INFORME CTI DEL 25 AL 31 DE MARZO DE 2023

Resumen de amenazas

	Crítica	Alta	Media	Baja	Info.
APT	0	6	1	2	0
Cadena de suministro	1	1	1	0	0
Amenazas contra datos	0	0	2	1	4
Amenazas contra disponibilidad	0	1	1	1	0
Ingeniería social	0	3	1	2	0
Malware	0	1	15	1	0
Ransomware	0	5	4	5	0

APT

Alta: Se ha observado una **actividad considerablemente elevada por parte del grupo APT Kimsuky, atribuido a la Oficina General de Reconocimiento de Corea del Norte (RGB)**, el principal servicio de inteligencia exterior del país, destacando esta semana los siguientes eventos:

- Kimsuki se ha dirigido a **organizaciones gubernamentales, académicos y grupos de expertos en los Estados Unidos, Europa, Japón y Corea del Sur** durante los últimos cinco años. Está utilizando **tácticas avanzadas y agresivas** de ingeniería social, espionaje y criptominería.
- Los actores de amenazas de Corea del Norte, como Kimsuky, están **robando criptomonedas para financiar operaciones** de piratería bajo un mandato aparente de Pyongyang para ser **autosuficientes**.
- El grupo Kimsuky está utilizando **Alternate Data Stream (ADS) para ocultar su malware**. Este malware es un **Infostealer** que recopila datos iniciando el VBScript incluido dentro de un archivo HTML.
- Kimsuky Group distribuye un **archivo de Word malicioso disfrazado** de plantilla de perfil de correos electrónicos que se hacen pasar por cierto profesor. El malware ha sido **distribuido en GitHub**.

Alta: **Blue Shield of California** está notificando a más de 63,000 clientes que sus datos fueron potencialmente exfiltrados en un compromiso que involucra el **software de transferencia segura de archivos GoAnywhere de Fortra** y uno de los proveedores de salud mental cubiertos por el plan de salud para menores. Se une a la **larga lista de víctimas de ClOp, de todo el mundo**, debido a la explotación de esta vulnerabilidad.

Alta: El **grupo de espionaje ruso Winter Vivern continúa su campaña contra territorios de la OTAN**. Se ha descubierto que ha estado explotando activamente las **vulnerabilidades en los puntos finales de Zimbra** sin parchear desde febrero de 2023 **para robar los correos electrónicos de funcionarios de la OTAN, gobiernos, personal militar y diplomáticos**.

Media: El **APT chino de ciberespionaje Mustang Panda** ha estado apuntando a más de **200 entidades relacionadas con el transporte marítimo, fronterizo e inmigración** como parte de una campaña reciente. Las superposiciones de

focalización observadas llevaron a la identificación de múltiples subgrupos, incluidos los **Grupos 724, 1358 y 5171**, cada uno de los cuales opera típicamente en diferentes sectores y geografías, exhibiendo diferentes herramientas y TTP.

Baja: Se ha identificado una reciente campaña de **distribución de malware vía phishing que apunta a la industria de energía nuclear china**. Las TTP parecen coincidir con las de **Blitter APT**, del sur de Asia.

Baja: Notificada una **nueva familia de implantes no detectada** dirigida a servidores Linux, a la que se ha llamado **Mélofée**. Se ha vinculado con gran confianza este malware a **grupos APT patrocinados por el estado chino**, en particular, el notorio grupo **Winnti**.

Cadena de suministro

Crítica: Se está observando actividad maliciosa emanando de un archivo firmado legítimo del **proveedor de soluciones VoIP/IP PBX 3CX (aplicación 3CXDesktop) señalizando a la infraestructura controlada por un actor de amenazas de Corea del Norte** y desplegando cargas útiles de segunda etapa. **Afecta a miles de usuarios en todo el mundo, y se le considera el último ataque de alto perfil a la cadena de suministro, después de SolarWinds y Kaseya**.

Alta: **OpenAI** dice que un **error de la biblioteca del cliente Redis** estuvo detrás de la interrupción y **fuga de datos** de ChatGPT del lunes pasado, donde los usuarios vieron la información personal y las consultas de chat de otros usuarios. Se ha visto afectada la **información personal y los datos de pago del 1'2% de suscriptores** de ChatGPT.

Media: Al monitorear un ecosistema de código abierto, se han descubierto **más de 60 nuevos paquetes maliciosos PyPI (Python Package Index)** entre principios de febrero y mediados de marzo de 2023. Estos paquetes se relacionan con **ataques de día cero dirigidos a la cadena de suministro**.

Amenazas contra los datos

Media: Las **autoridades de Polonia** han denunciado este lunes que varias **páginas web del Gobierno, del servicio de Contrainteligencia, y de la empresa de industria militar Dezamet**, han sufrido ciberataques perpetrados durante el fin de semana presuntamente por **atacantes de Rusia, como Killnet o NoNa057**.

Media: Un grupo de investigadores académicos de dos universidades en Boston y Bélgica han ideado un nuevo **ataque que puede interceptar el tráfico Wi-Fi en la capa MAC** (control de acceso a los medios), incluso entre clientes que no pueden comunicarse entre sí. Esto **permite que un atacante desconecte el dispositivo de la víctima y se conecte con la dirección MAC de ella**.

Baja: La empresa inmobiliaria **Meriton** ha revelado que **se extrajeron casi 36 GB de datos** en un incidente cibernético que afectó a su unidad de negocio Meriton Suites, debiendo notificar a casi 1900 empleados e invitados de Meriton Suites sobre la infracción.

Informativa: Un **error de configuración en la plataforma de Azure de Microsoft habría permitido el acceso** a servicios de la compañía tecnológica permitiendo la manipulación de los **resultados de búsqueda en Bing** y el espionaje y robo de datos de trabajadores que usan las 'apps' de Office 365. **Microsoft corrigió de inmediato** la configuración incorrecta y agregó verificaciones de autorización adicionales para abordar el problema **y confirmó que no se había producido ningún acceso** no deseado.

Informativa: **Toyota Italia filtró accidentalmente datos confidenciales durante más de un año y medio**, hasta este mes de marzo, lo que permitió a los atacantes lanzar campañas de phishing contra su vasto grupo de clientes.

Informativa: GitHub reconoció haber descubierto esta semana que **la clave privada RSA SSH para GitHub.com había sido expuesta** efímeramente en un repositorio público de GitHub.

Informativa: **PowderRoom**, plataforma dedicada a contenidos de belleza de Corea del Sur, sufre una **filtración de datos que afecta a 1 millón de usuarios** al exponer públicamente una base de datos con información sensible durante más de un año.

Amenazas contra la disponibilidad

Alta: **Alliance Healthcare, la cuarta mayor empresa mayorista de medicamentos de España**, sufre un ciberataque que **impide la distribución de medicamentos** a las farmacias. No han trascendido datos acerca de autores ni tipología del ataque.

Media: **Walsall Healthcare NHS Trust (UK)**, que administra el Walsall Manor Hospital, dijo que se vio afectado por un incidente cibernético "contenido". **Varios hospitales en Europa y Estados Unidos** han sufrido ataques cibernéticos en las últimas semanas.

Baja: **Docomo Pacific, el mayor proveedor de servicios móviles, de televisión, Internet y telefonía** para los territorios estadounidenses de **Guam y las Islas Marianas del Norte** ha sufrido un ciberataque que derribó muchos de sus servicios.

Ingeniería social

Alta: El **Ministerio del Interior** alerta a los ciudadanos acerca de ciberestafas mediante **falsas ofertas de empleo y de alquileres.** Los ciberdelincuentes ofrecen excelentes condiciones y solicitan una transferencia en términos de gastos de gestión, o que llamen a teléfonos de tarifación especial.

Alta: Se ha detectado una **campaña de smishing** donde se informa al cliente acerca de un cargo en su cuenta de **Bankinter o Targobank** y que ha sido bloqueada, precisando realizar acciones accediendo a través del enlace proporcionado.

Alta: Se ha detectado una **campaña de smishing suplantando a La Moncloa ofreciendo el reclamo del reembolso anual de impuestos**, en una supuesta página del Gobierno. En ella también se suplantan diversas entidades bancarias (**Bankia, CaixaBank, BBVA y Santander**), entre las que se puede escoger para recibir el supuesto pago, y en las cuales se produce el robo de credenciales.

Media: Los spammers detrás de los **ataques de recolección de credenciales** están aprovechando el protocolo de archivo distribuido **InterPlanetary File System (IPFS) para distribuir enlaces** de phishing personalizados.

Baja: El **FBI** señala que los delincuentes se están haciendo pasar por los dominios de correo electrónico de las **empresas con sede en los EEUU** para iniciar compras al por mayor y defraudar a los proveedores mediante ataques **BEC**.

Baja: Los estafadores en **Argentina** están utilizando el nombre, la dirección física del comercio y las imágenes que figuran en Google Maps para crear un **falso perfil en Marketplace** y ofrecer figuritas a un precio atractivo.

Malware

Alta: Los **troyanos bancarios Mekoito y Grandoreiro regresan a España** con una nueva oleada de emails fraudulentos, ocultándose como **citaciones judiciales y comprobantes de pago**.

Media: **Operación de malware NullMixer** en curso que afecta a más de 8.000 objetivos en unas pocas semanas, con un énfasis particular en los objetivos de **América del Norte, Italia y Francia**. Incluye nuevos **cargadores polimórficos MaaS** y piezas de código potencialmente **vinculado a Corea del Norte**.

Media: Una nueva campaña de phishing se ha fijado en las **entidades europeas** para distribuir **Remcos RAT y Formbook a través de un cargador de malware denominado DBatLoader**. La carga de malware se distribuye a través de sitios web de **WordPress** que tienen certificados SSL autorizados.

Media: Una oleada de **instaladores del navegador Tor con troyanos** apunta a **Rusia y Europa del Este** con malware de **secuestro de portapapeles** que roba las transacciones de criptomonedas de los usuarios infectados.

Media: Una serie de **vulnerabilidades de día cero** que se abordaron el año pasado fueron **explotadas por proveedores comerciales de spyware** para apuntar a dispositivos Android e iOS. Han sido ubicadas en **Italia, Malasia, Kazajstán y Emiratos Árabes**.

Media: Descubierto nuevo malware, denominado "**OpcJacker**", distribuido a través de **publicidad de VPN falsa**. Cuenta con capacidades de registro de teclas, tomar capturas de pantalla, robar datos confidenciales de los navegadores, cargar módulos adicionales y reemplazar las direcciones de criptomonedas en el portapapeles.

Media: Un nuevo conjunto de herramientas modular llamado **'AlienFox'** permite a los actores de amenazas buscar servidores mal configurados para **robar los secretos de autenticación y las credenciales** para los servicios de correo electrónico basados en la nube.

Media: Un grupo de actividad de amenazas **patrocinado por el estado chino rastreado como RedGolf** se ha atribuido al uso de una **puerta trasera personalizada de Windows y Linux llamada KEYPLUG**.

Media: Un grupo de atacantes desconocido está **apuntando a los agentes de servicio al cliente en las empresas de apuestas y juegos** con un nuevo malware llamado **IceBreaker**. La carga útil es un archivo LNK que parece ser un .jpg, que **los atacantes cargan en la sesión de chat** con los agentes de atención al cliente, para explicarle un supuesto problema, y les piden que descarguen el archivo.

Media: Se registra un incidente en una **empresa mediana del sector de la tecnología médica**, donde se ha encontrado un **malware muy ofuscado que ocultaba el criptominero Monero** en los archivos WAV, y que se propagaba explotando la infame **vulnerabilidad EternalBlue**.

Media: Investigadores universitarios estadounidenses han desarrollado un nuevo ataque llamado "**troyano inaudible de ultrasonido cercano" (NUIT)** que puede lanzar **ataques silenciosos contra dispositivos alimentados por asistentes de voz**, como teléfonos inteligentes, parlantes inteligentes y otros IoT.

Media: Un **nuevo malware conocido como MacStealer** roba información de entornos con sistema operativo macOS de Apple para **desviar información confidencial** de los dispositivos comprometidos. Entre otros, roba datos y contraseñas del llavero de iCloud.

Media: Se han encontrado **nuevas variantes de IcedID (Forked IceID)** sin la funcionalidad habitual de fraude bancario y centrada en **instalar malware, como Emotet y ransomware**. Se ha detectado su utilización en 7 campañas, por 3 actores distintos, incluidos **agentes IAB**.

Media: Un **nuevo Infostealer llamado "LummaC2"** se distribuye disfrazado de programas ilegales como cracks y keygens. Otros programas maliciosos como **CryptBot, RedLine, Vidar y RecordBreaker** (Raccoon V2) se distribuyen de manera similar.

Media: Observadas varias ráfagas de ataque dirigidas a las **vulnerabilidades de Cacti y Realtek** en enero y marzo de este año y luego propagó el **malware ShellBot y Moobot**. Afecta a cualquier organización con **Windows o Linux**.

Media: Reciente campaña de malware se dirige a **billeteras de criptomonedas con un inyector de portapapeles** que reemplaza el contenido de este con direcciones de billeteras alternativas. Se trata de un **ataque simple, pasivo y difícil de detectar**.

Baja: Detectada campaña de correos electrónicos de **phishing suplantando al Servicio Interno de Rentas (IRS)** de EEUU como señuelo para distribuir e instalar el troyano **Emotet**.

Ransomware

Alta: Continúan los constantes ataques de la pandilla **Clop ransomware contra los servidores de almacenamiento seguro Fortra GoAnywhere** en todo el mundo.

- El gigante de bienes de consumo **Procter & Gamble (EEUU) ha confirmado una violación de datos** debido a un ataque de ransomware.
- **Crown Resorts, gigante australiano de casinos**, afirma haber sido víctima de un ataque de ransomware después de una violación de datos en un servicio de transferencia de archivos GoAnywhere

Alta: Alertada la Policía Nacional por una campaña de ransomware dirigida a **despachos de abogados en España**. Los delincuentes, **suplantando la identidad de una clínica estética (Hedonai)**, solicita sus servicios para el supuesto cobro de una deuda, enviando un correo de phishing con un link malicioso de descarga de malware.

Alta: El grupo LockBit lanza su versión 3.0, y está mostrando un nivel de actividad elevada en todo el mundo, incluida España:

- El **Grupo Covesa, el concesionario oficial de Ford en Barcelona y Girona**, ha sido este martes la última víctima de un ataque de ransomware por parte de **LockBit, concretamente su versión 3.0**.
- El grupo de ransomware **LockBit** ha filtrado datos que robó de la **Oficina del Sheriff del condado de Washington** en el noreste de Florida.

Media: La escuela **Tanbridge House School, en West Sussex (UK)**, se incluyó en el sitio web de extorsión de un grupo **Ransom House** el lunes por la noche. Este actor de amenazas es quien ha perpetrado el pasado ataque contra el Clinic de Barcelona.

Media: Ha aparecido una nueva operación de ransomware llamada **'Dark Power'**, y ya ha enumerado, **en su primer mes, a 10 víctimas** en un sitio de fuga de datos de la dark web, distribuyéndose estas por países de todo el mundo.

Media: Un estafador llamado "**OBN Brandon**" ha estado estafando a personas **influyentes de Instagram** y figuras del entretenimiento por cientos de miles de dólares al **cerrar sus cuentas y luego pedir dinero para volver a abrirlas**.

Media: Los grupos de ransomware **Buhti y IceFire Ransom** golpean el software de transferencia de archivos empresarial de **IBM Aspera Faspex** sin parches. Si bien la falla se corrigió en diciembre, IBM no pareció haber detallado de inmediato la vulnerabilidad.

Baja: La **Autoridad de Acueductos y Alcantarillados de Puerto Rico (AAA)** ha sido atacada por el grupo de ransomware **Vice Society**. Los funcionarios señalaron que la infraestructura crítica de la autoridad no se vio afectada por el incidente debido a la segmentación de la red.

Baja: El **gigante de las telecomunicaciones Lumen Technologies (EEUU)** descubrió dos incidentes de ciberseguridad recientes, incluido un ataque de ransomware.

Baja: Un ataque de ransomware en la **ciudad de Modesto (California)** ha sido reclamado por una operación de ciberdelincuencia de **larga duración más de un mes** después de que el gobierno local confirmara que fue atacado. **Snatch** se ha atribuido los hechos.

Baja: Casi medio millón de personas vieron filtrada su **información financiera confidencial** durante un ciberataque a **NCB Management Services**, una empresa de **Pensilvania** que compra deuda.

Baja: El **Instituto de Tecnología Espacial (IST)**, una universidad pública en Islamabad (**Pakistán**), ha sufrido un ciberataque del **ransomware Medusa**.