INFORME CTI DEL 18 AL 24 DE MARZO DE 2023

Resumen de amenazas

	Crítica	Alta	Media	Baja	Info.
APT	0	0	4	3	0
Cadena de suministro	0	0	0	1	1
Amenazas contra datos	0	0	2	0	2
Amenazas contra disponibilidad	0	0	1	0	0
Ingeniería social	0	2	1	2	0
Malware	0	2	13	5	0
Ransomware	0	8	4	3	1

APT

Media: Varios **proveedores de telecomunicaciones que operan en el Sudeste de Asia, Europa, África y Oriente Medio** son objeto de nuevos ataques cibernéticos desde principios de año. El conjunto de intrusión se ha atribuido a los **actores de espionaje chinos APT41 y Gallium**,en relación con una campaña de larga duración denominada **Operation Soft Cell** basada en superposición de herramientas.

Media: Identificada una **campaña china (Nansh0u)** que tenía como objetivo infectar **servidores Windows MS-SQL y phpMyAdmin en todo el mundo**. Las máquinas comprometidas incluyen más de 50.000 servidores pertenecientes a empresas de los **sectores de salud, telecomunicaciones, medios y TI**.

Media: El APT norcoreano **ScarCruft (RedEyes / APT37) está evolucionando sus TTP**, utilizando archivos de ayuda HTML compilada (CHM) de Microsoft armados para descargar malware adicional en las máquinas seleccionadas. Se ha identificado el uso de la **puerta trasera M2RAT** y el **implante de powershell Chinotto**.

Media: El actor de amenazas **Mustang Panda también ha estado cambiando activamente sus herramientas y TTP** para eludir las soluciones de seguridad. En una campaña reciente se ha visto cómo entrega señuelos a través phishing conteniendo **enlaces de Google Drive**, con lo que implementan **malware previamente no registrado** y herramientas interesantes utilizadas con fines de exfiltración.

Baja: Encontradas una serie de **backdooors personalizados y herramientas de ciberespionaje previamente no documentadas desplegadas en Israel por el grupo de APT POLONIUM**. Se trata de un grupo con sede en Líbano que coordina sus actividades con otros actores afiliados al **Ministerio de Inteligencia y Seguridad de Irán (MOIS)**. Amenaza a una gran cantidad de sectores diferentes, pero parece únicamente centrado en objetivos israelíes.

Baja: Descubiertos ataques de un nuevo APT que utilizó un **marco malicioso nunca antes visto llamado CommonMagic** y una **nueva puerta trasera llamada PowerMagic**. Se está dirigiendo a organizaciones de **los sectores administrativo, agrícola y de transporte** con fines de espionaje en varias regiones de **Ucrania**.

Baja: Los investigadores de seguridad descubrieron que el **grupo de ciberespionaje pakistaní SideCopy APT** emplea nuevas tácticas para atacar a los trabajadores de la **Organización de Investigación y Desarrollo de Defensa de la India** y robar secretos militares confidenciales.

Cadena de suministro

Baja: La **NBA** está notificando a los seguidores sobre una **violación de datos** después de que se robara parte de su información persona. Según comunicaciones, el evento se ha producido tras un **acceso no autorizado en un proveedor de servicios externo**, del ámbito de la comunicación por correo electrónico con los fans.

Informativa: **University of California San Diego Health** notificó a un número no revelado de pacientes que sus datos se compartieron inadvertidamente con terceros debido a que **su proveedor colocó herramientas de análisis en sus sitios web orientados al paciente** sin la autorización de UCSD Health.

Amenazas contra datos

Media: El fabricante líder de **cajeros automáticos de Bitcoin, General Bytes**, reveló que los piratas informáticos robaron criptomonedas de la empresa y sus clientes utilizando una **vulnerabilidad de día cero en su plataforma de gestión BATM**.

Media: El gigante de la industria del entretenimiento y del streaming **Lionsgate filtró las direcciones IP** de los usuarios e **información sobre el contenido** que ven en su plataforma. La filtración ha sucedido a través de una **instancia abierta de ElasticSearch**.

Informativa: Una **configuración incorrecta** en un sitio web propiedad de la **cadena de tiendas de comestibles Lowe's Market**, con sede en EE. UU., podría haber permitido que los atacantes obtuvieran el control de sus sistemas.

Informativa: La empresa de ciberseguridad **Black Lantern anunció esta semana Badsecrets**, una herramienta de código abierto que **puede ayudar a identificar secretos criptográficos** conocidos o débiles en muchos marcos web.

Amenazas contra la disponibilidad

Media: Se ha observado que el grupo de hacktivistas afiliado a Rusia conocido como **KillNet apunta con ataques DDoS a aplicaciones de atención médica alojadas en la infraestructura de Microsoft Azure** durante más de los últimos tres meses.

Ingeniería social

Alta: Se ha detectado una **campaña de phishing que trata de suplantar a la Agencia Tributaria** y utiliza una página web fraudulenta, similar a la legítima, con el fin de **obtener las credenciales de acceso** del usuario.

Alta: Investigadores detectan nueva **estafa dirigida a usuarios de Instagram de España**, Polonia, Francia, Australia y UK; concretamente, a seguidores de la popular **marca de ropa SHEIN**. Mediante comentarios, animan a usuarios a reclamar una tarjeta regalo facilitando sus **datos personales y de su tarjeta**.

Media: Una nueva técnica de los ciberdelincuentes de **phishing** consiste en utilizar **servidores de SharePoint secuestrados**, pero perfectamente legítimos, para **enviar notificaciones estándar** sobre compartición de archivos.

Baja: Nueva campaña híbrida de **phishing en EEUU** que se hace pasar por la **Administración del Seguro Social (SSA)**, que intenta engañar a los destinatarios para que llamen a un centro de llamadas criminal.

Baja: Estafadores en **Argentina** siguen haciéndose pasar por **centros oficiales de vacunación** y llaman por teléfono para solicitar un código de seis dígitos que les permite robar la cuenta de WhatsApp.

Malware

Alta: **Formbook**, una de las variantes de malware más activas en estos últimos meses, se está difundiendo ahora gracias a una **nueva campaña de e-mails para suplantar entidades bancarias españolas** (Banco Santander y Sabadell).

Alta: Una nueva campaña de piratería de **robo de tarjetas de crédito** está mostrando técnicas innovadoras al ocultar su código malicioso dentro del **módulo de pasarela de pago 'Authorize.net' para WooCommcerce**, lo que permite que la violación evada la detección por escaneos de seguridad. La campaña utiliza el skimmer **MageCart** modificado.

Media: Una nueva **botnet DDoS basada en Golang, rastreada como HinataBot**, apunta a enrutadores y servidores al explotar vulnerabilidades conocidas, con el objetivo de implementar **ataques DDoS**. Abusa de **vulnerabilidades antiguas y credenciales débiles**.

Media: Con el nuevo **regreso de la botnet Emotet** se ha detectado que, ahora, se distribuye utilizando archivos **adjuntos de correo electrónico de Microsoft OneNote**, con el objetivo de eludir las restricciones de seguridad de Microsoft e infectar a más objetivos.

Media: Identificado un **ataque sofisticado** y altamente malicioso dirigido a los **desarrolladores de .NET a través del repositorio de NuGet**, utilizando técnicas sofisticadas de typosquatting.

Media: **AresLoader** es un nuevo **cargador de MaaS** ofrecido por actores de amenazas con vínculos al **hacktivismo ruso** que se detectó recientemente en la naturaleza. La mayoría de los usuarios están impulsando variedades de MaaS ladrón, por lo que AresLoader ofrece una **herramienta de "aglutinante" que permite a los usuarios enmascarar su malware como software legítimo**.

Media: Un **troyano bancario denominado Mispadu** se ha vinculado a múltiples campañas de spam dirigidas a **países LATAM y Portugal** con el objetivo de robar credenciales y entregar otras cargas útiles. Se dirige a sitios web legítimos, comprometiendo **versiones vulnerables de WordPress** para convertirlos en su servidor C2.

Media: **DotRunpeX** es un **nuevo inyector escrito en .NET** que usa la técnica Process Hollowing y se usa para infectar sistemas con una variedad de familias de malware conocidas, como **AgentTesla, AsyncRAY, BitRAT, Redline, Remcos o Vidar**.

Media: Varios actores de amenazas ya han adoptado un **troyano bancario Android emergente denominado Nexus** para apuntar a 450 aplicaciones financieras y realizar fraudes. Este malware se distribuye como **MaaS**.

Media: Se ha localizado una serie de **apps infectadas por numerosos troyanos como el Joker**, además de un nuevo malware conocido como **Hook**. También se han identificado otros troyanos como **Autolucos o Harly**.

Media: Google suspendió la popular **aplicación de comercio electrónico económico Pinduoduo de Play Store** después de detectar **malware** en las versiones de la aplicación china descargable desde otras tiendas en línea.

Media: Se ha encontrado un **nuevo skimmer** (malware de robo de información de tarjetas de crédito en el momento de la transacción), llamado **Kritec Magecart, en tiendas Magento**.

Media: Un **paquete malicioso de Python en PyPI**, identificado como "**onyxproxy", usa Unicode** como una técnica de ofuscación para evadir la detección mientras **roba y extrae las credenciales** de la cuenta de los desarrolladores y otros datos confidenciales de los dispositivos comprometidos.

Media: Se ha descubierto una **nueva variante del ladrón BlackGuard** en la naturaleza, que infecta mediante ataques de phishing selectivo. El **MaaS** evolucionó desde su variante anterior y ahora llega con nuevas capacidades, apuntando a **57 criptobilleteras**.

Media: El malware **ChinaZ DDoS Bot se está instalando en servidores Linux SSH** administrados de manera inadecuada. El grupo ChinaZ instala varios bots DDoS en sistemas Windows y Linux, destacando los llamados **XorDDoS, AESDDos, BillGates y MrBlack**.

Baja: Un grupo monitoreado como **REF2924** está manejando un **nuevo malware de robo de datos denominado Naplistener** en ataques contra víctimas que operan en el **sur y sureste de Asia**. Están utilizando activos de red legítimos y código fuente abierto para pasar desapercibidos en ataques de robo de datos utilizando un **conjunto de malware personalizado** empeñado en la evasión.

Baja: Group-IB descubre más de **2400 páginas de trabajos fraudulentos** en una campaña en curso dirigida a **usuarios de habla árabe** en Egipto, KSA, Argelia y otros 10 países en Medio Oriente y África (MEA).

Baja: Están circulando correos de **phishing haciéndose pasar por la Registraduría Nacional de la República de Colombia** con el objetivo de infectar equipos con un troyano que espía y roba credenciales. Se ha detectado la distribución de **AsyncRAT**.

Baja: Un aviso conjunto de la Oficina Federal Alemana para la Protección de la Constitución (BfV) y el Servicio Nacional de Inteligencia de la República de Corea (NIS) advierte sobre **el uso de extensiones de Chrome por parte de Kimsuky para robar los correos electrónicos** de Gmail del objetivo, en Corea del Sur.

Baja: El grupo **APT-C-50 continúa apuntando a ciudadanos iraníes con su campaña Domestic Kitten**, pero utilizando una nueva versión del **malware FurBall** que se hace pasar por una aplicación de traducción para Android.

Ransomware

Alta: El ransomware se ha convertido en la **principal amenaza para el sector del transporte en la UE**, y la Agencia de Ciberseguridad de la Unión Europea (**ENISA**) espera que los grupos de ransomware interrumpan los **sistemas de tecnología operativa (OT)**.

Alta: Cada vez es más notoria la **campaña de ransomware que está llevando a cabo Cl0p (TA505, Rusia)**, dirigiéndose continuamente a grandes empresas, multinacionales y gigantes de todo el mundo mediante la **explotación del 0-day CVE-2023-0669 en la herramienta de transferencia segura de archivos GoAnywhere MFT, de Fortra**. Tal es así que Cl0p **afirma que ha logrado violar más de 130 organizaciones** hasta el momento Esta semana han destacado los eventos que han involucrado a las siguientes víctimas:

- **Hitachi Energy**, gigante y líder mundial en tecnología y energía, con sede en Suiza.
- **Saks Fifth Avenue,** minorista de marcas de lujo, con sede en Nueva York, EEUU).
- Administración de **Toronto**, ciudad de los EEUU.
- **Virgin Red** de UK, el club de recompensas de Virgin Group que permite a los clientes ganar y gastar puntos en los negocios de Virgin.
- **Fondo de Protección de Pensiones (PPF) de Reino Unido**, una corporación pública legal de UK.

Alta: **Ferrari** ha revelado una violación de datos luego de una demanda de rescate recibida después de que los atacantes obtuvieran acceso a algunos de los sistemas de TI de la compañía. Continúa así el **torrente de brechas de seguridad en la industria del automóvil**.

Media: La **compañía holandesa de logística marítima Royal Dirkzwager** sufrió un ataque de ransomware por parte del actor de amenazas **Play**.

Media: Identificado un **nuevo actor de amenazas de ransomware denominado CatB**, el cual ha llamado la atención por su continuo uso del **secuestro de DLL a través del Coordinador de transacciones distribuidas de Microsoft (MSDTC)** para extraer y lanzar cargas útiles de ransomware. Las similitudes sugieren que puede ser una **evolución del ransomware Pandora**.

Media: **LockBit ha akadido a la empresa Telepizza** a la lista de víctimas de su leak site de la Dark Web, no habiendo trascendido, de momento, más detalles al respecto.

Media: **PLEASE_READ_ME** es una campaña activa de ransomware dirigida a **servidores de bases de datos MySQL** y se remonta al menos a enero de 2020. Se basa en un mecanismo de explotación de credenciales débiles.

Baja: El grupo de ransomware **LockBit** se atribuye la responsabilidad de acabar con un distribuidor de **productos de oficina con sede en EEUU llamado Essendant**, del cual se ha informado en el boletín de la semana pasada.

Baja: Tras la **operación de Play Ransomware contra la ciudad de Oakland** el mes pasado, ahora el actor de amenazas **LockBit reclama de nuevo otra operación** de ransomware contra la misma ciudad, amenazando con filtrar archivos robados de sus sistemas.

Baja: Se ha detectado la **distribución del ransomware Nevada en Corea**. Este ransomware no infecta a los sistemas que se encuentren en naciones específicas de la Comunidad de Estados Independientes (CEI).

Informativa: El prolífico grupo **de BianLian adopta la extorsión en torno a la filtración de datos** y se aleja de las técnicas de encriptado, tras ser publicado un **desencriptador gratuíto por parte de Avast**. Cada vez son más los grupos de ransomware, como BianLian o **Karakurt** que se alejan del malware de bloqueo o criptográfico y amenazan directamente con el filtrado de información.