INFORME CTI DEL 29 DE ABRIL AL 5 DE MAYO DE 2023

Resumen de amenazas

	Crítica	Alta	Media	Baja	Info.
APT	0	0	2	2	1
Cadena de suministro	0	0	3	0	0
Amenazas contra datos	0	5	7	14	1
Desinformación	0	0	0	2	0
Amenazas contra disponibilidad	0	0	1	2	0
Ingeniería social	0	1	1	0	1
Malware	0	1	5	10	0
Ransomware	0	2	1	8	0

APT

Media: El grupo **APT28 (aka Strontium, Fancy Bear)**, vinculado a Rusia, está apuntando a los **organismos gubernamentales ucranianos con guías falsas de 'Actualización de Windows'**. Los correos electrónicos maliciosos fueron diseñados para aparecer como enviados por administradores de sistemas de departamentos de múltiples organismos gubernamentales, utilizando **direcciones con nombres de empleados reales** que se obtuvieron previamente en una fase de reconocimiento.

Media: **Kimsuki (APT43)**, patrocinado por Corea del Norte, **desarrolla capacidades de reconocimiento en una nueva campaña global**. Utiliza un nuevo componente de malware (**ReconShark**), distribuido mediante phishing, que contiene enlaces de OneDrive que conducen a la descarga de documentos maliciosos.

Baja: Investigadores encuentran un **archivo señuelo que hacía referencia a una organización de investigación militar estatal india y un misil nuclear en desarrollo**. El archivo estaba destinado a implementar malware con características que coincidían con el **grupo APT "SideCopy"**, especializado en espionaje y patrocinado por Paquistán.

Baja: Nueva campaña de **Earth Longzhi (subgrupo de APT41)** dirigida a **organizaciones con sede en Taiwán, Tailandia, Filipinas y Fiji**, tras meses de inactividad. El grupo muestra toda una variedad de TTP tendentes a la explotación, carga lateral DLL e instalación de controladores. Destaca una nueva técnica para **deshabilitar el software de seguridad mediante DoS de "ruido de pila" (stack rumbling)**.

Informativa: Recientes indicios apuntan a que **algunos APT pueden estar trabajando juntos o, al menos, aunando esfuerzos y compartiendo herramientas**. Algunos analistas han detectado esta posible tendencia tras el reciente uso, por parte de Tomiris, de malware conectado a Turla.

CADENA DE SUMINISTRO

Media: El **proveedor de servicios de TI alemán Bitmarck** anunció el 30 de abril que había desconectado todos sus sistemas debido a un ciberataque. El incidente **afectó a las compañías de seguros de salud** reglamentarias que tienen su TI operada por BITMARCK.

Media: El **proveedor europeo de transporte al aeropuerto, Terravision**, sufrió una violación de datos en febrero que expuso más de **2 millones de registros de clientes**, la cual se ha hecho pública ahora.

Media: **Orqa, un fabricante de gafas de carreras de drones** con vista en primera persona (FPV), afirma que un contratista introdujo un código en el firmware de sus dispositivos que actuó como una **bomba de tiempo** diseñada para bloquearlos. El suceso ha afectado a usuarios en todo el mundo.

AMENAZAS CONTRA LOS DATOS

Alta: El **Ayuntamiento de Sils (Girona)** ha sufrido un ataque informático con la imposibilidad de acceso a su propio sistema y a sus ficheros, provocando una **violación de los datos personales**, de los cuales es el responsable de tratamiento.

Alta: Un **actor de amenazas en Fuengirola** lleva a cabo una estafa, mediante **método 'man-in-the-middle'**, haciéndose con unos **€64K de dos empresas**, accediendo a datos de facturas pendientes para desviar los cobros. Se ha identificado y detenido a una mujer, pero evidencia el riesgo alto de estas campañas en territorio nacional.

Alta: Los piratas informáticos de **Magecart (compuesto por unos 7 grupos** diferentes) están secuestrando tiendas en línea para mostrar **formularios de pago falsos y de aspecto realista** para robar tarjetas de crédito de clientes desprevenidos. Estos **skimmers** están siendo detectados en una gran cantidad de **plataformas de pago online por todo el mundo**.

Alta: **T-Mobile reveló la segunda violación de datos de 2023** después de descubrir que los atacantes tuvieron acceso a la **información personal de cientos de clientes** durante más de un mes, a partir de finales de febrero de 2023.

Alta: El recuento de personas cuya información confidencial se está viendo comprometida por la **explotación de la vulnerabilidad de día cero en el software de transferencia segura de archivos GoAnywhere de Fortra** está **creciendo en millones** a medida que más entidades informan violaciones de datos a los reguladores.

Media: La **Agencia Espacial Europea (ESA)** puso a prueba la seguridad cibernética de su tecnología espacial y permitió a un equipo intentar interrumpir el funcionamiento del **nanosatélite OPS-SAT**. Los investigadores **lograron hackear** el satélite accediendo a su sistema de posicionamiento global, siendo capaces de controlar la actitud (orientación o posición) y la cámara de a bordo, evidenciando posibles brechas de seguridad.

Media: Actor de amenazas detenido por la Policía Cibernética de Ucrania por **vender los datos personales de más de 300M de personas**. Administraba **canales cerrados en Telegram** que usaba para robar información

como **pasaportes ucranianos y europeos**, números de licencia de conducir y de contribuyente, datos de **cuentas bancarias** y certificados de nacimiento.

Media: China acusa a la **CIA** de estar detrás de una **ola de ciberataques perpetrados durante los últimos 10 años contra varios países** (incluido China), los cuales continuarían en la actualidad. Los objetivos se habrían ido expandiendo a áreas como **institutos de investigación científica, infraestructuras energéticas, compañías tecnológicas y agencias del Gobierno**, entre otras. Según revela el informe, se habría aprovechado de **vulnerabilidades existentes que no habían sido hecho públicas** para atacar servidores, terminales y routers, así como aparatos ICS.

Media: Los **cuatro principales bancos del Reino Unido** están experimentando interrupciones relacionadas con sus sistemas de banca en línea y banca móvil, con cortes en la web y las aplicaciones. Se han visto afectados Lloyds Bank, Halifax, TSB Bank y Bank of Scotland, y fuentes apuntan a un **ciberataque como posible causa**.

Media: La **Asociación Nacional de Rifles de Calibre Pequeño (NSRA) de Reino Unido** ha advertido a los **miembros** sobre posibles fraudes y delitos cibernéticos posteriores después de que se violaron sus sistemas de TI.

Media: Un investigador logra **secuestrar más de una docena de paquetes de Packagist**, algunos con **cientos de millones de descargas** en su historial. Packagist es el registro principal de paquetes PHP que se pueden instalar a través de Composer, una herramienta de administración de dependencias.

Media: Ha sido observada en foros clandestinos la venta de una base de datos de **usuarios de Calvin Klein**, obtenida de la plataforma de comercio electrónico de la misma.

Baja: Alrededor de **85K personas** han sido víctimas de un grupo de ciberdelincuentes que aseguran haber extraído información confidencial de los **usuarios registrados en las aplicaciones de citas** CityJerks y TruckerSucker.

Baja: Un post que ha aparecido en un famoso foro de ciberdelincuentes vinculado a Rusia indica que actores de amenazas han obtenido acceso a **datos sensibles de 630M de usuarios de China**. Esto **supondría el 8% de la población mundial**.

Baja: **Coca-Cola FEMSA**, la mayor embotelladora de Coca-Cola y con **presencia en 10 países de LATAM**, ha informado al Mercado de Valores mexicano que ha sido víctima de un ciberataque ocurrido hace unos días, sin trascender información al respecto.

Baja: **Vantage Travel**, una **compañía estadounidense que ofrece cruceros de lujo**, ha sido víctima de un ciberataque. Fruto de este incidente, algunos usuarios han visto cómo en los últimos días sus viajes eran cancelados a última hora.

Baja: La **filial australiana de Amnistía Internacional (AIA)** envió un correo electrónico a sus seguidores informándoles de que **sus datos pueden estar en riesgo** por una "actividad anómala" detectada en su entorno TI. No se conoce la naturaleza del ataque ni la cifra de personas afectadas. No se puede establecer una causalidad evidente, pero, pocos días antes, **Amnistía Internacional había denunciado que Israel** empleaba tecnologías de reconocimiento facial para afianzar el apartheid.

Baja: **Alaska Railroad Corporation (ARCC)**, una compañía ferroviaria que opera en el estado de Alaska desde 1903, ha informado de que ha sido víctima de un incidente de violación de datos en el que los actores de amenazas extrajeron **datos confidenciales de proveedores, empleados actuales y anteriores**, afectando a miles de usuarios.

Baja: Los piratas informáticos explotaron una vulnerabilidad de contrato inteligente de la **plataforma de intercambio descentralizado de criptomonedas Level Finance**. Han conseguido drenar 214 000 tokens LVL y cambiarlos por 3345 BNB, con un **valor aproximado de $1M**.

Bajas: Se ha observado en fotos clandestinos la **venta de todo tipo de bases de datos, whebshell y credenciales relativas a empresas y organizaciones de todo el mundo**, como:

- Centro de Innovación Nacional (NIC) de Tailandia.
- Votantes de las elecciones estatales de EEUU de 2021.
- Ucraft, sitio de desarrollo web para usuarios no experimentados.
- Instituto Conjunto de la Universidad de Michigan-Shanghai Jiao Tong University (UM-SJTU JI).
- Departamento de Ingeniería de la Información de la Universidad Cheng Kung.
- Rentomojo, líder indio en renting de productos.
- BI.ZONE, empresa de gestión de riesgos digitales.

Informativa: El actor **Water Labbu se dirige a sitios web de otros estafadores de criptomonedas**, comprometiéndolos al **hacerse pasar por una aplicación descentralizada (DApp)** e inyectando código JavaScript malicioso en ellos.

DESINFORMACIÓN

Baja: Advertido un **notable incremento en operaciones de influencia (IO) apoyadas cibernéticamente por parte Irán**, de mano del grupo **Emennet Pasargad**. Se centran principalmente en **Israel**, seguido de **EEUU, Emiratos Árabes Unidos y Arabia Saudita**. Algunos de sus objetivos incluyen buscar reforzar la resistencia palestina, fomentar el malestar en Bahrein y contrarrestar la normalización en curso de los **lazos árabe-israelíes**, avergonzando a figuras prominentes de la oposición mediante el uso de personas falsas en línea para amplificar o promocionar los ataques.

Baja: Se mantiene una continua campaña de desinformación en torno a la **situación de los ciudadanos musulmanes de la India**, provocando sofisticadas, continuas y coordinadas oleadas de ataques de grupos **hacktivistas proislamistas de gran cantidad de Estados de Oriente Medio y del sudeste asiático**. La conclusión de una campaña de **ataques DDoS** se sucede con la apertura de otra, aglomerando **decenas de grupos** apuntando, como protesta por la injusticia percibida y los prejuicios, **contra las entidades gubernamentales de la India**.

AMENAZAS CONTRA LA DISPONIBILIDAD

Media: El **grupo de piratería ruso 'Sandworm'** se ha relacionado con un ataque a las **redes estatales de Ucrania** donde se utilizó **RoarBat** para destruir datos en dispositivos gubernamentales. Este script BAT archiva datos mediante WinRar, eliminándolos a medida que se van archivando.

Baja: En **represalia por los ataques a la infraestructura india**, hacktivistas simpatizantes de India reclamaron ataques **DDoS en organizaciones de Bangladesh, Indonesia, Malasia y Pakistán** en las redes sociales y sus canales de Telegram. **Unos 7 grupos diferentes han liderado** una ola coordinada de ataques, tomando forma **16 campañas** diferentes.

Baja: Continuando la nueva **campaña OpIsrael, Anonymous está lanzando ataques DDoS contra sitios web israelíes**, incluidas instituciones **gubernamentales, militares y financieras**, como una forma de protesta contra las políticas de Israel hacia Palestina. Los hacktivistas apuntan activamente a activos y organizaciones que dependen en gran medida del funcionamiento de bombas, válvulas, motores y otros **componentes de ICS**.

INGENIERÍA SOCIAL

Alta: Se ha detectado una campaña de **smishing suplantando a la Seguridad Social en la que solicitan actualizar la tarjeta sanitaria** por medio del enlace proporcionado para evitar perder los derechos que dicha tarjeta ofrece. Remiten un formulario de phishing para robo de datos personales.

Media: Alertan de un problema de **apps fraudulentas que suplantan a OpenAI en la App Store para MacOS**. Estas aplicaciones replican el logotipo de la firma de IA o utilizan nombres reconocibles para engañar a los usuarios, quienes pagan por un programa que promete un servicio que no cumple.

Informativa: La proporción de archivos **adjuntos HTML evaluados como maliciosos se ha más que duplicado**, del 21 % en mayo pasado a casi el 46 % en marzo de 2023. Se trata de una **herramienta popular para el phishing**, el robo de credenciales y otras amenazas de mensajería.

MALWARE

Alta: Continúa la campaña de utilización de **señuelo de tecnología IA generativa, como ChatGPT, para distribuir aplicaciones y extensiones maliciosas o troyanizadas**, así como para realizar estafas criptográficas. En muchos casos el elemento descargado incluye funciones de ChatGPT reales, además del malware, para ocultarse y evitar levantar sospechas.

Media: Un **nuevo malware llamado LOBSHOT** parece aprovecharse con fines financieros empleando **troyanos bancarios y capacidades de robo de información**. Es de tipo hVNC (cómputo de red virtual oculta) y se ha visto distribuido en la creciente campaña de uso de **malvetiring en Goggle Ads** para implementar malware bajo la apariencia de software legítimo. Se le vincula, con confianza moderada, a **TA505**.

Media: Se descubrió una nueva versión del **malware de robo de información ViperSoftX** con una gama más amplia de objetivos, incluidos los **administradores de contraseñas KeePass y 1Password**. También apunta a más **criptomonedas** que antes, presenta un cifrado de código más fuerte y funciones para evadir la detección.

Media: Actor de amenazas vietnamita lleva a cabo campaña de **malverposting por RRSS infectando 500K dispositivos en todo el mundo** durante los últimos 3 meses, distribuyendo variantes de **ladrones de información como S1deload y SYS01**.

Media: Facebook descubrió un nuevo **malware de robo de información distribuido en Meta llamado 'NodeStealer'**, que permite a los actores de amenazas robar cookies del navegador para secuestrar cuentas en la plataforma, así como **cuentas de Gmail y Outlook**.

Media: De forma similar a otros ataques referenciados en lo que va de año, el **grupo RaaS Black Basta** utiliza, para infiltrarse en redes, del **distribuidor Qbot (QakBot) para entregar cargas adicionales de Brute Ratel y Cobalt Strike**.

Baja: Continuando la **campaña de XMRig CoinMiner en servidores Linux SSH mal administrados**, se ha destacado recientemente una nueva versión de ataque en la que se observa el uso de **Shell Script Compiler (SHC)** y la inclusión de un mensaje personalizado del actor de amenazas que **dice "KONO DIO DA"**.

Baja: Descubierta **nueva herramienta de vigilancia de Android**, atribuida con confianza moderada al **Comando de Aplicación de la Ley de la República Islámica de Irán (FARAJA)**. Nombrado **BouldSpy**, va dirigido al **espionaje de minorías** y, a pesar de que incluye código de ransomware, este no se usa y no funciona, pero podría indicar un desarrollo en curso o un intento de distracción por parte del actor.

Baja: Continúa en activo el prolífico malware **PrivateLoader**; familia de **cargadores maliciosos**, escrita en C++ y descubierta por primera vez a principios de 2021. Es conocido por **distribuir una amplia gama de malware**, desde simples ladrones de información hasta rootkits y spyware complejos, utilizando cargas útiles.

Baja: Se ha confirmado la distribución del **ladrón RecordBreaker a través de una cuenta de YouTube** que se supone que fue pirateada recientemente. Este malware es conocido como una **nueva versión de Raccoon Stealer**, y se disfraza de instalador legítimo.

Baja: Identificada recientemente una botnet de Android, la cual sería la **versión troyanizada de la aplicación Psiphon** e identificada como **DAAM Android Botnet**. Cuenta con amplia gama de funcionalidades de **spyware** y de exfiltración de datos del sistema infectado.

Baja: Seguida una campaña de los actores **Operation Dragon Breath**, especializados en **juego de azar en línea y sus usuarios en el sudeste asiático**, basada en **técnicas de doble carga lateral**, agregando complejidad, capas de ejecución, variaciones e intercambio de componentes para evadir la detección.

Baja: El nuevo malware **Trojan.sysscan** tiene amplias capacidades para **extraer cookies y otras credenciales** que contienen detalles de autenticación dirigidos a **sitios web bancarios, de apuestas e impuestos**, así como información guardada por el software de punto de venta (PoS).

Baja: Descubiertos en el **repositorio PyPI varios archivos Python .whl (Wheel) maliciosos** que estaban distribuyendo un nuevo ladrón llamado **KEKW**. Se centra en el **robo de información** y en actividades de **clipper** de secuestro de transacciones de criptomonedas.

Baja: Un troyano llamado **Fleckpe se difunde a través de Google Play** como parte de aplicaciones de edición de fotos, paquetes de fondos de pantalla para teléfonos inteligentes, etc.

Baja: Se detecta una nueva variedad de malware denominada **FluHorse**, que se disfraza hábilmente como **aplicaciones populares de Android del este de Asia**. Se trata de una campaña muy sofisticada con un esquema de phishing para robar información confidencial, incluidas **credenciales de usuario y detalles de tarjetas** de crédito.

RANSOMWARE

Alta: **Cl0p continua su campaña mundial de explotación** de la CVE de la plataforma segura de intercambio de archivos **Fortra GoAnywhere MFT**.

- El proveedor de **salud mental pediátrica Brightline** sufrió una violación de datos que afectó a 783.606 pacientes.
- **Nation Benefits**, empresa que ofrece **beneficios complementarios en EEUU**, ha sido atacada por el grupo, viendose **afectados 3M de personas**

Media: Una **escuela secundaria del Reino Unido** ha confirmado que se vio afectada por un incidente cibernético que afectó su red de TI. La escuela **Hardenhuish** confirmó el ataque el jueves y dijo que los piratas informáticos obtuvieron acceso a la infraestructura de la red y luego **exigieron un rescate por restaurar** el acceso.

Baja: Observado un tipo de ransomware, de nombre **Rapture**, que se dirige a sus víctimas con un enfoque minimalista con herramientas que solo **dejan una huella mínima**. Aunque comparte ciertas similitudes con Paradise, el comportamiento de Rapture es diferente al primero.

Baja: **Americold, empresa estadounidense líder en logística y almacenamiento** en frío, se ha enfrentado a problemas de TI desde que su red fue violada en lo que parece indicar un ataque de ransomware.

Baja: El **condado de Spartanburg, en Carolina del Sur**, está lidiando con un ataque de ransomware que ha limitado sus sistemas telefónicos y de TI. Forma parte de un **continuo goteo de ataques a gobiernos locales con escasos recursos de EEUU**.

Baja: La **ciudad de Dallas, Texas**, sufrió un ataque de **ransomware Royal**, lo que provocó que cerrara algunos de sus sistemas de TI para evitar la propagación del ataque. Se han visto afectados su **Departamento de Policía** y sus **Juzgados**, entre otros.

Baja: Por su parte, el grupo de ransomware **Play continúa apuntando a ciudades de EEUU**, anunciando ahora otra violación de un gobierno local, esta vez nombrando a la **ciudad de Lowell, en Massachusetts**, como su última víctima.

Baja: **Naivas**, una de las cadenas de **supermercados más grandes de Kenia**, anunció la semana pasada una violación de datos de clientes luego de un incidente de ataque de ransomware. El **grupo ruso ALPHV (BlackCat)** se ha atribuido la responsabilidad.

Baja: Además, el grupo **ALPHV** también ha apuntado al **servicio de transporte público Uttar Pradesh,** Corporación Estatal de Transporte por Carretera propiedad del gobierno de la provincia más poblada de la **India**, derribando el servicio de venta de billetes.

Baja: La **pandilla de ransomware Avos** secuestró el sistema de transmisión de emergencia de la **Universidad de Bluefield, EEUU**, para enviar a los estudiantes y al personal SMS y correos electrónicos comunicando que sus datos habían sido robados.