CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

INFORME DE ACTIVIDADES, CIBERAMENAZAS Y TENDENCIAS

2020

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

CLASIFICACIÓN

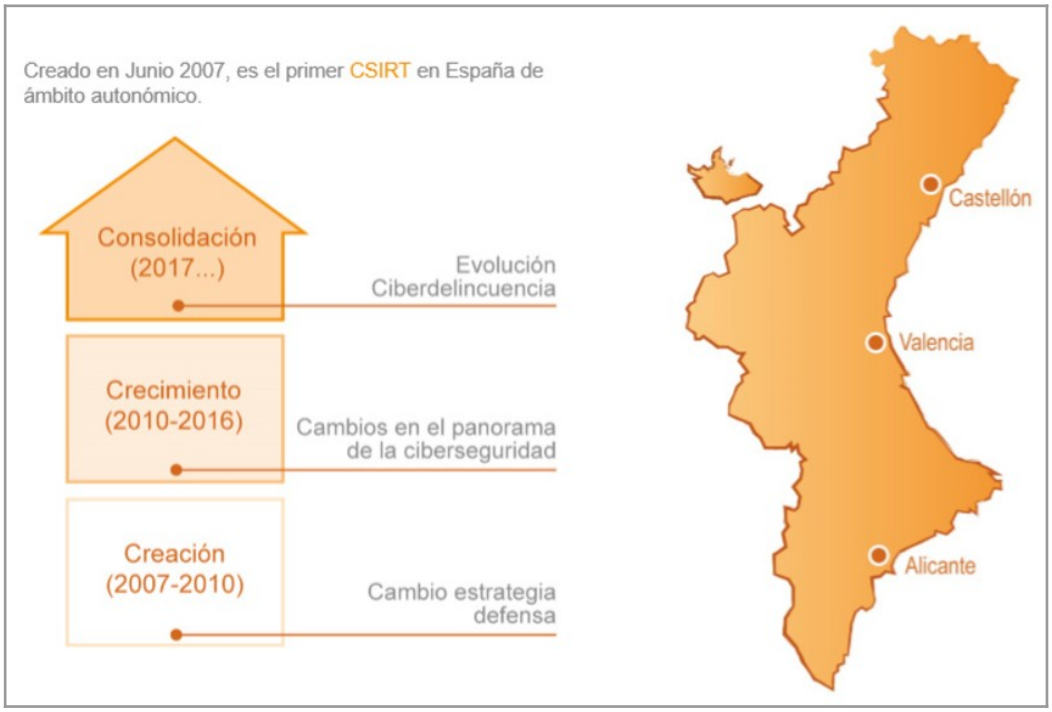
INDICE

SOBRE EL PRESENTE INFORME

La información recogida en este informe es, en gran medida, el resultado de la experiencia del CSIRT-CV durante 2020, en el desarrollo de sus competencias. Asimismo, se han tenido en cuenta otras fuentes documentales, nacionales e internacionales, públicas y privadas.

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 Valenciana por la seguridad en la red. En 2020 cumple 13 años de andadura, en los que se ha consolidado como un CSIRT de referencia a nivel nacional y con presencia internacional en foros como CSIRT.es, Trusted Introducer y FIRST.



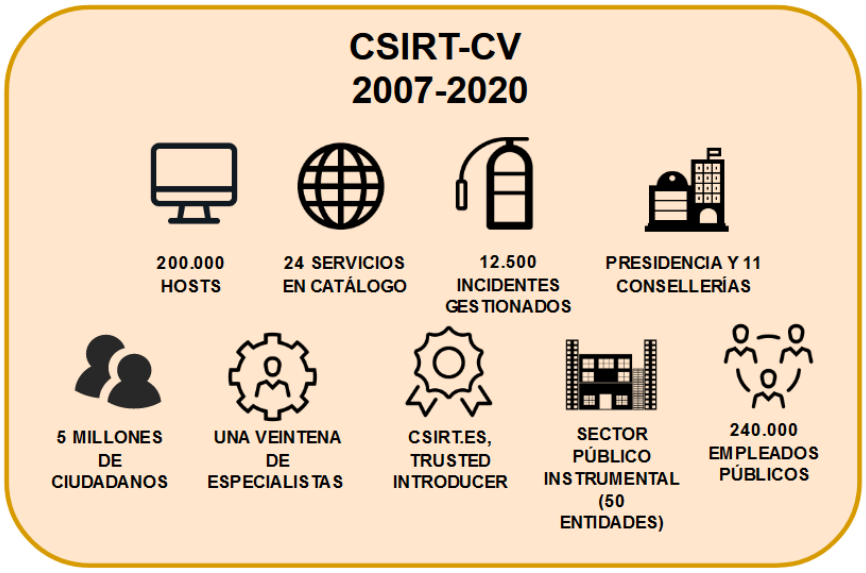
Se trata de una iniciativa pionera al ser el primer centro de estas características que se crea en España para un ámbito autonómico. Actualmente **CSIRT-CV** está adscrito a la Dirección General de Tecnologías de la Información y las Comunicaciones dentro de la Consellería de Hacienda y Modelo Económico.

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.

El ámbito de actuación del CSIRT-CV, como se observa, es muy amplio puesto que incluye a la Generalitat Valenciana, que en la actualidad está formada por Presidencia y 11 consellerías, entre las que se incluyen 2 vicepresidencias. También se incluye el sector público instrumental[1], junto con medio centenar de entidades. En total, el número de empleados públicos en la Comunitat asciende a cerca de 240.000[2]. Por último, es necesario mencionar que la Comunitat Valenciana representa cerca de un 11% de la población nacional con unos 5 millones de habitantes (2019), siendo la 4ª Comunidad Autónoma de España en cuanto a población se refiere.



1 http://www.gvaoberta.gva.es/es/sector-publico-instrumental

2 Según datos publicados en el Boletín Estadístico del Personal al Servicio de las Administraciones Públicas, a fecha julio 2019.

Respecto a la infraestructura TI de la Generalitat Valenciana, es altamente heterogénea y compleja, dando servicio a cerca de 200.000 dispositivos, entre los que se incluye tanto equipamiento IT como OT.

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.

PANDEMIA POR COVID19

La pandemia por coronavirus (SARS-CoV-2) iniciada en 2019-2020 fue reconocida como global el 11 de marzo de 2020 por la Organización Mundial de la Salud (OMS). En respuesta al número creciente de casos de COVID-19, el Gobierno de España declaró el 14 de marzo de 2020 el estado de alarma, lo que conllevó la imposición de una cuarentena nacional como medida de emergencia para reducir el contagio. Esta cuarentena obligó a todos los ciudadanos residentes en España a quedarse en sus residencias habituales, exceptuando diversas situaciones como la adquisición de alimentos o medicinas, acudir al puesto de trabajo en determinados sectores esenciales o atender emergencias.

Esta situación supuso que se implantara el teletrabajo en todos los ámbitos en los que fuese posible, incluida la Administración Pública; un alto porcentaje de empleados pasó a la modalidad de teletrabajo a partir del día 16 de marzo, a la vez que se habilitó la tramitación telemática de determinados servicios ante el cierre de presencial de oficinas. Este hecho provocó un impacto en los servicios tanto de CSIRT-CV como de toda Generalitat que tuvieron que ser adecuados a este nuevo escenario tal y como se explicará en epígrafes posteriores.

HITOS Y SERVICIOS PRESTADOS DURANTE 2020

1 TEST DE INTRUSIÓN

Este servicio proporciona un análisis exhaustivo mediante una serie de pruebas manuales de intrusión, utilizando técnicas exhaustivas de identificación de vulnerabilidades contra aplicaciones y sistemas.

En el transcurso del año, el equipo Red-Team del CSIRT-CV ha realizado 36 test de intrusión, de los que 19 han sido sobre plataformas Web, 15 sobre aplicaciones móviles, 1 sobre redes Wifi y otro sobre un sistema operativo.

Es de interés mencionar que este año se han hecho públicas las vulnerabilidades de tipo XSS descubiertas por el equipo de CSIRT-CV encontradas en el software Tiki-Wiki CMS:


incibe-cert_

Alerta Incidentes

Inicio / Alerta Temprana / Avisos Seguridad / Fallos de Cross Site Scripting (XSS) encontrados en el software Tiki-Wiki CMS

Fallos de Cross Site Scripting (XSS) encontrados en el software Tiki-Wiki CMS

Fecha de publicación: 31/03/2020
Importancia: 3 - Media

Recursos afectados:

Tiki Wiki CMS, versión 20.0 y anteriores.

Descripción:

INCIBE ha coordinado la publicación de una vulnerabilidad en el gestor de contenidos Tiki Wiki, con identificador INCIBE-2020-0134, descubierta por Pablo Sebastián Arias Rodríguez, Rubén Barberà Pérez y Jorge Alberto Palma Reyes de S2Grupo en el CSIRT-CV. Cuenta con un agradecimiento especial al equipo del CSIRT-CV (https://www.csirtcv.gva.es) compuesto por: Lourdes Herrero, Maite Moreno, José Vila, Adrián Antón, Adrián Capdevila, Aurora Villegas, Eva Lleonart, Fernando Cózar, Javier García, Manuel Rosa, Mario Ortiz, Mayte Aranda, Oscar Martínez, Sergio Hernández y Yolanda Olmedo que descubrieron un fallo XSS en el software Tiki-Wiki CMS

Figura 1: Detalle publicación de la vulnerabilidad descubierta en 2020 por CSIRT-CV

2 AUDITORÍAS DE VULNERABILIDADES

Este servicio consiste en la identificación de las vulnerabilidades presentes en los activos del solicitante analizando, gestionando y diseminando la información de la mejor manera posible mediante herramientas automáticas para que las debilidades detectadas sean corregidas antes de ser aprovechadas por un atacante real.

En 2020 se han realizado 119 auditorías de vulnerabilidades entre las habituales/rutinarias y otras ejecutadas bajo demanda. En el siguiente punto se explica un breve resumen de los resultados obtenidos tras las auditorías periódicas realizadas este año.

En estas auditorías se han auditado 34 organismos pertenecientes al ámbito de la Generalitat en el primer semestre del año, y 31 en el segundo.

Respecto a 2019, se puede observar que se ha experimentado un decremento de aproximadamente un 30% en el número de organismos con vulnerabilidades criticas.

3 AUDITORÍA DE SEGURIDAD SEMÁNTICA

Este servicio está centrado en la detección de posibles riesgos reputacionales, legales o técnicos en torno al uso de una marca o persona/s física/s en Internet.

No se han registrado peticiones de este servicio durante este año. Sin embargo, de forma proactiva se ha hecho un gran trabajo a raíz de varias situaciones de interés: campañas de desinformación sobre el coronavirus, uso de la información sobre la pandemia para crear sitios webs maliciosos, orquestación de posibles ciberataques contra el gobierno autonómico, campañas de desinformación relacionadas con la campaña de vacunación, etc.

4 VALIDACIÓN DE CÓDIGO

Este servicio tiene como objetivo hacer una revisión de código y auditar la implementación de la metodología de seguridad en el ciclo de vida del desarrollo de software.

No se han registrado peticiones de este servicio durante 2020, aunque es necesario matizar que en la mayoría de los test de intrusión ejecutados, se realiza una fase de validación del código de la aplicación objeto de análisis.

5 ANÁLISIS FORENSE

Tras un incidente de ciberseguridad, este servicio ofrece un análisis posterior con el objetivo de obtener toda la información pericial necesaria y elaborar un informe que pudiera ser requerido en procesos judiciales llevados a cabo por las autoridades competentes.

El equipo de CSIRT-CV ha realizado 2 análisis forenses durante 2020; uno de ellos derivado de la gestión de un incidente provocado por un grupo APT.

Cabe señalar que la gestión de muchos incidentes de seguridad implícitamente contempla un análisis forense de *logs* y registros que no se ha englobado como tal dentro de este servicio sino que se ha considerado como parte del servicio de Gestión de Incidentes.

6 BASTIONADO DE ENTORNOS

Este servicio proporciona asesoramiento sobre las pautas y directrices adecuadas para fortalecer el entorno propuesto, bien sea de sistemas, redes, aplicaciones o dispositivos. Por ejemplo: protección de una red WiFi, bastionado de un servidor Windows, etc.

Durante este año se ha registrado una solicitud de bastionado, en concreto como ayuda a la estandarización de la información publicada sobre versiones de software y trazas de errores en las aplicaciones.

Cabe destacar que muchas consultas técnicas que se atienden dentro del servicio de Consultoría, van ligadas al bastionado de sistemas o aplicaciones, y no se contabilizan en este servicio. Un ejemplo de ello fue la participación de CSIRT-CV en la securización del despliegue técnico de las infraestructuras TI de los hospitales de campaña, hoteles medicalizados y pabellones que, con motivo de la pandemia por la COVID-19, se pusieron en marcha en la Comunitat; CSIRT-CV aportó una serie de recomendaciones para minimizar el riesgo de estas infraestructuras TI aumentando así

su securización. Y otro las recomendaciones de bastionado derivadas de las gestiones de los incidentes que tampoco se contabilizan en este servicio.

Figura 2: Detalle del interior de un hospital de campaña en la Comunitat Valenciana

7 GESTIÓN DE INCIDENTES

Este servicio proporciona una solución integral a cualquier incidente de seguridad que se pueda producir, incluyendo entre ellos incidentes tales como: intento de fraude electrónico, phishing, compromiso por malware, detección de comportamiento sospechoso en el equipo o en las cuentas digitales, suplantación de identidad, robo de contraseñas, secuestro de información etc.

2020 deja la cifra de 1659 incidentes gestionados, ligeramente superior a los 1422 incidentes del año anterior. Este hecho podría ser debido a la situación de teletrabajo derivada de la pandemia; se observa durante este periodo un aumento de incidentes provocados por incumplimiento de la política corporativa de la Generalitat.

También se observa un aumento significativo de incidentes provocados por Código Dañino, intentos de obtención de información a través de Phishing, y por intrusiones. Esto supone un aumento en la actividad de los ciberdelicuentes sumado al hecho de

que, en los sistemas de detección de intrusos del CSIRT-CV se han incorporado nuevas fuentes de monitorización que ofrecen una mayor capacidad de detección sobre este tipo de incidentes.

En la figura siguiente extraída de HERA, se muestra una evolución temporal de los incidentes gestionados por tipología en los últimos doce meses donde se observa un aumento de los mismos entre los meses de marzo a mayo:

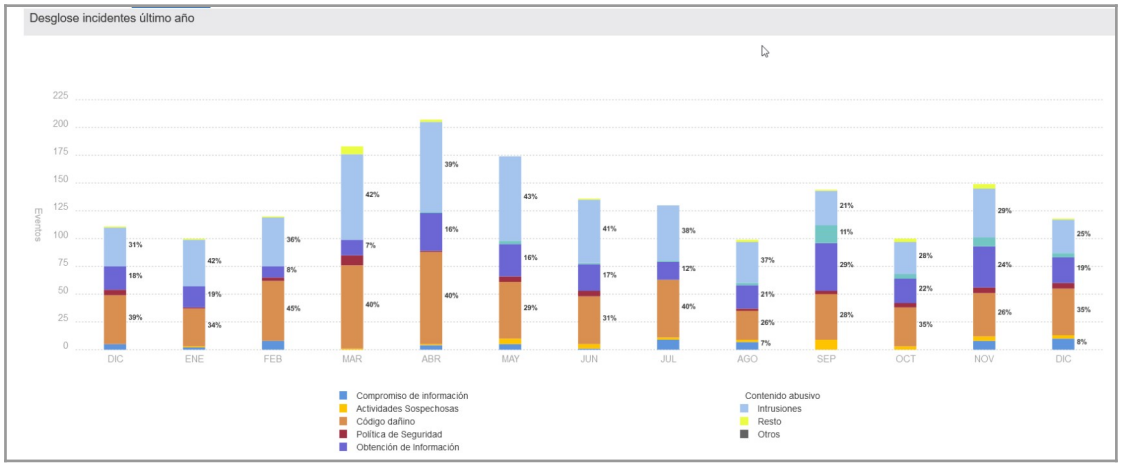


Figura 3: Desglose incidentes gestionados de en los últimos 12 meses por CSIRT-CV (diciembre de 2019 y diciembre de 2020)

Se quiere remarcar en este punto que, a lo largo de este año, se han gestionado varios incidentes relevantes, que se detallaran en los siguientes epígrafes.

8 GIR, GESTIÓN DE CRISIS Y OTROS INCIDENTES RELEVANTES

CSIRT-CV ofrece al resto de Generalitat un grupo de intervención rápida (GIR) ante incidentes de seguridad especialmente relevantes, prestando apoyo técnico y organizativo a Consellerías u otros organismos para, ante cualquier problema, recuperar el servicio interno y para los ciudadanos en el menor tiempo posible

En 2020 se ha activado el GIR en una ocasión, se han gestionado algunos incidentes de seguridad que merecen ser citados por su complejidad e impacto ocasionado y se ha dado respuesta a una situación de crisis excepcional, como es la declarada por la pandemia de la COVID-19:

8.1 GESTIÓN DE CRISIS. PANDEMIA Y TELETRABAJO

Tal y como se ha mencionado, la situación generada por el coronavirus supuso la implantación del teletrabajo de forma inmediata en todos los ámbitos en los que fuese posible; así un alto porcentaje de empleados públicos pasó a la modalidad de teletrabajo.

Para minimizar el impacto en la prestación de los servicios en esta excepcional situación, en la Generalitat, el 12 de marzo se puso en marcha el *"Comité Ejecutivo COVID-19"*. El principal objetivo de este comité fue el de la definición de los escenarios adecuados para posibilitar el teletrabajo a la mayor parte del personal de la Administración Pública.

Desde el mismo día 13 de marzo se suceden varias definiciones técnicas de posibles escenarios de teletrabajo para los que CSIRT-CV presentó una serie de recomendaciones de seguridad. Además, el Centro elaboró dos guías detalladas: una enfocada a los técnicos que tienen que implantar las medidas que se acuerden, y otra para los usuarios que van a teletrabajar, que se enviaron ambas a los interesados tanto del comité técnico como del ejecutivo.

El teletrabajo conlleva riesgos de ciberseguridad en muchos contextos, sobre todo en los casos en los que el teletrabajador hace uso de sus equipos personales y/o se conectan a redes WiFi domésticas. La seguridad del hogar del teletrabajador también influye en la seguridad de la propia red corporativa, tal como se describe en la Guía de Seguridad en el Teletrabajo[3] que publicó CSIRT-CV en 2018, y que fue tomada como referencia por diferentes instituciones como la Consellería de Innovación, Universidades, Ciencia y Sociedad Digital, para divulgar una serie de recomendaciones prácticas, dirigidas a empresas[4], para organizar el teletrabajo.

CSIRT-CV además, puso en marcha una serie de iniciativas internas para incrementar las medidas de seguridad ante el potencial aumento del riesgo derivado del teletrabajo y para fortalecer la vigilancia ante uno de los colectivos más críticos durante la pandemia, el sector salud:

- Se reforzó la vigilancia en dicho sector aumentado la sensibilidad en las sondas de detección de intrusos.

3 Guía de Seguridad en el Teletrabajo https://concienciat.gva.es/wp-content/uploads/2018/03/infor_guia_de_seguridad_en_el_teletrabajo.pdf

4 Guía práctica para organizar el teletrabajo http://innova.gva.es/documents/169273725/169715173/Gu%C3%ADa+pr%C3%A1ctica+para+organizar+el+teletrabajo/5588747e-f7f7-4567-ac62-62f862445e9a

- Se estableció la monitorización de un nuevo servicio de *leaks* de credenciales con el sector salud provisto por el CCN-CERT, que posteriormente se amplió para abarcar la mayoría de los dominios de la Generalitat
- Reforzó la vigilancia en las conexiones VPN
- Se probaron soluciones de *Endpoint* que ofrecieron diferentes fabricantes de forma gratuita, para proteger los equipos de usuario
- Se realizaron acciones informativas y de concienciación en el teletrabajo[5]
- Se realizaron auditorías a varias iniciativas desarrolladas para ofrecer información actualizada sobre la COVID-19 como publicación de nuevos portales y apps

Para hacer frente a la nueva situación -tal y como se ha comentado en puntos anteriores- se pusieron en marcha diferentes Hospitales de Campaña, Hoteles Medicalizados o Pabellones, en los cuales, tras evaluar desde el punto de vista de la ciberseguridad el despliegue técnico de estas infraestructuras TI, se aportó una serie de recomendaciones para minimizar el riesgo de las mismas aumentado su securización.

El teletrabajo ha provocado cambios en la infraestructura tecnológica de Generalitat Valenciana y en la forma en la que ésta presta sus servicios. Es por ello que, desde el punto de vista de la seguridad, se ha adaptado durante esta etapa la ciberdefensa y vigilancia al nuevo modelo que conlleva un tipo de riesgo y amenazas diferentes.

8.2 GIR: APT41

El origen de dicho ataque provenía del grupo APT41, atribuido a China y habitualmente con intereses centrados en el ciberespionaje en el sector financiero, Gobierno, telecomunicaciones, transporte y otros.

El ataque estaba enmarcado en una de las campañas más amplias de los últimos años de este actor chino, englobando a multitud de objetivos por todo el mundo. Sin embargo, se desconoce si APT41 escaneó Internet e intentó la explotación en masa, o seleccionó un subconjunto de organizaciones específicas para atacar.

5 Quédate en casa pero ciberseguro https://concienciat.gva.es/infografias/quedate-en-casa-pero-ciberseguro/

El equipo del CSIRT-CV detectó el incidente y puso en marcha el Grupo de Intervención Rápida, que llevo a cabo la contención y erradicación del incidente.

8.3 COMPROMISO EN AYUNTAMIENTOS

El pasado 5 de agosto CSIRT-CV recibió una notificación de la compañía FireEye indicando que existía una vulnerabilidad en productos utilizados por varios Ayuntamientos por el que presuntamente se habrían robado contraseñas y estaban a la venta en un foro de Rusia.

CSIRT-CV contactó con los ayuntamientos implicados y tras una investigación inicial se concluyó que las credenciales robadas no habían sido sustraídas explotando una vulnerabilidad sino a través de ataques de tipo phishing.

Se solicitó la revisión de conexiones desde direcciones IP anómalas pero no se detectó nada sospechoso excepto los accesos con las cuentas comprometidas y por lo tanto se bloquearon.

8.4 RANSOMWARE EN AYUNTAMIENTOS

Otra amenaza al alza que ha sido observada contra los Ayuntamientos es la distribución de ransomware, siendo las variantes observadas Dharma-Harma, Matrix y BlackHeart. Los dos primeros fueron distribuidos desde los controladores de dominio, previo compromiso de un servidor vulnerable, y el último mediante adjunto de correo o aplicación vulnerable utilizada por el teletrabajo.

CSIRT-V colaboró con los Ayuntamientos en el proceso de recuperación del entorno y vuelta a la normalidad así como en la denuncia a la Guardia Civil.

8.5 FRAUDE AL CEO

Este año, el CSIRT-CV ha gestionado un ingenioso incidente de tipo Fraude del CEO contra uno de los proveedores de la Generalitat.

Este intento de fraude se llevó a cabo en dos pasos, y ambos se realizaron por medio del correo electrónico. En primer lugar, los atacantes se hicieron pasar por la Generalitat para atacar vía phishing a un proveedor, acceder a sus correos, y recabar así información sobre facturas pendientes. En segundo lugar, se hicieron pasar por el proveedor esta vez atacando a la Generalitat, para que pagasen las facturas con parte

de la información real recabada, pero cuyas cuentas bancarias asociadas eran las de los atacantes.

Este fraude se detectó a tiempo y se recomendó su denuncia ante las fuerzas y cuerpos de seguridad.

8.6 CAMPAÑAS DE PHISHING

A lo largo de todo el año CSIRT-CV ha gestionado multitud de campañas masivas de *phishing* en la Generalitat; algunas generalistas, tratando temas como notificaciones de la Dirección General de Tráfico o la Agencia Tributaria y otras, más dirigidas, intentando suplantar el correo de la Generalitat e incluso redactadas en Valenciano.

Además, con la situación de la pandemia, han surgido nuevas campañas de *phishing* relacionadas con esta temática como gancho, en las que se pretende no solo adquirir credenciales de las víctimas sino también propagar malware como *Trickbot* o *Emotet*. No obstante, en la Generalitat no se ha detectado de forma significativa este tipo de campañas, siendo más habituales las mencionadas anteriormente.

El *spam* también es uno de los problemas con el que a diario lidian tanto los usuarios como el equipo de CSIRT-CV, ya que los usuarios no siempre son capaces de distinguir entre un correo *spam* (molesto, pero no dañino) de un correo malicioso (*phishing*, con adjuntos maliciosos, etc.).

8.7 MALWARE DARKGATE Y AUTOIT

En el transcurso del año, el equipo del CSIRT-CV identificó, a través de CARMEN, la presencia de una nueva variante del malware Darkgate; un código dañino con grandes capacidades, como el robo de credenciales, cifrado de contenidos, minería de criptodivisas, así como de técnicas anti-sandbox y evasión de antivirus

A partir de esta investigación, se revisó la existencia de los IOC obtenidos en todo el parque de la Generalitat, obteniéndose otros equipos afectados. Un denominador común era el uso de programas relacionados con la descarga de contenido P2P, como pueden ser BitTorrent, Vuze o Utorrent, entre otros. Se observó que los usuarios que usaban estos programas accedían a páginas “legítimas” –alojadas en España y Francia- para la descarga de series, películas o música. Se comprobó también que algunas de esas descargas no se correspondían con archivos “.torrent”, sino con código malicioso (.vbe - VBScript) que comprometía los equipos.

Como parte de la gestión del incidente, hay que destacar que se crearon reglas de detección *ad-hoc* para el NIDS, así como reglas de bloqueo en el IPS para impedir la descarga de las amenazas asociadas a la ejecución del código VBScript. Al mismo tiempo, se analizaron las categorías de filtrado de URL y se observó que existe una categoría concreta en el Firewall corporativo de la Generalitat, peer-to-peer, que detecta y permite bloquear todos los accesos web a páginas con contenido de descarga P2P. Por ello se solicitó y se bloqueó dicha categoría.

9 AUDITORÍA RGPD

Este servicio se ofrece para dar cumplimiento a la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales.

A pesar de que no se ha realizado ningún servicio como tal, se ha continuado con la revisión de los aspectos contemplados en la nueva Ley que pudieran afectar a CSIRT-CV.

10 ANÁLISIS DE RIESGOS

Este servicio ofrece la realización de un análisis de riesgos mediante la metodología MAGERIT

Durante el año 2020 se han llevado a cabo 2 análisis de riesgos, uno relacionado con el ámbito sanitario y el otro en relación a la auditoria del ENS de otro índole. No obstante, cabe destacar que previamente a la realización de las auditorias del ENS realizadas a las aplicaciones que se comentan en el siguiente apartado, se hace un pequeño análisis de riesgos, utilizando la metodología Magerit, que sirve de base para la evaluación de la seguridad de dichas aplicaciones.

11 AUDITORÍA ENS

Consta de una auditoría diferencial sobre el grado de cumplimiento del Esquema Nacional de Seguridad

Durante 2020, se ha auditado el cumplimiento ENS de algunas aplicaciones y servicios para diferentes organismos cuyos detalles son confidenciales.

12 CONSULTORÍA ISO 27001

Este servicio tiene como finalidad orientar para planificar una estrategia de mejora de la seguridad en base a una norma de referencia como es la ISO 27001:2013.

Durante 2020 se ha dado apoyo a un organismo interno de la Generalitat que utiliza esta norma como base para su SGSI.

13 CONSULTORÍA GENERAL

Este servicio ofrece soporte especializado ante cualquier consulta en las diferentes vertientes de la seguridad de la información: técnica, organizativa y legal.

Durante este año se han atendido 204 consultas de diferente índole relacionadas con la ciberseguridad, cifra significativa si se tiene en cuenta que en 2019 se atendieron 160 consultas. La mayoría de las consultas están relacionadas con los informes diarios que se emiten a las Consellerías y Organismos pero también se tratan temas como:

- Consejos sobre seguridad en navegadores Web y otras herramientas
- Formación para ciudadanos
- Certificados digitales
- Correos phishings
- Leaks de información

Cabe mencionar que cerca del 7% de dichas consultas provienen de ciudadanos.

14 PLAN VALENCIANO DE CAPACITACIÓN

Este servicio ofrece acciones formativas y de concienciación en ciberseguridad que puedan resultar de relevancia para el solicitante. Las acciones pueden ser cursos on-line o presenciales, jornadas, video-tutoriales, guías específicas, etc.

Para abordar el PVC de la mejor forma posible, se ha definido un calendario donde se contemplan acciones concretas de formación y capacitación en materia de ciberseguridad dirigidas a los diferentes colectivos identificados: **ciudadanos**, **GVA y organismos, empresas (PYMEs)**, **otras administraciones (**Ayuntamientos etc.**)**

Para realizar dichas acciones se han utilizado diferentes formatos y canales de comunicación: sesiones de concienciación, ponencias, publicaciones diarias en los portales de CSIRT-CV, jornadas en institutos, publicaciones en las RRSS del Centro (Facebook, Twitter), boletines de seguridad para suscriptores, correos, infografías, cartelería, folletos, campañas de concienciación, etc.

Las principales acciones del Plan Valenciano de Capacitación en 2020 se resumen a continuación:

14.1 INFORMES PUBLICADOS

Durante 2020 CSIRT-CV ha publicado su informe de actividad correspondiente al año 2019 en el portal principal, un análisis sobre el malware Emotet y también se han actualizado las guías de "Uso seguro de Android" y "Uso seguro de iOS" en el portal de concienciaT para su descarga.

Además en el segundo semestre se publicaron 2 informes más, el Informe de actividad del semestre 1 de 2020 y el informe de Análisis de Campaña Emotet, en el que se analizaba una de las muestras recibidas en GVA, y se daba a conocer cómo funciona internamente la amenaza.

Este año, el material publicado por CSIRT-CV en sus principales portales ha sumado mas de 52.000 descargas.

14.2 CAMPAÑAS DE CONCIENCIACIÓN

En 2020, CSIRT-CV ha lanzado cuatro campañas de concienciación (+1 especial) en las redes sociales en las que está presente, así como en el portal concienciaT:

- Campaña “Siete errores de ciberseguridad que no deberías cometer”. El objetivo de la campaña es, que a través de 7 errores que habitualmente se cometen al navegar por Internet, los usuarios entiendan los riesgos a que se someten y mejoren sus hábitos digitales.
- Campaña “Stop Fake News”. Relanzando de nuevo ésta campaña se pretendió ayudar a los ciudadanos a identificar noticias falsas con unos sencillos consejos.
- Campaña “Ciber-vuelta al cole: no te la dejes para septiembre”. Durante la pandemia por COVID-19 los niños han intensificado su contacto con la tecnología y dispositivos de casa. Muchos de ellos han adoptado nuevas

costumbres que a veces no son todo lo ciberseguras que deberían ser. Por este motivo y con el objetivo de que los menores se muevan por la Red con todas las garantías de seguridad, CSIRT-CV a través de esta campaña emite algunas recomendaciones tanto para ellos como para sus familias.

- Campaña especial “Mes Europeo de la Ciberseguridad”. Durante el mes de octubre se celebró esta campaña anual organizada por la Unión Europea, con el fin de promover la ciberseguridad entre los ciudadanos y las organizaciones.
- Campaña “Nuestros mayores seguros en la Red”. Una serie de consejos dirigidos a las personas mayores y su entorno cercano, con el propósito de concienciar sobre los riesgos y amenazas existentes en Internet, así como buenas prácticas aplicables en el uso de tecnologías y dispositivos móviles.

Figura 4: Detalle imagen utilizada para la campaña de concienciación "Ciber-Vuelta al cole"

14.3 SAPS: formación online a ciudadanos

Durante este año, en la plataforma SAPS se han formado 3905 alumnos en los cursos de CSIRT-CV. Además se han incorporado dos nuevos cursos, “Instalación y guía de uso de Wireshark”, y “Reglamento General de Protección de Datos (RGPD)” pasando a ser 19 los cursos que CSIRT-CV ofrece en su catálogo.

Los cursos que mas alumnos han tenido este año han sido el de “RGPD” con 324 alumnos, “Introducción a la seguridad informática” con 283 alumnos y el de “Navegación Segura” con 265 alumnos.

Dada la situación de confinamiento por la COVID-19, se aumentó el número de plazas por cada curso, llegando a las 1.500 disponibles en cada edición. En 2020, se han impartido dos ediciones semestrales, como viene siendo habitual. Destaca también la actualización continua de sus contenidos.

14.4 PLAN DE CAPACITACIÓN EN CIBERSEGURIDAD PARA EMPRESAS

El pasado mes de febrero, la Dirección de CSIRT-CV presentó el "Plan de capacitación en ciberseguridad para empresas" en una jornada sobre Prevención del Delito en el Sector Público Instrumental. Ese mismo día se publicaba en concienciaT un nuevo espacio denominado "Empresas" que permite el acceso a los contenidos del plan de capacitación.

Figura 5: Detalle promoción Plan de Ciberseguridad para empresas en la Comunitat Valenciana

La finalidad es ayudar a las empresas a mejorar su nivel de madurez en ciberseguridad y su confianza en el uso de la tecnología. Para conseguirlo, se ofrece formación y capacitación tanto a directivos como al resto de empleados, puesto que es necesario implicar a las personas para que el factor humano se convierta en uno de los pilares de la ciberseguridad de la organización.

Forma parte de este Plan de Ciberseguridad para Empresas, la herramienta Avalua'T que pretende ayudar a las empresas a autoevaluar el nivel de seguridad de sus sistemas y obtener una primera aproximación sobre los niveles de riesgo a los que se enfrenta su organización, atendiendo a su tecnología, sus procesos y sus empleados.

Además, esta herramienta ofrece una relación de aquellos aspectos a mejorar, por lo que servirá tanto para la evolución como para la mejora continua en ciberseguridad.

También forman parte de este Plan de Ciberseguridad para Empresas, diferentes cursos online y videos interactivos.

Figura 6: Detalle espacio "Empresas" del portal concienciaT

14.5 JORNADAS DE CIBERSEGURIDAD EN CENTROS DE SECUNDARIA

Antes de que se declarara el estado de alarma a mediados de marzo, CSIRT-CV pudo visitar 28 centros de secundaria de la Comunidad Valenciana para realizar las Jornadas de Concienciación en Ciberseguridad con los alumnos de 2º de ESO, padres y docentes. En octubre se retomó la actividad de nuestras jornadas en los centros educativos y en total se visitaron 41 centros en 2020.

Este año se han formado 4394 personas (3420 alumnos, 479 padres y 495 docentes) en estas jornadas, que desafortunadamente tuvieron que ser canceladas durante varios meses por la situación derivada de la pandemia.

14.6 MATERIAL GRÁFICO

Figura 7: Detalle infografía publicada en 2020

Este año se han publicado dos nuevas infografías en el portal de concienciaT. Por un lado, la correspondiente al "Día de Internet Segura" en formato PDF interactivo, para conocer y acceder a todos los contenidos ofrecidos en concienciaT. Y otra relacionada con la repentina situación de teletrabajo global a causa de la COVID-19, "Quédate en casa, pero ciberseguro".

Además, se han re-publicado otras infografías asociadas a distintos días señalados, así como la adaptación de cuatro de ellas enfocadas al ámbito de la Generalitat Valenciana.

14.7 PORTALES PRINCIPALES Y REDES SOCIALES

El portal principal de CSIRT-CV (www.csirtcv.gva.es) a finales de año renovó su imagen y diseño consiguiendo una navegación más cómoda e intuitiva, adaptada a los principales dispositivos móviles.

Una de las principales novedades de la nueva web, en cuanto a contenidos se refiere, es la sustitución de la antigua sección de noticias generalistas sobre ciberseguridad, por la incorporación de nuevos elementos gráficos para la publicación de las vulnerabilidades y alertas más relevantes en materia de seguridad.

La web del Centro incluye enlaces a servicios y herramientas específicas de CSIRT-CV, además de a otras páginas web con objetivos relacionados.

Con este cambio, se persigue la especialización técnica del portal, así como dotar de mayor prioridad y visibilidad a los avisos de seguridad más críticos, delegando la actualidad informativa en sus redes sociales Facebook y Twitter, así como en su otro portal web dedicado a la concienciación en ciberseguridad.

Figura 8: Aspecto de la nueva web de CSIRT-CV

Por otro lado, concienciaT es el portal más joven de CSIRT-CV (www.concienciat.gva.es). Ha tenido 22.063 visitas y, a pesar de ser un sitio de reciente creación, desde CSIRT-CV se está fomentando mucho su uso y la creación de nuevos contenidos, como los de la sección de "¿Sabías que…?", donde se publican todo tipo de consejos y posts sobre diferentes temáticas relacionadas, como siempre, con la ciberseguridad a nivel de los ciudadanos.

Figura 9: Detalle sección "¿Sabías que...?" del portal concienciaT

Respecto a redes sociales, CSIRT-CV cuenta en Facebook con 2.228 seguidores y cerca de 6.200 en Twitter.

15 DETECCIÓN DE INTRUSOS

Este servicio detecta los intentos de intrusión o incidentes que afecten a equipos y servicios del dominio protegible de la Generalitat.

15.1 FUENTES INTEGRADAS Y MEJORAS EN EL SIEM

Este año se ha ampliado la capacidad del SIEM para poder soportar las nuevas fuentes que se han integrado y las que se planea integrar en el futuro.

Además se han hecho una serie de mejoras significativas en el SIEM, sobre todo en el motor de correlación avanzada permitiendo por ejemplo aplicar excepciones mas precisas en ciertas reglas, mejorar la visualización del contenido de las alertas procedentes de determinadas fuentes, añadir campos para valores adicionales que permitan aumentar el nivel de complejidad de las reglas de correlación, etc.

También se ha iniciado un proceso de normalización e integración de las distintas fuentes de datos que nos permitirá en 2021 dotar de mayor potencia y flexibilidad a nuestro sistema de correlación.

Mencionar por último que se ha hecho un esfuerzo en poner en marcha el SIEM para el vSOC destinado a la mejora de la ciberseguridad de los ayuntamientos valencianos y en definir sus fuentes de datos, tanto a nivel de aplicaciones gestionadas por la Diputación como a nivel del propio ayuntamiento, y empezar a trabajar en su integración y correlación. La puesta en marcha de este servicio terminará en el segundo trimestre de 2021.

16 TENDENCIAS EN CIBERATAQUES

Con la llegada del confinamiento y del teletrabajo en muchos ámbitos, incluido el de la Generalitat Valenciana, las ciberamenazas han cambiado, centrándose en la explotación de nuevos puntos de entrada en las comunicaciones de las organizaciones (concentradores VPN, servicios en la nube, etc.) y en el aprovechamiento de los fallos de seguridad de los equipos y/o redes domésticas usados para el teletrabajo.

El principal ciberataque gestionado, por su relevancia durante este año, fue el relativo al compromiso de un servidor por una amenaza persistente avanzada. Este incidente destaca por la sofisticación del ataque, ya que sucedió a los pocos días del

descubrimiento de una vulnerabilidad de tipo 0-day que residía en el software MDM, y que fue explotada satisfactoriamente, consiguiendo así los atacantes penetrar en el sistema y adquiriendo, además, la capacidad de persistencia. La investigación sobre el incidente apuntó como posible autor a APT41, grupo de ciberespionaje avanzado de origen chino.

Se ha detectado un aumento significativo de reportes de incidentes provenientes de Ayuntamientos por distintos tipos de ransomware y compromiso de sistemas de acceso perimental, que se han usado más este año para que los usuarios pudieran acceder a sus equipos debido al teletrabajo. Esto pone de manifiesto la necesidad incrementar la protección sobre los Ayuntamientos y, en esta línea mencionar que este 2020 ha arrancado el proyecto vSOC por parte de CSIRT-CV y CCN-CERT, que dotará de una capa de seguridad extra sobre los Ayuntamientos de la Comunitat Valenciana que mejorará la capacidad de detección temprana de incidentes de seguridad en sus redes.

Los gestores de contenido (CMS) también han sido un objetivo elegido por los atacantes en numerosas ocasiones debido a su extendido uso dentro de la Generalitat Valenciana, y a la falta de actualizaciones de seguridad en más de una ocasión.

Entre las vulnerabilidades Web que más se han intentado aprovechar este año, predominan las relacionadas con la ejecución de código remoto sobre dispositivos domésticos, sobresaliendo los del fabricante Draytek. Es destacable también el continuado intento de explotación de vulnerabilidades, antiguas o recientes, relacionadas con bases de datos Oracle o MySQL.

Respecto a los ataques de denegación de servicio, se recibieron 18. Dos de estos ataques tuvieron afectación puntual de unos pocos minutos sobre elementos del perímetro de la red corporativa encargados de repartir las peticiones entrantes, aunque no sobre los propios servidores atacados.

Cabe también destacar el incremento y diversidad de ataques de ingeniería social detectados. Se recibieron numerosos phishings suplantando instituciones estatales como la DGT o la Agencia Tributaria, Correos o incluso la propia Generalitat Valenciana, haciendo uso de sus imágenes corporativas. Además, se han producido varios intentos del Fraude del CEO que finalmente no fueron exitosos.

En cuanto a la procedencia de los ciberataques por países, se ha identificado como los cinco principales a los Estados Unidos, España, Países Bajos, Rusia y China, seguidos por Alemania y Gran Bretaña. Es importante recordar que la geolocalización

desde la que se recibe el ataque no necesariamente corresponde con el origen del atacante, y que en la atribución a esos cinco países influye también el hecho de que en los mismos se concentre un mayor volumen de equipos y de servicios, por lo que existe una también mayor probabilidad de recibir ataques desde allí.

Es relevante mencionar el aumento de los incidentes en el sector salud. Esto se debe a dos motivos: el primero corresponde a la mejora de los sistemas de detección con la incorporación de una sonda IDS dedicada en la Consellería de Sanitat. El segundo refleja la tendencia observada a nivel mundial[6] de atacar a los activos sanitarios, ya que actualmente son uno de los objetivos más valiosos.

17 DETECCIÓN DE APT

El servicio de detección de Amenazas Persistentes Avanzadas se gestiona mediante la herramienta CARMEN desarrollada por el CCN y S2Grupo. La herramienta ha sido actualizada a su última versión y los analistas de CARMEN del CSIRT-CV asisten de manera periódica a formación especializada para explotar dicha herramienta con la mayor eficacia.

Se ha analizado el tráfico capturado por la sonda CARMEN haciendo uso de cuatro premisas:

1. Pautas que indiquen malware (anomalías).
2. Visitas de dominios incluidos en una lista negra o *blacklist* y dominios dinámicos.
3. Webs que contengan la cadena "GVA" y dominios sospechosos (.su, .ru,pw, xyz...)
4. Patrones típicos de *ramsomware, dridex, exploits* y otras amenazas conocidas.

Este año se ha reportado un total de 19 incidentes originados detectados vía "Threat Hunting" en CARMEN , la mayoría de criticidad MEDIA.

Mencionar que la capacidad de detección de Carmen ha aumentado, ya que se está desplegando Claudia, el endpoint de Carmen.

6 https://securityboulevard.com/2020/05/healthcare-cyberattacks-increasing-during-covid-19/

18 INFORMES Y ALERTAS. OBSERVATORIO

CSIRT-CV, en su función de Centro de Alerta Temprana, elabora una serie de informes sobre tendencias en seguridad y otros aspectos de interés para su ámbito entre los que destacan boletines de alerta puntuales, boletines públicos de seguridad quincenal, emisión diaria de informes personalizados a cada organismo o informes sobre malware.

Este año CSIRT-CV ha enviado un total 26 boletines quincenales y 47 boletines de alertas – la mayoría internos- cifra significativa, ya que supera los 19 boletines que se enviaron a lo largo de todo el 2019.

18.1 OBSERVATORIO DE SEGURIDAD

Además de lo ya indicado referente a los nuevos vectores de ataque derivados de la pandemia, cabe destacar que los ataques por ransomware evolucionan y se sofistican haciéndose más dirigidos y con la finalidad de obtener el mayor impacto posible. Los atacantes eligen cuál es el mejor momento para lanzar cada una de las fases del ataque, especialmente en la distribución del ransomware (*Human-operated ransomware*).

La situación geopolítica de los últimos años marca la tendencia creciente al ciberespionaje, una amenaza que confirma el interés de los atacantes por obtener información sensible de sus víctimas. Estos agentes están creando nuevas Tácticas, Técnicas y Procedimientos para intentar robar la propiedad intelectual de sus objetivos. El incremento de estas nuevas técnicas como *Living off the Land* o *fileless malware* dificultan la detección de las amenazas. Es fundamental, por tanto, ampliar la monitorización a los clientes finales y ser capaces de modelar su comportamiento para detectar posibles anomalías. Herramientas como CLAUDIA (agente *endpoint* de CARMEN) permiten detectar este tipo de situaciones, y en la Generalitat ya se está probando en diferentes entornos.

Mencionar por último que desde el mes de marzo se encuentran en curso multitud de campañas de desinformación en todo el mundo acerca de la COVID-19 y la pandemia global centradas en la publicación de contenido falso o distorsionado sobre diferentes narrativas: COVID-19 como arma biológica, xenofobia, control social, desconfianza en las instituciones, nuevo orden mundial, impacto económico, estadísticas falsas o

engañosas, orígenes y propagación del coronavirus, politización etc. Para el 2021 se prevé este tipo de narrativas en relación a la vacuna de la COVID-19 y el proceso de vacunación, por tanto, es preciso establecer un aumento de la vigilancia digital sobre esta nueva temática para detectar cualquier tipo de amenaza al respecto sobre nuestro ámbito.

19 CIBERSEGURIDAD INDUSTRIAL

Este servicio busca mejorar el nivel de ciberseguridad industrial de los sistemas SCADA gestionados por organismos de la Generalitat y las II.CC. De la Comunitat Valenciana.

Este año se han continuado monitorizando alertas contra dispositivos IoT, OT en Generalitat así como emitiendo los avisos pertinentes a través de boletines de alertas cuando se ha publicando una vulnerabilidad que afecte a este tipo de dispositivos.

Mencionar en este punto que, tal y como se ha mencionado anteriormente, CSIRT-CV participó en las recomendaciones de seguridad emitidas para el proyecto tecnológico que implicó el despliegue de los hospitales de campaña en la Comunitat. En dicho proyecto tecnológico se contemplaban diferentes tecnologías OT -además de IT- como un sistema de cámaras de video multiservicio, infraestructura para el alojamiento de equipamiento y alimentación ininterrumpida, sistema de llamada enfermería-paciente, sistema de megafonía IP y sistema radio PMR.

20 SISTEMAS DE DECEPCIÓN

Este servicio busca la detección temprana de intrusiones, la implementación de mecanismos de distracción y retraso para posibles atacantes, análisis de tendencias y mejora de los mecanismos defensivos a partir de la información recopilada.

La nueva plataforma de *deception* de CSIRT-CV ha sido desplegada. Hasta el momento, se ha definido que información es la más importante obtener y como procesarla y también se ha automatizado el proceso de adquisición de datos y generación de inteligencia. A lo largo de 2020 se ha trabajado en un informe para presentar públicamente los resultados de la Honey y actualmente está en proceso de finalización.

Figura 10: Dashboard Honeynet CSIRT-CV

21 I+D+i

Durante 2020 el equipo del centro ha participado en diferentes proyectos internos de investigación con el objetivo de mejorar nuestros servicios. Se destacan los siguientes:

- Mejoras en el servicio de correlación avanzada con el desarrollo de un piloto de correlador multifuente basado en programación orientada a objetos que aporta mayor flexibilidad en la integración de fuentes y diseño de reglas de correlación así como en el diseño de excepciones
- Investigación herramientas de detección y mitigación de *leaks* públicos
- Investigación del herramientas de Seguridad Semántica.

22 INTERCAMBIO DE INFORMACIÓN

Servicio intercambio de información relativa a ciberseguridad tanto en la Generalitat Valenciana como en empresas de la Comunidad

Entre los organismos que más información se intercambia está el CCN-CERT a través de LUCIA para el intercambio de información sobre incidentes de seguridad y también S2 Grupo – CERT con el que de forma periódica intercambiamos IOC y analizadores para CARMEN. Además este año se ha incrementado el intercambio de información a través del foro CSIRT.es sobre todo a través de la aplicación interna de mensajería desplegada por el CCN-CERT o la lista de correo del propio foro.

23 LABORATORIO DE MALWARE

Se dispone de un laboratorio de malware donde el equipo técnico de CSIRT-CV puede analizar artefactos para medir de un modo preciso el impacto y consecuencias reales de posibles códigos maliciosos en los activos de la Generalitat y de este modo diseñar las medidas de contención y erradicación más adecuadas en cada caso.

Este servicio vio incrementadas sus capacidades notablemente el pasado 2018 con el despliegue de un laboratorio físico y una Sandbox. Durante 2019 se ha continuado el trabajo de automatización y extracción de inteligencia y en 2020 ha alcanzado su estabilidad como servicio con una mayor capacidad de procesado y automatización de datos.

23.1 TENDENCIAS DE MALWARE

El estudio de los resultados obtenidos por el laboratorio de malware proporciona al equipo de seguridad, las nuevas tendencias empleadas por los ciberatacantes, como:

- Nuevas vulnerabilidades que están siendo aprovechadas.
- Nuevos formatos de fichero para la distribución de malware.
- Mejoras en los mecanismos de detección y categorización de amenazas.
- Nuevas técnicas de detección de las amenazas siendo analizadas.
- Reglas de detección de infecciones analizadas por el laboratorio.

En el transcurso del año 2020, el laboratorio ha analizado 2698 archivos, la mayoría provenientes de la plataforma de antivirus corporativo.

De los 2698 ficheros analizados, 1842 archivos han sido detectados como maliciosos y categorizados dependiendo de la funcionalidad de cada uno. En la siguiente tabla se puede comparar la cantidad de programas maliciosos detectados por tipología:

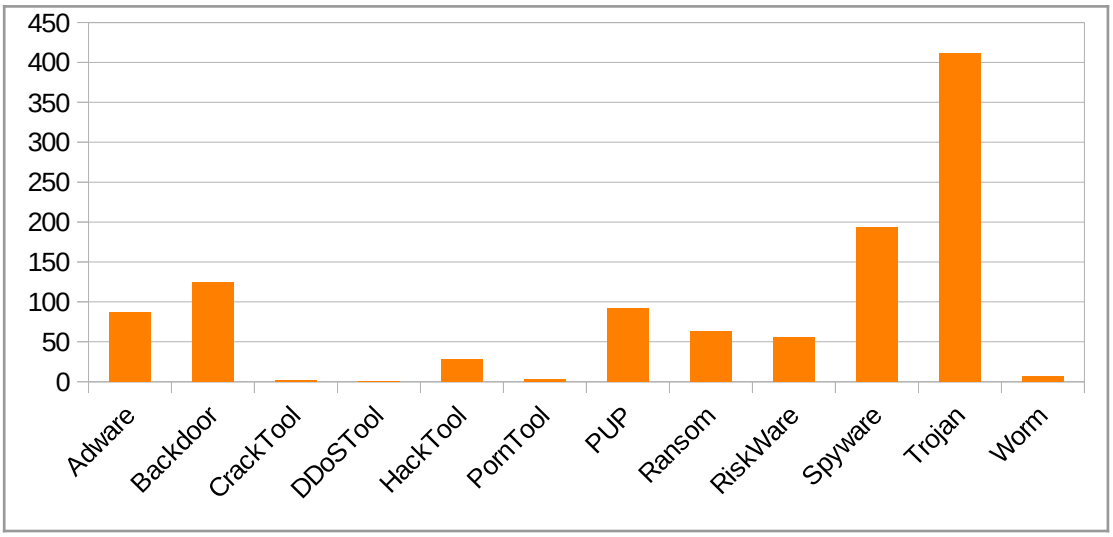


Figure 10: Cantidad de programas maliciosos detectados por tipo.

En la mayoría de estos ficheros analizados, se han encontrado capacidades de tipo *stealer*, las cuales buscan robar credenciales de aplicaciones instaladas en el equipo (clientes FTP, correo, conexiones remotas, etc.), credenciales almacenadas por los diferentes navegadores y captura de credenciales introducidas por el usuario en formularios web.

Durante la segunda mitad del año 2020 se ha visto incrementada la cantidad de programas maliciosos de tipo *downloader* como primer *stage* de infección, principalmente debido a las nuevas campañas de **Emotet** que han estado muy activas en esta segunda mitad del año. Estos *downloaders* normalmente son descargados al abrir un documento con macros maliciosas que descargan el ejecutable desde un sitio web al equipo y lo ejecutan en local. El ejecutable se ocupa de recoger información genérica del equipo y enviarla a un servidor *C2C*, el cual revisa la información del equipo y despliega nuevas capacidades del programa malicioso.

Debido a estas campañas mencionadas de Emotet, los formatos y extensiones de los documentos analizados suelen ser en su mayoría ficheros ofimáticos, actuando cómo primer paso en la infección de equipos, y ficheros ejecutables PE (Portable Ejecutable) principalmente comprimidos de forma que se dificulte su detección.

Si durante el pasado año, la técnica más común de infección fue el uso de ficheros ofimáticos que explotan vulnerabilidades de versiones antiguas de las herramientas de Microsoft Office, que permitían la ejecución del código malicioso al abrir el documento, este 2020 la técnica más utilizada ha sido la de utilizar macros que necesitan de la acción del usuario para activarlas y ejecutarlas, comenzando así la infección del sistema.

Respecto a los ficheros ejecutables recibidos tanto en correos de phishing, cómo los descargados por los documentos infectados, se ha detectado una gran cantidad de código maliciosos con capacidad de monitorización de equipos y *stealers* de credenciales como pueden ser Emotet (mencionado anteriormente) o Agent Tesla, los cuales tienen el objetivo de robar usuarios y contraseñas de los equipos que infectan mediante robo de archivos y capacidades de *keylogging*.

En la gráfica a continuación, se puede comprobar que los ficheros de tipo ofimáticos y ejecutables para Windows, son los más usados a la hora de distribuir código malicioso.

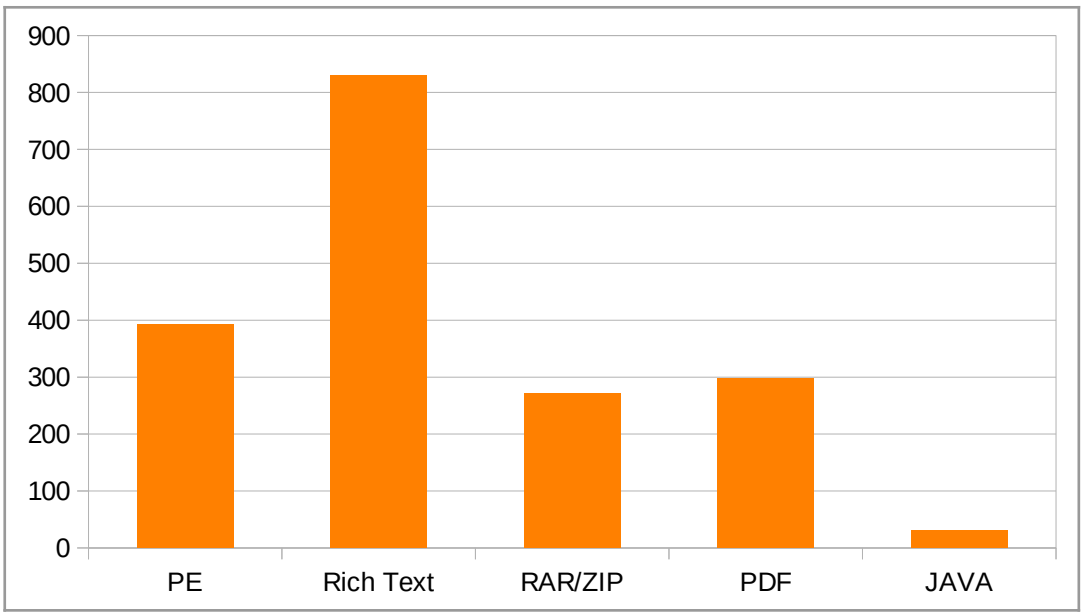


Figure 11: Cantidad de tipos de ficheros analizados.

Por otro lado, en los incidentes de tipo *phishing* o relacionados con el correo electrónico, gestionados por el equipo de CSIRT-CV, se ha detectado una gran cantidad de ficheros PDF tratando de engañar al usuario que lo recibe para navegar a diferentes URL maliciosas, evitando así que las direcciones del *phishing* puedan ser analizadas en el contenido del correo electrónico por los sistemas antispam, dificultando su detección. Por esta razón, los ficheros de tipo PDF son también uno de los ficheros más detectados como vía de entrada de malware.

A grandes rasgos, si se analiza la cantidad de ficheros detectados por tipo, se puede comprobar que las tendencias empleadas por los atacantes denotan el uso de diferentes técnicas, siendo la principal el **correo,** cómo punto de entrada en la organización. Si bien en 2019 los documentos ofimáticos eran la principal vía de entrada de malware, en 2020 se añade a esa técnica ficheros PDF y ejecutables comprimidos que engañan al usuario para navegar o ejecutar creyendo que se tratan de correos legítimos.

Respecto a las capacidades de detección y análisis de ficheros maliciosos, durante 2020, se ha dedicado un gran esfuerzo en la optimización de herramientas automatizadas de análisis dinámico y en la integración con el resto de herramientas del parque; el despliegue de la nueva sandbox ha permitido detectar y comparar a nivel técnico las nuevas campañas que han aparecido durante el año, generando reglas propias para categorizar nuevas campañas de malware recién distribuidas con técnicas que el resto de servicios públicos no detectaban en el momento.

24 MONITORIZACIÓN DE SERVICIOS WEB

Este servicio ofrece respuesta en tiempo real ante cualquier tipo de manipulación ilícita a los servicios web de la Generalitat.

Este monitoriza los principales sitios web de la Generalitat, tanto por alcance de los mismos, como por su criticidad. Dada la naturaleza de la información de este servicio, no se ofrecen más detalles públicamente.

25 PROMOCIÓN DEL CENTRO Y PLAN DE COMUNICACIÓN

Servicio enfocado a la comunicación y conocimiento de la actividad de CSIRT-CV a diferentes colectivos de la Comunidad Valenciana para fomentar un cambio de hábito general en la sociedad valenciana en pro de una mejora de la seguridad global de la ciudadanía.

Este servicio se ha desarrollado en 2020 -aunque con ciertas limitaciones por la pandemia- a través de diferentes acciones, que se enumeran a continuación.

25.1 EVENTOS Y JORNADAS

CSIRT-CV ha participado como ponente en 2020 en los siguientes eventos:

- Durante una jornada de prevención del ciberdelito, se presenta el plan de empresas de CSIRT-CV ante el sector público instrumental (Febrero, 2020)
- Entrevista en el programa La Ventana CV, de Radio Valencia SER a Lourdes Herrero, Directora del CSIRT-CV[7] (Marzo, 2020)
- Participación de Lourdes Herrero en la mesa redonda de FestinFor de la UPV "Seguridad de los datos a partir de la COVID19" (Mayo, 2020). El alcance del evento según los datos de audiencia es de unas 1000 personas.
- Participación en un programa de La SER por parte de Lourdes Herrero para hablar sobre ciberataques durante la pandemia (Mayo, 2020)
- Participación en el programa de radio "Al ras" de Á punt para hablar sobre la campaña de concienciación "Cibervuelta al cole: no te la dejes para septiembre"
- El 30 de septiembre, dentro del curso sobre Administración electrónica: Problemas, dificultades y retos del ADEIT, Lourdes Herrero interviene imparte la ponencia "CSIRT-CV: Un centro pionero en Ciberseguridad para todos los valencianos".
- El lunes 30 de noviembre, CSIRT-CV participó en las XIV Jornadas CCN-CERT. Durante la presentación, se expusieron las recomendaciones de seguridad que deberían afrontar las infraestructuras TIC de emergencia, como

7 https://twitter.com/radiovalencia/status/1235287567194566656

pueden ser hoteles medicalizados u hospitales de campaña que tan en boca de todos han estado durante la pandemia del COVID-19.

- Con motivo del X aniversario de Andalucía CERT, la directora del centro interviene en la mesa redonda de CERTs autonómicos el 16 de Diciembre.
- Por último, la cadena Ser emite una entrevista a Lourdes Herrero en la que se explica como la ciberseguridad se ha visto afectada por la pandemia , y como los ciberdelincuentes han aprovechado la situación de emergencia y la vulnerabilidad de los equipos personales usados durante el teletrabajo para aumentar sus ataques a empresas y administraciones.

CERTIFICACIÓN 27001

Como en años anteriores, tras la auditoría por parte de AENOR este año, CSIRT-CV de nuevo ha mantenido la certificación ISO 27001.

PRESENCIA EN MEDIOS

Tal y como se ha comentado anteriormente CSIRT-CV ha estado presente en varios programas de radio (Radio Valencia SER, Á punt) a lo largo del primer semestre del año, participando tanto en formato entrevista a la Directora del centro como en formato mesa redonda.

Varios medios se hicieron eco de la presentación oficial del Plan de ciberseguridad para empresas como Valencia Plaza, El Mundo o Las Provincias. Por supuesto, la DGTIC también en el espacio de noticias de su página principal:

- Valencia Plaza
- El Mundo
- Las Provincias
- DGTIC

El Director General de la DGTIC se reunió a finales de febrero con representantes de las diputaciones y la Federación Valenciana de Municipios y Provincias. Allí destacó la importancia de trabajar en ciberseguridad, aprovechando todo el camino recorrido por el Centro de Seguridad TIC de la Generalitat (CSIRT-CV) y el trabajo realizado con la Diputación de Valencia, con la que se ha iniciado un proyecto piloto que persigue mejorar la ciberseguridad en las entidades locales y ayudar a los ayuntamientos en el cumplimiento del Esquema Nacional de Seguridad (ENS), en especial en materia de concienciación y de vigilancia de la seguridad de su infraestructura TIC, así como de recolección, análisis y almacenamiento de registros y actividad de su red y activos críticos.

García Duarte incidió en la importancia de replicar y extender buenas prácticas y proyectos exitosos al resto del territorio valenciano, aprovechando aquella innovación y experimentación que se desarrolla en cualquier punto de la Comunitat Valenciana.

Desde la Diputación de Valencia se ha asegurado que este proyecto piloto podría ser una línea de trabajo muy importante. Varios medidos locales se hicieron eco de esta esta noticia.

Lourdes Herrero también fue entrevistada por el Diario Información de Alicante para un reportaje que se publicó en mayo sobre ciberdelitos.

Las campañas de concienciación, como es habitual, también tienen mucha repercusión en prensa. Por ejemplo, durante el mes de Julio la campaña de Cibervuelta al cole estuvo presente en diferentes medios:

- Generalitat Valenciana I
- Generalitat Valenciana II
- La Vanguardia
- Castellón información

También durante ese mes, varios medios se hacen eco de la firma del convenio de colaboración con CCN-CERT.

- Generalitat Valenciana
- Valencia News

En septiembre a raíz de la presentación del proyecto del Vsoc, varios medios se hicieron eco de la presentación del proyecto.

- Economia3
- NoticiasDe
- Valencia Plaza
- La Vanguardia
- El periodico de aquí

En octubre se publica en varios medios la presentación del portal de CSIRT-CV

- Generalitat Valenciana
- DGTIC
- El Periodic

Para cerrar el año, los medios de comunicación se hacen eco de la campaña “Nuestros mayores seguros en la Red”

- Cope
- La Vanguardia
- Noticiasde

A continuación se muestran una serie de capturas de pantalla que reflejan la difusión en la red social Twitter de la presencia en medios de CSIRT-CV así como en prensa:


GVA Hisenda
@GVAhisenda
@GVAhisenda a través del @CSIRTCV pone en marcha la campaña 'Ciber-vuelta al cole. No te la dejes para septiembre', dirigida a niños y adolescentes para fomentar un uso seguro y responsable de la red
Nota de prensa: bit.ly/3ickx1E
CSIRT-CV
Centre Seguretat TIC de la Comunitat Valenciana
#MenoresEnLaRed
ACOMPAÑA A TUS HIJ@S EN LA RED


Sofia Belles @sofia_belles · 19 feb.
Empezamos el día, visita al #CPD y #CSIRT de la #GVA con alumnos de FPB del @iespuzol @GVAeducacio @GVAadcv @GVAhisenda @CSIRTCV
2
11


CSIRT-CV
@CSIRTCV
Hoy finaliza la campaña de CSIRT-CV "Nuestros mayores seguros en la Red". Os animamos a que todos juntos aprendáis a manejar los dispositivos de forma segura.
Recordad que CSIRT-CV os ayuda en vuestro día a día: concienciat.gva.es/sabias_que/rec...
#CiberseguridadParaMayores
#FondosFEDER
NUESTROS MAYORES
SEGUROS EN LA RED.
FINAL DE CAMPAÑA
#CiberseguridadParaMayores
9:10 a. m. · 4 ene. 2021 · Twitter Web App
5 Retweets 7 Me gusta


CCN-CERT @CCNCERT · 20 may.
Desde @CSIRTCV han ido compartiendo en Twitter una serie de consejos para ser capaces de distinguir las noticias reales de las falsas o #FakeNews. Podéis consultarlos accediendo a este link: twitter.com/search?q=%23St...
#ContraLaDesinformacion #StopFakeNews
#ContraLaDesinformacion
#StopFakeNews
Inicio de la campaña
Contra la desinformación en el ciberespacio: ¡Stop Fake News!
CSIRT-CV
Centre Seguretat TIC de la Comunitat Valenciana
Todos Seguros En La Red.
STOP
FAKE NEWS
9
7


GVA FGV
@GVAfgv
#QuédateEnCasa ciberseguro. Sigue las recomendaciones de @CSIRTCV :
✓Sigue la actualidad desde las webs oficiales
✓Atención a estafas telefónicas, correos y sms
✓Cuidado con las fake news y mensajes que nos llegan por Whatsapp ... bit.ly/2WJGrRD
Metrovalencia y 2 más