S2 GRUPO

Cyber Threat Intelligence Report

TENDENCIAS 1T 2023

Lab52

Contenido

Resumen ejecutivo

A raíz de la recolección y análisis de la información obtenida de fuentes internas y externas a lo largo del primer trimestre del 2023, el equipo de ciberinteligencia de S2 Grupo, el Lab52, ha generado inteligencia para los servicios de seguridad de S2 Grupo.

El presente documento recoge la actividad registrada por parte de la división de ciberinteligencia de S2 Grupo, Lab52. Este informe recorre los sucesos más significativos del primer trimestre del año 2023 y, a través de un análisis, presenta unas conclusiones. El contenido está estructurado en cuatro grandes partes:

- Principales eventos geopolíticos del trimestre y estudio de tendencias extraídas de los indicadores de la base de datos de inteligencia del Lab52.
- Repaso de las principales campañas de ciber espionaje llevadas a cabo por los actores de la amenaza más activos, junto a su respectivo contexto geopolítico y haciendo énfasis en las innovaciones tecnológicas implementadas.
- Análisis del cibercrimen. Ransomware, malware y Deep Web.
- Representación gráfica de datos y estadísticas de vulnerabilidades reveladas en el primer trimestre del 2023, así como el análisis de las que han tenido un mayor impacto.

Tendencias del trimestre

Contexto geopolítico

La situación de las relaciones internacionales ha estado marcada por la continuación del conflicto entre Rusia y Ucrania. Se ha podido observar como a lo largo del trimestre numerosos países pertenecientes a la OTAN han respaldado de una manera mucho más significativa a Ucrania, especialmente a través del envío de armamento.

El bloque occidental ha estado suministrando material militar desde el inicio del conflicto. Sin embargo, los tanques y aviones de combate tienen el potencial de darle una ventaja militar a Ucrania y tener un impacto considerable en el progreso del conflicto. Esto supone un aumento del riesgo de que la guerra se extienda, convirtiéndose en un conflicto internacional e involucrando a más países. La principal preocupación de este escenario es el posible uso de armas nucleares y las consecuencias catastróficas que le acarrean. El viejo continente está invirtiendo todos sus esfuerzos en combatir a Rusia: Francia ha enviado más de un tercio de sus obuses, Dinamarca se ha quedado prácticamente sin artillería, España tiene un tercio de sus Leopard sin usar, y Alemania solo tiene munición para unas pocas horas, máximo días, en caso de batalla.

En este contexto, los presidentes de varios países europeos y la presidenta de la Comisión Europea han visitado a su homólogo chino en Pekín. Von der Leyen pidió a China que no suministrase armas a Rusia “de forma directa o indirecta” y señaló que la posición del gigante asiático con respecto a la guerra es “crucial” para la Unión Europea. Por su parte, Jinping se comprometió a “facilitar las conversaciones de paz y la solución política de la crisis de Ucrania”.

Li Shangfu, ministro de Defensa chino, visitó Rusia por primera vez. En su reunión con Vladímir Putin, Shangfu aseguró que “la cooperación militar entre China y Rusia se está desarrollando muy bien. Esto hace una gran contribución a mantener la seguridad global y regional”. En el ámbito económico las relaciones entre ambos países también son buenas. El año pasado, Rusia aumentó un 50% sus importaciones de gas a China mediante el oleoducto Poder de Siberia. Esta cantidad podría crecer tras la puesta en marcha de Poder de Siberia 2, cuya construcción atravesará Mongolia.

Por otro lado, Xi Jinping y Volodímir Zelenski mantuvieron una conversación telefónica el 26 de abril. El presidente chino mandará una delegación de diplomáticos a Ucrania para negociar la paz. Por su parte, Zelenski anunció el nombramiento de un nuevo embajador ucraniano en China.

De este modo, parece ser que China se está posicionando como el mediador entre el bloque proucraniano y prorruso en este conflicto armado.

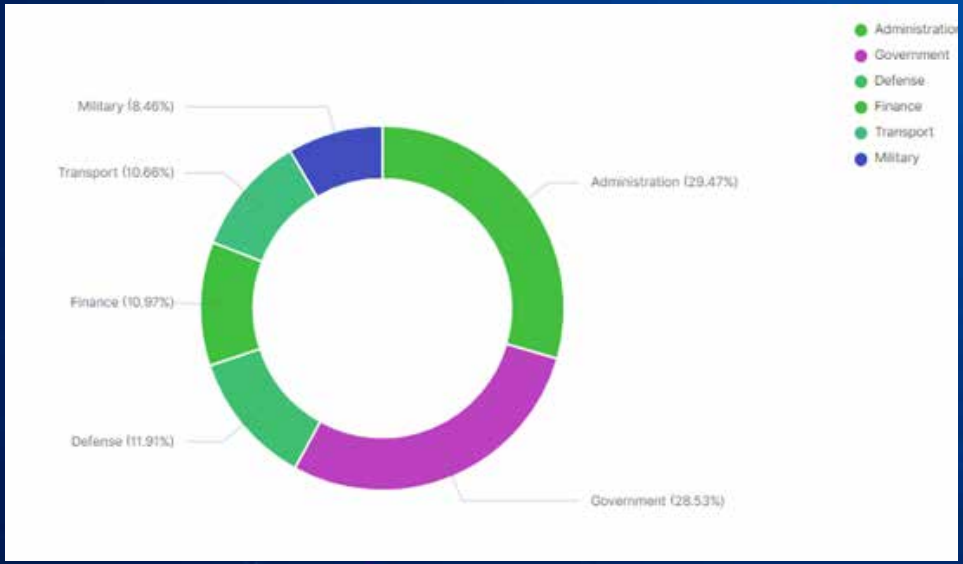
Sin embargo, parece ser que el gobierno de Xi Jinping no está limitando su papel como mediador al conflicto en Ucrania. Irán y Arabia Saudí han restablecido relaciones, que cortaron en 2016, y se espera que las embajadas en sus respectivos países vuelvan a operar con normalidad a corto plazo. Este acuerdo se produce después de un encuentro de sus mandatarios en China y tras dos años de negociaciones en Omán.

Suecia ha descubierto el mayor depósito de tierras raras en Europa con elementos químicos fundamentales para la construcción de baterías para vehículo eléctricos o tecnología militar. Estos elementos son parte de la guerra comercial entre las grandes potencias mundiales. Actualmente China es el mayor productor y exportador de tierras raras a nivel mundial. El descubrimiento de este yacimiento podría poner en riesgo el dominio chino del mercado internacional.

Análisis de los incidentes del trimestre

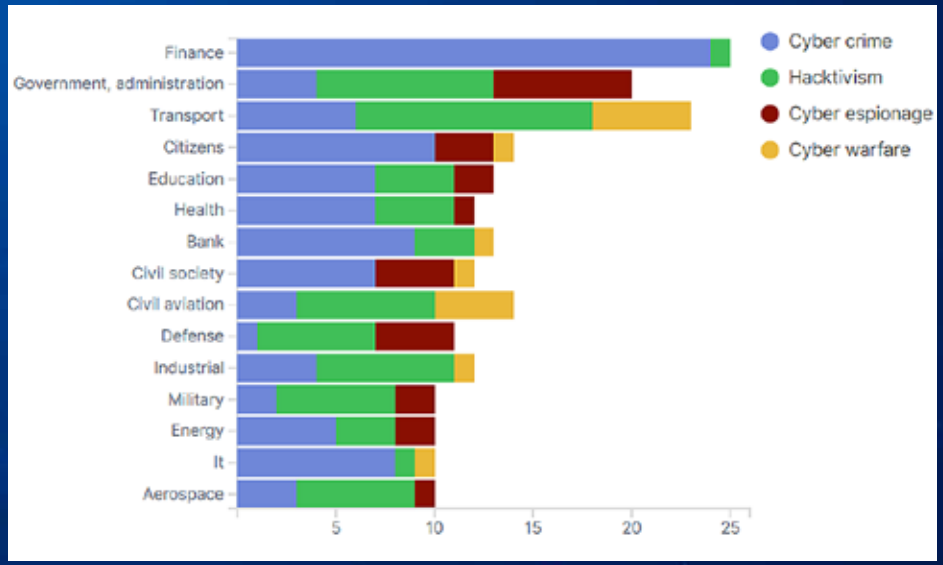
Gracias al registro de incidentes de seguridad de fuentes internas y externas, el Lab52 es capaz de analizar la evolución de estos e identificar las tendencias en materia de ciberamenazas del primer trimestre del 2023.

La representación gráfica del porcentaje de incidentes registrados por sector revela que, tanto la administración pública como los organismos gubernamentales han sido el principal objetivo de los atacantes durante este periodo. Seguidamente, el sector militar y de la defensa, representando casi un 20% de los incidentes registrados. Por último, el sector de la finanza y del transporte.



1. Porcentaje de incidentes

El próximo gráfico muestra la distribución de la tipología del ataque en función del sector. De este modo, tras un análisis se puede afirmar que sectores estratégicos, como pueden ser gobierno y administración, transporte, defensa y militar, son objetivo de ciberespionaje y hacktivismo. Mientras que otros sectores con mayor presencia del sector privado son más susceptibles de sufrir incidentes de cibercrimen debido a que la finalidad del ataque es puramente monetaria, como el financiero, donde representan más del 90% de los casos.



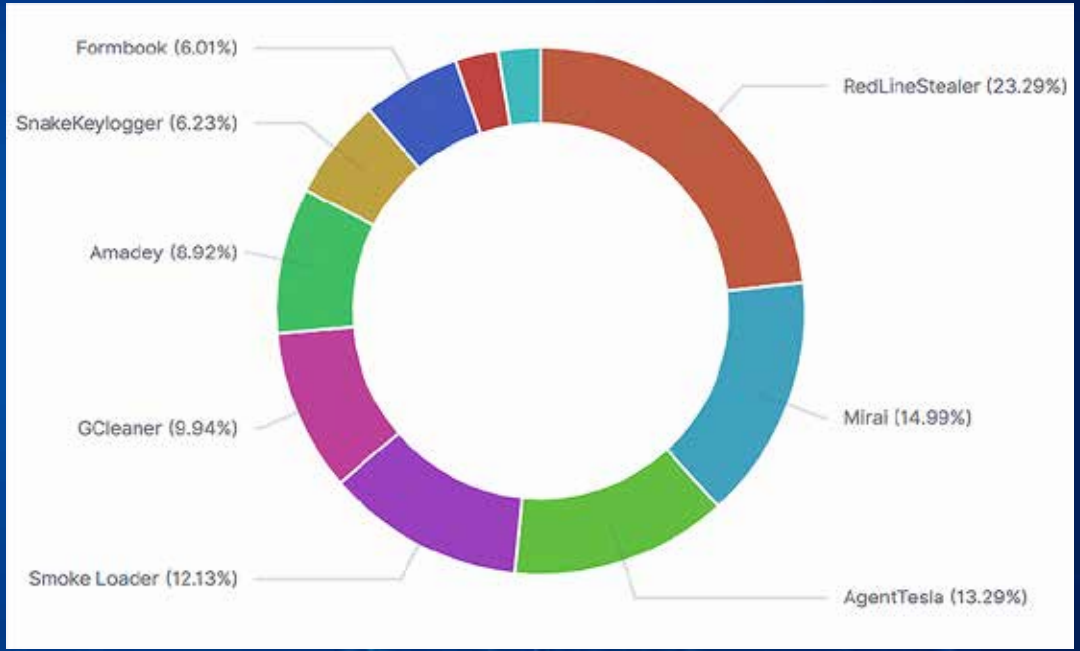
2. Distribución de ataques

Tendencias en malware

El Lab52 también lleva a cabo un ejercicio de recolección de muestras de fuentes internas y externas. De este modo, es posible identificar qué familias de malware han sido las más utilizadas a lo largo del trimestre. Respecto a los datos obtenidos en el trimestre anterior, se ha visto un incremento especialmente en la presencia de RedLineStealer y Mirai.

RedLineStealer se mantiene como la familia de malware más prevaleciente del trimestre. Pese a que el número total de muestras registradas ha disminuido con respecto al trimestre anterior, porcentualmente mantiene unos valores muy similares.

Por otro lado, se ha observado un incremento notable de las muestras registradas de Mirai, que se posiciona como la segunda familia de malware más vista durante el trimestre. Este fenómeno es debido probablemente a la gran proliferación de las actividades de los grupos hacktivistas de denegación de servicio y la necesidad de ampliar el número de activos de sus botnets.

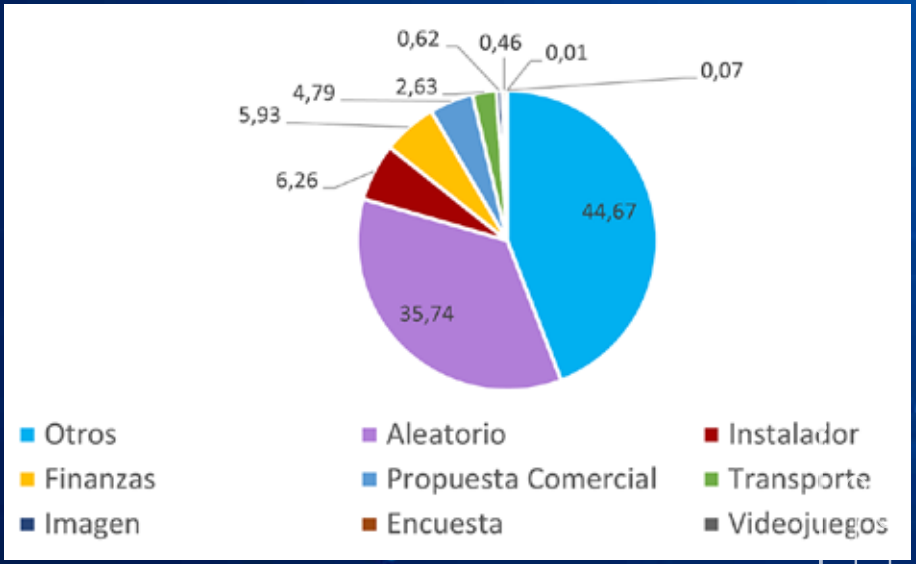


3. Tendencias en Malware

En cuanto a las temáticas utilizadas como señuelo por las distintas familias de malware, se puede observar como la aleatoriedad representa casi un 50% del total, lo que dificulta la creación de reglas de detección. Descartando la temática aleatoria, la suplantación de instaladores es la temática más común, seguida por la financiera y las propuestas comerciales.

Por otro lado, se han identificado dos fenómenos dignos de mención. En primer lugar, se ha observado como el método de pago SWIFT ha sido utilizado como temática del señuelo en numerosos ataques. El segundo fenómeno identificado es el uso de la temática de videojuegos en el señuelo, lo que podría indicar una focalización de los ataques en generaciones más jóvenes.

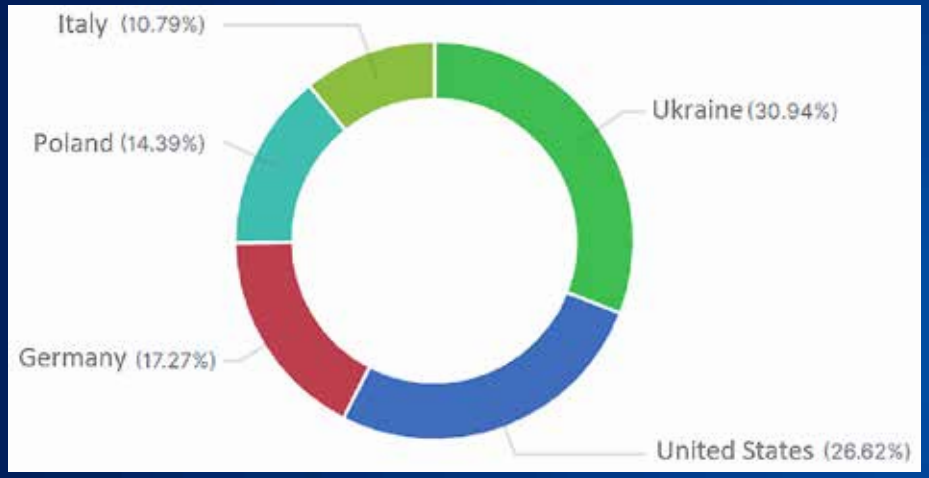
Además de la generación de inteligencia a partir de los incidentes de seguridad registrados, el equipo del Lab52 también lleva a cabo un ejercicio de análisis de los eventos geopolíticos y el contexto internacional, cuyo objetivo, entre otros, es detectar focos de riesgo. En el primer trimestre del año 2023, los principales focos de riesgo se centran en Rusia, Ucrania y Estados Unidos. Esto se debe al conflicto ruso-ucraniano. Alemania y el Reino Unido también tienen un alto nivel de riesgo, consecuencia de su grado de involucración en el conflicto. Mismamente, se pueden apreciar otros países con alto nivel de riesgo, como pueden ser Taiwán y China por la voluntad de independencia del primero, y Japón y Corea del Sur por las repetidas muestras de capacidades armamentísticas de Corea del Norte.



4. Temáticas utilizadas por malware para suplantación.

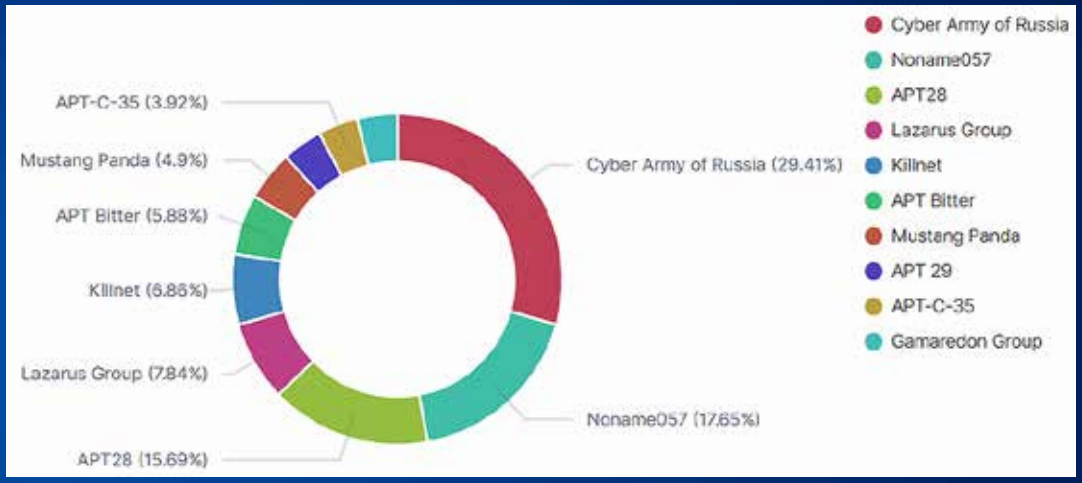
5 . Riesgo por país

El siguiente gráfico muestra los países más atacados durante el primer trimestre del año 2023. Comparando el gráfico anterior con este, se puede observar cómo existe una relación directa entre el nivel de riesgo de un país y la cantidad de ciberataques que recibe.



6. Distribución de los ciberataques por país víctima

De todos los eventos procesados por el equipo del Lab52 se han generado más de mil Indicadores de Compromiso en la base de datos de inteligencia de S2 Grupo. A continuación, se muestran los grupos más activos del periodo.



7. Top Amenazas basado en IoCs procesados

De la lista de los diez grupos más activos del primer trimestre, seis de ellos actúan en base a los intereses de Rusia, algunos desde un enfoque hacktivista (Cyber Army of Russia, Noname057, Killnet) y otros formando parte de distintas ramas del gobierno (APT28, APT29, Gamaredon Group). También se ha observado una gran actividad por parte del grupo norcoreano Lazarus Group, el cuál ha llevado a cabo un número de acciones de cibercrimen mayor de lo habitual.

Cuatro de los diez grupos tienen vínculos rusos, aunque también se ha observado una importante actividad de Mustang Panda y Lazarus. Es importante destacar que este último ha realizado un número de acciones de cibercrimen mucho mayor de lo habitual.

Pese a que los datos revelan que la mayoría de los incidentes de seguridad corresponden a acciones de cibercrimen, desde el inicio de la guerra de Ucrania se ha observado un incremento desmedido en el número de campañas de hacktivismo y ciberguerra.

Análisis de infraestructura

En lo que concierne a la propia infraestructura utilizada por actores, el mapa de la distribución geográfica del cuarto trimestre del año 2022 mostraba los siguientes datos:

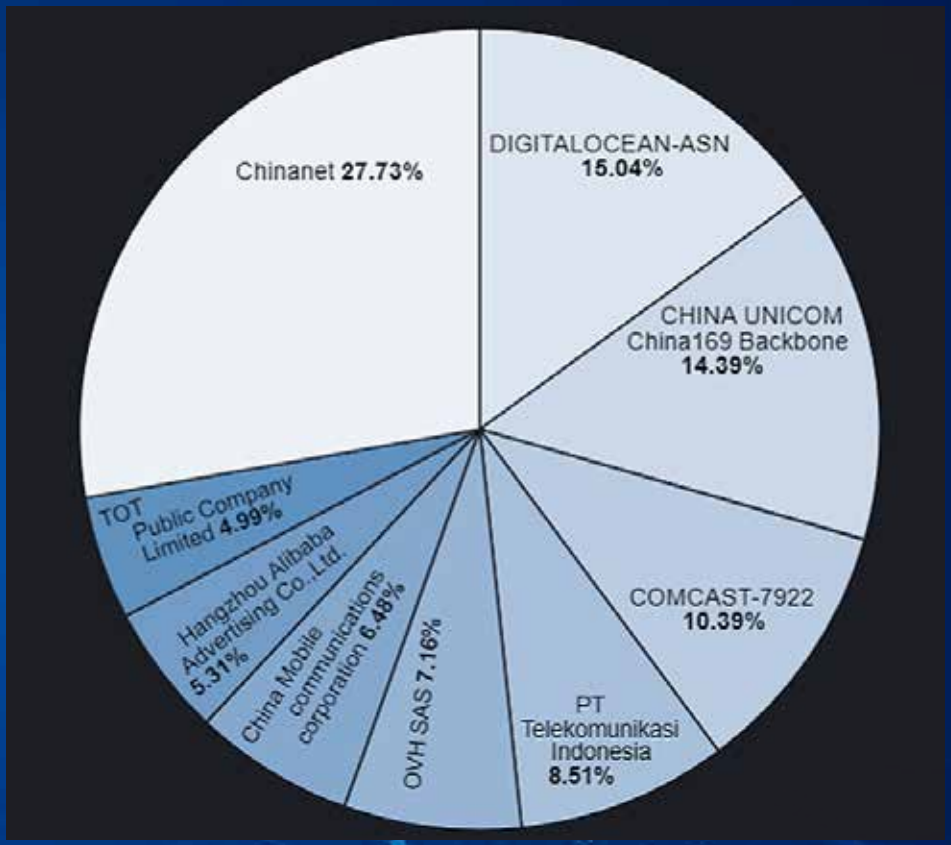
8. Infraestructura del 4T de 2022

La distribución geográfica de la infraestructura en el primer trimestre del año 2023 presenta ciertos cambios, como se puede observar en el siguiente mapa:

9. Infraestructura del 1T de 2023

Como se puede observar, el cambio más notorio es el aumento de la infraestructura en China. Los proveedores asociados con dicha infraestructura son Chinanet, CHINA UNICOM y China Mobile Communications. Esta infraestructura ha pasado a ser muy utilizada por los grupos hacktivistas, en detrimento de Biterika, que el trimestre anterior fue el segundo con más registros, ha desaparecido como una de las infraestructuras más utilizadas.

Es también interesante destacar que, tras la publicación de la utilización de Biterika por parte del grupo Killnet en el pasado trimestre, hayan pasado a utilizar Chinanet.



10. Número de registros por ASN 1Q

Campañas de Ciberespionaje

Actividad de grupos vinculados a Rusia

Grupos hacktivistas prorrusos

Si durante el último trimestre del año observamos una alta movilización de los grupos hacktivistas en respuesta a los actos con efectos geopolíticos llevados a cabo por Ucrania y Polonia, este trimestre grupos como NoName057 han ampliado el alcance de estas acciones y han incluido como objetivo a organizaciones estratégicas de los países que se han involucrado en el conflicto.

A lo largo del último trimestre del año 2022 se observó una gran movilización de grupos hacktivistas prorrusos que enfocaron sus esfuerzos en atacar Ucrania y Polonia como respuesta a las acciones llevadas a cabo por estos en el contexto del conflicto ruso-ucraniano.

En este primer trimestre del año 2023 se ha podido observar cómo estos mismos grupos hacktivistas (NoName057, Killnet, Cyber Army of Russia, etc.) han ampliado el alcance de sus ataques, incluyendo a su lista de objetivos a organizaciones estratégicas de aquellos países que se han involucrado en el conflicto. Teniendo como ejemplos:

- El aumento de ciberataques contra Italia después de que la primera ministra Giorgia Meloni visitase Kiev para trasladar su apoyo al Gobierno de Zelenski y al pueblo de Ucrania en el conflicto con Rusia.
- El aumento de ciberataques contra España tras la visita del presidente Pedro Sánchez a Kiev en la que confirmó ante Zelenski que España enviaría 6 tanques Leopard a Ucrania, pudiendo llegar hasta 10.

APT 28

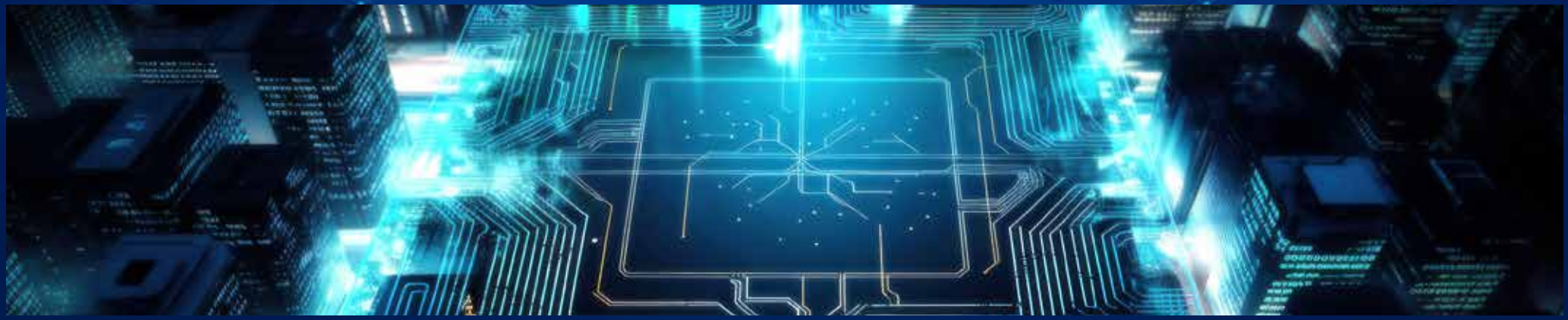
A mediados de marzo, Microsoft publicó la actualización de Outlook para la vulnerabilidad CVE-2023-23397. Se trata de una vulnerabilidad de escalada de privilegios que permite a los atacantes enviar correos electrónicos diseñados para explotar Outlook. Esta vulnerabilidad estaba siendo explotada por el grupo ruso APT 28 entre abril y diciembre de 2022 para atacar organizaciones europeas de múltiples sectores como: gubernamental, militar y energético. El objetivo de esta campaña era robar credenciales de Windows que utilizarían en el futuro en las fases de movimiento lateral y exfiltración.

APT 29

A finales del mes de marzo el Lab52 analizó dos ataques de phishing de una campaña contra entidades gubernamentales de países miembros de la Unión Europea llevada a cabo por el grupo ruso APT29, también conocido como NOBELIUM. El primer ataque se trata de un correo electrónico que suplanta el departamento de recursos humanos de una empresa tecnológica de desarrollo web con sede en Pakistán. El correo con asunto "Update! Invitation to the meeting" contiene un documento adjunto "invite.pdf". El vector de entrada del segundo ataque es un phishing que suplanta a una embajada de España. El mensaje del correo electrónico invita a las potenciales víctimas a formar parte de una reunión presencial sobre "The Future of international economic relations" en la embajada española. Seguidamente, con el pretexto de rellenar un formulario para confirmar su asistencia al evento, se adjunta un enlace malicioso. En ambos casos el resultado del phishing es la descarga de un archivo HTML que resulta ser una ISO con tres archivos: un ejecutable, una DLL maliciosa y una shellcode cifrada.

Gamaredon

Se detecta una nueva campaña de ciberespionaje del grupo APT Gamaredon contra instituciones ucranianas. Los actores se encuentran entregando un malware con capacidades de ejecutar comandos de forma remota e implementar cargas útiles. El vector inicial de distribución utilizado son correos de spearphishing que entregan un WebShell malicioso a través de técnicas de ingeniería social. Se utilizan como señuelos temáticas y documentos de instituciones ucranianas falsificadas. Con el fin de evadir los sistemas de detección, Gamaredon emplea múltiples técnicas de ofuscación. Gamaredon Group es un presunto grupo ruso de amenazas de espionaje cibernético que se ha centrado en organizaciones militares, ONGs, judiciales, policiales y sin fines de lucro en Ucrania desde al menos 2013.



Actividad de grupos vinculados a China

Mustang Panda

Especialmente innovadora ha sido la actividad vinculada a Mustang Panda, pues se detectó un nuevo backdoor, al cual se ha bautizado como “MQsTTang”. Permite al atacante ejecutar comandos arbitrarios en la máquina de la víctima utilizando el protocolo MQTT para la comunicación con el C2. Generalmente se usa este protocolo para las comunicaciones entre dispositivos IoT y controladores. Esto permite al atacante ocultar el resto de su infraestructura detrás de un intermediario. Por lo tanto, la máquina comprometida nunca se comunica directamente con el C2.

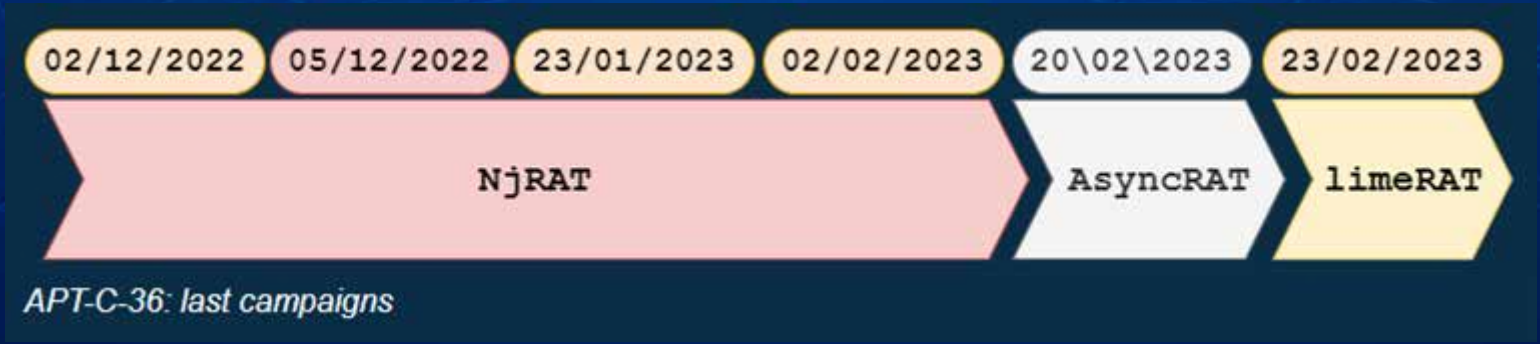
Actividad de otros grupos

APT-C-36

Desde el 2 de diciembre de 2022 hasta el 2 de febrero de 2023, se observaron múltiples campañas vinculadas con el grupo APT-C-36 en las que desplegaban NjRAT en su fase final. El 20 de febrero el Lab52 observó una campaña que variaba ligeramente con el resto y cuyo objetivo era desplegar AsyncRAT en las máquinas comprometidas.

A finales de febrero se observó el uso de LimeRAT, pero con un funcionamiento muy similar en el despliegue utilizado durante el resto de las campañas, desde las primeras cuyo objetivo era la ejecución de NjRAT. De este modo, tras el análisis realizado por el Lab52, LimeRAT se considera una evolución de NjRAT.

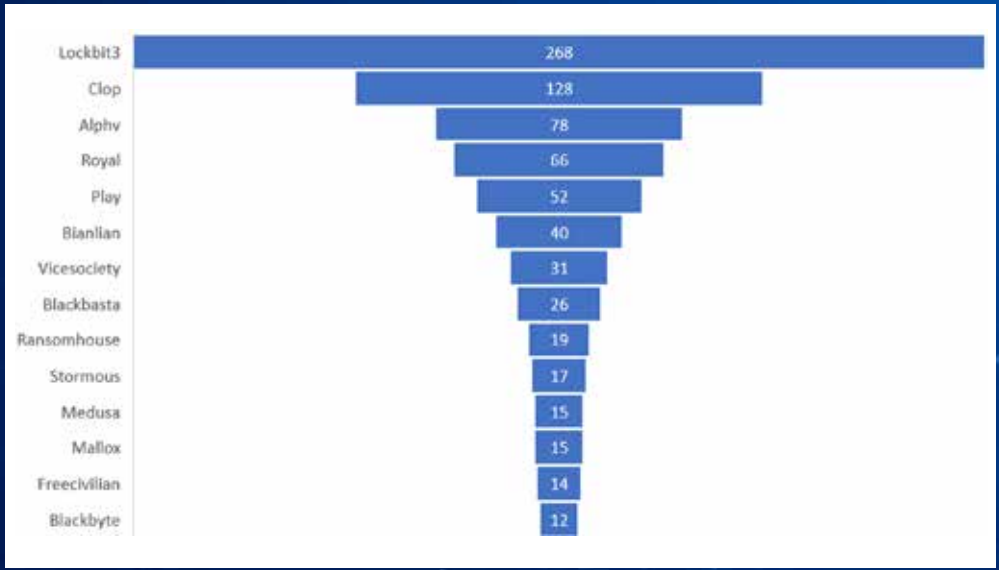
El diagrama muestra la evolución temporal del malware que se ejecuta después de la fase de infección.



Campañas de Cibercrimen

Ransomware

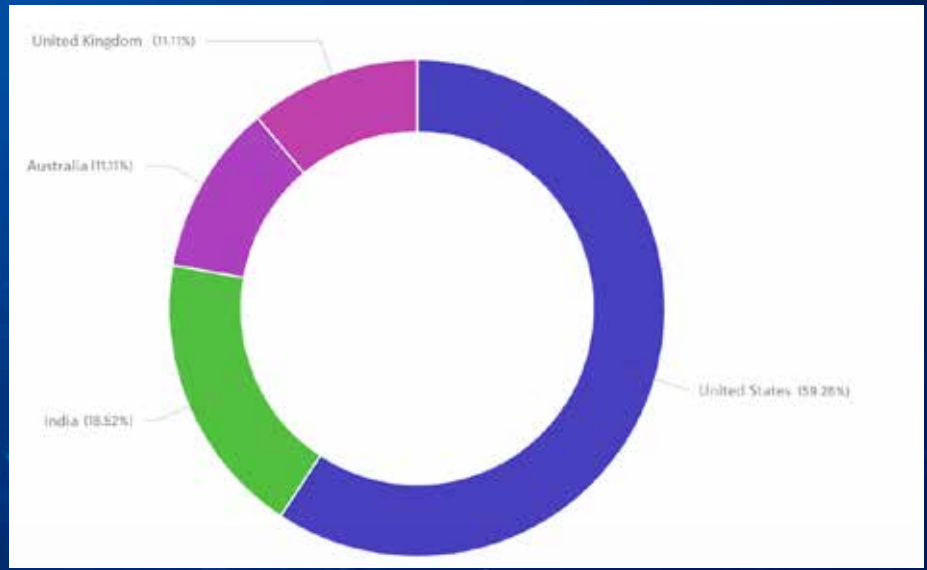
El ransomware sigue siendo una de las ciber amenazas más presentes y con mayor impacto a nivel global. Gracias a la recopilación y análisis de muestras, el Lab52 es capaz de dibujar una representación fidedigna de la presencia que tiene cada una de las distintas familias de ransomware en el panorama actual.



12. Familia de ransomware

A partir de los datos obtenido por el Lab52 se ha creado un gráfico que representa los países más afectados por el ransomware durante el primer trimestre del año 2023.

Por otra parte, el análisis de los sectores más afectados por las campañas de cibercrimen revela que los sectores de finanzas y bancario son los principales objetivos de las campañas de cibercrimen.



13. Países más afectados

Snake Keylogger, Guloader y Formbook

A lo largo del primer trimestre se ha podido observar un gran número de campañas contra España y Latinoamérica, especialmente con temáticas asociadas a temas bancarios y financieros. Es interesante destacar la proliferación de la utilización de Telegram como método de exfiltración de la información, además de la utilización de dominios dinámicos. Entre los organismos más suplantados encontramos los bancos españoles Santander, BBVA y Sabadell.

Keyloggers

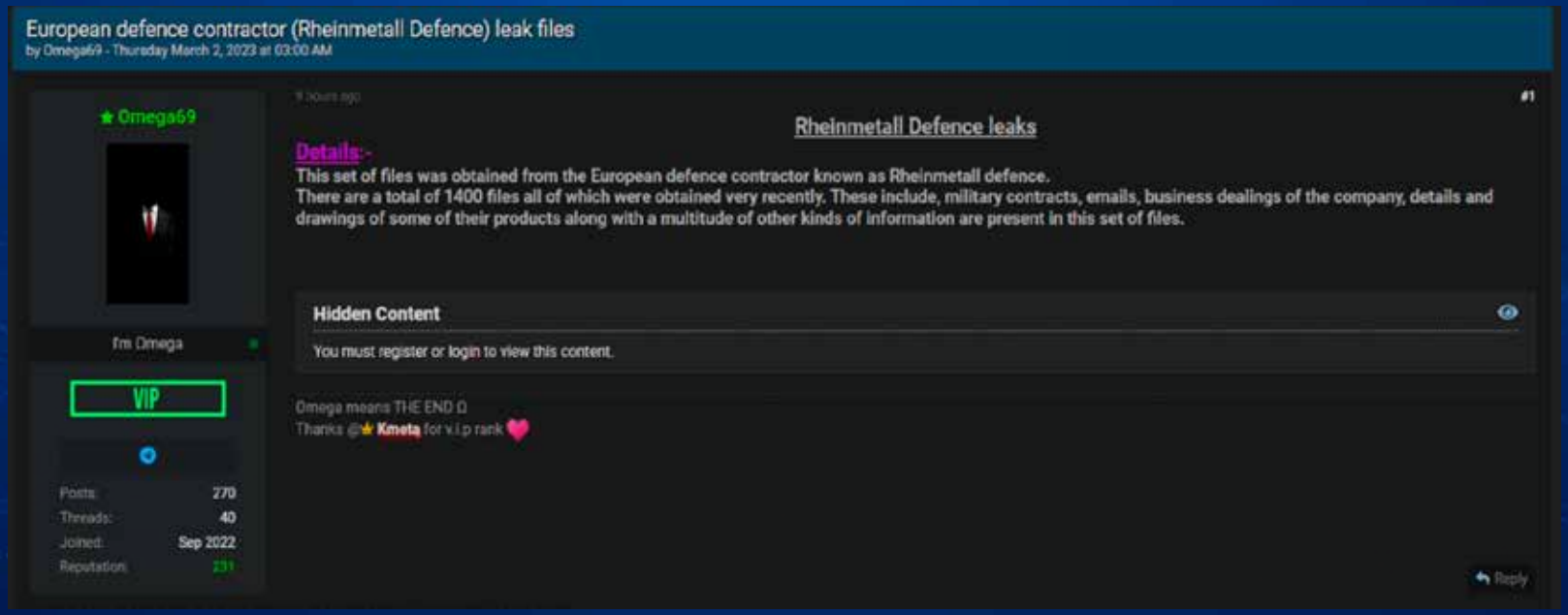
También se ha observado como un porcentaje muy alto de las campañas de ciber crimen despliegan keyloggers en las máquinas comprometidas. En una campaña analizada por el Lab52 se detectó un keylogger basado en PowerShell cuyo objetivo era registrar la actividad del portapapeles del usuario. Al detectar la combinación CTL+C o CTL+V mandaba la información a un servidor de Discord a través de un webhook.

Deep Web

A nivel de filtraciones de la Deep Web, se han observado un especial aumento de aquellas asociadas a temas de defensa. Entre las filtraciones encontramos las siguientes:

Rheinmetall

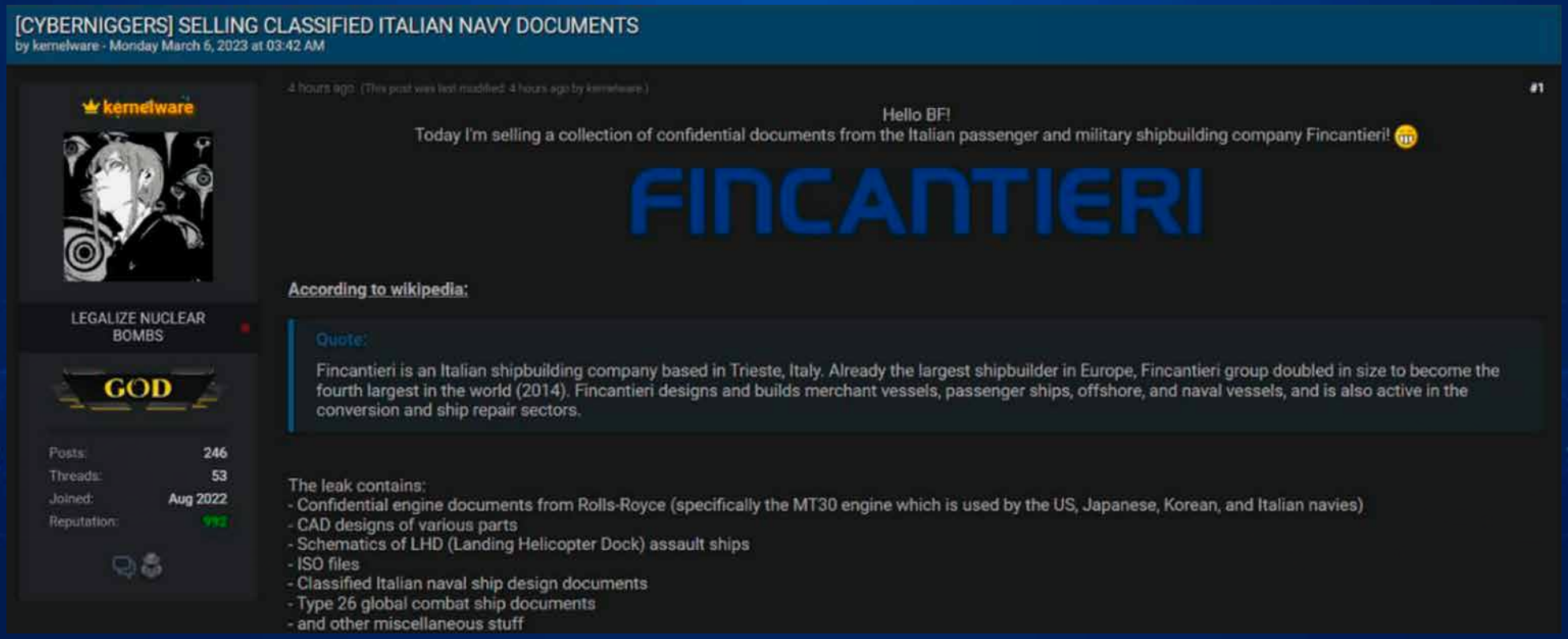
A principios de marzo se detectó a un actor llamado Omega69 vendiendo archivos exfiltrados de la empresa Rheinmetall Defence en un foro de la dark web conocido.



14. Fuga de datos de URheinmetall Defence.

Ficantieri

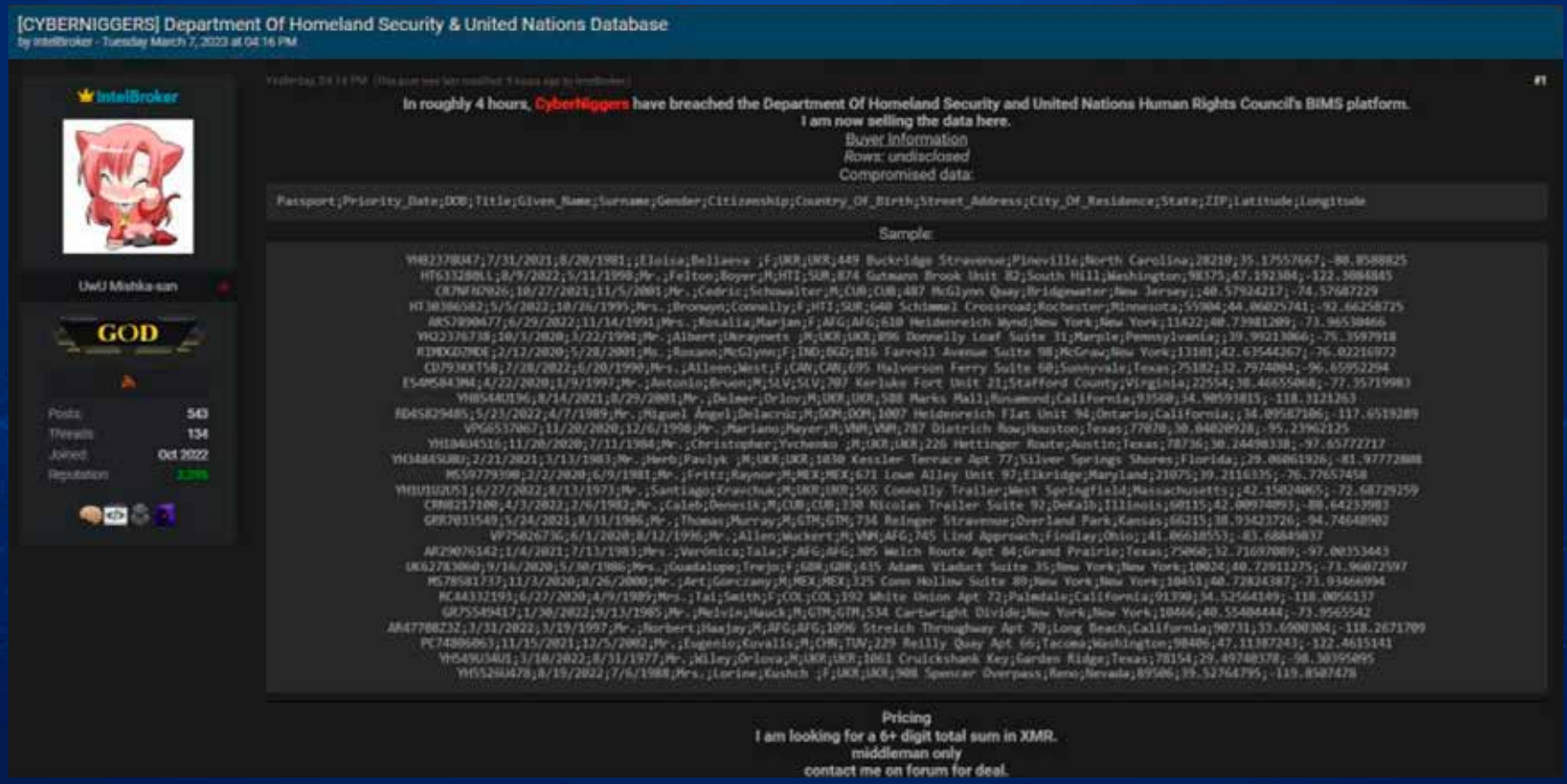
Tan solo unos días después del compromiso de Rheinmetall Defence, apareció en el mismo foro de la dark web un actor llamado kernelware que ofrecía información sobre la naviera italiana Fincatieri. Entre los datos que vendía se encontraban datos confidenciales sobre motores de Rolls-Royce, esquemas de buques de asalto LHD y documentos del buque de combate global Tipo 26.



15. Fuga de datos Fincatieri.

Departamento de Seguridad Nacional de los Estados Unidos

El 7 de marzo se publicó en un foro de la Deep web un anuncio sobre la venta de la base de datos del Departamento de Seguridad Nacional de EE. UU. y de las Naciones Unidas que contenía información personal detallada relativa tanto a los trabajadores de dichos organismos como a civiles.

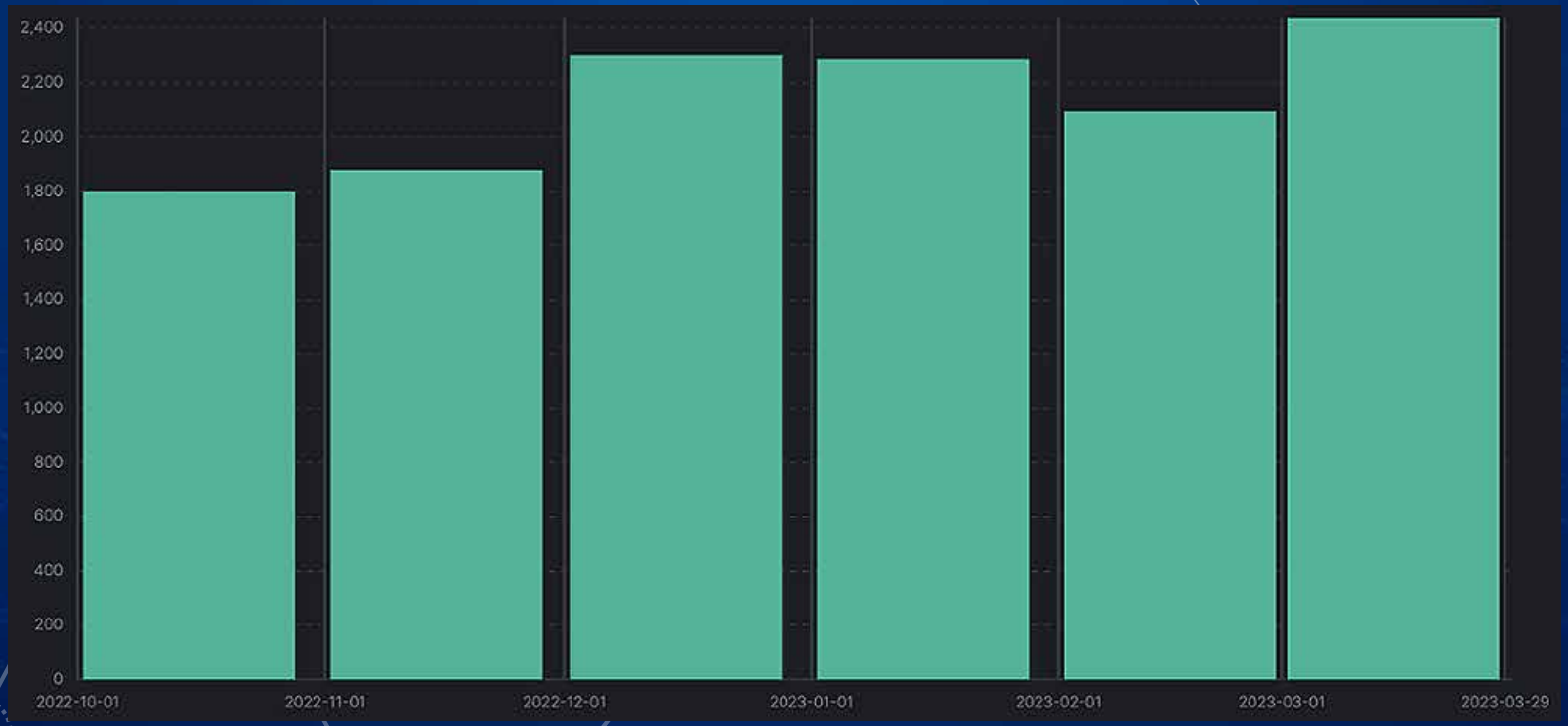


16. Fugas de datos del Departamento de Seguridad Nacional de los EEUU y Naciones Unidas.

Vulnerabilidades

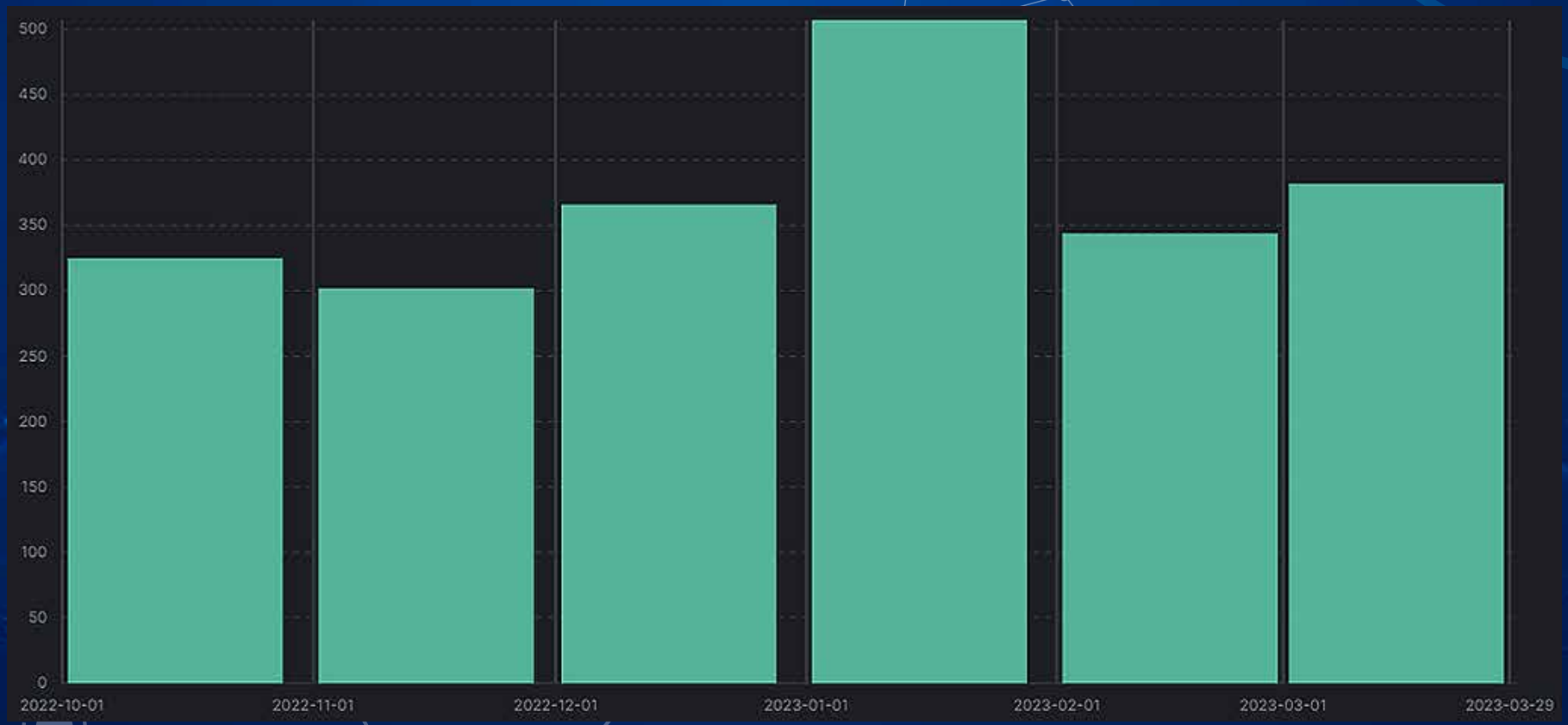
Datos y estadísticas de vulnerabilidades

La gráfica que se muestra representa el número total de vulnerabilidades publicadas entre octubre de 2022 y marzo de 2023. Como se puede observar, el número total de vulnerabilidades del primer trimestre de 2023 ha aumentado en comparación con el último trimestre de 2022. Este pico en las vulnerabilidades se debe a la publicación de 80 vulnerabilidades de criticidad muy alta asociadas al Hub de Insteon



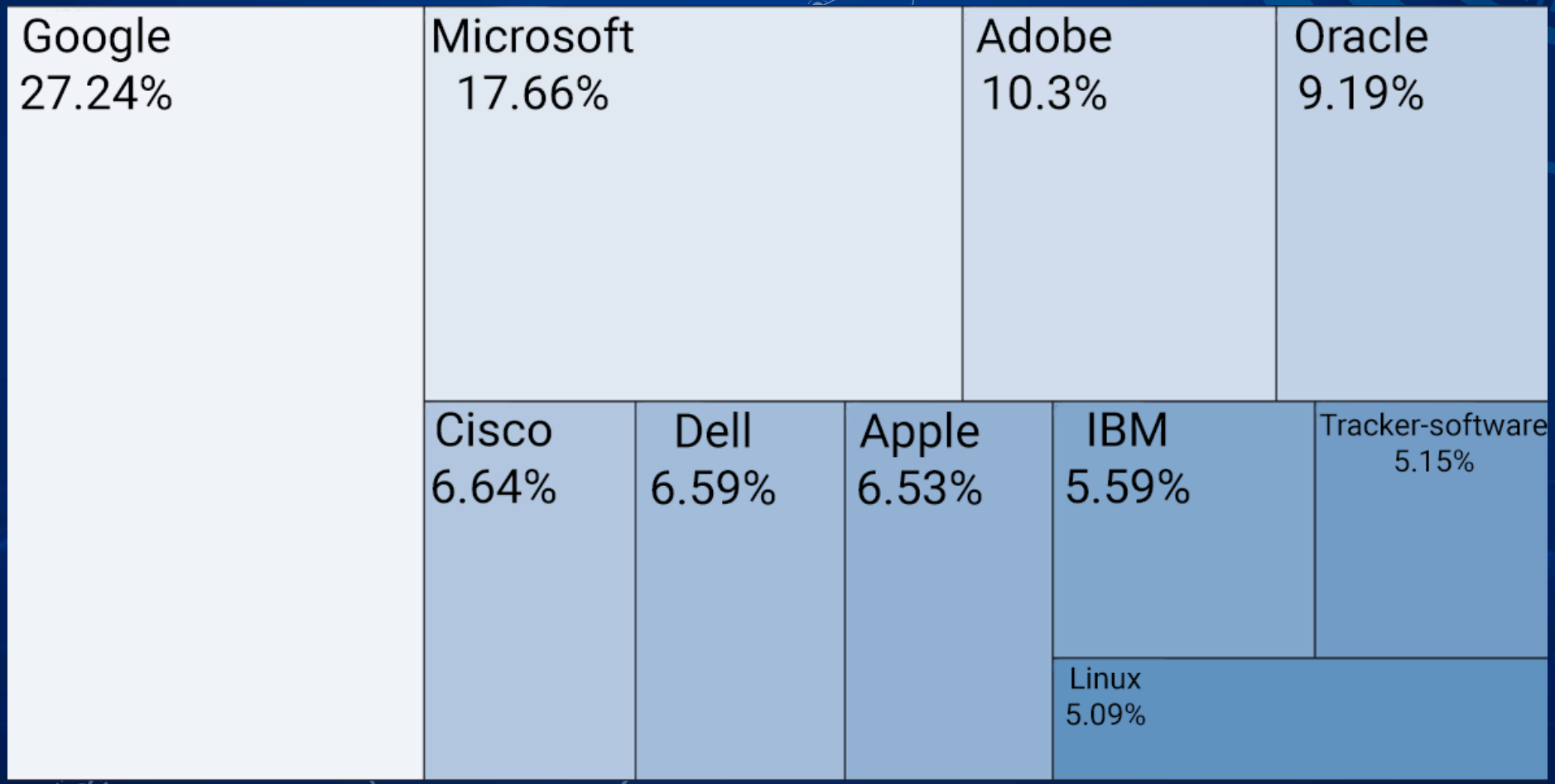
17. Número de vulnerabilidades por mes.

La distribución mensual de la cantidad de vulnerabilidades críticas publicadas revela un pico durante el mes de enero que supone un aumento de alrededor de un 25% con respecto al resto de meses.



18. Número de vulnerabilidades críticas por mes.

El top 10 de firmas afectadas por vulnerabilidades durante el periodo es el siguiente:



19. Porcentaje de vulnerabilidades por vendedor en T1.

Vulnerabilidades destacables

Microsoft Office/Outlook CVE-2023-23397

Un atacante que explote con éxito esta vulnerabilidad podría acceder al hash Net-NTLMv2 de un usuario que podría ser utilizado como base de un ataque NTLM Relay contra otro servicio para autenticarse como el usuario.

Microsoft Windows11/Windows Server2022 CVE-2023-23392

Un atacante no autenticado podría enviar un paquete especialmente diseñado a un servidor objetivo que utilice la pila de protocolos HTTP (http.sys) para procesar paquetes.

Fortinet-FortiOS CVE-2023-25610

Una vulnerabilidad de desbordamiento del búfer en la interfaz administrativa de FortiOS y FortiProxy puede permitir a un atacante remoto no autenticado ejecutar código arbitrario en el dispositivo y/o realizar una denegación de servicio en la interfaz gráfica de usuario, a través de solicitudes específicamente diseñadas.

GOOGLE-Android CVE-2023-20946

En onStart de BluetoothSwitchPreferenceController.java, existe un posible bypass de permisos debido a un adjunto. Esto podría conducir a una escalada remota de privilegios en la configuración de Bluetooth sin necesidad de privilegios de ejecución adicionales. La interacción del usuario no es necesaria para la explotación.

Apple - macOS Ventura 13.2.1/ iOS 16.3.1/iPadOS 16.3.1 CVE-2023-23529

La vulnerabilidad permite a un atacante remoto ejecutar código arbitrario en el sistema de destino. La vulnerabilidad existe debido a un error de confusión de tipo al analizar contenido web en WebKit. Un atacante remoto puede engañar a la víctima para que visite un sitio web especialmente diseñado, desencadenar un error de confusión de tipo y ejecutar código arbitrario en el sistema de destino. Tenga en cuenta, la vulnerabilidad está siendo explotada activamente en la naturaleza.

Conclusiones

La involucración del bloque occidental en favor de Ucrania en el conflicto ruso-ucraniano aumenta el riesgo de una escalada de tensiones y la posibilidad de una extensión del conflicto armado a nivel internacional. En este escenario de inestabilidad China se está posicionando como la figura mediadora entre ambos bloques, lo que podría tener un gran impacto en su poder de influencia a nivel internacional durante las próximas décadas.

Los datos recogidos por el Lab52 durante el primer trimestre del año 2023 revelan que los sectores estratégicos y críticos de países occidentales como gobiernos, administraciones públicas y defensa han sido atacados recurrentemente por actores de la amenaza avanzados. El análisis de los ataques, amenazas y víctimas parece indicar que existe una relación directa entre estos incidentes y el conflicto ruso-ucraniano. Destacan los grupos hacktivistas, que han sido los grupos más activos durante este primer trimestre.

En cuanto al malware utilizado en los incidentes registrados durante el primer trimestre, se ha observado un predominio del uso de las familias de malware RedLineStealer, Mirai y Agent Tesla. Por otro lado, parece ser que la infraestructura china es la más utilizada por los actores de la amenaza para llevar a cabo sus ciberataques.

El número de vulnerabilidades publicadas ha aumentado con respecto al trimestre anterior y se han registrado vulnerabilidades de alta criticidad en productos ampliamente utilizados de Google, Microsoft y Cisco, entre otros.

La información publicada en este informe ha sido generada a partir del análisis de los datos recolectados por el Lab52 de fuentes internas y externas como parte del servicio de ciber inteligencia proporcionado por S2 Grupo.

GRUPO

Anticipando un mundo
ciberseguro

MADRID
BARCELONA
VALENCIA CERT
VALENCIA HQ
SEVILLA
SAN SEBASTIÁN

SANTIAGO DE CHILE
C.D. MÉXICO
BOGOTÁ
BRUSELAS
LISBOA
RÓTERDAM

Síguenos en: • @s2grupo • s2grupo.es