INFORME CTI DEL 15 AL 21 DE ABRIL DE 2023

Resumen de amenazas

	Crítica	Alta	Media	Baja	Info.
APT	0	1	4	5	2
Cadena de suministro	0	0	2	3	0
Amenazas contra datos	0	2	5	4	1
Desinformación	0	0	1	0	0
Amenazas contra disponibilidad	0	0	1	0	0
Ingeniería social	0	2	2	2	0
Malware	0	1	14	4	0
Ransomware	0	2	4	3	1

APT

Alta: El actor de ciberespionaje rastreado como **Blind Eagle** ha sido vinculado a una nueva cadena de ataque de múltiples etapas que conduce al despliegue del troyano de acceso remoto **NjRAT** en sistemas comprometidos. Este actor suele actúa principalmente en Colombia, pero también, **eventualmente, en España** y toda LATAM.

Media: **APT28 (aka Strontium o Fancy Bear)**, integrado por los Servicios de Inteligencia rusos (**GRU**), aprovechan una **vulnerabilidad en el acceso del Protocolo Simple de Administración de Redes (SNMP) a los routers de Cisco** en todo el mundo, incluidos los de **Europa**, instituciones gubernamentales de EEUU y aproximadamente 250 víctimas ucranianas.

Media: El **gobierno ruso** continúa utilizando una variedad de **ataques de phishing y operaciones de desinformación**, incluidas acciones de piratería y filtración, para respaldar su invasión de Ucrania e intentar causar la **interrupción de la infraestructura crítica**, al mismo tiempo que intentar **influir en la narrativa** acerca de la guerra.

Media: Detectada nueva actividad de explotación del **spyware Pegasus**, del PSOA (proveedor de malware) **NSO Group**, después de encontrar infecciones en varias regiones por todo el mundo afectando a **iPhone antiguos con iOS 15 y iOS 16**. En varios casos en **México** se ha evidenciado un trío de **cadenas de exploits de cero clics** de nombres FINDMYPWN, PWNYOURHOME y LATENTIMAGE.

Media: Evidencias sugieren el regreso del **malware personalizado SysUpdate, del APR Iron Tiger**, el cual incluye nuevas funciones y agrega compatibilidad con infecciones de malware para la **plataforma Linux**.

Baja: Un subclúster maduro del **APT Charming Kitten (APT35, asociado a los Servicios de Inteligencia de Irán)** ha estado armando rápidamente, en los últimos meses, **vulnerabilidades en aplicaciones empresariales comunes** y ha

llevado a cabo campañas de phishing altamente específicas para acceder de manera exitosa a entornos de los **sectores de la energía y el transporte en EEUU**.

Baja: **MuddyWater, APT iraní relacionado con su Ministerio de Inteligencia (MOIS), utiliza SimpleHelp**, una herramienta legítima de administración y control de dispositivos remotos, para garantizar la persistencia en los dispositivos de las víctimas en Oriente Medio y EEUU.

Baja: El **grupo de estado-nación chino Winnti (APT41) apuntó a una organización de medios taiwanesa** para entregar la herramienta redteam de código abierto **Google Command and Control (GC2)** en medio de un abuso más amplio de la infraestructura de Google con fines maliciosos.

Baja: **Shadow Force**, activo desde 2013 apuntando a **corporaciones y organizaciones en Corea del Sur**, está realizando cambios en el malware y las TTP utilizadas en sus ataques, abundando **la puerta trasera Viticdoor** y criptomineros como **CoinMiner**.

Baja: Nuevo **malware para Linux, Poseidon, implementado por el APT pakistaní Transparent Tribe** (APT36), conocido por atacar a las organizaciones del gobierno indio, al personal militar y a los contratistas de defensa.

Informativa: El PSOA (proveedor de malware) israelí **QuaDream**, que hace unos días estuvo en el centro de las miradas debido a la comercialización del spyware EndofDays (aka KingsPawn), está **cerrando sus puertas definitivamente** debido a dificultades financieras.

Informativa: El **líder de Killnet, Killmilk, revela la identidad del nuevo líder de Anonymous Russia, Raty** (descubierto como Arseni Yeliseyeu), en un esfuerzo por consolidar el poder entre los ciberdelincuentes prorrusos. Tras ser Raty arrestado, Killmilk nombró a otro actor llamado "Radis" para encabezar Anonymous Russia en ausencia del primero.

Cadena de suministro

Media: **Rheinmetall, industria armamentística y de automoción alemana**, sufrió un ataque cibernético a la división de su negocio que trata con **clientes industriales**, principalmente en el sector automotriz. Afirma que su división militar no se vio afectada.

Media: Se confirma que el **pasado ataque a Capita**, proveedor británico de servicios de outsourcing a IC de Reino Unido, así como a multinacionales destacadas, ha sido producto de un **ataque de ransomware llevado a cabo por Black Basta**. Parece que se haya **pagado el rescate** o que, al menos, se esté negociando uno.

Baja: **NCR, empresa estadounidense de consultoría de software y tecnología**, está sufriendo una interrupción en su plataforma de punto de venta Aloha después de ser atacado por un ataque de ransomware reclamado por la banda rusa **BlackCat/ALPHV**.

Baja: Se ha concluido que el **ataque de la cadena de suministro de software de Lazarus al desarrollador de teléfonos de escritorio 3CX fue, a su vez, fruto de un ataque a la cadena de suministro por separado y previamente no revelado a Trading Technologies**, un fabricante de software de comercio financiero con sede en Chicago. La fuente infección habría sido un paquete de software comercial retirado, pero aún descargable, llamado X_Trader, descargado por un empleado de 3CX. Este sería el **primer ataque a la cadena de suministro que conduce a otro ataque a la cadena de suministro**, ambos en el sector del desarrollo de software.

Baja: El **proveedor de infraestructura de red** con sede en Carolina del Norte, **CommScope**, confirmó que sufrió un ataque de ransomware a fines del mes pasado y ahora está investigando reclamos de información robada filtrada en la web oscura. El ataque ha sido reivindicado por **Vice Society**.

Amenazas contra los datos

Alta: Los atacantes están utilizando **Eval PHP, un complemento de WordPress legítimo obsoleto**, para comprometer sitios web mediante la inyección de **puertas traseras sigilosas**.

Alta: El **minorista de vehículos Volvo en Brasil**, Dimas Volvo, estuvo **filtrando archivos confidenciales a través de su sitio web durante casi un año**. Sería el último caso de la **constante filtración de datos que está afectando a la práctica totalidad de fabricantes de la industria de la automoción en todo el mundo**.

Media: Los primeros meses de 2023 han visto un **aumento del 41 % en el promedio de ataques semanales por organización dirigidos a dispositivos IoT**, en comparación con 2022, utilizando varias **vulnerabilidades** explotables y afectando, principalmente al **sector de la educación y la investigación**.

Media: Se ha encontrado multitud de **routers obsoletos y descartados de varias empresas que habían sido retirados sin haber borrados sus datos y configuraciones**, y posteriormente puestos a la venta de segunda mano. En ellos **han quedado disponibles datos** de los clientes, claves de autenticación, listas de aplicaciones y mucho más.

Media: Muchos **dispositivos médicos IoT aún funcionan en SO no compatibles y permanecen sin parches**, a pesar del creciente número de ataques al sector de la salud. Los investigadores aluden principalmente a los **sistemas de llamada a enfermeras**, identificando casi 1 de cada 2 dispositivos con CVE sin parchear, con más de un tercio de dichas CVE de riesgo crítico.

Media: **Affinity, desarrollador de software** de publicación, diseño gráfico y edición de fotos con sede en el Reino Unido, informó recientemente a los miembros de su foro sobre una **violación de datos**.

Media: **Aplicaciones de acondicionamiento físico como Strava filtran información de ubicación confidencial** de los usuarios, incluso cuando han utilizado funciones en la aplicación para configurar específicamente zonas de privacidad para ocultar su actividad dentro de áreas específicas.

Baja: La **plataforma de comercio de criptomonedas Bitrue**, con sede en Singapur, ha declarado que se robaron **USD 23 millones** de una de sus propias billeteras digitales.

Baja: Un **ciberataque en un hospital de Ontario**, Canadá, del cual no han trascendido detalles, está provocando retrasos en la atención programada y no urgente.

Baja: El **grupo de medios colombiano Caracol Radio** ha sufrido un ciberataque en sus emisoras y plataformas digitales, **afectando notablemente el funcionamiento** de los sistemas de emisión de publicidad, operaciones de gestión de contenido en radio, publicación digital y streaming.

Baja: La popular **plataforma de alquiler india RentoMojo** comenzó el jueves a informar a los clientes sobre un incidente de **violación de datos en la nube** que podría afectar a cientos de miles de usuarios registrados. El grupo **ShinyHunters** ha comenzado a contactar con los clientes.

Informativa: **Siemens Metaverse**, un espacio virtual del metaverso construido para reflejar máquinas reales, fábricas y otros sistemas altamente complejos ha **expuesto datos confidenciales**, incluidos los planes de oficina de la empresa y los dispositivos IoT.

Desinformación

Media: El **Ministerio de Defensa Nacional de Polonia** emitió una advertencia el miércoles sobre una **reciente campaña de desinformación producida por el grupo bielorruso Ghostwriter**, enviando mensajes falsos a los ciudadanos polacos sobre el posible **reclutamiento para la brigada lituana-polaca-ucraniana**, un ejército multinacional centrado en la realización de operaciones humanitarias y de mantenimiento de la paz. Los piratas informáticos afirmaron falsamente que la brigada participará en operaciones militares en Ucrania.

Amenazas contra la disponibilidad

Media: El **Centro Nacional de Seguridad Cibernética (NCSC)**, una de las principales agencias de seguridad del **Reino Unido**, ha hecho sonar la alarma sobre los **grupos rusos "alineados con el estado" que podrían lanzar ataques destructivos contra la infraestructura nacional crítica**.

Ingeniería social

Alta: Una nueva campaña de phishing en España intenta **obtener credenciales de correo de empresarios, empleados o autónomes que utilizan servicios de Webmail tipo Zimbra** o similares.

Alta: La nueva **Ley de Bienestar Animal**, que afecta directamente a los dueños de animales domésticos, se ha convertido en **objetivo de los ciberdelincuentes**, quienes utilizan técnicas de phishing para engañar a los usuarios y robar sus datos personales al **suplantar a organizaciones animalistas** o informar sobre la nueva ley de bienestar animal.

Media: Se ha estado observando una **campaña de malvertising a través de Google adds dirigida a personas mayores**, creando cientos de **sitios web falsos a través de la plataforma Weebly** para alojar contenido señuelo para engañar a los motores de búsqueda y rastreadores mientras redirige a las víctimas a una alerta de computadora falsa.

Media: Varios investigadores han observado un **gran aumento en los fraudes por correo electrónico de extorsión** durante el último mes. La intención de estos correos es **intimidar a las personas para que paguen** una cantidad específica de dinero para **evitar consecuencias desagradables** de diversa índole, a menudo falsas, como supuestos ataques derivados o la difusión de contenidos privados de la víctima que aseguran poseer.

Baja: Los ciberdelincuentes han estado aprovechando técnicas de ingeniería social para **hacerse pasar por Zelle, popular red de pagos digitales con sede en EEUU**, y robar dinero de sus clientes. Han utilizado métodos de **phishing y spoofing** para engañar a sus víctimas.

Baja: De un modo análogo a lo sucedido tras la quiebra del Silicon Valley Bank (SVB), ahora los ciberatacantes están **aprovechando la quiebra del criptogigante FTX para crear varios sitios de phishing** solicitando a los usuarios que envíen su dirección de criptobilletera para recibir un reembolso.

Malware

Alta: Detectadas en **Google Play, al menos, 16 aplicaciones** que tienen alojada una carga util de un nuevo **malware Clicker**. En total, estas apps contarían con **20M de instalaciones**. Tras notificar a Google, las aplicaciones ya no están disponibles.

Media: Aumento significativo de la distribución mediante phishing del malware **EvilExtractor**, herramienta dirigida a Windows con **funcionalidades de spyware y un módulo ransomware (Kodex Ransomware)**. La mayoría de sus víctimas se encuentran en **Europa** y América.

Media: Un **nuevo troyano de Android llamado 'Chameleon'** ha estado apuntando a usuarios en **Australia y Polonia** desde principios de año, **imitando** el intercambio de criptomonedas CoinSpot, una agencia del gobierno australiano y el banco IKO.

Media: Se ha descubierto una nueva campaña de **Lazarus**, considerada parte de la **"Operación DreamJob" (aka DeathNote)** dirigida a usuarios de **Linux** con malware por primera vez. Va dirigida a **personas que trabajan en software o plataformas DeFi** con ofertas de trabajo falsas en LinkedIn u otras redes sociales y plataformas de comunicación.

Media: **Fortra ha analizado la oleada de ataques a su producto GoAnywhere MFT** (principalmente a cargo de ClOp Ransomware), explotando la CVE-2023-0669, y ha identificado en muchos de los entornos la instalación de dos herramientas adicionales: **Netcat**, para establecer puertas traseras, y **Errors.jsp**, para crear webs dinámicas.

Media: CISA informa de un nuevo malware identificado como una **variante del malware conocido como ICONICSTEALER**. Esta variante de malware se utilizó en el ataque a la cadena de suministro del software comercial **3CXDesktopApp**.

Media: Continúa la **evolución del gusano Raspberry Robin**, siendo actualmente uno de los malware más distribuidos, e utilizados por **actores como IcedID, ClOp** y más. Destaca por tener **gran cantidad de trucos y evasiones únicos e innovadores**, y por contar con dos **exploits para escalada de privilegios**, otorgándole capacidades en el área de explotación. Agrega varias cadenas de evasión en muchas etapas, lo que hace que su depuración sea, en palabras textuales de los investigadores, **"un infierno"**.

Media: Producidos **varios incidentes de ransomware (dos de Medusa Locker y uno de Lockbit)** en los que los atacantes intentaron desactivar los clientes de EDR con una **nueva herramienta de evasión de defensa denominada AuKill**. Esta herramienta abusa de una versión obsoleta del **controlador Process Explorer, de Microsoft**.

Media: El **grupo de ransomware Play está utilizando dos nuevas herramientas a medida** que le permiten enumerar todos los usuarios y computadoras en una red comprometida (**Infostealer.Grixba**) y copiar archivos del Servicio de instantáneas de volumen (VSS) que normalmente están bloqueados por el sistema operativo (**herramienta Costura**).

Media: Una nueva versión de una **variante de Mirai llamada RapperBot** es el último ejemplo de malware que utiliza **vectores de infección poco comunes** o desconocidos para tratar de propagarse ampliamente. RapperBot apareció por primera vez como **botnet de IoT**.

Media: Descubierta **nueva familia de malware de puerta trasera, denominada "Domino"**, que se supone creada por desarrolladores asociados con el grupo **FIN7**, y que actualmente está siendo usado por **Trickbot** (antiguos miembros de Conti) para entregar el ladrón Project Nemesis, el cargador Dave Loader y otras puertas traseras de Cobalt Strike.

Media: Un **novedoso malware de robo de credenciales llamado Zaraza bot** se ofrece a la venta en un canal ruso de piratas informáticos de Telegram y también utiliza el popular servicio de mensajería como C2. **Se dirige a una gran cantidad de navegadores web (hasta 38** navegadores web diferentes, incluidos Google Chrome, Microsoft Edge, Opera, AVG Browser, Brave, Vivaldi y Yandex).

Media: Tras encontrar, la semana pasada, evidencias de una campaña inactiva de **Qbot**, se ha descubierto que el malware ahora se distribuye en **campañas de phishing que utilizan archivos PDF y Windows Script Files (WSF)** para infectar dispositivos Windows. Los mensajes se basan en **correos comerciales reales** a los que los atacantes habían tenido acceso, lo que les brindaba la oportunidad de unirse al hilo de correspondencia con sus propios mensajes.

Media: Se ha detectado y analizado el **cargador 'in2al5d p3in4er'**, el cual utiliza una **técnica de evasión sorprendentemente simple pero altamente efectiva**, utilizado para realizar la entrega efectiva y sigilosa del **ladrón Aurora**. El cargador apunta a estaciones de trabajo de punto final que utilizan técnicas avanzadas anti-VM (máquina virtual).

Media: Evidencias sugieren el regreso del **malware personalizado SysUpdate, del APR Iron Tiger**, el cual incluye nuevas funciones y agrega compatibilidad con infecciones de malware para la **plataforma Linux**.

Baja: Una nueva campaña, denominada **Operación Quinea Pig, intenta distribuir el RAT AgentTesla** apuntando principalmente a **México, Colombia y Ecuador** mediante correos de phishing especialmente dirigidos. En algunos casos se ha **suplantado la identidad de un operador de logística** mundialmente conocido.

Baja: El grupo **8220 Gang** está utilizando la **vulnerabilidad Log4Shell para instalar CoinMiner en los servidores VMware Horizon**. Entre las víctimas había empresas coreanas relacionadas con la **energía** con sistemas vulnerables y sin parches.

Baja: Se ha distribuido en Japón, **mediante Google Play, un malware disfrazado de una app de seguridad móvil** legítima, llamada **Smartphone Anshin Security**. Este es un malware de fraude de pago que roba contraseñas y abusa del proxy inverso dirigido a los servicios de pago móvil.

Baja: Los **proveedores de servicios de telecomunicaciones en África** son el objetivo de una nueva campaña de espionaje orquestada por el actor chino **Evasive Panda (aka Daggerfly)** al menos desde noviembre de 2022. Han empleado diferentes familias de malware, como **MgBot**, y abusado del RMM legítimo **AnyDesk**.

Ransomware

Alta: El grupo de ransomware **LockBit ha creado encriptadores dirigidos a Mac por primera vez**, probablemente convirtiéndose en la primera operación de ransomware importante que apunta específicamente a macOS.

Alta: La pandilla de ransomware **Medusa** ha puesto en línea lo que afirma es una **fuga masiva de materiales internos de Microsoft, incluido el código fuente de Bing y Cortana**. De momento, se desconoce la legitimidad del material y la veracidad de la declaración.

Media: Los investigadores de seguridad advierten que los ciberdelincuentes utilizan cada vez más el **software de acceso remoto (RMM) Action1** para permanecer en redes comprometidas y ejecutar ataques de ransomware. Se han relacionado ataques de este tipo con el **grupo Monti**.

Media: La banda de ransomware **Vice Society** está implementando un **script PowerShell nuevo y bastante sofisticado para automatizar el robo de datos** de redes comprometidas, utilizando binarios y scripts Living off the Land (**LotL**) para pasar inadvertidos.

Media: Se está encontrando el recién descubierto **ransomware Trigona instalado en servidores MS-SQL** mal administrados.

Media: Un ransomware llamado **BabLock (aka Rorschach)** ha captado recientemente la atención debido a su **cadena de ataque sofisticada y de rápido movimiento** que utiliza técnicas sutiles pero efectivas. Aunque se basa principalmente en LockBit, es una mezcla de partes diferentes del ransomware reunidas y no se cree que comparta los mismos autores.

Baja: El gobierno local de un **suburbio de St. Louis, Missouri**, está investigando un "incidente de seguridad de la red" que se cree que comenzó el mes pasado pero que aún afecta los sistemas. El **grupo Royal Ransomware** se ha atribuido la autoría.

Baja: La **aseguradora de salud sin fines de lucro Point32Health, Massachusetts**, dice que desconectó los sistemas para contener un ataque de ransomware identificado esta semana.

Baja: El **ransomware BlackBit se está viendo distribuído en Corea**, disfrazado como **svchost.exe**. Se han identificado características similares con el ransomware LokiLocker.

Informativa: En referencia al **supuesto ataque de LockBit** de la semana pasada a la empresa IT británica de ciberseguridad "**Darktrace**", se ha descubierto que los ciberdelincuentes **han confundido dicha empresa con DarkTracer, empresa CTI de Singapur**, siendo de esta última, y no de la primera, de la que han filtrado datos en su leak site.