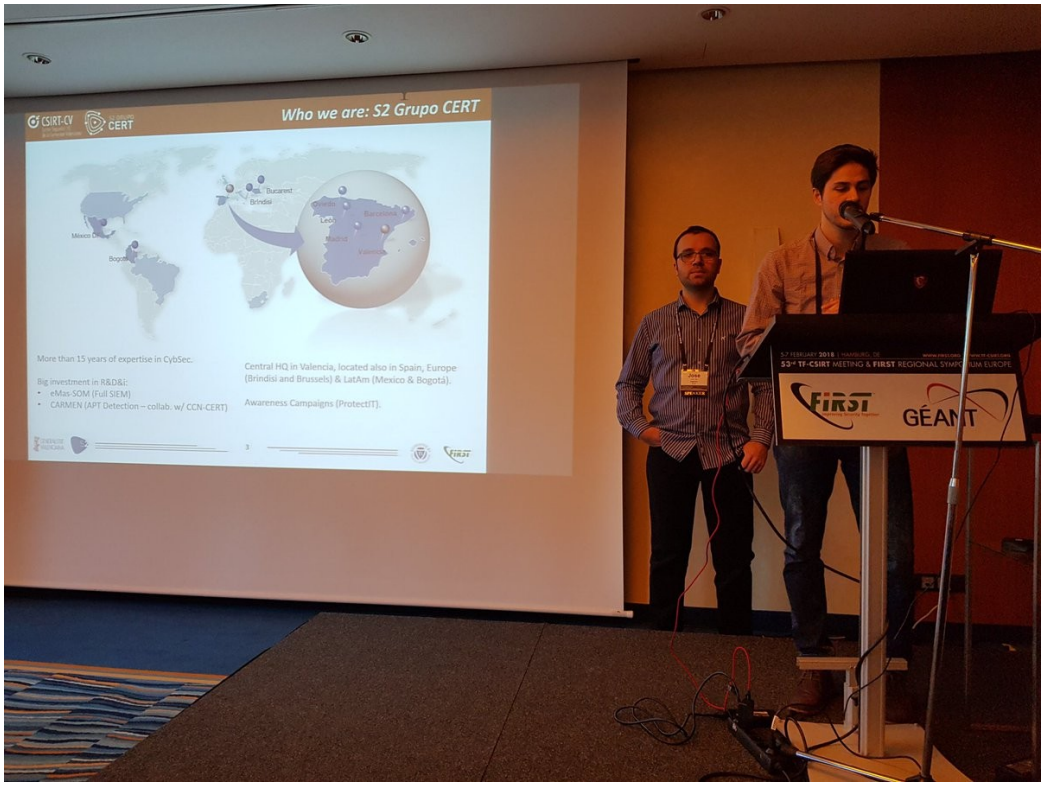


Figura 4: CSIRT-CV exponiendo una charla en el TF-CSIRT del pasado febrero

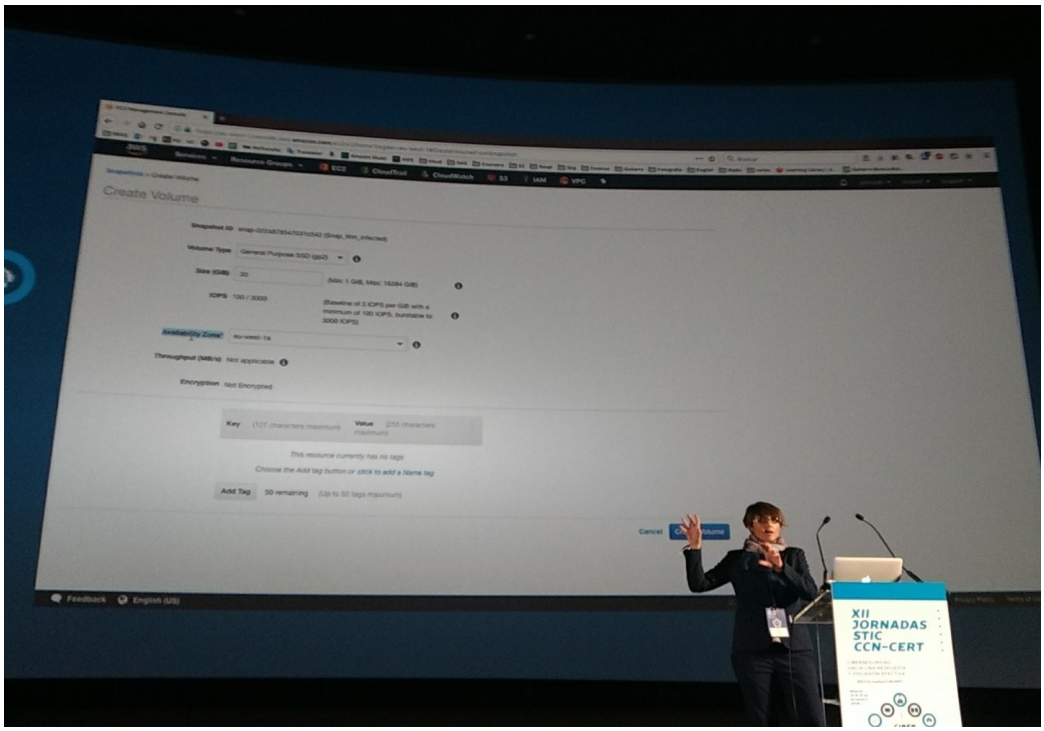


Figura 5: CSIRT-CV exponiendo en las Jornadas STIC del CCN-CERT