INFORME CTI DEL 8 AL 14 DE ABRIL DE 2023

Resumen de amenazas

	Crítica	Alta	Media	Baja	Info.
APT	0	2	3	3	1
Cadena de suministro	0	0	1	1	0
Amenazas contra datos	0	4	2	2	0
Amenazas contra disponibilidad	0	0	0	0	1
Ingeniería social	0	1	0	3	1
Malware	1	5	5	5	1
Ransomware	0	1	3	3	0

APT

Alta: Recibe el nombre de **Balada Injector** la **campaña masiva de malware en WorpdPress** que se encuentra activa desde 2017, la cual aprovecha todas las vulnerabilidades de complementos y temas conocidas y descubiertas recientemente. Se estima ya el **millón de sitios infectados**, ubicándose constantemente entre las 3 principales infecciones detectadas y limpiadas.

Alta: Según informes, **las filtraciones de datos, las estafas de phishing y las infecciones de malware atribuibles a ChatGPT van en aumento**. Las infracciones de seguridad cibernética más importantes en las que ChatGPT ha estado involucrado aumentan constantemente y se ha encontrado casi **dos nuevos eventos preocupantes cada semana** durante marzo y abril de 2023 .

Media: El Servicio de Contrainteligencia Militar y el equipo CERT Polska (CERT.PL) observaron una **campaña de espionaje generalizada vinculada a los servicios de inteligencia rusos (GRU)**, concretamente al grupo **APT29 (aka Nobelium, o The Dukes)** destinada a recopilar información de los ministerios de relaciones exteriores y entidades diplomáticas. La mayoría de los objetivos identificados de la campaña se encuentran en los **Estados Miembros de la OTAN, la Unión Europea** y, en menor medida, en África.

Media: Un **PSOA (proveedor de malware)** israelí rastreado como **DEV-0196, utiliza el spyware "KingsPawn" de QuaDream** —otro gran PSOA de Israel con el cual se le relaciona— para atacar a **personalidades de alto riesgo en Europa**, América del Norte, Medio Oriente y el Sudeste Asiático. El malware, también denominado **ENDOFDAYS**, se está implementando como **exploit 0-click para iPhone**.

Media: Identificado el grupo **DeathNote como un subclúster activo de Lazarus**. Este subgrupo ha apuntado recientemente al **sector académico y automotriz en Europa del Este**. Más tarde ha cambiado su enfoque a puestos relacionados con **contratistas de defensa y servicios diplomáticos**. Por último, se le ha visto apuntando a objetivos en **Corea del Sur**.

Baja: Se ha observado que el **grupo de estado-nación iraní conocido como MuddyWater** lleva a cabo **ataques destructivos en entornos híbridos de Medio Oriente bajo la apariencia de una operación de ransomware**. El actor se dirige tanto a infraestructuras locales como en la nube, en asociación con otro grupo de actividad emergente denominado **DEV-1084** .

Baja: El actor pakistaní **Transparent Tribe, centrado anteriormente en personal militar y gubernamental indio**, ha ampliado recientemente su alcance para incluir **instituciones educativas** y estudiantes en el subcontinente indio. **Crimson RAT** es un elemento básico constante en el arsenal de malware del grupo.

Baja: El grupo **Bitter (T-APT-17)** ha sido detectado distribuyendo **malware CHM (Microsoft Compiled HTML Help) a ciertas organizaciones chinas**.

Informativa: El equipo de hacktivistas ucranianos **Cyber Resistance pirateó el correo electrónico del teniente coronel Sergey Alexandrovich Morgachev**, un oficial de la **Dirección Principal de Inteligencia de Rusia** del Estado Mayor General del Ejército Ruso (GRU), confirmando finalmente que se trata del **líder del grupo de hackers rusos APT28 (aka Fancy Bear)**, formado por oficiales del 85º Centro Principal de Servicios Especiales del GRU, unidad militar #26165.

Cadena de suministro

Media: El gigante belga de recursos humanos y nómina **SD Worx** ha sufrido un ciberataque que les ha obligado a cerrar todos los sistemas de TI para sus servicios en el **Reino Unido e Irlanda**. SD Worx presta servicios a **5,2M de empleados para más de 82.000 empresas**.

Baja: **Monument Inc.**, servicio de asesoramiento sobre abuso de alcohol en línea con sede en Nueva York, está **notificando a más de 100K clientes sobre una filtración de datos** relacionada con el uso previo de la empresa de **herramientas de seguimiento** en sus sitios web.

Amenazas contra datos

Alta: El **ayuntamiento de Alcalá de Henares** ha detectado un intento de ciberataque a sus infraestructuras ocurrido en la madrugada de este lunes. El **CCN-CERT se ha puesto en contacto inmediato** y no consta afección ni impacto derivado del ataque.

Alta: **Kodi**, plataforma multimedia de entretenimiento, sufre un ciberataque en el que se ha **robado información de más de 400K personas**, entre la que se incluye nombres, correos y contraseñas.

Alta: Se estima que **la IA PassGAN es capaz de descifrar el 51 por ciento de las contraseñas comunes en menos de un minuto**, siendo las credenciales de más de 18 caracteres las que generalmente son más seguras contra los 'crackers'.

Alta: **Hyundai** ha sido víctima de un ciberataque en el que los datos personales de **miles de clientes han sido expuestos, al menos en Francia e Italia**. Este sería el último evento relativo a la actual oleada de ataques a la industria de la automoción, donde se están viendo afectados la práctica totalidad de los fabricantes.

Media: Identificado el surgimiento de un **nuevo actor de amenazas, llamado "ARES"**, involucrado en la **venta de bases de datos de autoridades corporativas y gubernamentales**, el cual se sospecha que está intensificando sus esfuerzos para agregar más actores de amenazas y filtraciones a su plataforma ARES Leaks.

Media: El **grupo hacktivista ruso Jocker DPR afirma que violó DELTA**, el sistema de gestión del campo de batalla (BMS) de Ucrania. No obstante, **se considera que sus logros son exagerados** y que únicamente haya obtenido acceso a una cuenta de usuario individual.

Baja: **Más de un millón de registros financieros** expuestos en un incidente de datos que involucra a una empresa fintech norteamericana llamada **NorthOne Bank**. Los documentos filtrados incluían facturas de personas y empresas que usaron una aplicación para pagar productos y servicios.

Baja: El **Departamento de Salud y Servicios Humanos de Iowa (HHS)**, en EEUU, confirma que los datos personales de más de **20K habitantes** que reciben asistencia de **Iowa Medicaid** quedaron expuestos debido a un ciberataque.

Amenazas contra la disponibilidad

Informativa: Los **ataques DDoS hipervolumétricos** en el primer trimestre de 2023 han pasado de depender de enjambres de dispositivos IoT comprometidos, individualmente débiles, a **aprovechar servidores privados virtuales (VPS) vulnerables**, utilizando credenciales de API filtradas o exploits conocidos.

Ingeniería social

Alta: Actores maliciosos han lanzado una **campaña de suplantación de la Agencia Tributaria** a través de correos electrónicos para el **robo de credenciales**, aprovechando los meses en los que se realiza la declaración de la renta para crear confusión.

Baja: El **FBI alerta de la presencia de empresas que explotan a víctimas de sextorsión** con fines de lucro, ofreciendo, mediante pago, **servicios engañosos de "asistencia"**, proporcionados normalmente por agencias sin fines de lucro y fuerzas del orden público.

Baja: Ciberdelincuentes **se hacen pasar por agentes de la ley o fiscales de China** para atacar a los **ciudadanos chinos con sede en EEUU**. Les dicen que son sospechosos de delitos financieros y las amenazan con arrestarlas o agredirlas si no les pagan.

Baja: Nueva campaña de **phishing, con foco principal en Argentina, hace creer a la víctima que su computadora fue infectada con un spyware** y que el atacante tiene en su poder un video comprometedor, que divulgará a menos que pague 650 dólares en BTC.

Informativa: Recientes estudios evidencian que los **actores de amenazas que se centran en las técnicas de phishing utilizan cada vez más Telegram** para automatizar sus actividades y proporcionar diversos servicios.

Malware

Crítica: Por parte del SOC de Seresco, **se ha detectado en España (Asturias y Galicia) una campaña activa de phishing que distribuye el cargador GuLoader** oculto en ejecutables maliciosos o en fichero comprimidos, que se hacen pasar por documentos relacionados con facturas, servicios contables y asuntos financieros dirigidos a empresas. Este cargador **entrega a su vez malware adicional, como ladrones y RAT**,y contiene múltiples etapas de shellcode. Actualmente es conocido por ser **uno de los cargadores más avanzados del mundo**, con numerosas técnicas de antianálisis. Fuentes informan de la **distribución del RAT Agent Tesla** aprovechando este vector de entrada.

Alta: Al mismo tiempo, observada en **EEUU campaña análoga** **de ataques de phishing dirigidos a empresas de contabilidad y preparación de declaraciones de impuestos para entregar el cargador GuLoader**, utilizando señuelos de temática fiscal y aprovechando el final del año fiscal. Se ha detectado a GuLoader, a su vez, **distribuyendo** **Remcos RAT** en las organizaciones.

Alta: Los investigadores han descubierto vendedores de malware que anuncian un **ladrón de información, llamado reverse-shell**, en el Índice de paquetes de Python (**PyPI**) con solo una capa mínima de ofuscación. Se ha identificado al actor como el **grupo español de MaaS llamado SylexSquad**.

Alta: Alertan de un **nuevo método para robar coches con un truco de IoT**, mediante el cual el ciberdelincuente puede **ingresar al sistema de control de los vehículos a través de los faros**. Desde ese punto se puede acceder la **red de comunicación interna** del automóvil gracias a un protocolo IoT del vehículo, haciendo posible encender y detener el coche, abrir puertas y ventanas y varias acciones más. Ha afectado a **Toyota modelo RAV4**, pero introduce en peligroso precedente para la generalidad de nuevos vehículos.

Alta: Reciente investigación acerca de las amenazas de **Google Play Store** que se venden en los foros clandestinos, tales como **MaaS**, destaca la **venta de cargadores** cuyo propósito es inyectar código malicioso o no deseado en una aplicación alojada en este servicio.

Alta: Los piratas informáticos están **comprometiendo los sitios web** para inyectar secuencias de comandos que muestran **errores falsos de actualización automática de Google Chrome que distribuyen malware** a visitantes desprevenidos.

Media: Se ha encontrado un **documento falsificado malicioso que fingía ser de la empresa ucraniana Energoatom**, una empresa estatal que opera las plantas de **energía nuclear** de Ucrania, que entrega la **puerta trasera Havoc Demon** mediante macros de Word.

Media: Una nueva **herramienta de recolección de credenciales y secuestro de SMTP llamada 'Legion'** se vende en el canal de Telegram de los actores **Forza Tools**, y se dirige a los servicios de correo electrónico en línea para ataques de **phishing y spam**.

Media: Un proveedor de seguridad descubre **casi 7K paquetes maliciosos en el repositorio PyPI**, solo en el mes de marzo. Los ladrones de información comprendían una cantidad significativa de estos componentes maliciosos, incluidos **imitadores del ladrón W4SP**, como uno llamado "**microsoft-helper**" de un autor que se describe a sí mismo como "**idklmao**".

Media: Continuando con las estafas relacionadas con la temporada de impuestos, en este caso, se encuentra el **malware Xworm alojado en un directorio abierto en www[.]farmaciasmv[.]com**. El archivo tiene apariencia de PDF pero, sin embargo, es un LNK.

Media: Los ciberdelincuentes están **secuestrando páginas de Facebook** y utilizando publicaciones patrocinadas para ofrecer **descargas de ChatGPT y Google Bard AI, que en realidad propagan el malware RedLine Stealer**.

Baja: El FBI ha prevenido sobre el uso de **estaciones de carga públicas de teléfonos móviles** donde actores maliciosos pueden utilizar los **puertos USB como una forma de introducir 'malware' en los 'smartphones'**, una práctica conocida como '**Juice Jacking**'.

Baja: **Israel** enfrenta nueva **ola de ciberataques dirigidos a infraestructura crítica**, sistema de aguas y satélites. Las autoridades creen que estos ataques cibernéticos pueden ser parte de **OpIsrael**, organizado por piratas informáticos propalestinos, como los **hactivistas GhostSec**. Esto se suma a los últimos ataques advertidos por la Organización Cibernética Nacional, que ya han afectado los **sistemas de riego, infraestructura general, medios, organizaciones gubernamentales, instituciones médicas, servicio postal y entidades educativas**.

Baja: Se ha encontrado una **biblioteca de software malicioso, llamada Goldoson**, dirigida a **Android** y apuntando a más de **60 aplicaciones populares en Corea del Sur**. Tiene funcionalidad para recopilar listas de aplicaciones instaladas y un historial de información de dispositivos Wi -Fi y Bluetooth, incluidas las ubicaciones de GPS cercanas. También va armada con un componente de adware.

Baja: La plataforma de intercambio de **criptomonedas y blockchain de Corea del Sur, GDAC**, ha sido víctima de un devastador ataque que resultó en el **robo de criptomonedas por un valor aproximado de casi USD 14 millones**.

Baja: Se ha identificado en **Corea** una **campaña inactiva (2018-2022) de distribución del malware Qakbot** a través de archivos PDF maliciosos adjuntos a **correos electrónicos secuestrados y reenviados** como respuesta a correos electrónicos existentes.

Informativa: **Dirty Vanity** es una nueva técnica de inyección de código que **abusa de la bifurcación y el desvío de EDR**, un mecanismo menos conocido que existe en los sistemas operativos Windows.

Ransomware

Alta: **Funcionarios gubernamentales en Tasmania** confirmaron el viernes que el grupo ruso de **ransomware ClOp filtró más de 16,000 documentos confidenciales** luego de un incidente de robo de datos hace dos semanas. Este sería el último ataque de la **prolífica campaña que desempeña ClOp explotando la vulnerabilidad de GoAnywhere de Fortra** por todo el mundo,

Media: **LockBit 3.0** ha afirmado haber pirateado con éxito a la empresa **Darktrace, empresa líder en ciberseguridad** reconocida por sus soluciones de respuesta y detección de amenazas impulsadas por IA, con sede en Cambridge, Reino Unido. Se desconoce, de momento, la veracidad de los hechos.

Media: El **astillero alemán Lürssen**, con sede en Bremen y destacado fabricante de algunos de los superyates más grandes del mundo, ha sido golpeado con un ataque de ransomware el fin de semana pasado.

Media: Se ha observado a la **banda de ransomware "Read The Manual" (RTM) apuntando a entornos corporativos** con su malware y obligando a sus afiliados a seguir un estricto conjunto de reglas. El grupo presenta un **elevado punto de madurez** y se esfuerza en operar bajo el radar. Se le circunscribe a la **Comunidad de Estados Independientes** en Europa del Este y Asia (CEI).

Baja: Se han detectado una serie de intentos de implementar el **ransomware Nokoyawa valiéndose de un 0-day en servidores de Microsoft Windows**. El actor de amenazas se destaca por el uso de una gran cantidad de **exploits de**

controladores Common Log File System (CLFS) similares pero únicos, probablemente desarrollados por el mismo autor, apuntando **a pequeñas y medianas empresas en el Medio Oriente, América del Norte y anteriormente en las regiones de Asia**, y afectando a minoristas y mayoristas, energía, fabricación, atención médica, desarrollo de software y otras industrias.

Baja: El **Departamento de Policía y la Oficina del Fiscal del condado de Camden**, Nueva Jersey, sufren sendos ataques de ransomware y aún están investigando el incidente. El ataque ha estado **bloqueando muchos archivos** de investigación criminal y capacidades de administración cotidianas.

Baja: Un **sistema de escuelas públicas en Rochester**, Minnesota, anunció que cancelaría las clases para las **42 escuelas** que opera después de haber sido atacado por un supuesto ataque cibernético.