S2 GRUPO

Informe de ciberinteligencia

TENDENCIAS 4T 2022

Lab52

Contenido

Resumen ejecutivo

Este informe es un resumen de la actividad más significativa detectada por el último trimestre del año por parte del Lab52.

El informe está dividido en cuatro grandes partes. En primer lugar, se presentan los principales eventos geopolíticos del trimestre, así como las tendencias a través de los indicadores obtenidos en nuestra base de datos de inteligencia.

A esto les sigue un repaso a las principales campañas de ciberespionaje llevadas a cabo por los principales actores junto a su respectivo contexto geopolítico, haciendo énfasis en las innovaciones tecnológicas implementadas.

También serán analizadas las principales campañas de cibercrimen, como la reaparición de Emotet o el malware Raspberry Robin.

Finalmente, se presentarán los datos de vulnerabilidades, así como el análisis de las que han tenido un mayor impacto en el periodo.

La inteligencia obtenida y analizada por parte del equipo de ciberinteligencia Lab52 durante el trimestre ha generado una serie de conclusiones y generado la respectiva inteligencia para los servicios de seguridad de S2 Grupo.

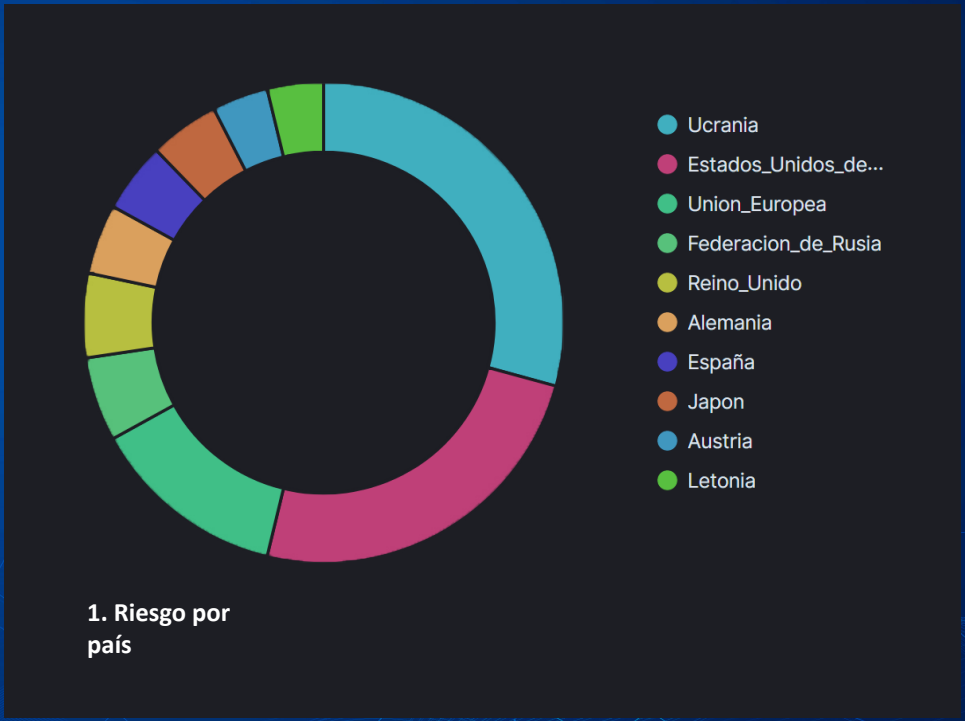
Tendencias del trimestre

Las tendencias en el último trimestre de 2022 han estado especialmente influenciadas por el conflicto rusoucraniano, lo que ha conducido a un incremento de hostilidades de los grupos pro-rusos, tanto en acciones de ciberguerra como de hacktivismo.

Otras situaciones también han supuesto un evento importante en las respectivas regiones:

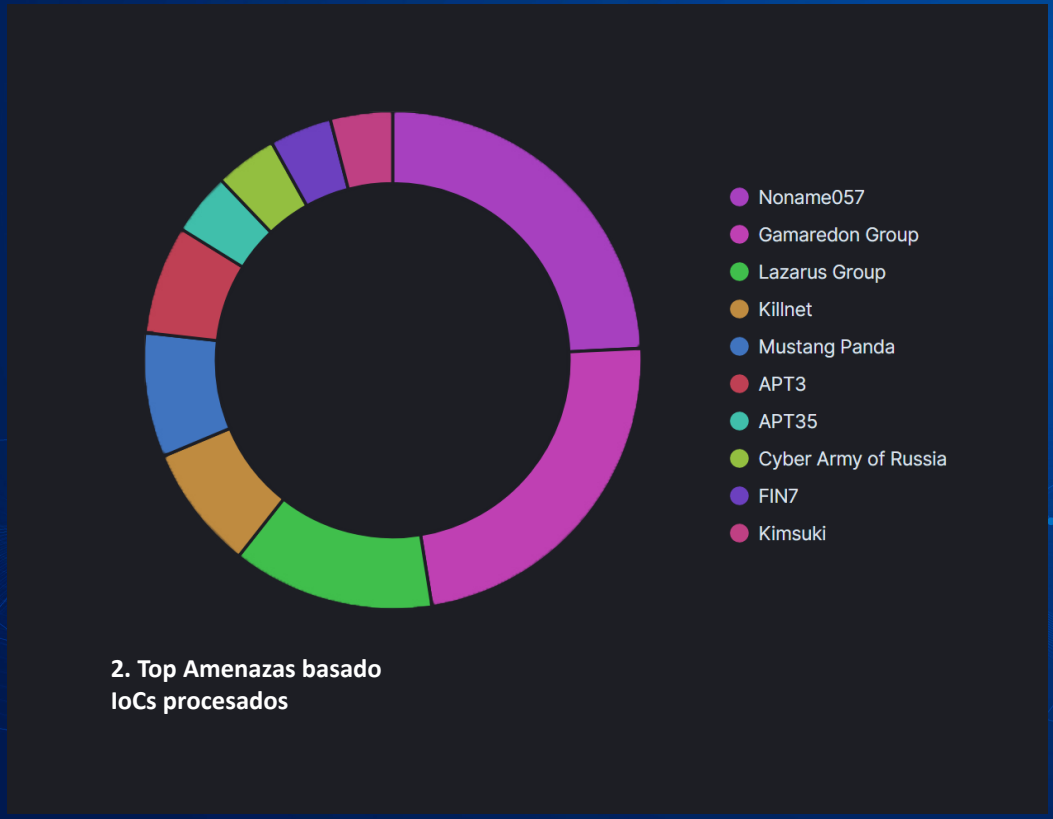
- Protestas de mujeres en Irán por las restricciones impuestas por el régimen
- Golpe de Estado en Burkina Faso
- Crisis energética entre Libia y Túnez
- Lanzamiento de misiles de Corea del Norte contra objetivos prooccidentales
- Incremento de tensión entre Serbia y Kosovo
- Elecciones generales en Brasil

A raíz de la información recolectada sobre la escena política, se han identificado en los eventos que Ucrania, seguido por Estados Unidos y la Unión Europea son los lugares con mayor riesgo geopolítico.



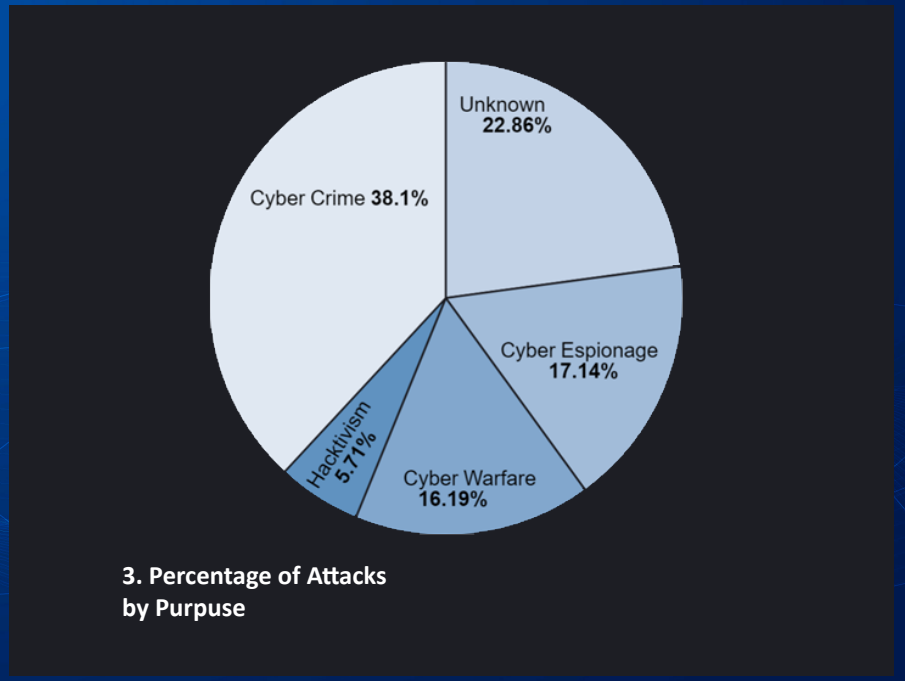
1. Riesgo por país

De todos los eventos procesados por el equipo de Lab52 se han generado más de mil Indicadores de Compromiso en la base de datos de inteligencia de S2 Grupo. Los siguientes grupos han sido identificados como los más activos del periodo:



2. Top Amenazas basado IoCs procesados

Aunque la principal motivación sigue siendo el cibercrimen, desde el inicio de la guerra entre Rusia y Ucrania, el porcentaje de campañas de ciberguerra y hacktivismo ha aumentado.
Los objetivos de las campañas durante el periodo se han distribuido del siguiente modo:



3. Percentage of Attacks by Purpuse

Análisis de infraestructuras

En lo que concierne a la propia infraestructura utilizada por actores, su localización se distribuye como lo siguiente:

4. Infraestrutura del 4T

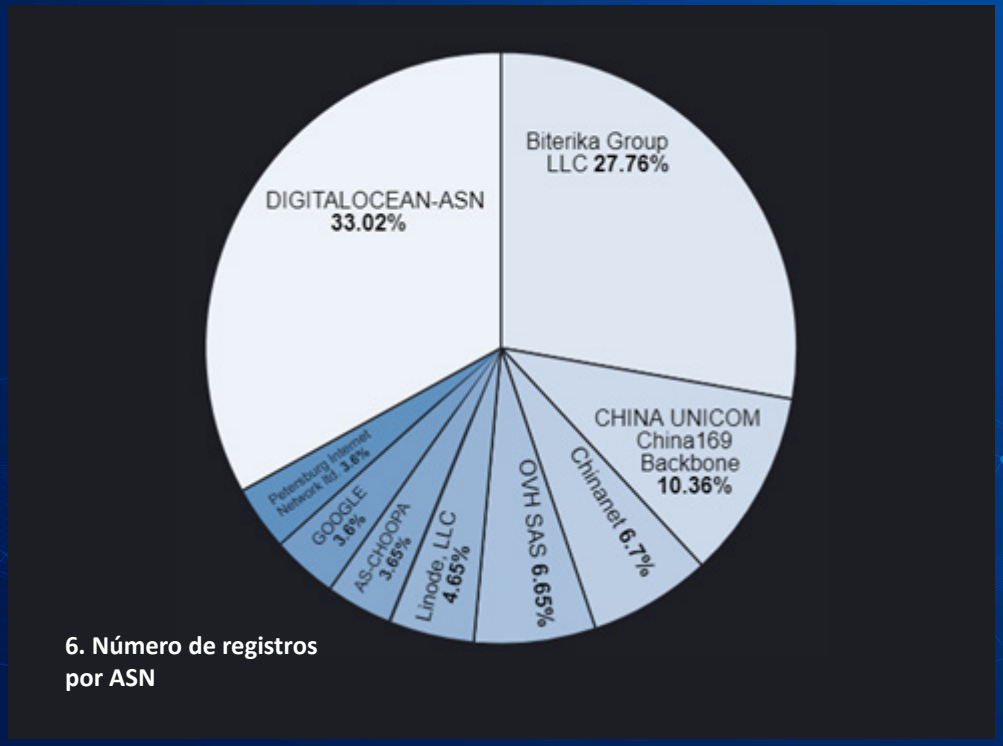
5. Infraestructura 1T-3T

Como se puede observar, apenas ha variado en lo que respecta al resto de año, exceptuando una nueva infraestructura registrada por APT36 (también conocido como Transparent Tribe), debido al uso del rango del proveedor DIGITALOCEAN ubicada en Canadá. Un número importante de registros puede observarse en la región de Toronto.

Sin embargo, DIGITALOCEAN-ASN ha sido el proveedor con mayor número de registros en nuestra base de datos de inteligencia. Esto se debe a que es un proveedor con una regulación muy laxa, lo que permite identificar que seguirá siendo utilizada por diferentes actores en el futuro.

El ASN Biterika Group LLC ha aparecido como el segundo ASN más usado en el periodo, un proveedor relativamente pequeño. Esto se debe a su utilización en campañas de denegación de servicio llevadas a cabo por actores hacktivistas prorrusos.

Biterika es un ASN ubicado en Rusia, lo que permite alinear al propio proveedor con intereses estatales.



6. Número de registros por ASN

Campañas asociadas a intereses estatales

Ciberguerra y hacktivismo

El pasado octubre el conflicto rusoucraniano llegó a un nuevo estado tras la proclamación de los referéndums y la anexión de las autoproclamadas repúblicas de Donetsk y Lugansk como parte de Rusia, así como la amenaza del uso de armamento nuclear contra enemigos.

Estos eventos han conducido a una alta movilización de grupos asociados a intereses rusos, tanto en campañas de ciberguerra como hacktivismo.

El grupo Sandworm, un grupo dedicado a acciones disruptivas ha estado activo durante el mes de noviembre, llevando a cabo ataques de ransomware, especialmente contra organizaciones de transporte y logística ubicadas en Ucrania y, en menor medida, Polonia.

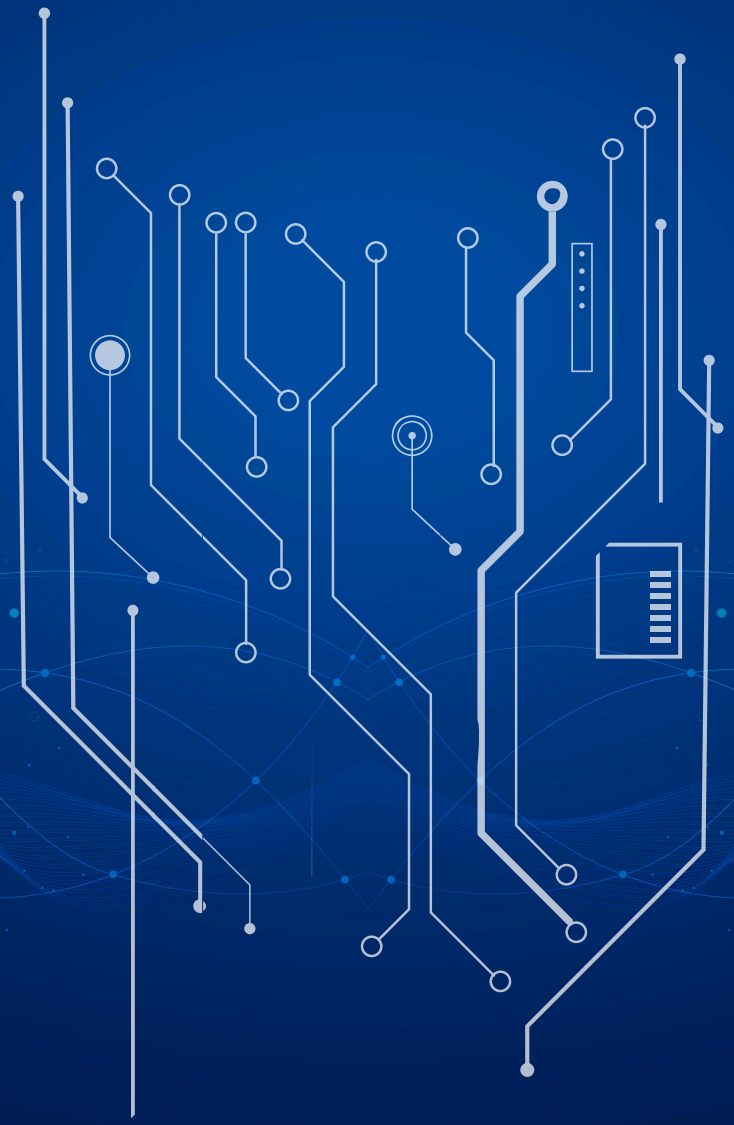
Además de ellos, los grupos NoName057 y Cyber Army of Russia han llevado a cabo acciones coercitivas, así como de denegación de servicio. Mientras que NoName057 tiene como objetivos entidades bálticas y polacas, Cyber Army of Russia está focalizada en entidades ucranianas. Todo parece apuntar que ambos grupos no están asociados al gobierno ruso.

Abuso de servicios web

A final de noviembre, se ha reportado una campaña asociada a APT29, el cual ha realizado acciones contra entidades italianas .

En esta campaña, APT29 ha mantenido varios procedimientos vistos anteriormente, como por ejemplo la utilización de Spear Phishing a través de pdf para el Acceso Inicial para, finalmente, utilizar un fichero ISO para la descargar de payloads maliciosos o el uso de claves de registro para la persistencia.

La mejora de los procedimientos de este grupo radica en la utilización de servicios legítimos para la exfiltración de información, como Dropbox, Trello o Slack.



Explotación de Windows Credential Roaming

A principios de noviembre, Mandiant publicó un report donde se comentaba un ataque contra instituciones diplomáticas europeas.

El ataque es especialmente relevante debido a la utilización de una vulnerabilidad de día cero para la escalada de privilegios vía Credential Roaming. La vulnerabilidad fue parcheada por Microsoft en septiembre (CVE-2022-30170) y permite a los atacantes tomar el control del atributo msPKIAccountCredentials de LDAP y, tras añadir un Roaming Token, escribir un número arbitrario de bytes en cualquier fichero del sistema.

UNC4166

También directamente asociada las hostilidades rusas contra Ucrania, Mandiant reportó una campaña que utilizaba el compromiso de la cadena de suministro como Acceso Inicial, infectando instaladores de Windows 10 mediante ficheros ISO que eran compartidos a través de plataformas de Torrent.

Como metodologías, es interesante destacar distinguir el uso de capacidades open source. Por ejemplo, STOWAWAY para la deshabilitación de las protecciones de sistemas Microsoft , o SPAREPART para el parseo de la tabla de firmware .

Además, el uso del script gathernetworkinfo.vbs, instalado por defecto en sistemas Windows permite la obtención de información de red del equipo donde se ejecuta.

Actividad contra Rusia: Cloud Atlas

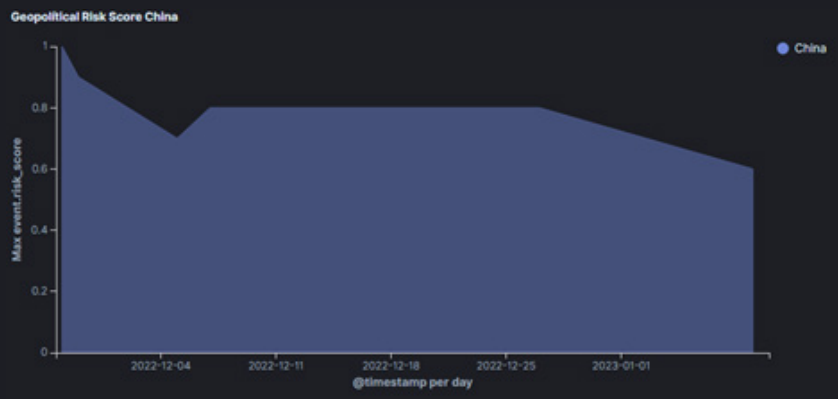
Rusia también ha sido objeto de acciones de ciberespionaje, como por ejemplo las que ha llevado a cabo Cloud Atlas contra Rusia, Bielorusia y Transnitria .

El grupo, activo desde 2014, lleva a cabo el Acceso Inicial a través de phishings dirigidos con documentos de Microsoft Office utilizando servicios de correo como Yandex, Mail.ru o Outlook.com.

Tras esto, la infección se inicia con el backdoor PowerShower, un implante utilizado en otras campañas de Cloud Atlas la cual dispone de capacidades de reconocimiento de proxy.

Contexto geopolítico de China

La actividad china del último trimestre ha estado marcada por el 20º Congreso Nacional del Partido Comunista de China, donde han sido definidas las líneas generales de su programa político para los próximos cinco años, lo que parece reafirmar la continuidad de Xi Jinping después de 2027. Tal y como se puede ver en el gráfico del riesgo en las relaciones internacionales de China, ha habido una caída de la actividad pública desde que el ejército chino expulsó un misil estadounidense que entró "ilegalmente" en aguas adyacentes a las Islas Spratly a finales de noviembre.



7. Evolución del riesgo de China

Mustang Panda: Ciberespionaje utilizando el conflicto ruso-ucraniano como cebo

Como resultado de varias publicaciones se ha determinado que hay una campaña muy importante de Mustang Panda, el cual ha sido uno de los grupos más activos del trimestre, utilizando la guerra en Ucrania.

Para el Acceso Inicial se está utilizando ficheros .rar cuyos nombres están vinculados a la temática del conflicto y que contienen un fichero .lnk, un fichero .dat, una dll y un fichero con una extensión aleatoria de tres letras, que es un binario legítimo y cuyo propósito es cargar el payload del fichero .dat.

El propósito de la campaña es desplegar el malware PlugX sin ser detectable por los sistemas de seguridad, del cual se han detectado nuevas variantes.

Lazarus con objetivos financieros

Otro grupo que ha tenido mucho impacto durante el trimestre ha sido Lazarus, asociado con intereses norcoreanos.

Es interesante destacar el incremento de ataques que han tenido un objetivo únicamente financiero, especialmente teniendo como objetivo compañías dedicadas a trading de criptomoneda. De este modo, BlueNoroff, unidad asociada a Lazarus está llevando a cabo ataques de spearphishing. Estos ataques han reutilizado procedimientos vistos anteriormente, como es el contacto directamente con las víctimas a través de LinkedIn, aunque también han incluido otras plataformas como WhatsApp, Discord o Twitter.

Un ejemplo es la utilización de ficheros Word para el Acceso Inicial. Dentro de ficheros .iso o .vhd se dropean binarios legítimos o scripts legítimos, como son mshta, rundll32 o SyncAppvPublishingServer.vbs, ejecutando técnicas de bypass MOTW.

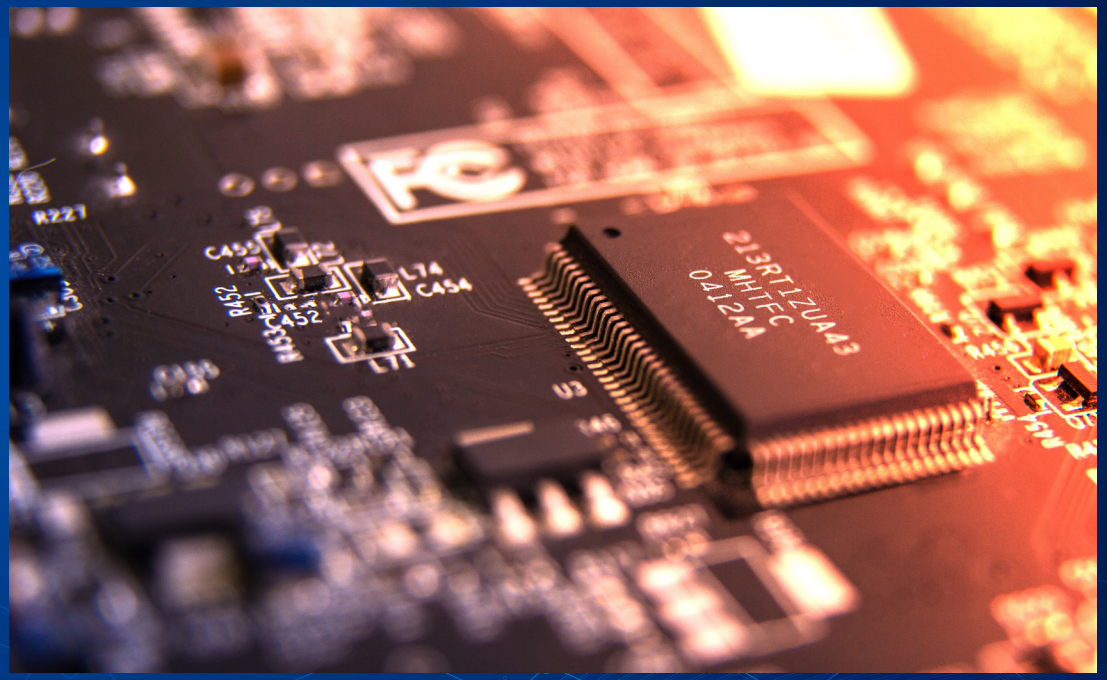
En la misma línea, también implementa funcionalidades para deshabilitar el EDR y antivirus, sobrescribiendo la sección .text de la librería ntdll precargada.

Con el mismo objetivo se han identificado ataques de suplantación de cadena de suministro, identificando aplicaciones de criptomoneda (en este caso QTBincoinTrader) que tienen instaladores MSI dentro del mismo, que despliega el malware AppleJeus.

Cibercrimen

Emotet

Uno de los principales eventos ha sido la reaparición de Emotet a principios de noviembre. Como remarcó la cuenta de Twitter @Cryptolaemus , después de cuatro meses de inactividad. A través del robo de la cadena de correo, distribuyen como adjuntos ficheros Excel que incluyen DLLs y ejecutan el binario de Windows regsvr32, con el objetivo de desplegar payloads adicionales.



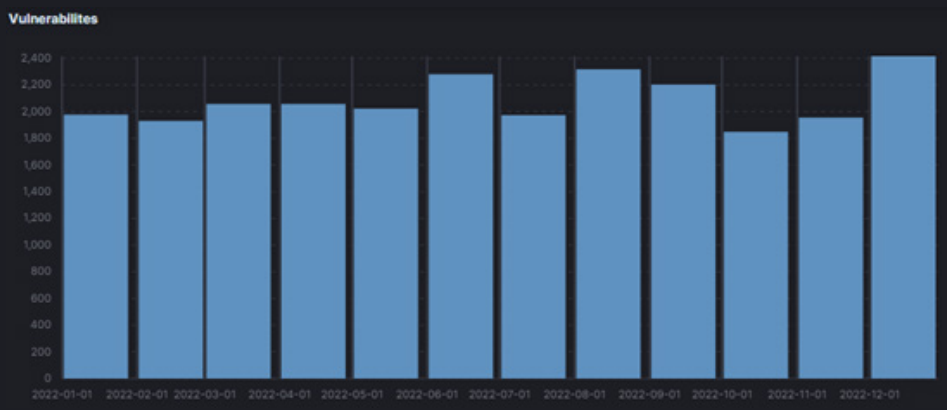
Raspberry Robin

En cuanto al número de incidentes, el más destacable ha sido el malware Raspberry Robin, el cual sigue siendo tendencia pues, como se ha publicado en numerosas ocasiones, ha sido detectado en múltiples organizaciones, lo que apunta a una finalidad financiera.

El malware es distribuido vía USB, que descarga un MSI vía MSIExec y wmic, lo que termina siendo el payload de Raspberry Robin que contacta a su servidor C2 vía clientes Tor.

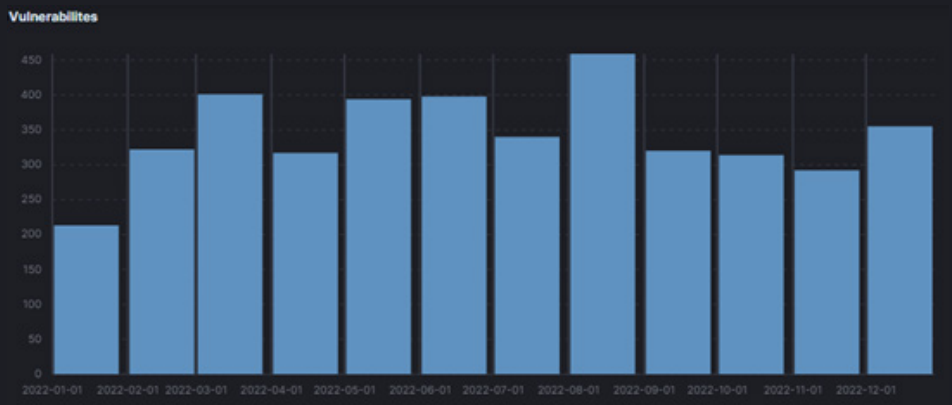
Vulnerabilidades

El número de vulnerabilidades durante el periodo ha aumentado, especialmente en el mes de diciembre, tal y como se puede ver en el gráfico inferior:



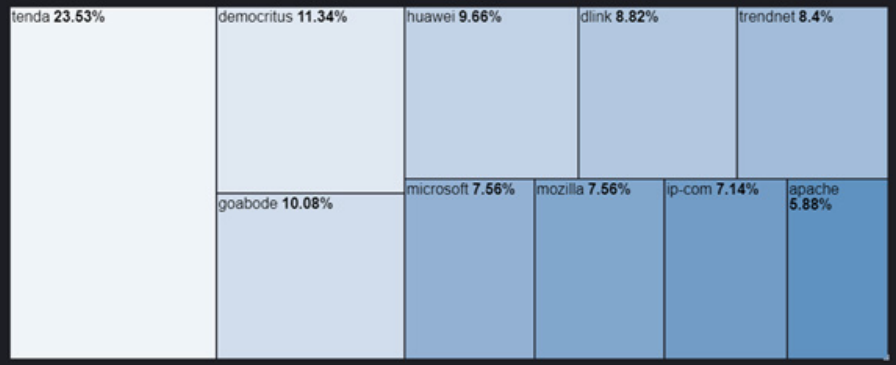
8. Número de vulnerabilidades por mes

Sin embargo, considerando únicamente las vulnerabilidades críticas, ha habido una disminución comparada con el resto del año.



9. Número de vulnerabilidades críticas por mes

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



10. Porcentaje de vulnerabilidades críticas por firma en 4T

Vulnerabilidad crítica en Citrix

El CVE-2022-27513 afecta a Citrix ADC y Citrix Gateway SSL VPN, el cual permite el control del escritorio remoto a través de phishing. Esta vulnerabilidad sólo es explotable si el dispositivo está configurado como VPN con la funcionalidad de RDP proxy activada.

RCE crítico en FortiOS “in the wild”

Fortinet advirtió de una vulnerabilidad basada en el overflow del búfer basado en heap que permite a un atacante no autenticado en ejecutar comandos en FortiOS SSL-VPN. Esta vulnerabilidad estaba siendo explotada activamente previamente a la notificación.

0-day explotado por APT37

El CVE-2022-41128 es una vulnerabilidad derivada de un error en el motor de scripting del lenguaje JScript9, explotado por APT37, según Microsoft . La explotación requiere que una versión no actualizada de Windows visite una página web o un servidor compartido, probablemente a través de una descarga o un enlace derivado de un phishing. En ese punto, un atacante puede ejecutar código. Debido al escenario, es probable que sea utilizado en exploit kits.

Conclusiones

Como se ha observado, la guerra entre Rusia y Ucrania continúa siendo el tema principal, tanto de los grupos implicados en el conflicto como de los grupos no implicados directamente, a través de la utilización de la temática para el acceso inicial del compromiso. Del mismo modo, actores como Cloud Atlas también están poniendo el objetivo en Rusia.

Se espera que, tras el Congreso Nacional del Partido Comunista chino, China vuelva tomar un papel activo en las relaciones internacionales, como también un nuevo empuje en la actividad de las cibercampañas. En el pasado grupos asociados a China han utilizado vulnerabilidades de servicios web expuestos para comprometer organizaciones. En esta línea, la publicación de las vulnerabilidades de Citrix y FortOS pueden ser vectores de entrada para estos grupos en los próximos meses.

A nivel de cibercrimen, se esperan nuevas oleadas de campañas de Emotet, lo que puede conducir a un incremento de incidentes de ransomware.

La información publicada en este informe ha sido generada de los datos recolectados, tanto a nivel público como privado por Lab52, como parte del servicio de ciberinteligencia proporcionado por S2 Grupo.

S2 GRUPO

Anticipando un mundo **ciberseguro**

MADRID
Avda de Manoteras 46
BIS 6ºC
28050 Madrid
T (34) 902 882 992

BARCELONA
Llull, 321
08019 Barcelona
T (34) 933 030 060

VALENCIA CERT
Ramiro de Maeztu, 7
46022 Valencia
T (34) 963 110 300
F (34) 963 106 086

VALENCIA HQ
Dr Joan Reglà, 6 bajo
46010 Valencia
T (34) 963 110 300
F (34) 963 106 086

SEVILLA
Calle Gonzalo Jiménez
de Quesada 2, Planta 18
Edificio Torre Sevilla
41092 Sevilla
T (34) 902 882 992

SAN SEBASTIÁN
C/ Juan Fermín Gilisagasti
nº 2 (Zuatzu)
Edificio Pi@ - Oficina 121
20018 Donostia
T (34) 902 882 992

SANTIAGO DE CHILE
Calle de Padre Mariano
Nº 82 of. 1102
Comuna de Providencia
T +56 9 9440 4365

C.D. MÉXICO
Monte Athos 420
CDMX 11000
T (+52) 55 5035 7868

BOGOTÁ
Carrera 14, nº 98-51,
Oficina 701
T (57) 601 745 74 3

BRUSELAS
Rue Beillard, 20
1040 Bruselas
T (32) (0) 474 532 974

LISBOA
Av. do Brasil, 1
1749-008 Lisboa
T (351) 21 7923729

ROTTERDAM
Stationsplein 45, 4th floor
3013 AK Rotterdam
The Netherlands
T (34) 963 110 300

Síguenos en: • @s2grupo • s2grupo.es