INFORME CTI DEL 20 AL 26 DE MAYO DE 2023

Resumen de amenazas

	Crítica	Alta	Media	Baja	Info.
APT	0	0	5	6	1
Cadena de suministro	0	0	1	0	0
Amenazas contra datos	0	1	4	1	0
Desinformación	0	1	0	1	0
Amenazas contra disponibilidad	0	0	2	1	1
Ingeniería social	1	3	5	6	0
Malware	0	3	13	2	1
Ransomware	0	1	6	2	2

APT

Media: Los **APT estatales de Rusia, Irán y Corea del Norte apuntan cada vez más a las PYMES a nivel mundial**, comprometiendo su infraestructura para llegar a los gobiernos, las fuerzas armadas y las principales entidades corporativas.

Media: Hallada nueva información sobre el ATP que, en marzo, fue detectado desplegando implantes **PowerMagic y CommonMagic en ciertas zonas de Ucrania**. Ahora, se han detectado **focos en el centro y oeste** del país con **víctimas individuales, de organizaciones diplomáticas y de entidades de investigación**, en una campaña que utiliza un marco modular conocido como **CloudWizard**.

Media: Un actor de amenazas identificado por los investigadores como **UAC-0063** ha mostrado interés en dirigir una **campaña de espionaje a Ucrania**, Mongolia, Kazajstán, Kirguistán, Israel e India. El objetivo sería el de **recopilación de Inteligencia**.

Media: El APT patrocinado por Corea del Norte, **Kimsuky**, se dirige a **servidores web** en los que, tras la violación exitosa, instala el **malware de puerta trasera Metasploit Meterpreter**, así como de un **malware proxy** desarrollado en GoLang.

Media: El APT **Lazarus**, patrocinado por Corea del Norte, lleva a cabo ataques contra **servidores web Windows IIS**. Emplea técnica de **carga lateral de DLL** para ejecutar malware.

Baja: Un grupo de ciberespionaje chino rastreado como **Volt Typhoon ha estado apuntando a organizaciones de infraestructura crítica de amplio espectro en EEUU**, incluidas bases militares, gobierno, industra,

transportes e IT, desde al menos mediados de 2021. El vector de ataque a sido un 0-day desconocido en Fortinet FortiGuard.

Baja: El APT **GoldenJackal**, generalmente, dirige **operaciones de espionaje a entidades gubernamentales y diplomáticas en el Medio Oriente y el sur de Asia**. A pesar de llevar activo varios años es un grupo generalmente desconocido pero que muestra nivel constante de actividad, lo que indica un **actor capaz y sigiloso**.

Baja: Se ha observado nuevamente al APT norcoreano **Kimsuky** usando un **malware personalizado llamado RandomQuery** como parte de una operación de **reconocimiento y exfiltración de información**. Implementando igualmente ReconShark (ya mencionado en anteriores ocasiones), apunta a los servicios de información, así como a las organizaciones que apoyan a los activistas de derechos humanos y a los **desertores de Corea del Norte**.

Baja: Detectada la aparición de un **nuevo APT de nombre Trila**, orientado a la ejecución de comandos de consola remota dirigido contra **entidades gubernamentales libanesas**. Utiliza herramientas y malware simple y casero para infectar y **exfiltrar información**.

Baja: Los **piratas informáticos chinos atacaron al gobierno de Kenia** en una serie generalizada de intrusiones digitales de varios años contra ministerios e instituciones estatales clave. Los hackeos tendrían como objetivo, al menos en parte, obtener **información sobre la deuda** que la nación le debe a Beijing.

Baja: El **spyware Pegasus**, del PSOA israelí NSO Group, fue desplegado en **Armenia en medio de la guerra con Azerbaiyán**. Apuntó a **periodistas, activistas, funcionarios gubernamentales y civiles armenios** y, a pesar de haber ocurrido ya en 2020, sería el **primer caso conocido de software espía Pegasus utilizado en medio de una guerra**.

Informativa: Notificado un **aumento de las campañas APT** durante el primer trimestre del año, registrando **nuevas TTP y herramientas actualizadas**, así como la **expansión** de ataques a nivel geográfico y sectorial por todo el mundo. También han aparecido **nuevos grupos**.

CADENA DE SUMINISTRO

Media: La **empresa industrial armamentística y de automoción alemana Rheinmetall**, la cual sufrió un ataque cibernético el mes pasado, ha confirmado que el responsable del mismo ha sido el grupo **Black Basta**.

AMENAZAS CONTRA LOS DATOS

Alta: **Barracuda**, empresa conocida por sus soluciones de seguridad de red y correo electrónico, advirtió hoy a los clientes que algunos de sus **dispositivos Email Security Gateway (ESG)** fueron violados la semana pasada al apuntar a una **vulnerabilidad de día cero ahora parcheada**.

Alta: Brutal aumento en los ataques dirigidos a una **vulnerabilidad XSS en el complemento de WordPress Beautiful Cookie Consent Banner**. Se han bloqueado **casi 3 M de ataques, en sólo 24H**, contra más de 1,5 M de sitios, desde casi 14 K direcciones IP.

Media: La multinacional estadounidense Meta Platforms, propietaria de **Facebook, Instagram y WhatsApp**, ha sido sancionada con una multa de € 1.200 M por la Comisión de Protección de Datos de Irlanda (DPC) en relación con la **transferencia de datos personales de sus usuarios desde la Unión Europea a los Estados Unidos**.

Media: Investigadores han presentado un **nuevo ataque llamado 'BrutePrint'**, que utiliza **fuerza bruta con las huellas dactilar**es en los teléfonos inteligentes Android modernos para eludir la autenticación del usuario y tomar el control del dispositivo.

Media: El servicio VPN gratuito **SuperVPN ha expuesto 133 GB de datos**, incluidos **360 M de reg**istros de usuarios, como las direcciones IP. SuperVPN es el mismo proveedor de servicios VPN gratuito que filtró los datos de los clientes en mayo de 2022.

Media: Se ha rastreado a un actor de amenazas de nombre **GUI-vil**, proveniente de Indonesia, motivado financieramente y **centrado en la nube y en la minería de criptomonedas** no autorizadas. Se han observado explotaciones de **instancias EC2 de AWS**.

Baja: Un ataque cibernético en **Norton Healthcare** está provocando demoras en farmacias y laboratorios. Norton Healthcare es un **sistema de atención médica de Kentucky** con más de 40 clínicas y hospitales en Louisville, Kentucky y sus alrededores.

DESINFORMACIÓN

Alta: Se ha observado un **aumento de bulos y desinformación relacionados con el proceso electoral en España**. La mayoría de estos bulos se han centrado en el **proceso de votación**, como el **recuento** de papeletas y la **documentación requerida** para votar desde el extranjero.

Baja: Un **fake de una explosión en el Pentágono** difundido por una **cuenta de Twitter verificada** causa el pánico en las redes. Se trataba de una imagen que se cree que fue generada con IA y **llegó a ser compartida por algunos canales** de noticia.

AMENAZAS CONTRA LA DISPONIBILIDAD

Media: Encontrado nuevo **malware para redes OT e ICS, de nombre COSMICENERGY**, cargado en una utilidad pública de escaneo de malware en diciembre de 2021 por un **remitente en Rusia**. Está diseñado para causar **interrupciones e impacto físico en dispositivos y terminales comúnmente utilizados en las operaciones de transmisión y distribución eléctrica en Europa**, Medio Oriente y Asia, y se comparan sus capacidades con las de **INDUSTROYER**.

Media: **Hacktivistas rusos venden un nuevo malware DDoS-As-A-Service**, conocido como **MDBotnet**, en un foro de ciberdelincuencia. Ha sido diseñado para llevar a cabo **ataques DDoS** en víctimas específicas mediante el empleo de una técnica de ataque de **inundación HTTP/SYN**.

Baja: El actor de amenazas iraní **Agrius** continúa operando **contra objetivos israelíes**, enmascarando **operaciones de influencia destructiva** como ataques de ransomware. En ataques recientes, el grupo implementó **Moneybird**, un ransomware nunca antes visto.

Informativa: Los **ataques DDoS** se han convertido en una **táctica principal para los grupos de hacktivistas**, entre todos los demás métodos de ataque, para causar interrupciones en cualquier infraestructura o servicio digital orientado a Internet. Destacan hacktivistas **rusos** como Killnet, hacktivistas anónimos **proucranianos** y grupos que operan en torno a **Oriente Medio y Sudeste Asiático**, en campañas como #OpIsrael y #OpIndia.

INGENIERÍA SOCIAL

Crítica: Una actual **campaña de phishing muy sofisticada envía correos perfectamente redactados, de apariencia real y firmados por el Gobierno, simulando proceder de la Red SARA** (Sistemas de Aplicaciones y Redes para las Administraciones), que conecta las redes de las Administraciones Públicas Españolas e Instituciones Europeas para facilitar el **acceso a los servicios y el intercambio de información**.

Alta: Continúan las campañas de **phishing suplantando a la Agencia Tributaria**. En el último ejemplo, se envía un **correo falso avisando de una nueva notificación electrónica**, e insta al usuario a iniciar sesión en el enlace que se proporciona en el correo, el cual redirige una página similar a la legítima para **robar la Cl@ve Permanente**.

Alta: **España entra en el 'top 10' mundial** de los países con más víctimas por ciberdelincuencia, en el puesto 10º. Un estudio internacional elaborado por una empresa holandesa de ciberseguridad (Surfshark) incluye por primera vez al país en este ranking, detectando el **phishing como principal amenaza** mundial.

Alta: Una **operación de PHaaS a gran escala**, conocida como **BulletProofLink o Anthrax**, está cambiando de táctica para permitir que los atacantes **eviten la detección de anomalías** mediante el uso de direcciones IP localizadas. En un nuevo informe se previene a las empresas sobre el **aumento alarmante de los ataques BEC y las tácticas en evolución** empleadas por los ciberdelincuentes, destacando, en concreto, el uso de plataformas como BulletProofLink.

Media: Una campaña de **recolección de credenciales de alto volumen** está utilizando un programa legítimo de boletines por correo electrónico (**SuperMailer**) para enviar gran cantidad de correos de phishing diseñados para **evadir las protecciones** de la puerta de enlace de correo electrónico seguro (SEG).

Media: Los actores de amenazas están **eludiendo las detecciones de seguridad basadas en la ubicación geográfica** utilizando una combinación de **plataformas CaaS** y la compra de **direcciones IP locales**, evadiendo alertas de "viaje imposible".

Media: Nueva campaña de phishing dirigida a **personas y empresas interesadas en ChatGPT**, donde el correo viene marcado con el **logotipo de OpenAI y con idéntico desarrollo de HTML**, pero cambiando los enlaces de redirección.

Media: Algunos incidentes de phishing están relacionados con un **proveedor de estafas llamado Inferno Drainer**, que se especializa en estafas de **múltiples cadenas** y cobra principalmente el 20% de los activos robados. Han robado alrededor de $ 5.9 M en activos y tienen **casi 5 K víctimas** hasta ahora.

Media: Detectada una recientemente campaña de phishing en la que el atacante envía un correo electrónico a un usuario de empresa que **afirmando ser del "Departamento de recursos humanos"**, proporcionando un enlace para **enviar sus solicitudes de vacaciones** anuales.

Baja: Aumento del riesgo del **phishing contextual después de desastres naturales**, como los recientes **huracanes o tifones en EEUU**, ya que los atacantes se dirigen a las posibles víctimas del desastre aprovechando TTP de ingeniería social.

Baja: El grupo **Kimsuky** ha creado un **sitio de correo web que se ve idéntico a ciertos institutos de investigación de políticas nacionales**, configurando la página de inicio de sesión falsa con identificaciones autocompletadas de personas y organizaciones comerciales, de medios y relacionadas con **Corea del Norte**.

Baja: Detectado **ataques de abrevadero en al menos 8 sitios web israelíes pertenecientes a empresas de logística**, orquestados por un actor patrocinado por Irán (se baraja cierta sospecha de atribución a **Tortoiseshell**). Los sitios infectados **recopilan información** preliminar del usuario a través de un script, y a estos suelen acudir frecuentemente grupos específicos de perfiles, tales como **oficiales gubernamentales, periodistas o ejecutivos**.

Baja: La **cartera de criptomonedas Metamask** se ha convertido en **señuelo de spoofing**, distribuyendo una app fraudulenta en sus dispositivos Android, de apariencia similar a la real, para acceder a sus claves de recuperación y robar las criptodivisas.

Baja: Ciberdelincuentes comparten **falsas ofertas**, por redes sociales, para **restablecer cuentas de WhatsApp** bloqueadas por la plataforma para que sus propietarios puedan volver a utilizarlas siempre que aporten una cantidad de dinero.

Baja: Detectado un caso de phishing en el que utilizan una **combinación de cuentas de Microsoft 365 comprometidas y correos electrónicos cifrados .rpmsg** para entregar el mensaje. Se ha implementado mediante la vulneración de una cuenta de **Talus Pay**, empresa de procesamiento de pagos estadounidense.

MALWARE

Alta: Se ha confirmado recientemente que **StrelaStealer Infostealer se está distribuyendo a los usuarios españoles**, adjunto en correos maliciosos de phishing. El correo, en español, contiene un **cuerpo de mensaje acerca de tarifas de pago**, indicando al usuario que verifique la factura adjunta. StrelaStealer roba las credenciales del correo.

Alta: Un grupo de piratería brasileño ha estado apuntando a **treinta instituciones financieras privadas y gubernamentales portuguesas** desde 2021 en una campaña de malware llamada **'Operación Magalenha'**. Ejemplos de entidades objetivo incluyen **ActivoBank, Caixa Geral de Depósitos, CaixaBank, Citibanamex, Santander, Millennium BCP, ING, Banco BPI y Novobanco**.

Alta: Descubierto un **ladrón de información** que puede lograr persistencia en la máquina de una víctima **modificando su cliente de Discord** y parcheando la aplicación.

Media: Se ha recibido una alerta por parte de CISA acerca de **explotación activa de una vulnerabilidad media en dispositivos Android**, concretamente los que ejecutan versiones 11, 12 y 13 de Android. No hay información acerca del modo en el que se está produciendo la explotación, pero, en el pasado, los **vendedores comerciales de software espía** han utilizado las vulnerabilidades en los teléfonos Samsung para implementar software malicioso.

Media: Descubierto un troyano (**AhMyth Android RAT**) en la **aplicación para dispositivos Android iRecorder-Secreen Recorder**, que era capaz de grabar audio utilizando el micrófono del dispositivo y robar distintos tipos de archivos.

Media: El PSOA (proveedor de malware) **Intellexa comercializa un paquete de spyware móvil conocido como 'ALIEN' y 'PREDATOR'**. Ambos componentes trabajan juntos para eludir las funciones de seguridad tradicionales del **sistema operativo Android**. Es posible que también pueda ir dirigido a iOS.

Media: Se ha detectado al **malware DarkCloud** distribuyéndose a través de correo electrónico no deseado. DarkCloud es un infostealer que **roba las credenciales** de las cuentas guardadas en los sistemas infectados, y se ha detectado junto con el **malware ClipBanker**.

Media: continúan las campañas de distribución de malware dirigidas **a espectadores de Youtube que buscan crackers para software**. Inducen a las víctimas a ejecutar binarios que, en realidad, resultan ser recolectores de credenciales, ladrones o criptomineros. Han destacado **Vidar Stealer, Laplas Clipper y XMRig Miner**.

Media: Hallada una **nueva versión de Legion**, la herramienta **MaaS** emergente **centrada en la nube**, diseñada para recopilar credenciales de servidores web mal configurados y aprovechar estas credenciales para el abuso de correo electrónico.

Media: Actores malintencionados **evaden las medidas antispam, antibot y antiabuso de los servicios web** en línea a través de **proxis residenciales y servicios de ruptura de CAPTCHA**. Aunque estas herramientas todavía funcionan según lo diseñado, los ciberdelincuentes pueden comprar fácilmente **servicios CaaS** que están hechos específicamente para vencer a los CAPTCHA.

Media: Se identifica una **nueva red de bots, llamada Dark Frost Botnet**, que apunta a la **industria del juego**. Inspirada en **Gafgyt, Qbot, Mirai y otras cepas** de malware, se ha expandido para abarcar cientos de dispositivos comprometidos.

Media: Observada una **variante de Mirai, llamada IZ1H9**, que usa varias **vulnerabilidades** para propagarse a múltiples dispositivos, permitiendo al atacante controlarlos completamente y convertirlos en parte de la botnet. Suele utilizarse para **ataques DDoS**.

Media: Investigadores encuentran ladrones **de información basados en Rustlang que apuntan a Windows**, los cuales se distribuyen **disfrazados de aplicaciones** o plataformas legítimas, abusando de los espacios de código de **GitHub**.

Media: Una serie de **sitios web de phishing que se hacen pasar por CapCut**, el popular software de edición de video, atraen a los usuarios para que descarguen y **ejecuten varios tipos de familias de malware**, como ladrones, RAT, etc.

Media: Una nueva campaña dirigida a **servidores MS-SQL mal administrados** muestra el uso de sqlps (SQL Server PowerShell) para la distribución de malware, concretamente el **RAT Remcos**.

Media: Se han descubierto **varios paquetes npm** que llevan el nombre de las **bibliotecas de NodeJS** que, incluso, incluyen un ejecutable de Windows que se parece a NodeJS, pero en su lugar sueltan un binario de **TurkoRAT**.

Baja: Identificada una **puerta trasera personalizada basada en powerShel**, y llamada **PowerExchange**, notificada el pasado año en torno a la **Operación Total Exchange**, que tuvo lugar contra una **entidad gubernamental en Emiratos Árabes**. Mientras el resto de las amenazas se clasificaron correctamente, esta había permanecido sin identificar hasta ahora.

Baja: Investigadores han localizado un **nuevo controlador de kernel, denominado WinTapix**, distribuido predominantemente por **Oriente Medio**. Permite la ejecución remota de código y el acceso persistente al host y al resto de la red.

Informativa: Comienza a analizarse el encriptador **AceCryptor** como pieza de malware con identidad propia. Ha sido ampliamente utilizada desde 2016 para **empaquetar decenas de malware, como DJVU, SmokeLoader o Redline**, siendo un habitual MaaS.

RANSOMWARE

Alta: El **concejo de Cangas, en Vigo (Pontevedra)**, sufre un ataque de ransomware por parte de **LockBit 3.0**, viéndose afectadas las **nóminas** de los trabajadores, toda la **gestión tributaria** y la práctica totalidad de **programas externos**. Los atacantes han exigen una recompensa para descifrar los datos.

Media: Un grupo de ciberdelincuentes motivado financieramente conocido como **FIN7 resurgió el mes pasado**, vinculado con ataques en los que el objetivo final era el despliegue de **cargas útiles de ransomware Clop** en las redes de las víctimas.

Media: **CryptNet** es un nuevo grupo de **RaaS** que se ha anunciado en foros clandestinos desde al menos abril de 2023. El grupo afirma realizar **ataques de doble extorsión** al combinar la exfiltración de datos con el cifrado de archivos.

Media: En un reciente ataque del **ransomware BlackCat** se ha observado una nueva capacidad, concretamente un **nuevo controlador de kernel firmado** e implementado en la fase de evasión de la defensa, que se superpone con los controladores maliciosos anteriores revelados por tres proveedores.

Media: La banda de **ransomware Cuba** se atribuyó la responsabilidad del ataque cibernético de este mes en **The Philadelphia Inquirer**, que interrumpió temporalmente la distribución del periódico e interrumpió algunas operaciones comerciales.

Media: Encontrada una **cepa de ransomware nueva y única llamada "Obsidian ORB"**, cuyo código fuente se ha relacionado con el ransomware Chaos. Obsidian ORB **no solicita pago en criptomonedas, sino a través de tarjetas de regalo**, incluidas plataformas populares como Roblox, Paysafe, Payday, Steam, etc.

Media: El actor de ransomware **Buhti está utilizando variantes de las familias de ransomware LockBit y Babuk** filtradas para atacar los sistemas Windows y Linux, para luego utilizar su propia **herramienta de exfiltración personalizada**. Muestra rapidez y habilidad en la **explotación de vulnerabilidades**.

Baja: Singapur habría registrado la **tasa más alta de ataques de todos los países** encuestados este año. Ya hay

Baja: **Singapur** habría registrado la **tasa más alta de ataques de todos los países** encuestados este año. Ya hay un **84% de sus organizaciones** que aseguran haber sido víctimas de estos incidentes, frente a solo un 65% que lo fueron el año anterior.

Informativa: Según un estudio, el **vector más significativo en los ataques exitosos de ransomware** en 2022 involucró la **explotación de aplicaciones públicas**, que representó el 43 % de todas las infracciones, seguido del **uso de cuentas comprometidas** (24 %) y **correo electrónico malicioso** (12 %).

Informativa: Otro estudio revela que e**n el 93 % de los incidentes de ransomware los actores de amenazas tienen como objetivo los repositorios de respaldo**, lo que da como resultado que el 75 % de las víctimas pierdan al menos algunos de sus respaldos durante el ataque, y que **casi el 40 % sean eliminados** por completo.