INFORME CTI DEL 4 AL 10 DE MARZO DE 2023

Resumen de amenazas

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

APT

Media: Se ha identificado un prometedor **grupo europeo conocido como FusionCore**, quienes ofrecen **servicios MaaS, HaaS e IAB**. Disponen de una web donde ofrecen una amplia variedad de herramientas y servicios disponibles, así como de **malware personalizable**, incluido ransomware.

Media: Las operaciones cibernéticas de las **agencias de inteligencia rusas están siendo reforzadas por NTC Vulkan**, empresa relacionada con herramientas de **piratería, desinformación, ataque a IC y control de Internet** por todo el mundo.

Media: Un grupo aparentemente proislámico que ha atacado numerosos objetivos en Europa con ataques DDoS en los últimos meses, al cual se le conoce por **Anonymous Sudan, parece ser en realidad** un subgrupo del colectivo hacktivista ruso conocido como **Killnet**.

Media: Identificada recientemente **STYX Marketplace, una nueva plataforma CaaS** de comercio electrónico cibercriminal con un enfoque especializado en **fraude financiero y lavado de dinero**, ofreciendo una variedad de servicios para facilitar este tipo de delitos.

Baja: Crece la tensión ante las **continuas actividades cibernéticas maliciosas de Corea del Norte** como medio de autofinanciación y apoyo de sus programas de armas, ante lo que **EEUU, Corea del Sur y Japón** expresan su preocupación en un comunicado conjunto. En este sentido, investigadores advierten sobre el grupo **ARCHIPELAGO**, el cual está atacando al **personal militar y del gobierno, grupos de expertos, legisladores, académicos e investigadores** en Corea del Sur, EE. UU. y otros lugares. El actor invierte tiempo y esfuerzo en construir una relación con los objetivos durante días o semanas.

Baja: El **APT Mantis**, que se cree que opera desde los territorios palestinos, continúa montando ataques, desplegando un conjunto de herramientas actualizado y manteniendo una **presencia persistente en Oriente Medio y Palestina**.

Cadena de suministro

Media: Investigadores descubren evidencia de que el **grupo Lazarus de Corea del Norte es responsable del ataque a la cadena de suministro de software en 3CX DesktopApp**, un popular programa VoIP utilizado por las principales empresas multinacionales. Se ha encontrado el **backdoor Gopuram coexistiendo con AppleJeus**, y se consolidan **Europa, EEUU y Australia como zonas más afectadas**.

Media: **Western Digital**, fabricante tecnológico y proveedor de servicios de almacenamiento de datos con sede en California, anuncia que su red ha sido violada y una parte no autorizada obtuvo acceso a múltiples sistemas de la compañía. Diferentes **dispositivos y servicios cloud tanto de WD como de Sandisk se han visto afectados**.

Media: El **proveedor británico de servicios de outsourcing Capita** anunció que un ciberataque impidió el acceso a sus aplicaciones internas de **Microsoft Office 365**. Entre sus clientes se encuentran **organizaciones de infraestructura crítica en el Reino Unido**, como el Servicio Nacional de Salud (NHS), el ejército del Reino Unido y el Departamento de Trabajo y Pensiones, así como **empresas destacadas como O2, Vodafone y Royal Bank of Scotland**.

Media: Una **herramienta de identificación digital, proporcionada por OCR Labs a las principales empresas**, instituciones financieras y agencias gubernamentales del mundo, filtró credenciales confidenciales. Algunos de sus clientes son BMW, Vodafone, el gobierno australiano, Westpac, ANZ, HSBC y Virgin Money, y se ha confirmado que se han visto afectados **QBANK, Defense Bank, Bloom Money, Admiral Money, MA Money y Reed**.

Baja: **Uber** sufre, una vez más, una **violación de datos relativa a información de sus conductores**, esta vez producto de un ataque a los **sistemas TI del bufete de abogados Genova Burns**.

Baja: **eFile.com, un proveedor de servicios de software** de archivos electrónicos autorizado por **el Servicio Interno de Rentas (IRS) de EEUU** utilizado por muchos para presentar sus declaraciones de impuestos, ha sido descubierto distribuyendo **malware de JavaScript**. Es el segundo ataque relacionado con el IRS en apenas una semana, y se baraja LockBit como posible autor del mismo.

Informativa: Se **filtra código fuente e información confidencial de Samsung** después de que varios de sus ingenieros hayan acudido a **ChatGPT** para resolver unos errores de código. Posteriormente, dichas consultas fueron filtradas en la **brecha de seguridad sufrida por OpenAI**.

Amenazas contra datos

Alta: **Yoigo** ha confirmado a través de un comunicado enviado a sus clientes que ha sido víctima de un ciberataque y que **algunos de los datos privados han podido ser comprometidos**. Han asegurado que no se trata de un ataque ransomware.

Alta: Los piratas informáticos están **explotando activamente** una vulnerabilidad de alta gravedad en el popular **complemento Elementor Pro WordPress** utilizado por más de once millones de sitios web.

Media: **Documentos secretos que brindan detalles de los planes de Estados Unidos y la OTAN para ayudar a preparar a Ucrania** para una ofensiva de primavera contra Rusia podrían haberse **filtrado en las plataformas de redes sociales**. Los documentos confidenciales incluyen gráficos, detalles de entregas de armas y fuerza de los batallones, entre otros.

Media: Se ha detectado en foros clandestinos gran cantidad de puntos de **venta de registros completos de información (fullz) y de información de identificación personal (PII)**, incluyendo números de seguridad social, fechas de nacimiento, nombres y apellidos, información crediticia y de tarjetas, licencias de conducir, etc. Uno de esos fullz afecta a más de **20K registros de un portal de clubes deportivos con sede en Francia**.

Media: La **Oficina de Antecedentes Penales del Reino Unido (ACRO)** ha estado luchando contra un "incidente cibernético" durante dos meses, creando retrasos para los solicitantes de visa y **exponiendo potencialmente la información del cliente** a un compromiso.

Media: La **Real Asociación Holandesa de Fútbol** dice que los piratas informáticos pudieron robar la **información personal de sus empleados** durante un ataque cibernético.

Baja: Igualmente presente en los foros clandestinos ha sido el ofrecimiento, por parte de cibercriminales, de **servicios de falsificación de todo tipo de documentos públicos y oficiales**, tales como extractos bancarios, licencias de conducir, pasaportes, documentos de identificación, facturas, registros de vehículos, selfies con con documentos, etc.

Baja: La **firma estadounidense de préstamos TMX Finance** ha revelado una grave violación de los datos de los clientes, la cual daría a los estafadores la oportunidad de intentar el fraude de identidad, como apertura de nuevas líneas de crédito.

Baja: Filtrada **base de datos con 600K archivos** adjuntos de atención al cliente relacionados con el **sitio web Z2U**, que incluían imágenes de personas con tarjetas de crédito, pasaportes y otros documentos de identidad y contraseñas. La web comprende comercio tanto legítimo como dudoso.

Baja: Una **vulnerabilidad en la aplicación Retail Tool de Tesla** permitió a un investigador **hacerse cargo de las cuentas de los exempleados**. Diseñado con soporte para inicios de sesión de empleados y proveedores, TRT almacena varios tipos de información empresarial.

Informativa: Entre 2019 y 2022, grupos de **empleados de Tesla** compartieron en privado, a través de un sistema de mensajería interno, **videos e imágenes a veces muy** invasivos grabados por las cámaras de los automóviles de los clientes.

Amenazas contra la disponibilidad

Media: El último informe conjunto publicado por el Centro de Análisis e Intercambio de Información de Servicios Financieros (FS-ISAC) y Akamai muestra que los **ataques DDoS están aumentando nuevamente**, centrándose concretamente en las **entidades financieras europeas**.

Media: La página web del **Parlamento de Finlandia** ha sufrido este martes un **ataque DDoS**, coincidiendo con la conversión del país en el Estado Miembro número 31 de la OTAN. El **grupo ruso Noname 057(16)** se ha atribuido el ataque.

Media: Detectado un nuevo ataque, denominado **proxyjacking**, que aprovechó la **vulnerabilidad Log4j** para acceder e instalar un agente que convirtió la cuenta comprometida en un servidor proxy. Luego, el atacante **vendió las direcciones IP de la víctima** a los servicios de proxyware con fines de lucro.

Baja: Se detectó una campaña maliciosa **cargando muchos paquetes de spam en NPM**, lo que resultó en una DoS y provocó que el servicio de registro **no estuviera disponible esporádicamente**. NPM es un componente crítico para los desarrolladores de software modernos.

Baja: La **CISA** dijo que ayudó a **docenas de hospitales estadounidenses a responder a una serie de incidentes DDoS** la semana pasada que fueron lanzados por el grupo de piratería pro-Kremlin conocido como **Killnet**.

Ingeniería social

Media: Las **estafas mediante BEC están evolucionando** del clásico robo de efectivo mediante la suplantación de proveedores que buscan el pago, a **engañar a las empresas haciéndose pasar por compradores**, para que les envían bienes y materiales a crédito y luego saltarse el pago, revendiendo a su vez la mercancía.

Media: Investigadores detectan actores de amenazas creando **cuentas gratuitas en Quickbooks** y utilizándolas para robar dinero e información de los usuarios finales. Para ello utilizan la **técnica BEC 3.0**: registrarse para obtener una cuenta gratuita en algún lugar legítimo, enviar una factura u otra comunicación e incorporar la actividad maliciosa dentro de eso.

Media: Se ha detectado una nueva oleada de **estafas dirigidas a los sectores de la hostelería y del turismo**, ofreciendo servicios de alquiles en localizaciones como Bali, Dubai, Egipto o Tailandia con **precios sujetos a negociaciones** posteriores, así como **reservas fraudulentas a conciertos, cruceros, tours guiados** y similares. Igualmente, destaca un mercado clandestino en crecimiento que **vende puntos de vuelo, recompensas de hoteles y credenciales robadas de cuentas de aerolíneas**.

Media: **YouTube** ha alertado de una campaña de correos electrónicos maliciosos que **suplantan su marca** con el objetivo de robar las cuentas de los usuarios con el pretexto de un **supuesto cambio en las políticas de monetización** de la plataforma.

Malware

Media: **Typhon Reborn**, malware ladrón de información, presenta su **V2 con capacidades mejoradas** contra el análisis y la máquina virtual (VM) para evadir la detección y dificultar el análisis. **Se espera su aparición en próximos ataques**, certificándose muestras en la naturaleza y múltiples compras en los foros.

Media: Descubierta una **nueva variedad de malware (Rilide)** que apunta a navegadores basados en Chromium como Google Chrome, Microsoft Edge, Brave y Opera. **Se disfraza como una extensión legítima de Drive** y permite a los actores de amenazas llevar a cabo un amplio espectro de actividades maliciosas.

Media: Un empleado de **una empresa de servicios públicos ucraniana** descargó e instaló una versión sin licencia de Microsoft Office desde un sitio web de torrents, lo que provocó que dos **RAT (DarkCrystal y DWAgent)** infectaran los sistemas de la empresa, los cuales se han podido relacionar con el **actor de amenazas ruso Sandworm**.

Media: Múltiples anuncios en fotos clandestinos amenazan con poner a la venta toda una gama de malware dispuesta para su uso:

- Anuncio de lanzamiento próximo del **criptominero AVC Crypto Steealer**, invitando a todos a participar en el proyecto como **MaaS**. El malware dice tener un 90% de éxito e incorporar tecnicas innovadoras.
- Oferta de venta de código fuente de un **malware multifuncional denominado Latrodectus Hasselti**. La descripción afirmaba que el malware fue desarrollado a medida con la mayor parte de su código basado en **exploits de día cero**; tiene ladrón de información, registrador de teclas, **troyano** de acceso remoto (RAT) y funcionalidad de **ransomware**; y puede "matar" cualquier mecanismo de protección antivirus.

- Oferta de venta de **malware multifuncional con robo de credenciales, registro de teclas y funciones de RAT**. Más tarde ese mismo día, el actor ofreció vender un ladrón capaz de robar datos del navegador Google Chrome.
- Oferta de venta de **malware de ladrón de información denominado OSX - MacOS Stealer**, el cual supuestamente puede **extraer credenciales de pago y acceso** de los navegadores, acceder al llavero de contraseñas y a archivos de bases de datos de múltiples formatos. También puede acceder a hashes de múltiples **criptobilleteras**.
- Oferta de venta de **ladrón de información denominado Meow Stealer** que supuestamente recopila datos de navegadores web, criptobilleteras; correo electrónico, FTP, clientes de juegos, mensajería, administradores de contraseñas, y más.

Media: Investigador descubre importantes **fallos del proveedor de IoT Nexx**, que vende una gama de dispositivos "inteligentes" que incluyen abridores de puertas, alarmas para el hogar y enchufes de alimentación conmutables de forma remota. Estos fallos permiten acciones tales como **desactivación, apertura y control** de los dispositivos.

Media: Los **usuarios portugueses** están siendo atacados por un **nuevo malware con nombre en código CryptoClippy** que es capaz de robar criptomonedas como parte de una campaña de publicidad maliciosa.

Baja: **Worok**, un nuevo grupo de **ciberespionaje** que utiliza herramientas previamente desconocidas, ha estado apuntando a **organismos gubernamentales y compañías de alto perfil** en distintos países, principalmente **Asia**.

Informativa: Un **investigador engañó a ChatGPT** para crear un **malware sofisticado con capacidades de exfiltración indetectables**, eludiendo las protecciones contra el uso malicioso del chatbot. El malware divide los documentos, los inserta en archivos de imagen y los envía a Google Drive.

Ransomware

Alta: Aparece el **ransomware 'Rorschach' de autopropagación y cifrado rápido**. Es personalizable y utiliza una rutina de cifrado de archivos muy eficaz que lo convierte en la **familia de ransomware más rápida que existe actualmente**. Se dirige principalmente a **EEUU, Europa, Oriente Medio y Asia**. El grupo, también conocido como **BabLock**, no dispone de sitio de fugas y sus solicitudes de rescate son relativamente modestas (50K-1M USD), lo que les permite operar sigilosamente bajo el radar.

Media: Ha aparecido una **nueva pandilla de ransomware llamada 'Money Message'**, que se dirige a víctimas en **todo el mundo** y exige rescates de millones de dólares para no filtrar datos y liberar un descifrador. El grupo ha incluido ya en su portal de extorsión a **MSI, fabricante taiwanés de piezas de PC**.

Media: Detectado un nuevo **afiliado de ransomware ALPHV, rastreado como UNC4466**, dirigido a instalaciones de **Veritas Backup Exec** expuestas públicamente para acceso inicial a entornos de víctimas. Parece un cambio de orientación del tradicional robo de credenciales al ataque oportunista de CVE.

Media: El **grupo de ransomware Royal** parece haberse dirigido a **más de 1,000 organizaciones con un ataque de ingeniería social**. En él informan falsamente a la víctima que ha sido atacada por el **ficticio grupo "Midnight Group"**, facilitando un archivo donde, supuestamente, se enumeran los datos robados, pero que en realidad es un cargador de malware.

Media: La pandilla de ransomware **Medusa** ha reclamado un ataque cibernético en la **Universidad Abierta de Chipre (OUC)**, que causó graves interrupciones en las operaciones de la organización.

Baja: **Falsos actores de ransomware** apuntan a las **empresas estadounidenses** y las extorsionan con publicar o vender datos supuestamente robados a menos que les paguen. A veces añaden también la **amenaza de un ataque DDoS** si se niegan a pagar.

Baja: **SONDA**, la **multinacional TI más grande del sector en LATAM**, ha sido añadida a las víctimas de **Medusa Ransomware**. La investigación sigue en curso, y SONDA confirma la contratación de MANDIANT para darle respuesta.

Baja: El **Montgomery General Hospital**, de West Virginia, ha sufrido un ataque de ransomware que ha extraído y encriptado **datos heredados de servidores antiguos**. Debido a la antigüedad de los datos, el hospital no ha valorado el pago del rescate.