S2 GRUPO

Cyber threat intelligence report

TRENDS Q4 2022

Lab52

Contents

Summary

This report is a summary of the most significant activities detected during the fourth quarter of 2022 by Lab52.

The report is divided into four main sections. First, we will present the major geopolitical events of the quarter, as well as the trend indicators obtained from our intelligence database.

This will be followed by a review of the cyberespionage campaigns carried out by the main actors within their respective geopolitical context, with special emphasis on the technological innovations implemented.

The main cybercrime campaigns, such as the reappearance of Emotet or the Rasperry Robin malware, will also be analysed.

Finally, vulnerability data for the period will be presented, as well as an analysis of the vulnerabilities with the greatest impact published during the period.

The intelligence gathering and analysis carried out by the Lab52 cyberintelligence team has led to a series of conclusions and generated intelligence for S2 Grupo's security services.

Quaterly Trends

Trends in the last quarter of 2022 may be particularly influenced by the Russian-Ukrainian conflict, which has led to an increase in hostilities from pro-Russian groups, both in terms of cyber-warfare and hacktivism.

Other situations have also been a major event in their respective regions:

- Women's demonstrations in Iran in protest at restrictions imposed by the Iranian regime

- Coup d'état in Burkina Faso

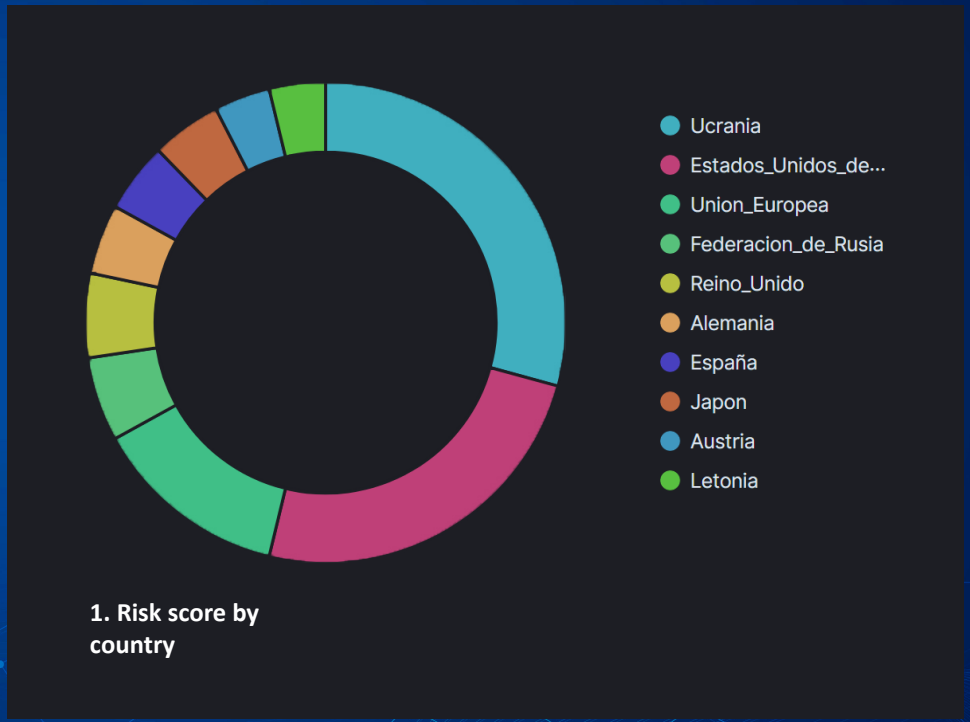
- Energy crisis between Libya and Tunisia

- North Korean missile launches against pro-Western targets

- Increased tension between Serbia and Kosovo

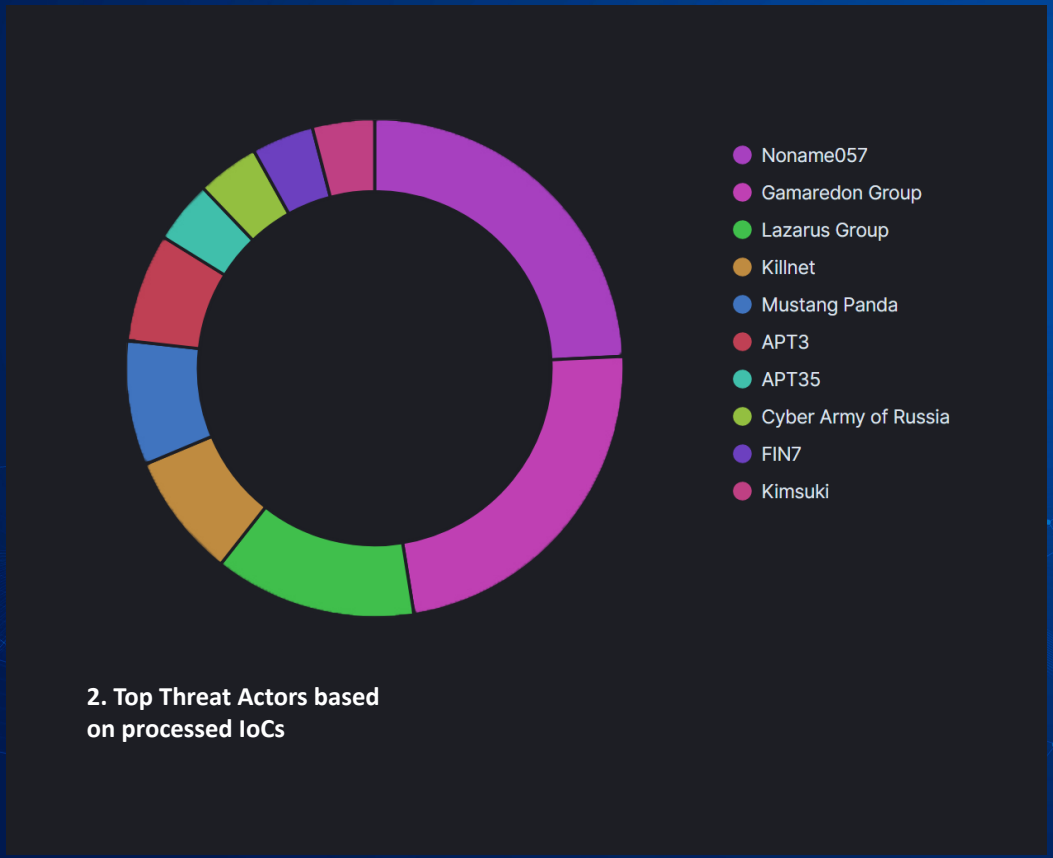
- General elections in Brazil

Among the data on the international political scene, we find that the geopolitical events that happened in last quarter have identified Ukraine, followed by the United States and the European Union, as places with most geopolitical risk.



1. Risk score by country

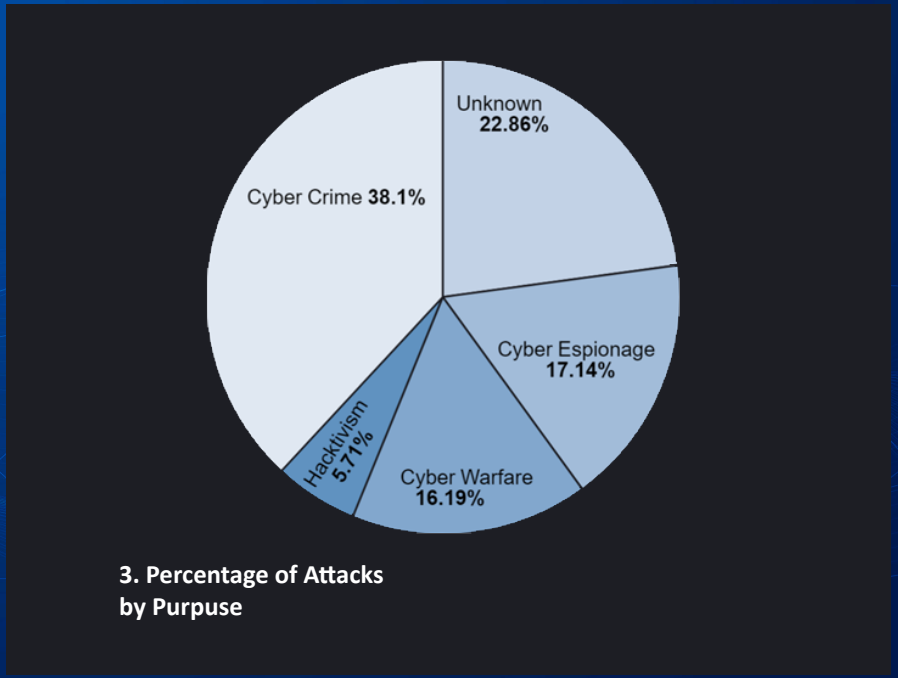
From all the intelligence processed by Lab52's team, thousands of IoCs have been stored in S2 Grupo intelligence database. The following groups have been identified as the top 10 most active during the period:



2. Top Threat Actors based on processed IoCs

Four of top ten groups have Russian links or origins, although there has also been considerable activity associated with both Mustang Panda and Lazarus. Interestingly, the latter has carried out a much higher number of cybercrime campaigns than usual.

Although the general motivation is cybercrime, there remains, as since the beginning of the Russian-Ukrainian conflict, a significant percentage in both cyber warfare and hacktivist campaigns. The purposes of the campaigns durign the period can be distributed as follows:



3. Percentage of Attacks by Purpuse

Infrastructure analysis

As far as the infrastructure itself is concerned the location of the infrastructure used by the actors has been distributed as follows:

4. Threat Actor infrastructure 4Q

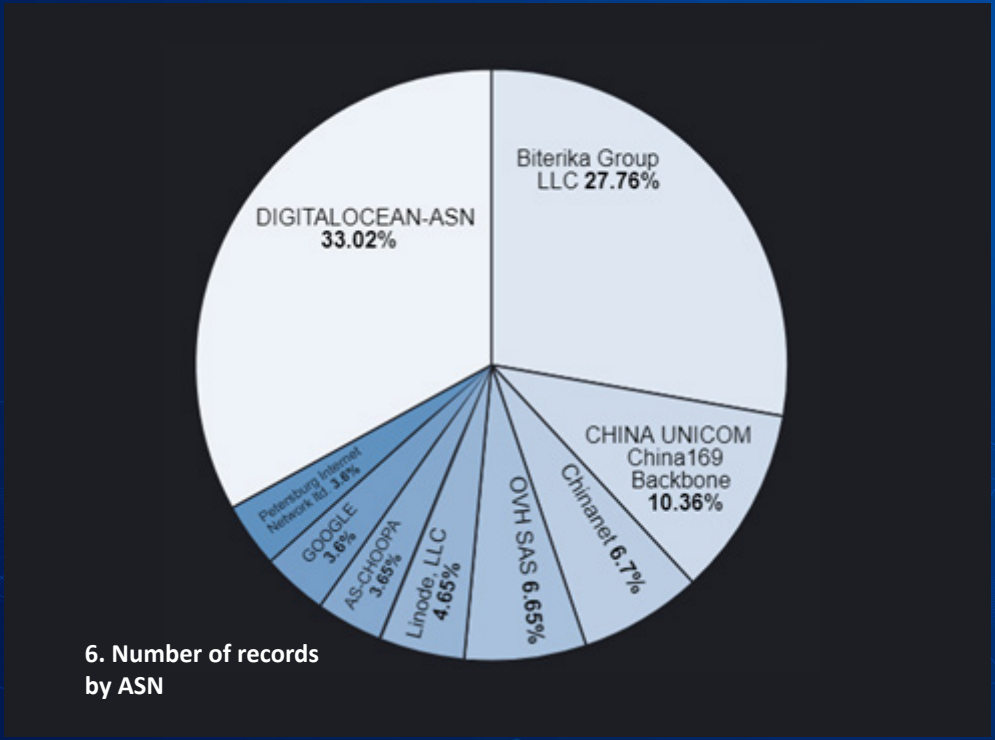
As can be seen, it has hardly varied from the general trend during the rest of the year, , except for new infrastructure registered by APT36 (also known as Transparent Tribe), due to the use of the Canadian range of the DIGITALOCEAN provider. A significant number of records can be observed in Toronto region.

5. Threat Actor infrastructure 1Q-3Q

However, this is only due to the use of this range, as DIGITALOCEAN-ASN has been the supplier with the most records in our intelligence database. The identification of DIGITALOCEAN as the most widely used ASN identifies it as a very loosely regulated provider, which suggest that it will continue to be used by different actors in the future.

While it is true that Biterika Group LLC has emerged as the second most used ASN, a relatively little known provider, it has been associated with denial-of-service campaigns carried out by pro-Russian hacktivist actors.

Biterka is an ASN hosted in Russia, which makes it possible to identify how this provider is aligned with state interests.



6. Number of records by ASN

Cybercampaings during the period

Cyber Warfare and Hacktivism

In October the Russian-Ukrainian conflict reached a higher stage after the proclamation of the referendums and annexation of the self-styled republics of Donetsk and Lugansk as Russian, as well as the threat of the use of nuclear weapons on enemies.

These events have led to a particularly strong mobilization of cyber-groups associated with Russian origin, both in cyberwarfare and hacktivist campaigns.

The Sandworm group, a leading group in disruptive actions, has been active during the month of November, carrying out different ransomware attacks, especially against transport and logistics companies in Ukraine, although, to a lesser extent, Poland has also been targeted.

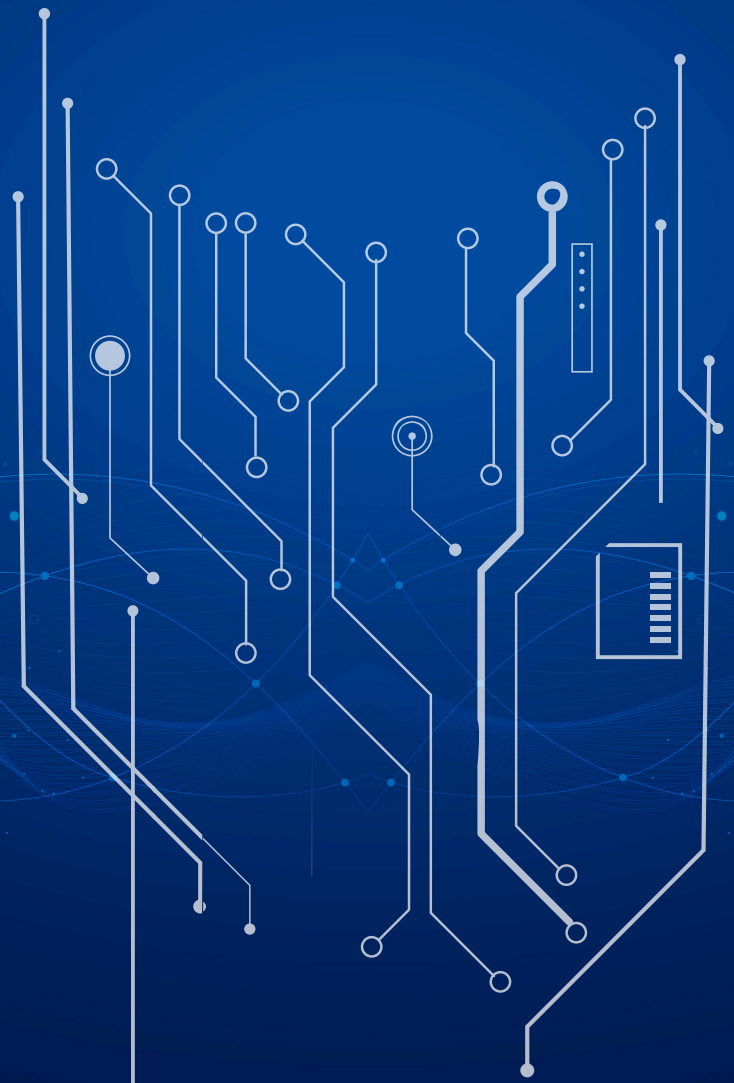
Among them, the most active, especially in coercive actions, have been the NoName057 group and Cyber Army of Russia, both of which are carrying out denial-of-service attacks. While NoName057 is targeting entities in the Baltics and Poland, Cyber Army of Russia is targeting Ukrainian entities. Presumably, both groups are non-governmental.

Web Service abuse

At the end of November, a campaign associated with APT29 was reported against Italian entities .

In this campaign, APT29 maintained many of the procedures seen previously, such as, for example, the use of Spearphishing through pdf documents as Initial Access vector to finally use of ISO file to download malicious payloads or the use of HKCU\Software\Microsoft\Windows\CurrentVersion\Run registry keys for persistence.

The improvement in the group's procedures is the use of legitimate web services for the exfiltration of information, such as Dropbox, Trello or Slack.



Windows Credential Roaming Exploitation

In early November, Mandiant published a report on an attack that took place earlier this year on European diplomatic institutions.

The attack was particularly relevant due to the use of a zero-day vulnerability for privilege escalation via Credential Roaming. This vulnerability was patched by Microsoft in September (CVE-2022-30170) and allowed attackers who had control over the LDAP attribute msPKIAccountCredentials, after adding a Roaming Token, to write an arbitrary number of bytes to any file on the system.

UNC4166

Also directly linked to the Russian hostilities against Ukraine, Mandiant reported a campaign using supply chain compromise as the Initial Access path, infecting Windows 10 installation ISOs that were shared via torrent sharing platforms.

As methodologies, it is interesting to distinguish the use of public capabilities. For example, for the disabling of the Microsoft protection systems, backdoors like STOWAWAY and parsing capabilities of the firmware table implemented in SPAREPART.

Also, the use of the script gathernetworkinfo.vbs, installed by default on Windows systems, which allows obtaining network information from the computer.

Activity against Russia: Cloud Atlas

Russia has also been the target of cyber espionage actions, as the Cloud Atlas group has carried out actions against Russia, Belarus and Transnistria.

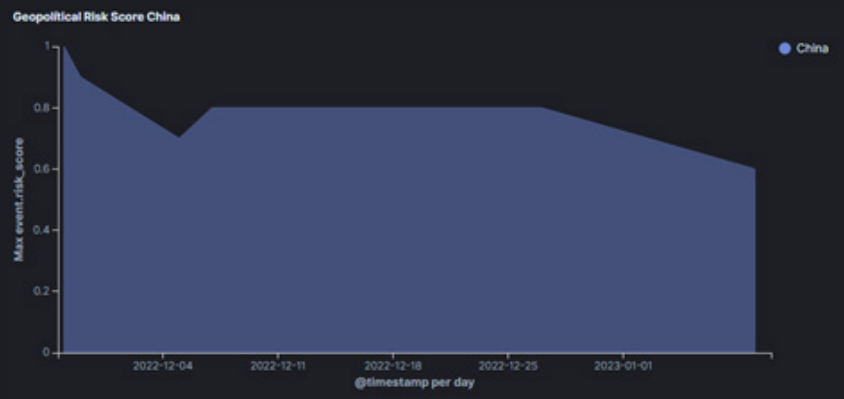
The group, which has been active since 2014, carries out the infection through targeted phishing campaigns via Microsoft Office documents and using mail services such as Yandex, Mail.ru or Outlook.com.

Through this, it initiates the infection with the PowerShower backdoor, an implant used in other Cloud Atlas campaigns and which has proxy recognition capabilities.

China geopolitical context

The last quarter in Chinese activity has been marked by the 20th National Congress of the Communist Party of China, where the general lines of its political programme for the next five years were defined, which seems to reaffirm Xi Jinping's continuity beyond 2027. As can be seen in the graph of risk in China's international relations, there has been a drop of public activity since the Chinese Army expelled a U.S. missile cruiser that "illegally intruded" into waters adjacent to the Spratly Islands at the end of November.

Despite this, cyber-espionage campaigns have not diminished in intensity.



7. Evolution of China's risk score

Mustang Panda: Cyberespionage using the Russian-Ukrainian conflict as a hook

As a result of several publications, it has been determined that there is a major campaign by Mustang Panda, which has been one of the most active groups in the quarter, using the interest in the conflict between Russia and Ukraine.

For Initial Access, it is using .rar files whose name is linked to the theme of the conflict and which contain an .lnk file, a .dat file, a .dll and a file with a random three-letter extension, which is actually a legitimate binary, whose purpose is to load the .dat containing a malicious shellcode.

The purpose of the campaign is to deploy PlugX malware unnoticed by security systems, of which new variants have also been detected.

Lazarus conducting financial motivated campaigns

Another group that has had a lot of impact during the quarter has been Lazarus Group, associated with North Korean interests.

It is interesting to note an increase in the trend of attacks whose target is purely financial, especially targeting companies associated with cryptocurrency trading. Thus, BlueNoroff, a unit associated with Lazarus is carrying out Spearphishing attacks. These attacks have reused the procedures seen previously, such as contacting the victim directly through LinkedIn, although in this case they have also used platforms such as WhatsApp, Discord or Twitter.

One of the attacks had Word files as initial access. Inside .iso or .vhd files, dropping binaries or legitimate scripts such as mshta, rundll32 and SyncAppvPublishingServer.vbs are carrying out MOTW bypass techniques.

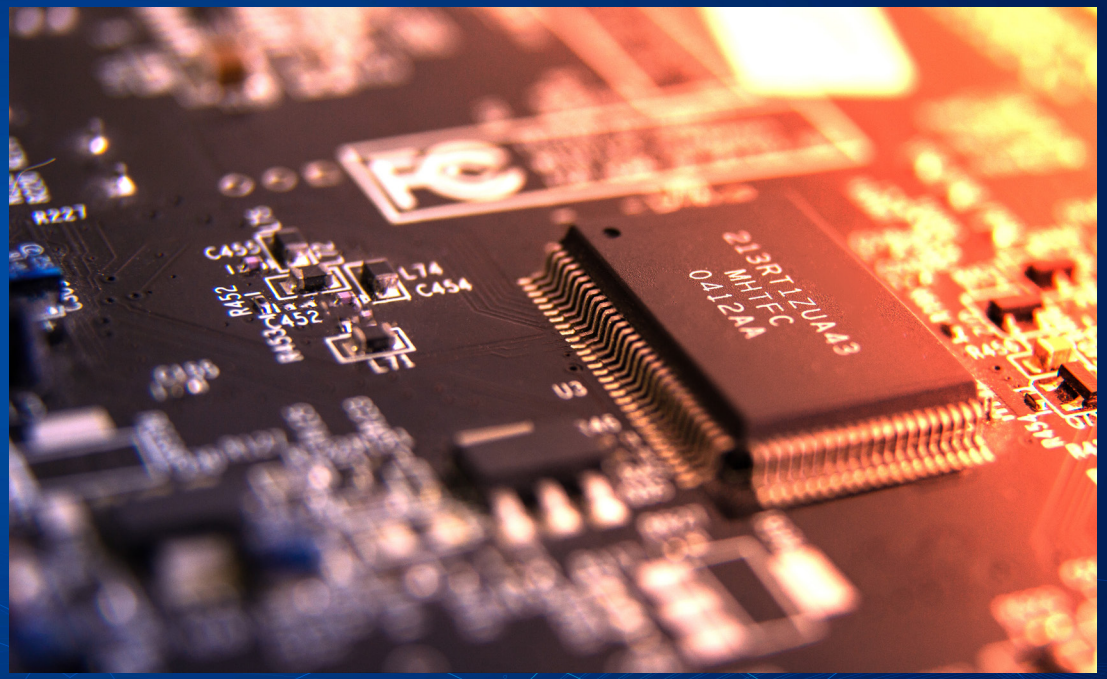
In the same vein, it also implements the functionality to disable EDR and Antivirus capabilities by overwriting the .text section of the preloaded ntdll library .

Also for the same purpose, supply chain spoofing attacks, identifying cryptocurrency applications (in this case QTBitcointTrader) that have MSI installers bundled with them, which deploy AppleJeus malware.

Cybercrime

Emotet

One of the main events of the period was the reappearance of Emotet in early November. As highlighted by the Twitter account @Cryptolaemus , after four months of inactivity. By stealing chain mail, they distribute Excel attachments that include DLLs and execute the Windows regsvr32 binary, with the aim of deploying additional payloads.



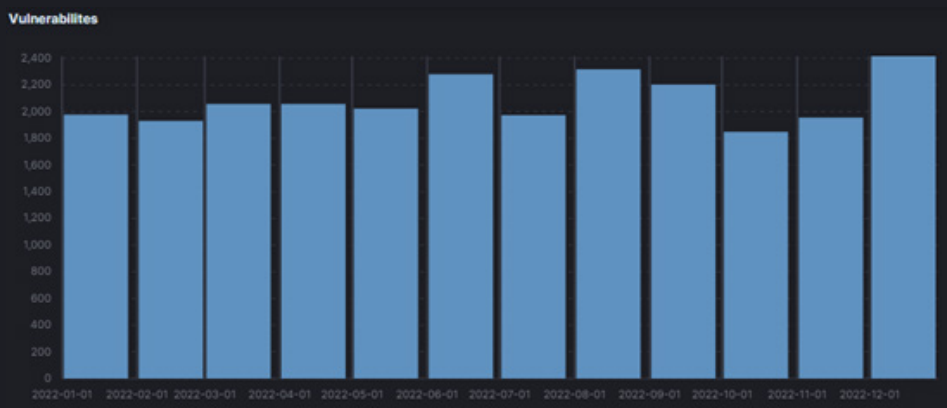
Raspberry Robin

One of the main threats in the period has been Raspberry Robin malware, which continues to be a trend, malware that, as has been discussed on numerous occasions, has been widely detected in organizations of all kinds which point to a financially motivation.

Malware distributed via USB, it downloads an MSI via MSIExec and wmic, which turns out to be the Raspberry Robin payload that contacts its C2 server via Tor clients.

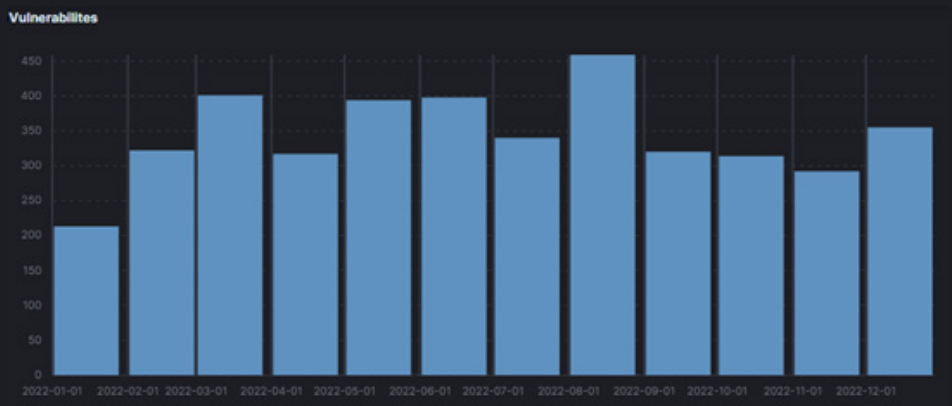
Vulnerabilities

The number of vulnerabilities during the period has increased, especially due to releases in the month of December, as can be seen in the graph below:



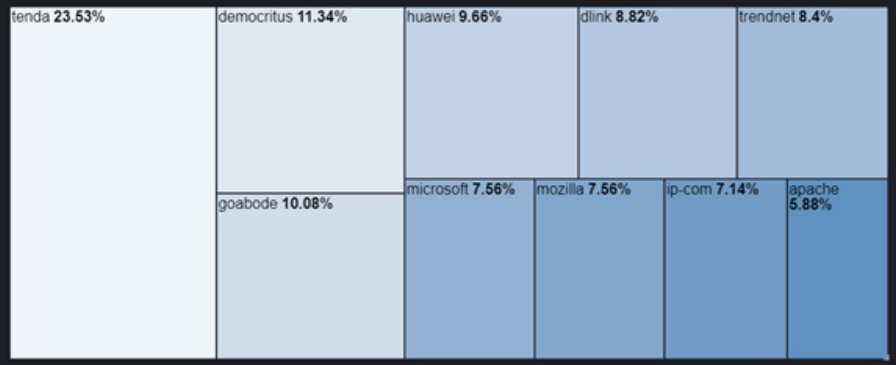
8. Number of vulnerabilities by month

However, considering the critical vulnerabilities, this is a decrease compared to the rest of the year.



9. Number of critical vulnerabilities

The top 10 vendors affected by critical vulnerabilities during the period were as follows:



10. Percentage of critical vulnerabilities by vendor in 4Q

Critical vulnerability in Citrix

CVE-2022-27513 affects the Citrix ADC and Citrix Gateway SSL VPN service that allows remote desktop takeover througth phishing. This vulnerability is only exploitable if the device is configured as a VPN with RDP proxy functionality enabled.

Critical RCE in FortiOS exploited in the wild

Fortinet warned a heap-based buffer overflow vulnerability that allow to an unauthenticated attacker to execute commands or arbitrary code in FortiOS SSL-VPN. This exploit was exploited in the wild.

0-day exploited by APT37

CVE-2022-41128 is a vulnerability derived from a bug in the JScript9 scripting language engine, exploited by the North Korean APT group37 according to Microsoft . Exploitation requires an unpatched version of Windows to visit a shared server or a specially crafted website, probably via a phishing link or download. At that point, the attacker can execute arbitrary code on the affected system at the user's privilege level. Microsoft did not provide any information on the scope of this scenario, but considering that it is a browse-and-own scenario, it is expected to be usable in exploit kits.

Conclusions

As we have seen, the war between Russia and Ukraine continues to be the theme, both as the main motivation for groups with interests in the different sides, but also as a theme for initial access by groups not a priori involved in the conflict. However, hostilities carried out by groups associated with Russia are causing groups such as Cloud Atlas to act on Russian targets.

It is expected that, after 20th National Congress of the Communist Party of China, China will once again take a leading role in international relations, and of course, a new push in its cyber-campaigning activity. In the past, groups associated with China have used vulnerabilities in exposed web services to compromise organizations. The publication of vulnerabilities in Citrix and FortiOS may be entry vectors for these groups in the coming months.

At the cybercrime level, new waves of Emotet campaigns are expected, which could lead to an increase in ransomware incidents.

The information published in this report has been generated from intelligence generated from both private and public sources by the Lab52 team as part of the cyber intelligence service provided by S2 Grupo.

S2 GRUPO

Anticipating a **cyber secure** world

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

Follow us in: • @s2grupo • s2grupo.es