INFORME CTI DEL 11 AL 17 DE MARZO DE 2023

Resumen de amenazas

	Crítica	Alta	Media	Baja	Info.
APT	1	3	3	3	0
Cadena de suministro	0	0	0	2	0
Amenazas contra datos	0	1	2	6	3
Amenazas contra disponibilidad	0	1	0	2	0
Ingeniería social	0	2	2	3	0
Malware	0	3	8	4	1
Ransomware	0	1	7	4	0

APT

Crítica: El actor de amenazas **STRONTIUM (APT28)**, patrocinado por el Estado ruso (y especialmente vinculado con sus Servicios de Inteligencia), **explota activamente la vulnerabilidad 0-day de Microsoft Outlook/365**, de escalada de privilegios sin interacción del usuario. Hay evidencias de ataque desde abril de 2022, afectando principalmente, en Europa, a **entidades gubernamentales y militares, industria, petróleo/gas y transporte**.

Alta: El estancamiento militar lleva a **Moscú a cambiar el foco, migrando de los ataques a la disponibilidad al ciberespionaje**, el robo de datos y las operaciones psicológicas. Atacan activamente la infraestructura civil y crítica con la esperanza de que abra la puerta a operaciones de influencia y futuras negociaciones. Microsoft dice que Rusia ha apuntado a **17 naciones europeas en 2023**, y a 74 países desde el comienzo de la guerra.

Alta: Se ha detectado campaña en curso de **Nobelium** (prolífico APT patrocinado por los **Servicios de Inteligencia rusos) dirigida a los países UE**. Específicamente, apunta a sus **entidades y sistemas diplomáticos** para transmitir información confidencial acerca de la política de la región, de la ayuda que se le brinda a los ciudadanos ucranianos que huyen del país y de la brindada al gobierno de Ucrania.

Alta: Un grupo ruso de piratería avanzado llamado **'Winter Vivern' apunta a organizaciones gubernamentales europeas y proveedores de servicios de telecomunicaciones para realizar espionaje**, usando escaneos antivirus falsos para instalar el spyware **Aperetif**.

Media: Un grupo de espionaje de Corea del Norte asociado al **Grupo Lazarus emplea familias de malware previamente indocumentadas** como parte de una campaña de phishing dirigido a **organizaciones tecnológicas y de medios estadounidenses y europeos** desde junio de 2022. Afecta principalmente a investigadores de seguridad y organizaciones de medios con **ofertas de trabajo falsas** que conducen al despliegue de tres nuevas familias de malware personalizadas.

Media: Un nuevo actor de amenazas, denominado **YoroTrooper**, ha estado ejecutando varias **campañas de espionaje exitosas desde al menos junio de 2022**, implementando toda clase de **malware** ladrón y de acceso remoto. Sus objetivos principales son **organizaciones gubernamentales y energéticas de Estados de la CEI y de Europa** del Este, así como una IC de atención médica de la UE y la Organización Mundial de Propiedad Intelectual.

Media: Se ha encontrado malware del grupo **APT Iron Tiger** comprometiendo los servidores de la **aplicación de chat Mimi** en un **ataque a la cadena de suministro**. Un servidor albergaba una muestra de **HyperBro** y un ejecutable Mach-O malicioso llamado "rshell", apuntando a usuarios tanto de **Windows, como de Mac o Linux**.

Baja: **APT Dark Pink** se ha relacionado con un conjunto de ataques dirigidos a **entidades gubernamentales y militares en el sudeste asiático** con un malware llamado **KamiKakaBot**. Su objetivo es el robo de información, la ejecución de código remoto, con avanzadas técnicas de ofuscación y evasión.

Baja: El grupo **Tick APT** lleva a cabo un **importante ataque a la cadena de suministro**, introduciendo malware en una **empresa de desarrollo de software de prevención de pérdida de datos, en Asia oriental**, resultando en la distribución de malware en los dispositivos de los clientes de la empresa. Los atacantes desplegaron 3 familias de malware y un **descargador sin documentar (ShadowPy)**, y la cartera de clientes de la empresa incluye **entidades gubernamentales y militares**.

Bajo: Un **sofisticado ataque en la nube de varias etapas** resulta en pérdida de datos sensibles de un cliente anónimo. Involucra una **cadena de explotación compleja**, incluido el robo de credenciales, el despliegue de malware como señuelo y el movimiento lateral entre los **servicios de AWS**. Las TTP del evento se asocian al retirado grupo de amenazas **TeamTNT**.

Cadena de suministro

Baja: El grupo de ransomware **LockBit afirma haber robado valiosos archivos de SpaceX**, empresa espacial de Elon Musk, después de violar los sistemas de la empresa de producción de piezas de repuesto **Maximum Industries**. Si bien el proveedor puede haber sido pirateada, no es raro que estos grupos hagan afirmaciones exageradas sobre el impacto de sus ataques o el valor de los datos que han obtenido.

Baja: **Latitude Financial Services (Latitude) reveló una violación de datos** después de sufrir un ataque cibernético, lo que provocó el **robo de credenciales de un trabajador** de la firma. Luego, estas credenciales se usaron para iniciar sesión en dos de los proveedores de servicios de la empresa para robar **datos de clientes**.

Amenazas contra datos

Alta: **Kernelware**, el actor de amenazas de quien la semana pasada tuvimos la noticia de que se había introducido y robado información de HBD Financial Services y HACER Ind., filtra ahora **21 GB de datos de Acronis, empresa suiza de protección de datos y seguridad en la nube**.

Media: Las **elecciones parlamentarias de Estonia** de este mes fueron atacadas sin éxito por ataques cibernéticos, presuntamente perpetrados por **actores rusos**. No ha trascendido más información al respecto, pero su Primera Ministra declara estar bajo una **ola masiva de ataques desde hace un año**.

Media: El **sitio de la dark web BidenCash**, dedicado a la venta de datos de tarjetas de crédito y débito robadas, cumplió un año y lo celebró **publicando de forma gratuita una base de datos con 2.165.700 tarjetas** de crédito y débito.

Baja: El equipo de **GSC Game World** (Ucrania) ha explicado que la cuenta de uno de sus trabajadores en una aplicación de trabajo colectivo con imágenes ha sido **'hackeada' por un grupo que dice ser ruso** y que está usando los datos robados para "**chantajear e intimidar**".

Baja: La plataforma de atención médica remota **'Cerebral'** está enviando avisos de **violación de datos a 3,18 millones de personas** que han interactuado con sus sitios web, aplicaciones y servicios de telesalud.

Baja: El **desarrollador de tecnología médica Zoll Medical** está notificando a aproximadamente **un millón de personas** que su información personal podría haberse visto comprometida en una **violación de datos** reciente.

Baja: El **sistema de registro de defunciones en Hawái** tuvo una violación de datos, con potencial afección a **asuntos pendientes de los fallecidos**, como cuentas, patrimonio, reclamo de seguro de vida o beneficios de sobreviviente del Seguro Social.

Baja: **Independent Living Systems (ILS)**, una administración de atención médica con sede en Miami y proveedor de soluciones de atención administrada, sufrió una violación de datos que expuso la **información personal de 4,226,508 personas**. La cantidad de personas afectadas hace que esta sea la mayor violación de datos en el sector de la salud revelada este año.

Baja: Dos personas, pertenecientes a un grupo delictivo neoyorquino conocido como "**Vile**", han **violado una base de datos policial** y usado los datos robados para **extorsionar a sus víctimas** haciéndose pasar por oficiales de policía.

Informativa: La **multinacional de aviación Safran Group**, con sede en Francia, y el octavo proveedor aeroespacial más grande del mundo, estaba **filtrando datos confidenciales debido a una mala configuración** de sus sistemas. La vulnerabilidad dejó a la empresa en riesgo de ataques cibernéticos probablemente durante más de un año.

Informativa: Investigadores encuentran un **entorno desprotegido** y archivos de configuración alojados en el sitio web oficial de **BMW Italia**, destinados a almacenarse localmente, que incluían datos sobre entornos de producción y desarrollo. Se están observando continuas brechas de seguridad de los datos manejados por la práctica generalidad de fabricantes de automóviles.

Informativa: **WebsitePlanet** fue informada recientemente del descubrimiento de una **base de datos no protegida** con contraseña que contenía registros relacionados con una **plataforma de venta de criptomonedas**. Los registros incluían nombres de clientes, números de cuentas bancarias, registros de compras y ventas, y más.

Amenazas contra la disponibilidad

Alta: Se han detectado **intentos de ataques DDoS a cuatro hospitales catalanes este 2023**. Grupos de ciberdelincuentes rusos los han incluido en su lista de objetivos y constan notificaciones de amenazas contra ellos desde febrero.

Baja: **Essendant**, un distribuidor mayorista de artículos de papelería y de oficina de EEUU, está experimentando una **grave interrupción de varios días que impide cualquier actividad**. No han trascendido los motivos, pero se deduce un ataque informático.

Baja: Una operación cibernética maliciosa generalizada ha **secuestrado miles de sitios web dirigidos a audiencias de Asia oriental** para redirigir a los visitantes a contenido para adultos y páginas de apuestas.

Ingeniería social

Alta: Ciberdelincuentes ha lanzado una campaña de phishing en las que **suplantan la identidad de personalidades conocidas y medios de comunicación** (como El País, ABC o El Mundo), a través del envío de correos electrónicos con **noticias falsas de criptomonedas**, con los que obtienen la información personal de la víctima.

Alta: Se ha detectado una campaña de **mensajes fraudulentos a través de WhatsApp suplantando a la empresa de cerveza Mahou**. El objetivo es redirigir al usuario a una web fraudulenta, con el motivo de un concurso que está organizando Mahou por el Día del Padre.

Media: Un **kit de phishing adversary-in-the-middle (AiTM)** de código abierto ha interesado a una serie de actores de amenazas por su capacidad para orquestar **ataques a escala**. La creación del kit se atribuye al actor **DEV-1101**, y se ha localizado a otro actor conocido como **DEV-0928** realizando un patrón de ataque destacado, con una **campaña de más de 1M de correos** electrónicos desde septiembre de 2022.

Media: Nueva **estafa en Twitter a clientes de bancos**. Se aprovecha de los clientes que tuitean a sus bancos, por ejemplo, para presentar una queja o solicitar asistencia. Pero estos clientes, en cambio, reciben una respuesta del estafador, a través de un tweet de cita, atrayéndolos a llamar al **número de "línea de ayuda" del estafador**.

Baja: Circula por WhatsApp un engaño que promete un **subsidio ofreciendo supuestas ayudas económicas en varios países de América Latina**. Utilizan técnicas de ingeniería social, como phishing o spoofing, suplantando páginas del Gobiermo, para mostrar anuncios maliciosos.

Baja: **Subvención falsa de la Administración de Pequeñas Empresas (SBA)** utilizada en una nueva estafa de phishing en **EEUU**. El actor envía comunicados reales de la SBA con una cuenta de correo y un adjunto maliciosos, redirigiendo a la víctima a una página de robo de credenciales.

Baja: Tras la quiebra del **Silicon Valley Bank (SVB)**, ya hay en curso varias campañas de **phishing, registro de dominios sospechosos y preparación de ataques BEC** dirigidas a los antiguos clientes de la entidad, ofreciéndoles servicios falsos relacionados con el colapso del banco.

Malware

Alta: El malware **Xenomorph para Android** ha lanzado una nueva versión que agrega capacidades significativas, incluido un nuevo marco de sistema de transferencia automatizado (ATS) y la capacidad de robar credenciales para 400 bancos. Se distribuye como **MaaS, especialmente en España**, y parece ser **uno de los troyanos más avanzados y peligrosos en circulación**.

Alta: Se ha detectado que uno de los objetivos principal de la **nueva versión mejorada de la botnet Prometei** tiene como objetivo entregar a su víctima el **malware de criptominería Monero** y herramientas actualizadas de **robo de credenciales**. Como se ha adelantado en semanas anteriores, Prometei está teniendo una **difusión global**.

Alta: Se ha observado cada vez más que los actores de amenazas usan **videos de YouTube para propagar variedades de malware ladrón como Raccoon, RedLine y Vidar**. Los videos se disfrazan de tutoriales para descargar de forma

gratuita sofware de pago que requiere licencias. Algunos de los vídeos han sido **generados mediante IA**, y ya se han detectado víctimas en España.

Media: Se han descubierto docenas de sitios web **imitando Telegram y WhatsApp**, dirigidos principalmente a usuarios de Android y Windows, con versiones troyanizadas **clipper**, que roban y modifican el contenido del portapapeles para buscar **fondos de criptomonedas**.

Media: Malware chino **SilkLoader**, diseñado para cargar **balizas Cobalt Strike, vendido a ciberdelincuentes rusos**. Se relaciona SilkLoader con varias intrusiones operadas por humanos que probablemente fueron el precursor de un ataque de ransomware.

Media: Los delincuentes crean **sitios web falsos de streaming que ofrecen ver las películas nominadas a los Oscar** de forma gratuita, incluyendo películas aún no estrenadas. Estas páginas motivan a los usuarios a proporcionar información personal y bancaria, y descargar archivos que contienen malware.

Media: Operación de amenazas **DUCKTAIL** resurge con nuevos LNK, PowerShell y otras tácticas personalizadas para evitar la detección. El malware persigue **robar cookies** del navegador y exfiltrarlas por Telegram, localizando cuentas comerciales de Facebook para administrarlas.

Media: **GoBruteforcer** es un nuevo tipo de malware de **botnet** que está escrito en Golang y se dirige a servidores web, específicamente aquellos que ejecutan **servicios phpMyAdmin, MySQL, FTP y Postgres**.

Media: El descargador **BATLOADER** continúa utilizándose ampliamente en la actualidad. En el último caso conocido, **abusa de Google Ads** para entregar cargas útiles secundarias como **Vidar Stealer y Ursnif**. Una de las características clave de sus operaciones es el uso de tácticas de **suplantación de identidad de software** para la entrega de malware.

Media: La CISA y el FBI determinaron que múltiples actores de amenazas cibernéticas, incluido un actor **APT**, explotar**on la vulnerabilidad de Progress Telerik en el servidor de Internet Information Services (IIS) del gobierno de EEUU**, consiguiendo ejecutar en él código remoto y descargar malware.

Media: El malware **ShellBot** se está instalando en **servidores Linux SSH mal administrados**. ShellBot, también conocido como PerlBot, es un **malware DDoS Bot** desarrollado en Perl y, de forma característica, utiliza el protocolo IRC para comunicarse con el servidor C&C.

Media: Detectada una nueva **campaña de cryptojacking dirigida a cústeres de Kubernetes para Dero Mining**, Se concentra en ubicar clústeres de Kubernetes con acceso anónimo habilitado en una API de Kubernetes y escuchar en puertos no estándar accesibles desde Internet.

Baja: Descubierto recientemente un **malware CHM**, supuestamente creado por el grupo **Kimsuky** (Corea del Norte), disfrazado de **cuestionario sobre asuntos estatales**. Si el destinatario acepta la entrevista, se envía un adjunto para instalar el malware.

Baja: Una **nueva versión de GoatRAT** funciona como un troyano bancario, dirigido específicamente a los **bancos brasileños**. Además, durante os últimos seis meses, varios troyanos bancarios para Android, incluidos **BrasDex, Xenomorph y PixPirate**, han incorporado un **marco ATS** para realizar transferencias no autorizadas.

Baja: El malware de Android **'FakeCalls'** está circulando nuevamente en **Corea del Sur**, imitando las llamadas telefónicas de más de 20 organizaciones financieras e intentando engañar a los clientes bancarios para que revelen los datos de sus tarjetas de crédito.

Informativa: Investigadores en Corea han presentado un nuevo **ataque de canal encubierto llamado CASPER que puede filtrar datos de ordenadores desconectados** de la red a un teléfono inteligente cercano. El ataque utiliza los **altavoces internos para transmitir audio de alta frecuencia** en forma de código binario o morse, y se vale de una infección previa por malware.

Ransomware

Alta: Los responsables del **ciberataque que sufrió la Diputación de Córdoba** a primeros del pasado mes de febrero han amenazado a la institución provincial con divulgar la información que, supuestamente, han logrado de forma fraudulenta, de la **Empresa Provincial de Informática (Eprinsa).**

Media: En lo que probablemente sea obra de **Vice Society**, el **internado estatal más grande del Reino Unido**, Wymondham College, ha anunciado que se ha convertido en víctima de un "ataque cibernético sofisticado".

Media: El **Centro Hospitalario Universitario San Pierre de Bruselas** ha sido objeto de un ataque informático por el que no se sabe si se ha pedido un rescate. Se convierten en la última institución objeto de una serie de ciberataques contra hospitales europeos.

Media: Presunto actor de espionaje chino **(UNC3886) utiliza ESXiArgs para explotar el 0-day de FortiOS** parcheado este mes en ataques dirigidos al gobierno y a grandes organizaciones que han llevado a la corrupción del sistema operativo y los archivos y la pérdida de datos.

Media: **Ring, una empresa de cámaras y seguridad para el hogar y sistemas domésticos inteligentes** propiedad de Amazon, podría haber sufrido un ataque de ransomware por parte del grupo **ALPHV vinculado a Rusia**. No está claro qué datos se robaron o qué rescate se exigió, pero las implicaciones potenciales para los clientes podrían ser graves.

Media: El grupo de ransomware **BianLian Gang continúa evolucionando** y agregando a su lista cada vez más número de víctimas. Muestran alto nivel en seguridad operativa y habilidades de penetración, y han evolucionado del método del cifrado al de la extorsión por fuga de datos. Afecta, **principalmente, a EEUU, con presencia residual en Europa**, India y Oceanía.

Media: Alertan de **nueva cepa de ransomware denominada "Trigona"**, la cual apunta a industrias de fabricación, finanzas, construcción, agricultura, marketing y alta tecnología. Se involucra en comportamientos como obtener acceso inicial al entorno de un objetivo, realizar reconocimiento, transferir malware a través del software de administración y monitoreo remoto (RMM), crear nuevas cuentas de usuario e implementar ransomware.

Media: **Magniber Ransomware Group** explota---------- una **vulnerabilidad 0-Day de Microsoft** basada en firmas de SmartScreen, aprovechándolo para entregar ransomware.

Baja: La **empresa estadounidense de ciberseguridad Rubrik** ha confirmado que sus datos fueron robados utilizando una vulnerabilidad de día cero en la plataforma de transferencia segura de archivos **Fortra GoAnywhere**. El ataque se le atribuye al grupo ruso de ransomware **ClOp**.

Baja: La **Autoridad de Vivienda de la Ciudad de Los Ángeles (HACLA)** advierte sobre un "evento de seguridad de datos" después de que el grupo de ransomware **LockBit** haya apuntado a la organización y filtrado datos robados en el ataque.

Baja: Un ataque de ransomware elimina la capacidad de procesamiento de pedidos, de envío de productos y de proporción de servicios de **MKS Instruments**, fabricante estadounidense de equipos de semiconductores. El ataque le supondrá **pérdidas estimadas de $200M**.

Baja: Descubierta recientemente la distribución del **ransomware Mallox disfrazado de programa relacionado con DirectPlay**. Se ha detectado en servidores MS-SQL vulnerables de Corea.