INFORME CTI DEL 4 AL 10 DE MARZO DE 2023

Resumen de amenazas

	Crítica	Alta	Media	Baja	Info.
APT	0	3	0	1	0
Cadena de suministro	0	0	0	2	0
Amenazas contra datos	0	2	1	7	0
Desinformación	0	0	1	0	0
Amenazas contra disponibilidad	0	0	1	1	0
Ingeniería social	0	2	3	0	0
Malware	0	2	11	3	2
Ransomware	0	2	3	3	0

APT

Alta: Varios grupos APT utilizan campañas de phishing y malware para dirigirse a los solicitantes de empleo. Utilizan técnicas de **spoofing y typo squating para distribuir malware (Emotet, Agent Tesla, Cryxos, Nemucod**) tanto a empleadores como a solicitantes de empleo en EEUU, Asia u Europa, incluyendo España.

Alta: Creciente interés de los ciberdelincuentes por las debilidades de la seguridad en la infraestructura de carga de vehículos eléctricos (EV). Se han observado **vulnerabilidades** que pueden dirigir a ataques DDoS, robo de información o *man in the middle*, así como ejecución de **versiones obsoletas de Linux**.

Alta: Identificada campaña de persistencia a largo plazo del grupo UNC4540 mediante ejecución de **malware en dispositivos SonicWall Secure Mobile Access (SMA)** sin parches. Implementa una variante de TinyShell que tiene la funcionalidad de robar credenciales de usuario, proporcionar acceso de shell y persistir a través de actualizaciones de firmware.

Baja: Operación de ciberespionaje de larga duración del grupo chino Sharp Panda, dirigida a **entidades gubernamentales del sudeste asiático**. Se han valido de correos de phishing para distribuir documentos RTF armados con el kit RoyalRoad y una nueva versión del cargador SoulSearcher.

Cadena de suministro

Baja: AT&T, la multinacional de telecomunicaciones más grande del mundo (EEUU) está notificando a aproximadamente 9 millones de clientes que parte de su información quedó expuesta después de que un **proveedor de marketing fuera pirateado**.

Baja: Un ataque de ransomware contra el gigante de la ingeniería Black & McDonald ha puesto en riesgo la integridad de Canadian Base Operators, quien tiene contratos con el **Departamento de Defensa Nacional de Canadá**. Estos últimos afirman no haberse visto afectados.

Amenaza contra datos

Alta: Hacienda reportó otro ataque cibernético más que puso en jaque a los funcionarios, llegando a bloquear todos los sistemas operativos. Están investigando los posibles daños causados, y algunas fuentes apuntan que han logrado **robar parte de las credenciales** de la Agencia Tributaria.

Alta: Investigadores detectan que el 92% de las aplicaciones de servicios bancarios y financieros más populares en EEUU y Europa contienen **brechas de seguridad** que exponen secretos y datos altamente sensibles y fáciles de extraer.

Media: Una violación de datos de la tecnológica Acer Inc. resulta en el robo de un total de **160 GB de 655 directorios y 2869 archivos**. Un actor conocido como ***Kernelware*** se atribuye la responsabilidad y ofrece la venta de los datos.

Baja: DC Health Link sufrió una importante filtración de datos que potencialmente expuso información de miles de afiliados. La violación de datos **afecta a miembros y personal de la Cámara de Representantes de EEUU**. Al menos un actor de amenazas (***IntelBroker***) está vendiendo la información en un foro de piratería.

Baja: Una vulnerabilidad grave en la plataforma de Toyota Customer 360 permitió a un investigador de seguridad acceder a la **información personal de los clientes de la automotriz en México**. Es importante resaltar que es el tercer incidente en el que se ve involucrado Toyota en lo que va de año, en el ámbito de seguridad de los datos.

Baja: Se han producido varias violaciones de datos en grandes empresas y multinacionales de todo el mundo:

- La cadena estadounidense de comida rápida Chick-fil-A notifica aproximadamente a 71,000 personas que sus cuentas de usuario se vieron comprometidas en una **campaña de relleno de credenciales** de dos meses de duración.
- El grupo **Dark Angels** roba 3 TB de información corporativa y de empleados de la multinacional brasileña Andrade Gutiérrez, la cual opera en los sectores infraestructura, energía, petróleo y gas, y transportes.
- La **subsidiaria de Commonwealth Bank en Indonesia** sufre un ataque del que se deriva el acceso no autorizado al software de gestión de proyectos.
- El actor ***Kernelware*** (el mismo de la violación de datos de ACER Inc.) publicó archivos supuestamente robados de HDB Financial Services. El pirata informático dice que los archivos contienen **más de 73 millones de entradas**.

Desinformación

Media: Rusia continúa con su campaña de desinformación en torno a la guerra de Ucrania a través de **ingeniería social avanzada** realizada por un grupo de amenazas identificado como **TA499** (Vovan y Lexus). Realizan suplantación de identidad del Primer Ministro ucraniano y de embajadas oficiales para grabar altas personalidades americanas y europeas, tanto por llamada como por videoconferencia.

Amenaza contra la disponibilidad

Media: El sitio web del servicio de impuestos de Polonia fue atacado por un **ataque DDOS** perpetrado por el grupo prorruso **NoName057(16)**.

Baja: Advertida una campaña de redirección generalizada en la que 10K sitios web de pequeñas y grandes empresas, dirigidos a audiencias de Asia oriental, se han visto comprometidos utilizando **credenciales de FTP legítimas**.

Ingeniería social

Alta: Tanto **PYMES** como nuevas empresas se están viendo afectadas por una campaña creciente de estafas de bombeo de SMS, las cuales abusan de la generación de **contraseñas de un solo uso (OTP)**.

Alta: La Policía Nacional advierte de suplantaciones de identidad en RRSS utilizando el **cebo de la inversión en criptomonedas**.

Media: Detectada nueva campaña de estafas impulsadas por IA en varios países de Europa. Los actores utilizan técnicas de **phishing, vishing y spoofing de temática ChatGPT** para conducir a la víctima a realizar inversiones fraudulentas.

Media: Destaca un esquema fraudulento utilizando plataformas de Google donde los atacantes imitan cuentas de streamers populares de Youtube para persuadir a las víctimas de **acceder a un código QR**.

Media: INCIBE informa de la detección de una campaña de phishing que trata de suplantar a la plataforma de reservas de alojamiento Booking. Utilizan la técnica de **Browser in the Browser (BitB)**, tratando de robar credenciales a través de ventanas emergentes.

Malware

Alta: Se ha detectado un nuevo malware para cajeros automáticos, denominado **FiXS**, que actualmente tiene como objetivo a los bancos mexicanos, aunque los expertos esperan que **muy pronto llegue a España**. Se instala un componente físicamente en el ATM para extraer efectivo de forma ilícita, al igual que otras familias ya conocidas.

Alta: El malware PoC desarrollado por investigadores, y bautizado como **BlackMamba**, es capaz de evadir la seguridad EDR moderna, dado que **cambia su código sobre la marcha** puede pasar por alto la última tecnología de detección de seguridad automatizada, lo que demuestra el potencial para crear **malware indetectable**.

Media: Descubierto un paquete de Python malicioso cargado en el Índice de paquetes de Python (PyPI) que contenía un **ladrón de información** con todas las funciones y un troyano de acceso remoto **(RAT) rastreado como Colour-Blind**.

Media: Una campaña en curso que emplea el llamado **HiatusRat** apunta a los modelos de **enrutador comercial DrayTek Vigor 2960 y 3900** para robar datos de las víctimas y construir una red proxy encubierta. Afecta predominanteente en Europa, EEUU y América del Sur.

Media: Se están observando campañas de BEC que distribuyen Remcos RAT utilizando el **cargador de malware DBatLoader** en Europa del Este. Se incluye el uso del **cargador TrickGate** almacenado en todo tipo de archivos y URL.

Media: El juego de cadena de bloques Sandbox advierte a su comunidad que un incidente de seguridad provocó que algunos usuarios recibieran **correos electrónicos fraudulentos haciéndose pasar por el juego**, tratando de infectarlos con malware.

Media: La **botnet** Emotet vuelve al ruedo tras 3 meses de pausa, enviando **correos electrónicos maliciosos**. Los correos distribuyen archivos .zip adjuntos, que entregan documentos de Office con macros maliciosas, las cuales descargan el DLL de Emotet.

Media: La **botnet Prometei** mejora componentes y capacidades de infraestructura, automatizando procesos y desafiando el análisis forense. Se basa en inteligencia de código abierto y se han difundido **versiones mejoradas de Linux**.

Media: Se ha rastreado un ladrón de información avanzado llamado ***SYS01***. Utiliza señuelos y técnicas de carga similares a los de otro ladrón de información recientemente denominado ***S1deload***, pero la carga útil real es diferente. El malware **apunta a cuentas comerciales de Facebook mediante el uso de anuncios de Google**, dirigiéndose a empleados críticos de infraestructura gubernamental, empresas manufactureras y otras industrias.

Media: Se ha visto al grupo **8220 Gang** implementando la carga útil ScrubCrypt en servidores Oracle Weblogic. El malware **ofusca y cifra las aplicaciones** y les permite esquivar los programas de seguridad.

Media: La temática ChatGPT afecta a usuarios de Facebook ofreciendo una **extensión falsa de acceso rápido**, la cual aparece en publicaciones patrocinadas, la cual, si bien conecta con la API de ChatGOT, también recopila información y se apodera de las cuentas de Facebook.

Media: Al menos dos ladrones diferentes, **Rhadamanthys y RedLine**, estaban abusando del plan de promoción del motor de búsqueda de Google para entregar cargas maliciosas. Parecen usar la misma técnica de imitar sitios web asociados a Notepad ++ y Blender 3D.

Media: Se ha descubierto recientemente la distribución del mal**ware Netcat dirigido a servidores MS-SQL**. Netcat es una utilidad que permite a los usuarios enviar y recibir datos desde destinos específicos en una red conectada por el protocolo TCP/UDP.

Baja: El grupo **Transparent Tribe** se vale de una campaña de HoneyTrap para incitar a usuarios a descargar **aplicaciones de contacto troyanizadas con CapraRAT**. El ataque se ha dirigido a usuarios Android con orientación militar y política de Asia Central.

Baja: Se ha descubierto recientemente la instalación del malware PlugX y Sliver a través de los programas de control remoto chinos **Sunlogin** y la vulnerabilidad de ejecución remota de código de **Awesun**. Se sospecha de varios **APT chinos** tales como Mustang Panda, Winnti, APT3 y APT41.

Baja: Descubierto el malware CHM, creado por el grupo **RedEyes** (también conocido como APT37, ScarCruft), siendo distribuido a usuarios coreanos.

Informativo: El teléfono de un alcalde polaco vinculado a la oposición estaba infectado con el **software espía Pegasus**. Se sospecha que los **servicios especiales de Polonia** están utilizando un software de vigilancia para espiar a los opositores al gobierno.

Informativo: **Cobalt Illusion**, patrocinado por el estado de Irán, dirige su campaña de espionaje para erradicar a las **activistas de derechos humanos** que causan problemas al régimen.

Ransomware

Alta: El **Hospital Clínic de Barcelona** ha notificado este domingo que ha sufrido un ciberataque ransomware que ha afectado a los servicios de urgencias, laboratorio y farmacia del centro. El ataque se ha asociado al grupo **Ransom House**.

Alta: El **FBI** y **CISA** emiten una alerta para advertir a las organizaciones sobre la creciente amenaza que representa el **ransomware Royal**, el cual afecta a organizaciones en **numerosos sectores**, incluida IC, comunicaciones, educación, sanidad e industria manufacturera.

Media: Se están implementando **nuevas versiones de Linux del ransomware IceFire** dentro de las intrusiones de la red empresarial de varias organizaciones del sector de medios y entretenimiento en todo el mundo. Afecta a la reciente **vulnerabilidad de compartición de archhivos IBM Aspera Faspex**, y se suma a la creciente lista de malwares que están lanzando, en las últimas semanas, versiones para Linux.

Media: El grupo de ransomware **Vice Society** agregó la Universidad de Ciencias Aplicadas de Hamburgo (**HAW Hamburg**) a su sitio de fuga. Se suma a la larga lista de instituciones educativas europeas afectadas, concretamente de habla alemana.

Media: Relacionado el grupo detrás del ransomware **MedusaLocker** con la distribución activa del ransomware **GlobeImposter**. El actor ha aprovechado para instalar otras cargas como Port Scanner y Mimikatz, y se supone que se distribuyen **a través de RDP**.

Baja: La banda de **Play Ransomware** ha asumido la responsabilidad de un ciberataque en la ciudad de **Oakland** (EEUU) que ha interrumpido los sistemas de TI desde mediados de febrero.

Baja: La **pandilla Medusa** (distinta del ransomware *MedusaLocker*) está exigiendo un rescate de $ 1M al **distrito de Escuelas Públicas de Minneapolis** (MPS) para eliminar los datos supuestamente robados en un ataque.

Baja: Descubierta la distribución reciente del **ransomware de cifrado iswr** en Corea. Presenta ciertas similitudes con STOP, y ASEC ya ha publicado una herramienta gratuita de desencriptado.