INFORME CTI DEL 13 AL 19 DE MAYO DE 2023

Resumen de amenazas

	Crítica	Alta	Media	Baja	Info.
APT	0	0	1	2	0
Cadena de suministro	0	0	2	1	0
Amenazas contra datos	0	1	5	10	0
Amenazas contra disponibilidad	0	1	0	0	0
Ingeniería social	0	2	2	1	0
Malware	0	0	8	3	1
Ransomware	0	3	5	7	1

APT

Media: Identificada una secuencia de ataques cibernéticos dirigidos **contra entidades europeas de asuntos exteriores**, atribuidas a un grupo APT patrocinado por el estado chino denominado "**Camaro Dragon**". El grupo ha apuntado a **rúters TP-Link**.

Baja: El APT **Lancefly** está utilizando una **puerta trasera personalizada (Merdoor)** en ataques dirigidos a **organizaciones en el sur y sureste de Asia**, en una actividad que ha estado en curso durante varios años. Disponen también de una versión actualizada del **rootkit ZXShell**.

Baja: Las **tensiones recientes entre China y Taiwán** se han intensificado debido a la creciente **presencia militar de China**, lo que ha derivado en un aumento en los ataques de **malware e ingeniería social** en Taiwán. Los sectores más afectados son **IT, manufactureras y logística**.

Cadena de suministro

Media: El fabricante francés de **productos electrónicos Lacroix** cerró tres fábricas como resultado de un ciberataque que "interceptaron" durante el fin de semana.

Media: Descubiertos nuevamente **más de 30 nuevos ataques 0-day en paquetes maliciosos del repositorio PyPI**. Es posible que alguno de estos conjuntos pueda ser el mismo que en ocasiones anteriores.

Baja: **Credit Control Corporation (CCC)**, una empresa de **servicios de cobro de deudas**, fue víctima recientemente de un ciberataque que provocó una filtración de datos que comprometió los datos personales de **numerosas instituciones sanitarias**.

AMENAZAS CONTRA LOS DATOS

Alta: Un fallo en Android muestra en el panel de' Privacidad' que **WhatsApp ha accedido forma innecesaria al micrófono de los dispositivos móviles**. Además, un ingeniero de Twitter advierte que la aplicación utilizó el micrófono en segundo plano **mientras dormía**.

Media: Una vulnerabilidad en un complemento de campos personalizados de **WordPress** que afecta a **más de 2 M de sitios** ha sido **aprovechada por atacantes apenas 48H** tras la presentación de una PoC en el informe de WP Engine.

Media: **Discord** notifica a los usuarios sobre una violación de datos que ocurrió después de que la **cuenta de un agente de soporte externo se vio comprometida**, exponiendo toda su cola de tickets de soporte, correos electrónicos, mensajes y adjuntos.

Media: Una fuga de datos en el sistema de **La Malle Postale, empresa de transporte** que atiende a senderistas en rutas de senderismo populares en Francia, que expuso los **datos personales de 90K clientes**.

Media: La **aerolinea AS Air Baltic Corporation**, de bandera de Letonia, ha reconocido que un "error técnico" expuso los **detalles de la reserva de algunos de sus pasajeros** a otros pasajeros de airBaltic.

Media: Los **piratas informáticos rusos** se han interesado repentinamente en la obtención de **datos personales de la población ucraniana** y han montado ataques exitosos contra más de un tercio de las **principales aseguradoras del país**.

Baja: La información personal **de 237 K empleados actuales y anteriores del gobierno de EEUU** quedó expuesta en una filtración de datos en el **Departamento de Transporte de Estados Unidos (USDOT)**, producto de una violación de datos.

Baja: Los datos de **vehículos Toyota de 2,15 M de usuarios en Japón** (casi toda la base de clientes que se suscribieron a sus plataformas en la nube desde 2012) se han hecho públicos debido a un error humano. También ha afectado a **Lexus**, y se ha producido en un contexto de impulso de la **conectividad y la gestión en nube**, relacionadas con servicios de conducción autónoma y características de IA.

Baja: Un proveedor de atención médica rural de Utah (**Uintah Basin Healthcare**) está notificando a **más de 100K personas** sobre un ataque que involucra información de salud de personas que recibieron atención durante más de una década.

Baja: Desenmascarado un **insider en Ubiquiti Networks, Inc.** (tecnológica estadounidense disruptiva en redes inalámbricas) tras robar Gb de datos confidenciales, hacerse pasar por un adversario y **extorsionar a la compañía por casi $ 2 M**.

Baja: Según datos recientes, actores **afiliados a Corea del Norte** han robado entre **$ 721 M y $ 2300 M en activos de criptomonedas de Japón** desde 2017, lo cual equivaldría a, como mínimo, el **30% del total de dichas pérdidas a nivel mundial**.

Baja: Grupo de **piratas informáticos chino** roba información de **empresas coreanas** aprovechando vulnerabilidades en **servidores SQL o servidores web IIS**. Se ha confirmado una **empresa de semiconductores y otra de fabricación inteligente mediante IA**.

Baja: El diario **Philadelphia Inquirer** está trabajando en la restauración de los sistemas afectados por lo que se describió como un ataque cibernético que golpeó su red durante el fin de semana.

Baja: El **Departamento de Transporte de Washington** se ha visto afectado por una violación de datos que puede haber expuesto **información de identificación personal de empleados** del gobierno federal. La brecha ocurrió dentro del sistema que soporta **TRANServe** (programa de beneficios).

Baja: El **Bristol Community College**, institución universitaria de Massachusetts (EE.UU.), ha informado de que ha sido víctima de un ciberataque. Si bien el ataque ocurrió a finales del año pasado, este no ha sido notificado hasta hace unos días.

Baja: La **plataforma india de admisión universitaria Leverage EDU** filtró casi **240K archivos confidenciales**, incluidos pasaportes de estudiantes, documentos financieros, certificados y resultados de exámenes. La base de datos se encontraba en un **sitio al que se podía acceder sin autentificación**.

AMENAZAS CONTRA LA DISPONIBILIDAD

Alta: Encontrada y desarticulada una **red en España dedicada a la reventa de citas de extranjería** tras **interceptarlas por medio de un 'bot' informático que bloqueaba el sistema de citas online** de extranjería. Gracias a este 'bot', lograban **hacerse con las citas disponibles para posteriormente revenderlas**, a pesar de ser un trámite gratuito.

INGENIERÍA SOCIAL

Alta: Nuevo caso de **smishing suplanta al Gobierno de España** apelando a la expectativa de **recibir un dinero extra a través de la Declaración Anual de la Renta**. Los principales afectados están siendo los usuarios del **BBVA, Banco Santander, Caixa Bank y Bankia**.

Alta: Nueva campaña de **smishing, suplantando a Correos**, para solicitar al usuario el número de su calle con la intención de entregar un supuesto paquete. El mensaje es una estafa que **roba los datos personales y bancarios** de la víctima.

Media: Nueva campaña de phishing se **hacía pasar por un proveedor de seguridad de correo electrónico** para atraer a los destinatarios a proporcionar sus credenciales de usuario a través de un **archivo adjunto HTML malicioso**.

Media: Una pandilla cibernética motivada financieramente, rastreada como **'UNC3944'**, utiliza ataques de **phishing y de intercambio de SIM** para secuestrar **cuentas de administrador de Microsoft Azure** y obtener acceso a máquinas virtuales.

Baja: Un **proveedor de VoIP de California (XCast Lab)** ha sido acusado de violar las reglas de telemercadeo al brindar servicios que enviaron miles de **millones de llamadas automáticas ilegales** a consumidores estadounidenses, relacionadas con llamadas de **spam y estafa**.

MALWARE

Media: Se encuentran **extensiones troyanizadas de VSCode con más de 45K descargas que roban información personal vulnerable y habilitan puertas traseras**. Estas estuvieron disponibles para su descarga en VSCode Extensions Marketplace.

Media: Aumenta de forma alarmante el **número de ventas de MaaS del tipo ladrones de información**, ampliamente disponible en foros y mercados clandestinos. Los más populares continúan siendo **Raccoon, Vidar y Redline**.

Media: Un grupo de amenazas, de nombre **Lemon Group, vende dispositivos móviles preinfectados con dos cargadores diferentes** capaces de implementar componentes adicionales. Las víctimas se distribuyen por **180 países y por todos los continentes**, siendo los más afectados **Asia** (con más de la mitad de los casos) y **Amércia** del Norte y del Sur.

Media: El grupo **Water Orthrus** ha estado activo recientemente con dos nuevas campañas. **CopperStealth usa un rootkit** para instalar malware en los sistemas infectados, mientras que **CopperPhish roba información** de tarjetas de crédito.

Media: Observado un aumento notable en el uso de la **puerta trasera Geacon** (implementación basada en Go de Cobalt Strike). Cuenta con una versión gratuita libre (Geacon **Plus**) y otra de pago privada (Geacon **Pro**).

Media: Analizado un nuevo malware llamado **Minas**, de implementación estándar, pero con **avanzadas técnicas de evasión** mediante cifrado, generación aleatoria de nombres y técnicas de **secuestro, inyección y persistencia**.

Media: Una campaña de distribución de malware mediante phishing (rastreada como **MEME#4CHAN**), lleva meses en activo, aprovechando un **código de PowerShell lleno de memes bastante inusual**, seguido de una carga útil de **XWorm** muy ofuscada para infectar a sus víctimas.

Media: El grupo de actores de amenazas conocido como "**8220 Gang" emplea nuevas estrategias** para sus respectivas campañas, incluidos **exploits para la utilidad de Linux "lwp-download"** y una vulnerabilidad de **Oracle WebLogic**.

Baja: Se está rastreando una campaña en curso del **grupo de amenazas OilAlpha**, la cual parece vincularse a actores de amenazas que apoyan al **grupo insurgente Houthi, en Yemen**. Parecen tener como objetivo entidades asociadas con el **sector no gubernamental** en toda la Península Arábiga.

Baja: El malware **SparkRAT se distribuye dentro del instalador de un determinado programa VPN** (solo disponible en coreano, aunque la web admite inglés, chino y japonés). Los expertos estiman que muchas **personas en China** instalan el programa para garantizar un acceso fluido a Internet.

Baja: Se ha descubierto recientemente **Infostealers disfrazados de juegos para adultos** que se distribuyen a **usuarios japoneses**. Se cree que se han distribuido a través de **torrents** o sitios web de descarga ilegal.

Informativa: Por cuarto año consecutivo, el **volumen de tráfico de bots dañinos** (aplicaciones de software automatizado malicioso capaces de abuso, uso indebido y ataques a alta velocidad) **creció al 30,2%**, un aumento del 2,5 % con respecto al año anterior.

RANSOMWARE

Alta: El grupo **LockBit dirige su operación de ransomware hacia Euskaltel, R y Telecable**, empresas pertenecientes al **grupo MásMóvil**, provocando problemas en los sistemas y en el servicio de atención al cliente. Se han visto comprometidos más de **3 TB de datos**.

Alta: FBI y CISA advierten que la pandilla **Bl00dy Ransomware** ahora también está explotando activamente una **vulnerabilidad de ejecución de código remoto de PaperCut** para obtener acceso inicial a las redes. Se centran en el **sector educativo**.

Alta: Una nueva **operación de RaaS llamada MichaelKors** se ha convertido en el último malware de cifrado de archivos para atacar los **sistemas Linux y VMware ESXi** a partir de abril de 2023. Sigue aumentando así la lista de grupos y malware notables dirigidos a ESXi, tales **como ALPHV, Black Basta, Defray, ESXiArgs, LockBit, Nevada, Play, Rook y Rorschach**.

Media: El **RaaS Qilin**, activo desde mediados de 2022, se ha estado distribuyendo desde entonces mediante técnicas de spearphishing, alcanzando ya **IC, sistema sanitario y de educación de diferentes países** de los 5 continentes.

Media: Detectado un incremento de actividad del **RaaS LV**, el cual parece estar basado en el ransomware REvil. Recientemente ha perpetrado un ataque que involucró el compromiso del entorno corporativo de una **empresa con sede en Jordania**, pero los operadores del RaaS han manifestado en el pasado su **interés por las entidades de Canadá, EEUU y Europa**.

Media: Hallada nueva familia de ransomware denominada **BlackSuit**, la cual es usada por actores de amenazas para atacar **usuarios de Windows y Linux** apunando a **servidores Vmware ESXi**. Su variante Linux comparte similitudes con el ransomware Royal.

Media: Los operadores del ransomware **CheckMate** han estado apuntando al **protocolo de comunicación Server Message Block (SMB)** utilizado para compartir archivos para comprometer las redes de sus víctimas. Se cree que los actores que manejan el ransomware son rusos, y apuntan eminentemente a **PYMES**.

Media: Una nueva operación de ransomware (**MalasLocker**) está pirateando **servidores Zimbra** para robar correos electrónicos y cifrar archivos. Sin embargo, en lugar de exigir el pago de un rescate, los actores **solicitan que la víctima haga una donación de caridad a alguna organización sin fines de lucro** y les envíen el justificante.

Baja: Nueva variante ransomware llamada **Maori** está diseñada para **ejecutarse en Linux** y **codificada en Go**, lo que es inusual y **aumenta su dificultad de análisis**. Por el momento no parece estar muy extendido.

Baja: Descubierto un nuevo grupo llamado **RA Group**, activo al menos desde el mes pasado y que está **expandiendo sus operaciones rápidamente por EEUU y Corea del Sur**, apuntando verticales como fabricación, gestión de patrimonio, proveedores de seguros y productos farmacéuticos. Su ransomware (**Rorschach**) sería un ejemplo de los nuevos ransomware que han aprovechado el **código fuente filtrado de Babuk**.

Baja: Confirmada la distribución del ransomware **LokiLocker en Corea**. Este ransomware es casi idéntico al ransomware BlackBit, disfrazándose ambos como svchost.exe y estando ofuscados con la misma herramienta, entre otras características.

Baja: El notorio grupo de ransomware **BianLian**, tras el lanzamiento de un descifrador producido por Avast, evoluciona sus TTP para adaptarse a la situación, **abandonando los sistemas de encriptación y centrándose en la extorsión directa** de filtrado de información tras su robo. Continúa apuntando a **IICC en EEUU y Australia**.

Baja: El proveedor de servicios de farmacia **PharMerica**, con presencia en 50 Estados, ha revelado una violación masiva de datos que **afecta a más de 5,8 millones de pacientes**, exponiendo sus datos médicos a los piratas informáticos. El ataque ha sido perpetrado por el grupo de ransomware **Money Message**.

Baja: El **proveedor de tecnología ScanSource** (EEUU) ha anunciado que ha sido víctima de un ataque de ransomware que afecta a algunos de sus sistemas, operaciones comerciales y portales de clientes. Ofrece **servicios de nube, conectividad SaaS, PoS, seguridad**, etc.

Baja: El grupo de ransomware **LockBit** publicó el martes 1,5 terabytes de información personal y financiera que el grupo dijo que robó del **Bank Syariah Indonesia** después de que fracasaron las negociaciones de rescate.

Informativa: Se está detectando un proceso de refinamiento y desarrollo en el proceso de infección del grupo **Royal Ransomware**, el cual se sabe que ha estado **construyendo su propio cargador**, de pequeño tamaño y con capacidades de implementación inmediata de una carga de cobalt strike y de creación de conexión C2.