INFORME CTI DEL 22 AL 28 DE ABRIL DE 2023

Resumen de amenazas

	Crítica	Alta	Media	Baja	Info.
APT	0	0	5	3	0
Cadena de suministro	0	0	1	2	0
Amenazas contra datos	0	4	4	10	0
Amenazas contra disponibilidad	0	0	1	2	0
Ingeniería social	0	1	1	3	0
Malware	0	0	10	4	0
Ransomware	0	2	4	2	0

APT

Media: Se ha observado, en sus últimas campañas, una **modernización en las TTP del APT Charming Kitten** (APT35, asociado a los Servicios de Inteligencia de Irán), incluido un nuevo malware **cuentagotas llamado BellaCiao**, muy complejo. Se han identificado **múltiples víctimas de IC en Estados Unidos y Europa**, pero también en Oriente Medio (Turquía) o India.

Media: Se ha observado que los piratas informáticos **BlueNoroff (subclúster de Lazarus)** vinculados a Corea del Norte utilizan una nueva familia de **malware macOS apodado RustBucket** y capaz de obtener cargas útiles adicionales de su servidor C2.

Media: El **APT de ciberespionaje de Corea del Norte RedEyes** (APT37) ha estado distribuyendo el **malware RokRAT a través de archivos LNK**, para recopilar credenciales de usuarios y descargar malware adicional.

Baja: Al contrario de otros APT, los cuales decrecen o se ocultan tras eventos de exposición pública, se está detectando un **crecimiento continuo, por todo el mundo, del APT Kimsuky**, alineado con el gobierno de Corea del Norte. Centrados en el espionaje, principalmente a **países enemigos del régimen (Corea del Sur, Japón y EEUU)**, suele apuntar a **sectores gubernamental, energético, farmacéutico y financiero**.

Baja: **Educated Manticore, subclúster del APT Charming Kitten**, de los Servicios de Inteligencia de Irán, supone una nueva amenaza de naturaleza agresiva, vinculado con implementaciones de **ransomware** y con la mejora significatica de mecanismos y **técnicas poco comunes para apuntar a Irak e Israel**. Se ha identificado una versión actualizada de una **puerta trasera de Windows llamada PowerLess**.

Baja: El grupo **Nomadic Octopus** se dirige, en su nueva **campaña Paperbug contra Tayikistán**, a funcionarios gubernamentales de alto rango, servicios de telecomunicaciones e infraestructuras de servicios públicos. Los tipos

de máquinas comprometidas van **desde computadoras personales hasta dispositivos OT**. Se detecta fuerte soporte de Inteligencia en la operación.

Baja: Descubierta una campaña del **APT chino Evasive Panda, dirigida a una ONG internacional en China**, con malware entregado mediante el **secuestro de actualizaciones de software** popular chino legítimo. El malware entregado ha sido **MgBot**, la puerta trasera insignia de Evasive Panda.

Baja: Se relaciona al grupo **Tomiris (habla rusa)** con campañas de **recopilación de inteligencia en Asia Central**. El actor de amenazas apunta a **entidades gubernamentales y diplomáticas en la CEI**, y representantes o exponentes de la CEI en otros estados. Se caracteriza por el desarrollo de numerosos implantes elementales pero eficientes, empleo ocasional de RAT comercial y personalidad ágil y decidida, abierta a la experimentación, p.e. con métodos de entrega mediante secuestro de DNS. Tomiris ha implementado en esta campaña **malware típicamente relacionado con el APT ruso Turla, en concreto la puerta trasera Kazuar**, haciendo que algunas fuentes, erróneamente, atribuyesen a estos la campaña en un inicio.

Cadena de suministro

Media: Los investigadores han descubierto que **más de 250M de artefactos de software y más de 65K imágenes de contenedores han sido expuestos debido a malas configuraciones**, lo que expone a las organizaciones a ataques potencialmente graves en la cadena de suministro de software.

Baja: **Fincantieri Marine Group, contratista naval comercial y de defensa de la Marina de los EEUU** y con vínculos con el gobierno, ha sido atacado por un **ransomware**, causando una interrupción temporal en ciertos sistemas informáticos en su red.

Baja: Se ha observado en foros clandestinos la venta de una **base de datos de 125GB de números de la Seguridad Social (SSN) de EEUU**. La fuente apunta a que la violación se ha producido en un **depósito S3 abierto de AWS**.

Amenazas contra los datos

Alta: Se ha observado, puesta a la venta en foros clandestinos, una **base de datos teóricamente perteneciente a la Sede de Defensa del Gobierno de España**.

Alta: El **Ayuntamiento de Carballo (A Coruña)** ha sido víctima de un ciberataque que provocó la paralización de toda su actividad administrativa.

Alta: Un **grupo HaaS llamado Delta Boys** ofrece en foros clandestinos programas de afiliados para socios, a los que ofrece aportar **bases de datos, credenciales de acceso, capacitaciones y vulnerabilidades** valiosas, tanto para uso propio como para reventa. En una de sus entradas, ofrece un pack de **videotutoriales de hacking a bases de datos de los Gobiernos de España, EEUU, UK e Israel**, así como a la NASA y diversas Universidades, así como objetivos militares y de inteligencia.

Alta: **Peugeot** filtra el acceso a la **información de sus usuarios en Perú**, habiéndose identificado un archivo de entorno expuesto alojado en su tienda oficial. Sería la última filtración de datos relativa a la constante brecha en la industria de la automoción mundial.

Media: **Digi, compañía de telecomunicaciones y proveedora de telefonía y servicios de internet**, sufre un ciberataque que expuso parte de los datos personales de algunos de sus clientes.

Media: Un **error en una característica de Microsoft Edge**, el navegador web basado en Chromium, ha enviado buena parte del contenido revisado y las URL visitadas por los usuarios al sitio web API de su **buscador, Bing**.

Media: Se ha descubierto un nuevo **ataque de canal lateral que afecta a varias generaciones de CPU Intel**, lo que permite filtrar datos a través del registro EFLAGS. El ataque funciona como un **canal secundario para Meltdown**, una vulnerabilidad crítica descubierta en 2018, que afecta a muchos microprocesadores basados en x86.

Media: Identificado el actor **FIN7** como responsable de los ataques de finales de marzo contra los **servidores con software Veeam Backup & Replication**. Parece que el acceso y ejecución inicial se lograron explotando una vulnerabilidad recientemente parcheada.

Baja: La **American Bar Association (ABA)**, la asociación de abogados y profesionales del derecho más grande del mundo, sufrió una violación de datos después de que los piratas informáticos comprometieran su red y obtuvieran **acceso a las credenciales** más antiguas de **1.466.000 miembros**.

Baja: Un actor no autorizado obtuvo acceso a los sistemas de **Shields Health Care Group (SHCG)** en marzo, exponiendo los números de licencia de conducir y otra información de identificación de más de **2,3 millones de pacientes**, según la empresa.

Baja: **ICICI Bank, multinacional india** nombrada infraestructura de información crítica por su gobierno, filtró **millones de registros con datos confidenciales** debido a una mala configuración, incluida información financiera y documentos personales de los clientes del banco.

Baja: El **grupo chino Tonto Team** está utilizando un archivo relacionado con productos antimalware para, en última instancia, ejecutar ataques maliciosos contra las **instituciones educativas, de construcción, diplomáticas y políticas de Corea**.

Baja: Se ha observado en **foros clandestinos** la venta de una serie de bases de datos, conteniendo accesos de administrador, datos de clientes, paneles de WP y WhebShell, entre otros:

- 340K registros de usuario del **sistema de pagos chino 5aitou**.
- **Common Folks**, tienda de libros online de la India.
- Web india **Data Recovery**.
- **ATMonline**, proveedor de préstamos asiático.
- **GGKU**, gran comercio chino online.
- Empresa de turismo tailandesa **ADT** (Asociación de Viajes Nacionales).

Amenazas contra la disponibilidad

Media: Los piratas informáticos prorrusos **KillNet lanzaron un ataque DDoS masivo contra la agencia europea de tráfico aéreo EUROCONTROL**. La Organización Europea para la Seguridad de la Navegación Aérea señaló que el ataque no tuvo impacto en las actividades de control del tráfico aéreo europeo.

Baja: Un **gasoducto canadiense** sufrió un ciberataque disruptivo, y funcionarios de Canadá y el grupo de piratería pro-ruso **Zarya** afirmaron que este **podría haber causado una explosión** (no confirmada). El incidente se reveló en documentos de inteligencia estadounidenses filtrados, los que sugieren que el grupo operaba directamente bajo la **Inteligencia Rusa**.

Baja: **Anonymous Sudan** (el cual se supone es una operación de **bandera falsa del grupo ruso Killnet**) se atribuyó la responsabilidad de los **ataques DDoS** que derribaron el sitio web personal del **primer ministro israelí** Benjamin Netanyahu y el secuestro de su cuenta de Facebook. Se cree que el grupo es responsable de los ataques a los sitios web de **Haifa Port** y de la empresa **Israel Ports Development**, y también se responsabilizaron por derribar el sitio web del **Instituto Nacional de Seguros**, así como el del **Mossad**, la agencia de espionaje de Israel. Por último, se han responsabilizado de gran parte de los **cortes de energía en Israel**, incluidas las principales ciudades como Tel Aviv y Beersheba, apuntando a la **Corporación Eléctrica de Israel (IEC)**.

Ingeniería social

Alta: Se mantiene una alarmante escalada en el uso de **técnicas de malvertising y malverposting, abusando de las redes y los servicios publicitarios para promocionar anuncios o entradas** de phishing o de propagación de malware, como páginas de spoofing, estafas financieras o extensiones y aplicaciones falsas. Al igual que ocurre con los anuncios y promociones en Google, también son numerosas las amenazas enviadas por las redes sociales que **ganan terreno mediante la promoción paga**.

Media: Se está produciendo, durante las últimas semanas, una sucesión de ataques conocidos **como "romance de criptomonedas", "CryptoRom", "pig butchering" o "matanza de cerdos"**; un tipo de estafa basada en establecer **relaciones amorosas de larga duración** con la víctima por RRSS e incitarle a realizar movimientos o **inversiones de criptomonedas**. En un último caso, un hombre de Florida (EEUU) ha sido estafado con **$480K en una falsa inversión**.

Baja: **PostalFurious**, pandilla de phishing de habla china, está dirigiendo una **campaña de smishing en Singapur y Australia**. En ella, los SMS contienen el nombre de una marca conocida y una URL abreviada para atraer a las víctimas a seguir el enlace a su página de phishing de apariencia legítima.

Baja: La cuenta de Twitter de **KuCoin, plataforma de comercio e intercambio de criptomonedas**, fue pirateada, lo que permitió a los atacantes promover una **estafa de obsequios falsos** que condujo al robo de más de $22,600 en criptomonedas.

Baja: Estafadores lograron posicionar en los **primeros resultados de búsqueda de Google** un sitio falso dirigido a usuarios de **Argentina** que se hace pasar por la **tienda de Le Qoc Sportif** para robar los datos de las tarjetas de pago.

Malware

Media: El descubrimiento de que **3CX fue violado por otro ataque anterior** a la cadena de suministro (Trading Technologies, mediante el paquete de software malicioso X-Trades) hizo muy probable que más organizaciones se vieran afectadas por esta campaña, que ahora resulta ser **mucho más amplia de lo que se creía** originalmente, incluidas dos **organizaciones de infraestructura crítica en el sector energético, una en EEUU y otra en Europa**.

Media: Se detecta la propagación maliciosa de **anuncios ocultos a través de aplicaciones de juegos de Android en Google Play**. Se cargaron oficialmente en Google Play con varios títulos y nombres de paquetes, con **más de 10M de descargas.**

Media: Una vulnerabilidad en los en **router Wi-Fi TP-Link Archer AX21** ha comenzado a ser explotada mediante la **botnet Mirai**, comenzando sus detecciones en **Europa del Este** y difundiéndose a otras partes del mundo.

Media: Un prolífico **ladrón de información MaaS de nombre "CryptoBot"** se estima que haya infectado a unas **670K computadoras en todo el mundo**. Generalmente está oculto en software troyanizado, aparentemente legítimo, de **Google Earth Pro y Google Chrome**. Google está llevando a cabo una campaña legal de persecución contra sus distribuidores (con sede principal en Pakistán) para retrasar y dificultar la propagación de este.

Media: Identificado en la darknet un mercado de **apps troyanizadas preparadas para su distribución por Google Play**. Además de las aplicaciones, se ofrecen **cuentas de desarrollador para subir las apps** infectadas, códigos de descarga maliciosos y hasta se puede contratar publicidad para lograr más descargas.

Media: Descubierta la primera evidencia de que los atacantes están **explotando el control de acceso basado en roles (RBAC) de Kubernetes (K8)** para crear puertas traseras. Los atacantes también implementaron **DaemonSets** para hacerse cargo y secuestrar los recursos de los clústeres de K8 que atacan.

Media: Se ha encontrado un **nuevo toolkit, llamado Decoy Dog**, que presenta una cohesión y una serie de **características muy inusuales que lo hacen único**, principalmente en lo relativo a **DNS**. Su principal componente, **Pupy**, es una RAT peligrosa y poderosa debido a su naturaleza sin archivos y sus comunicaciones C2 lentas y encriptadas.

Media: **Gh0st RAT**, malware de código abierto con décadas de antigüedad, apareció recientemente en campañas de phishing dirigidas a una **organización de tecnología médica europea ubicada en China**.

Media: Un canal de Telegram anuncia un nuevo **MaaS ladrón llamado Atomic macOS Stealer (AMOS)**. El malware está diseñado específicamente para apuntar a macOS y puede robar información confidencial de la máquina de la víctima, incluyendo **llaveros, archivos, datos del sistema, navegadores y criptobilleteras**.

Media: Analizada una muestra de **LimeRAT**, se ha observado que su marca distintiva es su **amplio espectro de actividades maliciosas, sobresaliendo** en exfiltración de datos, creación de botnets DDoS, criptominería y elusión de sistemas de detección. Comparte similitudes con njRAT.

Baja: Los sitios web de **varias universidades de EEUU** se han visto pirateadas y están **sirviendo Fortnite y spam de "tarjetas de regalo"**. Se han visto comprometidas las **páginas de Wiki** y documentación alojadas en universidades como Stanford, MIT, Berkeley, UMass Amherst, Northeastern, Caltech, entre otras.

Baja: Se ha observado al **ladrón de criptomonedas e información ViperSoftX** evadiendo la detección del cargador inicial y haciendo que su **señuelo sea más creíble** y no sea malicioso. Se ha **sofisticado** el método de cifrado y la actualización incluye un cambio mensual de servidor C2. Tiene presencia, sobre todo, en **sectores empresarial y de consumo en Australia, Japón y EEUU**.

Baja: Una vulnerabilidad crítica en la herramienta de colaboración **Atlassian Confluence** está siendo actualmente explotada para la **minería maliciosa de criptomonedas**, afectando a todas las versiones de **Confluence Server y Confluence Data Center**.

Baja: Los piratas informáticos chinos están implementando nuevas **variantes de malware de Linux en los ataques de ciberespionaje**, como una nueva variante del **RAT PingPull** (vinculado al **APT Gallium**) y una puerta trasera no documentada previamente rastreada como **'Sword2033'**. Se dirige contra objetivos en **Sudáfrica y Nepal**.

Ransomware

Alta: La **Ertzaintza** ha alertado de que en la última semana se ha producido un **incremento de casos denunciados de Ransomware** que afecta principalmente a **empresas y entidades públicas**. Destacan la explotación de **vulnerabilidades**.

Alta: Los atacantes están explotando **vulnerabilidades graves en el software de gestión de impresión PaperCut MF/NG** ampliamente utilizado para instalar los **RMM Atera y Syncro**, así como el **descargador TrueBot**. Este descargador se relaciona con el **grupo Silence** y es utilizado para implementar **ransomware ClOp**. La mayoría de los dispositivos potencialmente afectados se encuentran en **EEUU y Europa, incluida España**. En última instancia, Microsoft ha atribuido los ataques a las **operaciones de ransomware Clop y LockBit**, que utilizaron las vulnerabilidades para robar datos corporativos.

Media: Observado recientemente el **cargador modular Bumblebee** distribuido a través de **instaladores troyanos para software popular** como Zoom, Cisco AnyConnect, ChatGPT y Citrix Workspace. Se han visto anunciados en Google Ads, y va tradicionalmente dirigido a la **instalación de ransomware**.

Media: Se han detectado varias variantes de ransomware: **SDK**, variante de Phobos; **Recov**, variante de VoidCrypt; **CRLK**, variante de CrossLock; **Djvu**, variante de STOP; y **Skynetlock** y **Attackuk**, variantes de MedusaLocker.

Media: Los actores de **RTM Locker** han desarrollado una variedad de ransomware que es capaz de apuntar a máquinas Linux, el cual **infecta hosts Linux, NAS y ESXi** y parece estar inspirado en el código fuente filtrado del **ransomware Babuk**.

Media: Se sigue la pista del nuevo **ransomware UNIZA**, de encriptación de datos, el cual muestra su mensaje de **rescate a través de la ventana cmd.exe** y, como característica particular, **no agrega el nombre de archivo** de los archivos que encripta, lo que dificulta determinar qué archivos se han visto afectados.

Baja: La **Universidad Estatal de Truman en Kirksville, Missouri**, está en proceso de recuperación tras un ciberataque de la semana pasada que la obligó a cerrar la red del campus y ordenar que se apagaran todos los dispositivos proporcionados por la escuela.

Baja: **Yellow Pages Group**, un editor de directorios canadiense, ha confirmado que ha sufrido un ciberataque de ransomware. La **banda Black Basta** se adjudica la responsabilidad del ataque y ha publicado documentos y datos confidenciales durante los últimos días.