INFORME CTI DEL 6 AL 12 DE MAYO DE 2023

Resumen de amenazas

	Crítica	Alta	Media	Baja	Info.
APT	0	0	3	2	1
Cadena de suministro	0	1	1	2	0
Amenazas contra datos	0	0	0	5	0
Amenazas contra disponibilidad	0	0	1	0	1
Ingeniería social	0	1	3	1	0
Malware	0	3	13	3	0
Ransomware	0	0	3	8	2

APT

Media: Continúa la **campaña de explotación de vulnerabilidades de PaperCut**, sumándose a la misma, aparte de los ya citados anteriormente **Silence, LockBit y Cl0p**, los estados patrocinados por el estado de Irán conocidos como **Charming Kitten y Static Kitten**.

Media: El APT indio **SideWinder** está utilizando una **técnica de polimorfismo** basado en servidor para atacar a los **funcionarios del gobierno** de Pakistán, avanzando ahora en última instancia a **Turquía**.

Media: Identificada campaña de **Lazarus**, de finales del año pasado, contra **objetivos en Países Bajos y Bélgica** en los que ha utilizado correos de phishing especialmente dirigidos relacionados a **falsas ofertas de trabajo**. Han explotado una **vulnerabilidad en Dell** y utilizado su muy completo backdoor, conocido como **Blindingcan**.

Baja: El APT chino de ciberespionaje **Mustang Panda está centrando su interés en Australia** (con motivo de la oposición a la alianza militar Australia-UK-EEUU; AUKUS), distribuyendo el **malware PlugX** oculto en supuestos documentos biográficos del Secretario de Estado de Australia.

Baja: Detectada, entre 2022 y 2023, una **campaña de espionaje** que involucra una **nueva familia de malware denominada DownEx**, dirigido a **instituciones gubernamentales extranjeras en Kazajstán y Afganistán**. El archivo se hace pasar por un documento de un diplomático real y se centra en la exfiltración de datos.

Informativa: Nuevas investigaciones señalan que el grupo **Royal Ransomware** compromete a las víctimas a través de una **infección BATLOADER**, que los actores de amenazas generalmente propagan a través del envenenamiento de optimización de motores de búsqueda (**SEO**). Esta infección implica dejar caer un **Cobalt Strike Beacon** como precursor de la ejecución del ransomware.

CADENA DE SUMINISTRO

Alta: La **multinacional suiza ABB, un proveedor líder de tecnología de automatización y electrificación**, sufrió un ataque de ransomware por **Black Basta**, que supuestamente afectó las operaciones comerciales. La empresa trabaja con una **amplia gama de clientes y gobiernos locales por todo el mundo**, incluidos Volvo, Hitachi, DS Smith, la ciudad de Nashville y la **ciudad de Zaragoza**. Presta igualmente servicios a gran diversidad de **agencias federales** en EEUU, como el Departamento de Defensa, el Cuerpo de Ingenieros del Ejército, y Departamentos de Interior, Energía y Guardacostas, así como el Servicio Postal.

Media: **Sysco**, una empresa **líder mundial en distribución de alimentos**, ha confirmado que su red fue violada a principios de este año por atacantes que robaron **información confidencial**, incluidos datos comerciales, de clientes y de empleados.

Baja: **NextGen Healthcare**, gigante estadounidense proveedor de **tecnología sanitaria, sufre la segunda violación de datos en lo que va de año** tras el ataque de ransomware de ALPHV de enero.

Baja: La compañía **tecnológica estadounidense y subsidiaria de Siemens, Brightly Software**, ha sufrido un acceso no autorizado a la base de datos de su **plataforma en línea SchoolDude**. Es una plataforma de administración basada en la nube, utilizada por **más de 7K colegios**, universidades y escuelas K-12 de **distritos escolares de hasta 600K estudiantes**.

AMENAZAS CONTRA LOS DATOS

Baja: El **Colegio Estadounidense de Pediatras**, una organización antiabortista y antitrans de EE.UU., ha sufrido una importante **filtración de datos que incluiría más de 10K documentos**, registros financieros y fiscales, listas de miembros e intercambios de correos electrónico que abarcan más de una década.

Baja: Twitter reveló que un 'incidente de seguridad' provocó que los **tweets privados enviados a los Círculos de Twitter se mostraran públicamente** a los usuarios fuera del "Círculo" de destinatarios delimitado.

Baja: Los piratas informáticos accedieron a la **información personal confidencial de más de 45,000 personas en los EE. UU.** durante un ataque cibernético en diciembre en el **Metropolitan Opera**.

Baja: El APT norcoreano **Kimsuky** ha violado la red del **Hospital de la Universidad Nacional de Seúl (SNUH)**, uno de los hospitales más grandes del país, para robar **información médica confidencial** y detalles personales.

Baja: Se ha visto puesto a la venta un **exploit 0-day de explotación remota de código (RCE) para Ngimx**, servidor web/proxy inverso ligero de alto rendimiento y proxy para protocolos de correo electrónico.

AMENAZAS CONTRA LA DISPONIBILIDAD

Media: El **sitio web del Senado francés** estuvo fuera de línea el viernes pasado después de que piratas informáticos prorrusos afirmaron haberlo eliminado. El **grupo proruso NoName** se ha atribuido la autoría del ataque.

Informativa: Como parte de la **#Operation PowerOFF**, el Departamento de Justicia de EEUU incautó **13 dominios más vinculados a plataformas DDoS de alquiler**, también conocidas como **servicios 'booter' o 'stressor'**.

INGENIERÍA SOCIAL

Alta: El **INCIBE alerta de múltiples campañas de phishing** cuya finalidad es obtener las credenciales de acceso del gestor de correo. Afecta a empresarios, empleados y autónomos que hagan uso de su **gestor de correo electrónico a través de servicios de Webmail tipo Zimbra** o similares.

Media: Detectadas **campañas de phishing mediante QR maliciosos en EEUU y UK**, los cuales se presentan en forma de **multas de estacionamiento falsas** dirigidas a los conductores. Igualmente prolifera el uso de QR falsos en los **establecimientos y comercios** públicos.

Media: Una **oferta de PHaaS** no informada anteriormente llamada "**Greatness**" se ha utilizado en varias campañas de phishing desde al menos mediados de 2022. Utiliza **características avanzadas** como omisión de MFA, filtrado de IP e integración con bots de Telegram. **Apunta a Office 365 y las víctimas se reparten por EEUU, UK, Australia, Sudáfrica y Canadá**.

Media: Un grupo de amenazas con sede en Israel realiza una **campaña de BEC dirigida principalmente a empresas grandes y multinacionales** con un ingreso anual promedio de más de $ 10 K.M. Los atacantes **se hacen pasar por el director ejecutivo** del empleado al que apuntan, y se les atribuye **350 campañas** BEC desde febrero de 2021, con ataques de correo electrónico dirigidos a **empleados de 61 países en 6 continentes**.

Baja: Un **engaño en WhatsApp dirigido a México** aprovecha la celebración del **día de la madre** y suplanta la identidad de distintas empresas y organismos para engañar a las personas.

MALWARE

Alta: Identificada campaña de distribución de malware mediante phishing, la cual **suplanta la identidad de la Agencia Tributaria**. Bajo el pretexto de corregir unos **datos relativos al IRPF**, insta al usuario a descargar un ejecutable, el cual aloja el malware **AutoIT v3 Script**.

Alta: Se ha detectado una campaña de distribución de malware a través de **phishing suplantando a Endesa** en la que se informa al usuario puede **descargar su factura**, la cual está adjunta al correo. El ZIP adjunto contiene el **malware Grandoreiro**.

Alta: En **campañas recientes de GuLoader** se ha percibido un aumento en los **instaladores basados en NSIS**, entregados por correo electrónico como malspam, que usan bibliotecas de complementos para ejecutar el shellcode GU en el sistema de la víctima.

Media: Agencias de ciberseguridad e inteligencia de varias naciones informan que han **desmantelado la infraestructura del spyware Snake**, operado por **Turla** (perteneciente al Servicio Federal de Seguridad de Rusia, FSB). Se han encontrado **dispositivos de la OTAN afectados** por la red peer-to-peer de Snake.

Media: Los investigadores presentan el análisis de **drIBAN**, un malware detectado en una **operación de fraude persistente en Italia atribuida a TA-554**, en la cual se pretendía infectar las estaciones de trabajo de Windows dentro de entornos corporativos tratando de alterar las transferencias bancarias legítimas.

Media: Descubierto un **interesante señuelo con funciones de exfiltración** desplegado por el **actor Red Stubger** en el Este de **Ucrania**, apuntando a diversas zonas y entidades del país pertenecientes al **ejército**, el **transporte**, la **Administración** y la **IC**.

Media: **RapperBot** es un gusano que infecta **dispositivos IoT** con el objetivo final de lanzar **ataques DDoS** contra objetivos no HTTP, diferenciándose de otros gusanos al aplicar métodos de "**fuerza bruta inteligente**", comprobando la solicitud y basándose en ella para seleccionar las credenciales adecuadas. La nueva campaña de RapperBot ha comenzado a introducirse en el **cryptojacking**, específicamente en máquinas Intel x64. El nuevo bot combina **RapperBot + Monero XMRig**.

Media: Aumento de muestras de la **herramienta de Windows legítima Wetract.exe**, utilizadas de forma maliciosa por los atacantes **para distribuir malware** (como **Amadey** y **Redline Stealer**), para robar información o para obtener acceso remoto.

Media: Aparece nueva **botnet única llamada AndoryuBot**, la cual es distribuida a través de la **vulnerabilidad de Ruckus** y contiene **módulos de ataque DDoS**. Se propaga rápidamente y ya cuenta con varias versiones de desarrollo.

Media: El ladrón de información **Rhadamanthys evoluciona sus TTP**, cambiando su vector de distribución del phishing al **malvertising**, tanto de motores de búsqueda como de sitios web. Comparte fuerte conexión con el criptominero Hidden Bee.

Media: Los atacantes han estado usando **técnicas de Typosquatting**, utilizando letras minúsculas en los nombres de los **paquetes en el registro de Node Package Manager (NPM)**, para la posible suplantación de paquetes maliciosos.

Media: Se ha detectado la **distribución del ladrón Aurora mediante actualizaciones falsas del sistema**. El autor estaría utilizando **técnicas de malvertising** (promoción de anuncios maliciosos mediante pago) para distribuir ejecutables de supuestas actualizaciones necesarias.

Media: Identificado, en la reciente campaña del malware **Ducktail** de marzo, un archivo que **recopila datos del usuario**, como información del navegador, dirección IP y geolocalización, mientras también se **conecta a los dominios de Facebook y Telegram**.

Media: Aparece una **nueva variante, más sigilosa, de BPFdoor**. Es una puerta trasera pasiva, de bajo perfil y específica de Linux, que provee **persistencia a largo plazo** en redes y entornos ya violados, garantizando un período prolongado de tiempo post-compromiso.

Media: Se ha visto al **malware CLR SqlShell** siendo utilizado en varios ataques contra **servidores MS-SQL mal administrados**. Similar a WebShell, SqlShell admite varias funciones tras su instalación, como ejecución de comandos maliciosos.

Media: El criptominero **CUEMiner** (alojado en GitHub en el **proyecto SilentCryptoMiner**) presenta muchos y pequeños cambios, y combinación con multitud de URL y TTP, lo que indica que el malware es **utilizado simultáneamente y de varias formas por múltiples grupos**. Destaca su **distribución por BitTorrrent y OneDrive**, a través de software crackeado y troyanizado.

Baja: Un sitio web de phishing **imita una famosa web rusa (CryptoPro CSP) para distribuir el RAT DarkWatchMan**. Este malware evita escribir los datos capturados en el disco y los almacena en el registro, lo que minimiza el riesgo de detección.

Baja: Detectada campaña maliciosa que se distribuye a través del correo electrónico apuntando a **México** en la que buscan engañar a las personas para que abran una **página web (HTML), enviada en nombre de Banco Monex**, para descargar malware.

Baja: Una **empresa de juegos de azar en Filipinas** fue el objetivo de un actor de amenazas alineado con China como parte de una campaña que ha estado en curso desde octubre de 2021. Su táctica es **apuntar a los agentes de soporte** de las empresas víctimas a través de **aplicaciones de chat**.

RANSOMWARE

Media: **Alto Calore Servizi**, una empresa que provee de **agua potable a cerca de medio millón de personas en Italia**, está experimentando algunos problemas técnicos a causa de un ataque de ransomware. Este incidente habría inutilizado todos sus sistemas de TI, y ha sido reconocido por el **grupo Medusa**.

Media: Una nueva operación de ransomware llamada **Cactus** ha estado explotando vulnerabilidades en **dispositivos VPN** para el acceso inicial a redes de "**grandes entidades comerciales**". Muestra TTP habituales, pero con un toque propio para evitar la detección.

Media: Detectada **nueva variante de ransomware llamada Rancoz**, la cual se ha descubierto que aprovecha el **código base de Vice Society** para aumentar el impacto y el abanico de víctimas. Utiliza el método de la doble extorsión.

Baja: El mismo grupo de ransomware anteriormente normbrado, **Medusa**, ha apuntado también a un **centro de tratamiento oncológico de Australia**, de nombre **Princess Mary Cancer Centre**.

Baja: La nueva operación de ransomware **Akira** ha ido construyendo lentamente una lista de víctimas, incluyendo **redes corporativas en EEUU y Canadá** a las que exigen rescates de millones de dólares. Estas empresas se encuentran en diversas industrias y sectores, siendo su última víctima la **Universidad Mercer en Macon, Georgia**, de donde se ha sustraído información confidencial de estudiantes, padres y empleados.

Baja: La **empresa canadiense de software diversificado Constellation Software** confirmó que algunos de sus sistemas fueron violados por actores de amenazas que también robaron información personal y datos comerciales. El ataque ha sido reivindicado por la **banda rusa ALPHV** (BlackCat).

Baja: El **Departamento del Sheriff del condado de San Bernardino optó por pagar un rescate** de 1,1 millones de dólares después de que un ataque de ransomware infectara sus sistemas a principios de abril.

Baja: La **clínica médica y centro de cirugía Murfreesboro**, Tennessee, lucha por recuperarse por completo dos semanas después de un ataque cibernético que incluyó un intento de robo de datos que lo **obligó a desconectar sus sistemas de TI** y cancelar la mayoría de los servicios a los pacientes.

Baja: El grupo de ransomware **LockBit 3.0** filtró el lunes **600 gigabytes de datos críticos robados al prestamista indio Fullerton India**, dos semanas después de que el grupo exigiera un rescate de 3 millones de dólares a la empresa.

Baja: El **museo de arte nacional de Canadá** pasó las últimas dos semanas recuperándose de un ataque de ransomware que lo obligó a cerrar su sistema de TI.

Baja: Un ciberataque de hace 6 meses había provocado el robo de **varios de los nuevos temas del grupo de música Smashing Pumpkins**, antes del lanzamiento del disco, amenazando con filtrarlas en caso de no proceder al pago del rescate.

Informativa: Se ha observado como una g**ran cantidad de familias de ransomware dirigidas a hipervisores Vmware ESXi están basadas en el código fuente filtrado de Babuk (RaaS)**. Se relacionan con este código más de **10 familias de malware**, de los principales actores de ransomware como **Conti y REvil**.

Informativa: La empresa de ciberseguridad industrial **Dragos revela un intento frustrado de ataque de ransomware** después de que una conocida banda de ciberdelincuentes intentara violar sus defensas e infiltrarse en la red interna para cifrar dispositivos. Sólo obtuvieron acceso al servicio en la nube de SharePoint y al sistema de gestión de contratos de la empresa. Se sospecha del **grupo de ransomware BlackBasta**.