S2 GRUPO

Cyber Threat Intelligence Report

1Q 2023 TRENDS

Lab52

Contents

S2 GRUPO

Lab52

Executive summary

As a result of the collection and analysis of information obtained from internal and external sources throughout the first quarter of 2023, S2 Grupo's cyber intelligence team, Lab52, has generated intelligence for S2 Grupo's security services.

The present document presents the activity recorded by S2 Grupo's cyber intelligence division, Lab52. This report reviews the most noteworthy events of the first quarter of 2023 and, through an analysis, presents conclusions. The content is structured in four main parts:

- Main geopolitical events of the quarter and study of trends extracted from the indicators of the Lab52 intelligence database.
- Review of the main cyber espionage campaigns conducted by the most active threat actors, together with their respective geopolitical context and with an emphasis on the technological innovations implemented.
- Cybercrime analysis. Ransomware, malware, and Deep web.
- Graphical representation of data and statistics on vulnerabilities disclosed in the first quarter of 2023, as well as analysis of those that have had the greatest impact.

Quarterly trends

Geopolitical context

The situation in international relations has been defined by the continuation of the conflict between Russia and Ukraine. Throughout the quarter, many NATO countries have provided much more significant support to Ukraine, especially in the form of arms shipments.

The Western bloc has been supplying military aid since the beginning of the conflict. However, tanks and fighter jets have the potential to give Ukraine a military advantage and have a considerable impact on the progress of the conflict. This poses an increased risk of the war spilling over into an international conflict. The main concern in this scenario is the possible use of nuclear weapons and the catastrophic consequences that follow. The old continent is investing all its efforts in fighting Russia: France has sent more than a third of its howitzers, Denmark has practically run out of artillery, Spain has a third of its Leopards unused, and Germany only has enough ammunition for a few hours, maximum days, in the event of a battle.

In this context, the presidents of several European countries and the president of the European Commission visited their Chinese counterpart in Beijing. Von der Leyen called on China not to supply arms to Russia “directly or indirectly” and pointed out that the Asian giant’s position on the war is “crucial” for the European Union. Jinping pledged to “facilitate peace talks and a political solution to the crisis in Ukraine”.

Chinese Defence Minister Li Shangfu visited Russia for the first time. In his meeting with Vladimir Putin, Shangfu assured that “military cooperation between China and Russia is developing very well. This makes a great contribution to maintaining global and regional security. In the economic sphere, relations between the two countries are also good. Last year, Russia increased its gas imports to China via the Siberian Power pipeline by 50 per cent. This amount could grow after the commissioning of Siberian Power 2, which will be built through Mongolia.

Meanwhile, Xi Jinping and Volodymir Zelenskyy held a telephone conversation on 26 April. The Chinese president will send a delegation of diplomats to Ukraine to negotiate peace. Zelenskyy announced the appointment of a new Ukrainian ambassador to China.

In this way, China appears to be positioning itself as the mediator between the pro-Ukrainian and pro-Russian blocs in this armed conflict.

However, it seems that Xi Jinping's government is not limiting its role as mediator to the conflict in Ukraine. Iran and Saudi Arabia have re-established relations, which they severed in 2016, and embassies in their respective countries are expected to resume normal operations in the short term. The agreement follows a meeting of their leaders in China and two years of negotiations in Oman.

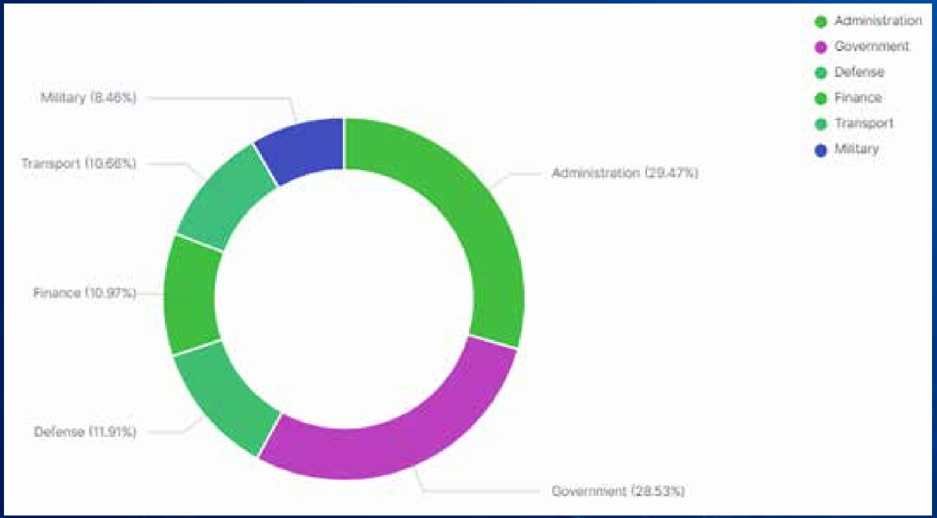
In addition, Sweden has discovered the largest deposit of rare earths in Europe with chemical elements essential for the construction of batteries for electric vehicles or military technology. These elements are part of the trade war between the world's major powers. China is currently the world's largest producer and exporter of rare earths. The discovery of this deposit could threaten China's dominance of the international market.

Analysis of the quarter's incidents

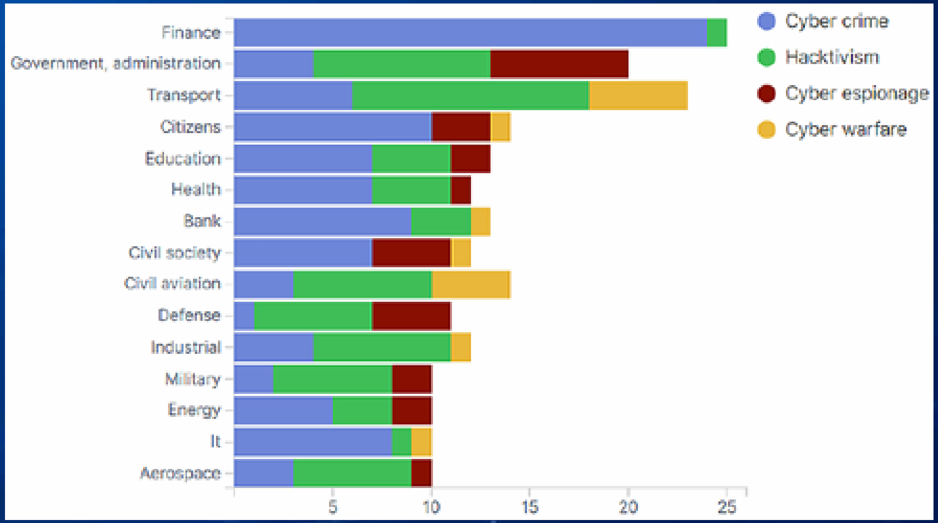
By recording security incidents from internal and external sources, Lab52 can analyse the evolution of security incidents and identify cyber threat trends for the first quarter of 2023.

The graphical representation of the percentage of recorded incidents by sector reveals that both public administration and government agencies have been the main target of attackers during this period. This was followed by the military and defence sector, which accounted for almost 20% of recorded incidents. Lastly, the finance and transport sector.

The following graph shows the distribution of attack typology according to sector. Thus, an analysis shows that strategic sectors, such as government and administration, transport, defence, and military, are targets of cyber espionage and hacktivism. While other sectors with a greater presence of the private sector are more susceptible to cybercrime incidents because the purpose of the attack is purely monetary, such as the financial sector, which accounts for more than 90% of cases.



1. Topmost attacked sectors in Q1 2023.



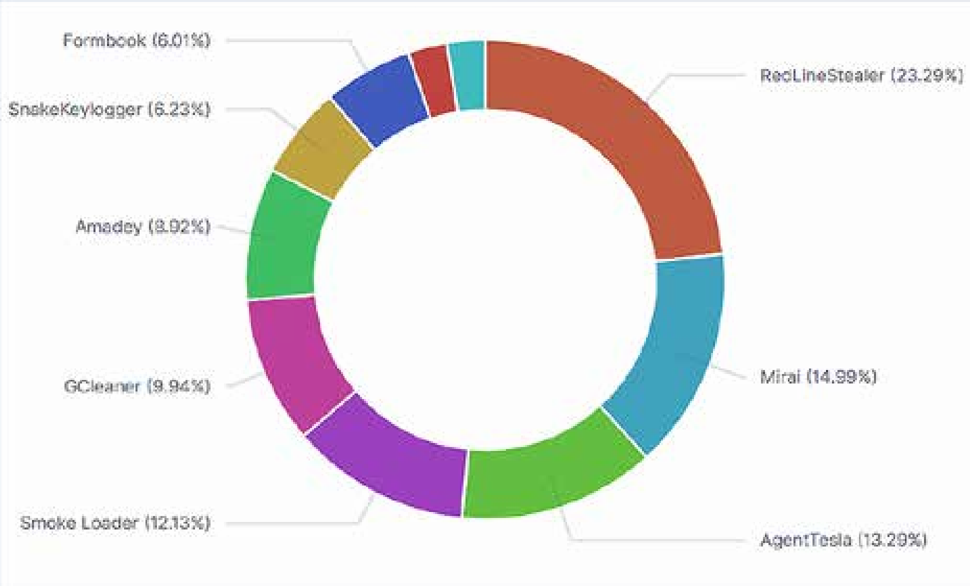
2. Attack motivation by sector.

Malware trends

Lab52 also conducts a sample collection exercise from internal and external sources. Therefore, it is possible to identify which malware families have been the most used during the quarter. Compared to the data obtained in the previous quarter, an increase was seen especially in the presence of RedLineStealer and Mirai.

RedLineStealer remains the most prevalent malware family in the quarter. Although the total number of registered samples has decreased compared to the previous quarter, the percentage has remained similar.

On the other hand, there has been a notable increase in the number of registered samples of Mirai, which has positioned itself as the second most seen malware family during the quarter. This phenomenon is probably due to the proliferation of the activities of hacktivist denial-of-service groups and the need to increase the number of active botnets.

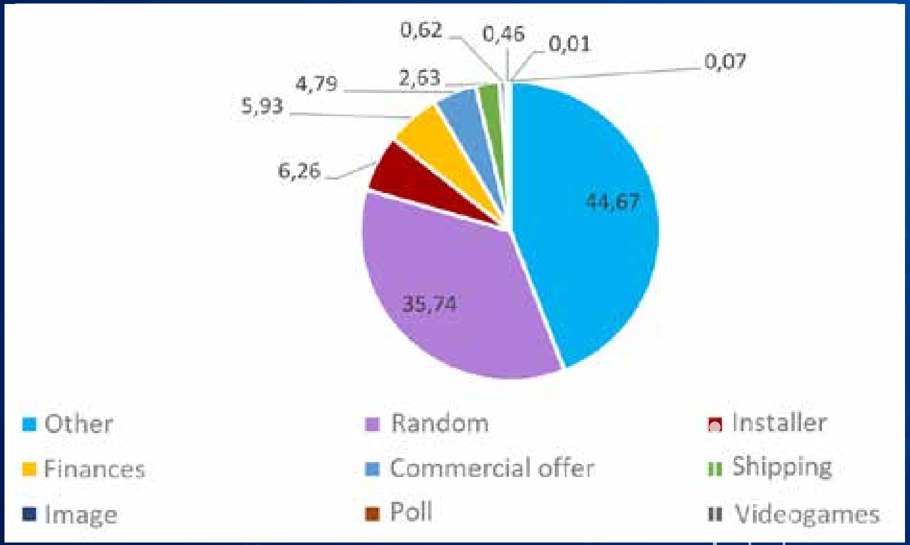


3. Top malware families seen during Q1 2023.

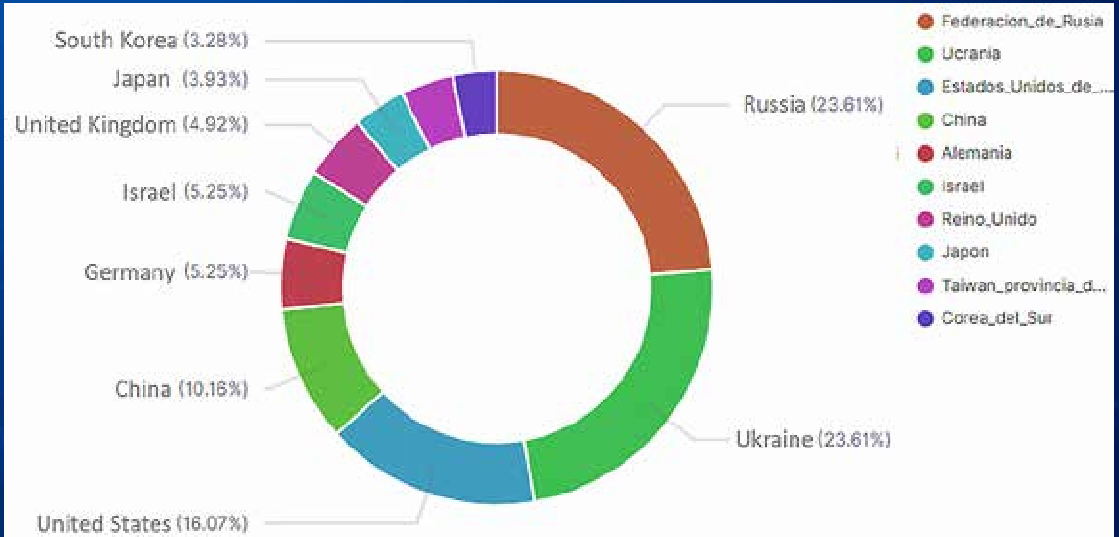
In terms of the themes used as lures by the different malware families, randomness accounts for almost 50% of the total, which makes it difficult to create detection rules. If we exclude the random theme, installer spoofing is the most common theme, followed by financial and commercial proposals.

On the other hand, two noteworthy phenomena have been identified. Firstly, it has been observed that the SWIFT payment method has been used as a lure theme in numerous attacks. The second phenomenon identified is the use of the video game theme in the lure, which could indicate a targeting of attacks on younger generations.

In addition to generating intelligence from recorded security incidents, the Lab52 team also conducts an analysis exercise of geopolitical events and the international context, which aims, among other things, to detect risk hotspots. In the first quarter of 2023, the main risk hotspots focus on Russia, Ukraine, and the United States. This is due to the Russian-Ukrainian conflict. Germany and the United Kingdom also have a high level of risk, a consequence of their degree of involvement in the conflict. Similarly, other countries with a high level of risk are Taiwan and China due to the former's desire for independence, and Japan and South Korea due to North Korea's repeated displays of weapons capabilities.

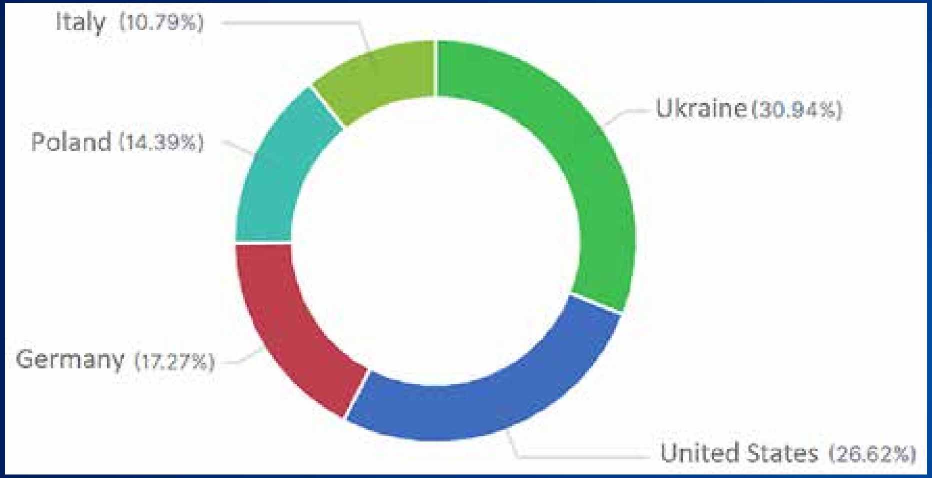


4. Themes used as malware lures.



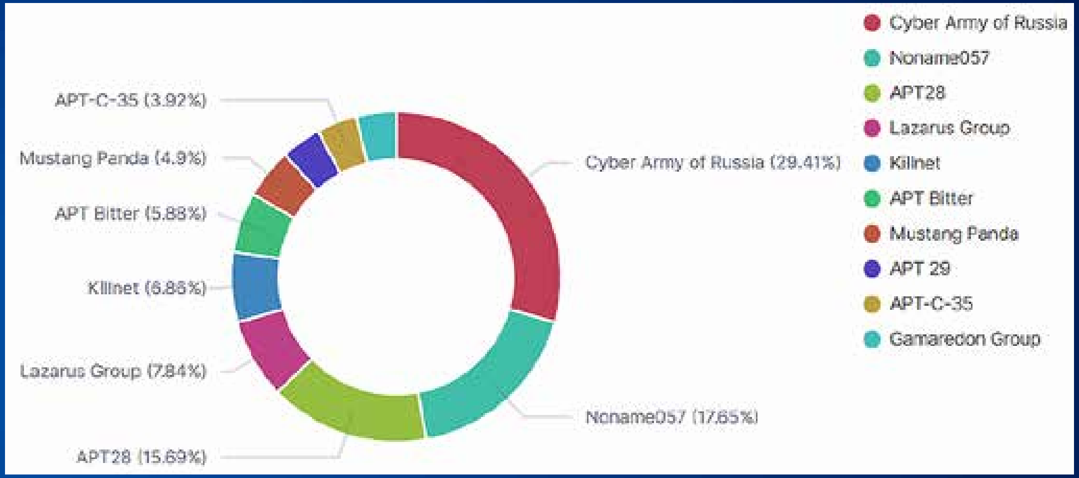
5 . Country risk

The following graph shows the most attacked countries during the first quarter of 2023. Comparing the previous graph with this one, it can be seen how there is a direct relationship between a country's level of risk and the number of cyber-attacks it receives.



6. Distribution of cyber-attacks by victim country.

Of all the events processed by the Lab52 team, more than one thousand Indicators of Compromise have been generated in the S2 Group's intelligence database. The most active groups in the period are shown below.



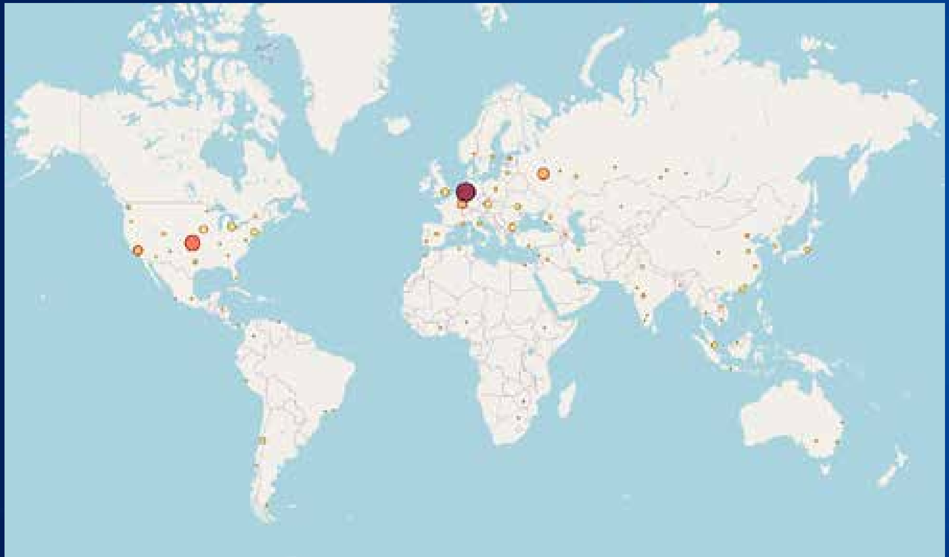
7. Top Threats based on processed IoCs

Of the list of the ten most active groups in the first quarter, six of them act based on Russian interests, some from a hacktivist approach (Cyber Army of Russia, Noname057, Killnet) and others as part of different branches of government (APT28, APT29, Gamaredon Group). A high level of activity has also been observed from the North Korean Lazarus Group, which has conducted a higher than usual number of cybercrime actions.

Although the data reveals that most security incidents are cybercrime actions, since the start of the war in Ukraine there has been an inordinate increase in the number of hacktivist and cyberwarfare campaigns.

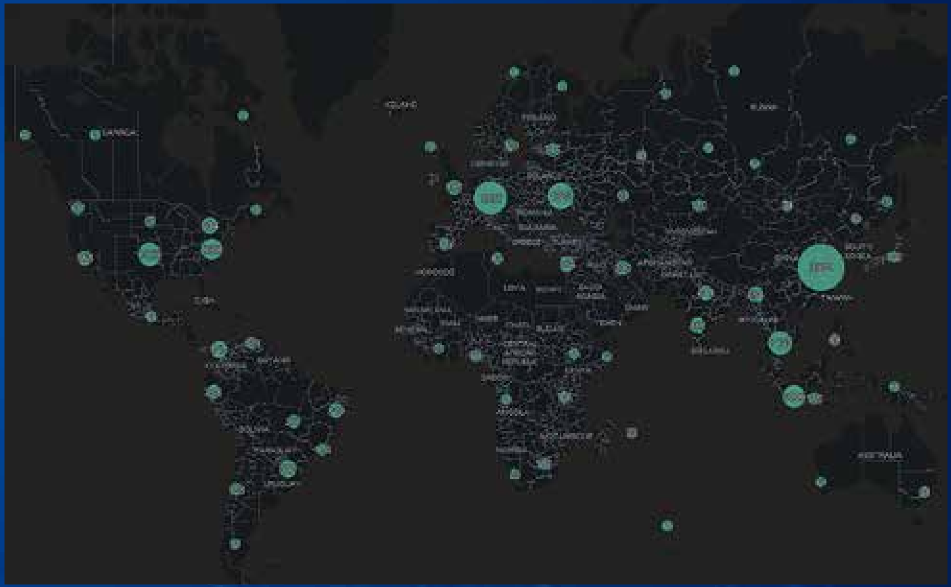
Infrastructure analysis

As far as the infrastructure used by the actors themselves is concerned, the map of the geographical distribution in the fourth quarter of 2022 showed the following data:



8. Q4 2022 Infrastructure

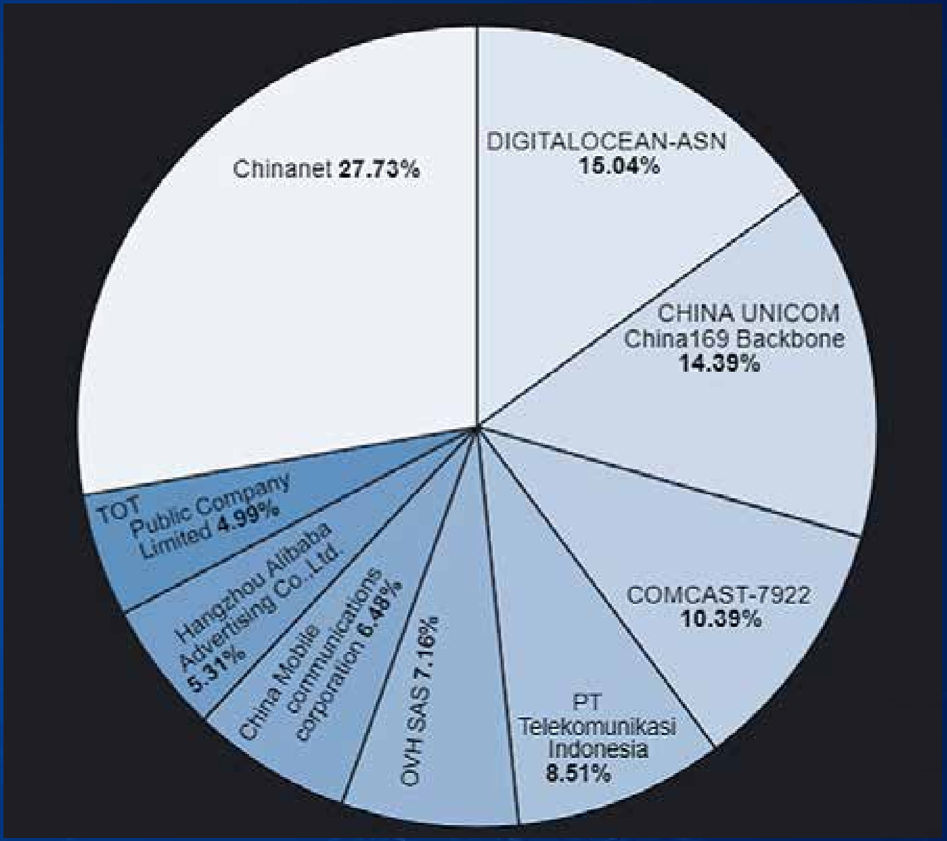
The geographical distribution of infrastructure in the first quarter of 2023 shows some changes, as can be seen in the following map:



9. 2023 Infrastructure

The most noticeable change is the increase in infrastructure in China. The providers associated with this infrastructure are Chinanet, CHINA UNICOM and China Mobile Communications. This infrastructure has become widely used by hacktivist groups, to the detriment of Biterika, which in the previous quarter was the second with the second most registrations, has disappeared as one of the most widely used infrastructures.

It is also interesting to note that, following the publication of the Killnet group's use of Biterika last quarter, they have switched to Chinanet.



10. Number of records per ASN 1Q

Cyber Espionage Campaigns

Activity of Russian-linked groups

Pro-Russian hacktivist groups

The last quarter of 2022 saw a large mobilisation of pro-Russian hacktivist groups that focused their efforts on attacking Ukraine and Poland in response to the actions conducted by them in the context of the Russian-Ukrainian conflict.

In the first quarter of 2023 these same hacktivist groups (NoName057, Killnet, Cyber Army of Russia, etc.) have expanded the scope of their attacks, including strategic organisations of those countries involved in the conflict in their list of targets. Examples include:

- The increase in cyber-attacks against Italy after Prime Minister Giorgia Meloni visited Kyiv to express her support for Zelenski's government and the Ukrainian people in the conflict with Russia.
- The increase in cyber-attacks against Spain following the visit of Prime Minister Pedro Sánchez to Kyiv in which he confirmed to Zelenski that Spain would send six Leopard tanks to Ukraine, with the possibility of up to ten.

APT 28

In mid-March, Microsoft released the Outlook update for vulnerability CVE-2023-23397. This is a privilege escalation vulnerability that allows attackers to send emails designed to exploit Outlook. This vulnerability was being exploited by the Russian APT 28 group between April and December 2022 to attack European organisations in multiple sectors such as: government, military, and energy. The goal of this campaign was to steal Windows credentials for future use in the lateral movement and exfiltration phases.

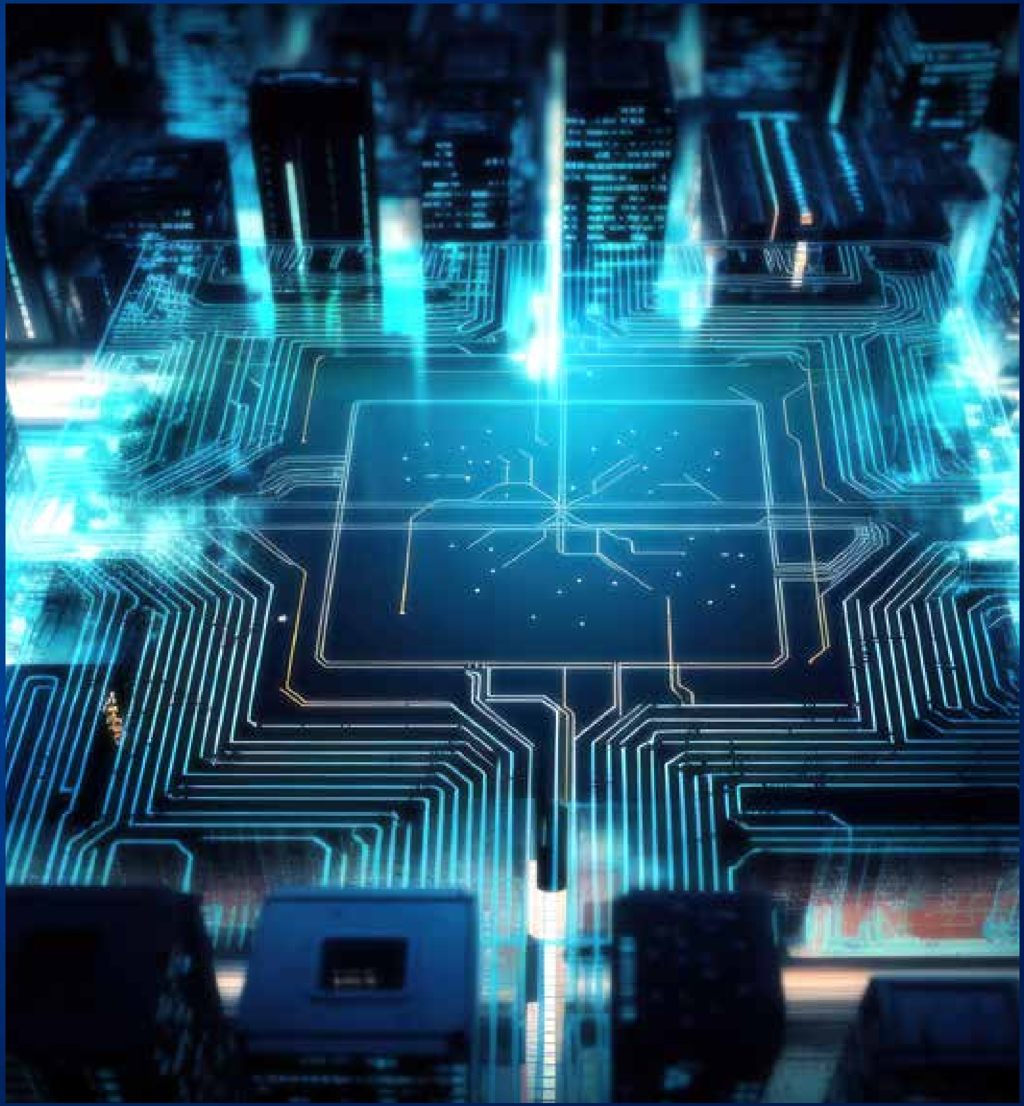
APT 29

At the end of March, Lab52 analysed two phishing attacks from a campaign against government entities in EU member states by the Russian group APT29, also known as NOBELIUM. The first attack is an email spoofing the human resources department of a web development technology company based in Pakistan. The email with the subject line "Update! Invitation to the meeting" contains an attached document "invite.pdf". The initial access technique of the second attack is a phishing attack impersonating a Spanish embassy. The email message invites potential victims to take part in a face-to-face meeting on "The

Future of international economic relations" at the Spanish embassy. Then, under the pretext of filling in a form to confirm their attendance to the event, a malicious link is attached. In both cases, the result of the phishing is the download of an HTML file that turns out to be an ISO with three files: an executable, a malicious DLL, and an encrypted shellcode.

Gamaredon

A new cyber espionage campaign by Gamaredon Group against Ukrainian institutions has been detected. The actors are delivering malware with capabilities to remotely execute commands and deploy payloads. The initial access vector used are spearphishing emails that deliver a malicious WebShell via social engineering techniques. Falsified Ukrainian institutional themes and documents are used as decoys. To evade detection systems, Gamaredon Group employs multiple obfuscation techniques. Gamaredon Group is an alleged Russian cyber espionage threat group that has targeted military, NGO, judicial, law enforcement, and non-profit organisations in Ukraine since at least 2013.



Activity of groups linked to China

Mustang Panda

Particularly innovative has been the activity linked to Mustang Panda, as a new backdoor was detected, which has been dubbed “MQsTTang”. It allows the attacker to execute arbitrary commands on the victim’s machine using the MQTT protocol for communication with the C2. This protocol is typically used for communications between IoT devices and controllers. This allows the attacker to hide the rest of his infrastructure behind an intermediary. Therefore, the compromised machine never communicates directly with the C2.

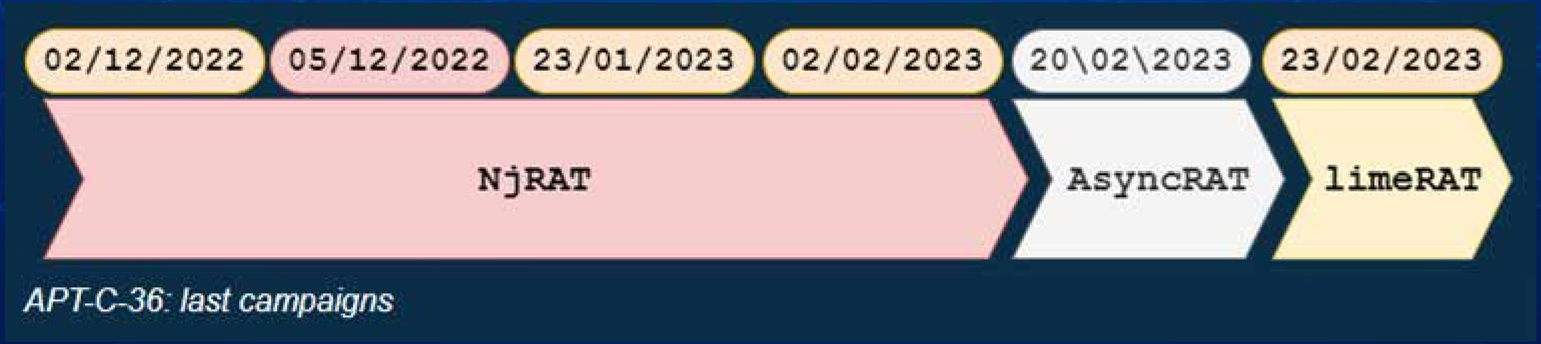
Activity of other groups

APT-C-36

From 2 December 2022 to 2 February 2023, multiple campaigns linked to the APT-C-36 group were observed deploying NjRAT in its final phase. On 20 February Lab52 observed a campaign that varied slightly from the rest and aimed to deploy AsyncRAT on compromised machines.

At the end of February, the use of LimeRAT was observed, but with a very similar operation in the deployment used during the rest of the campaigns, from the first ones whose objective was the execution of NjRAT. Thus, after the analysis conducted by Lab52, LimeRAT is considered an evolution of NjRAT.

The diagram shows the temporal evolution of the malware running after the infection phase.



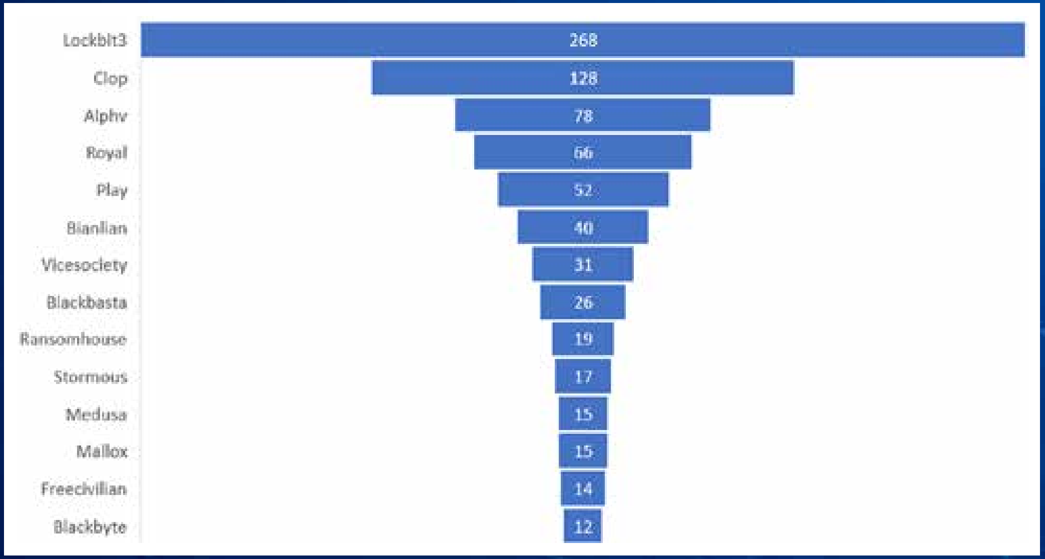
Cybercrime Campaigns

Ransomware

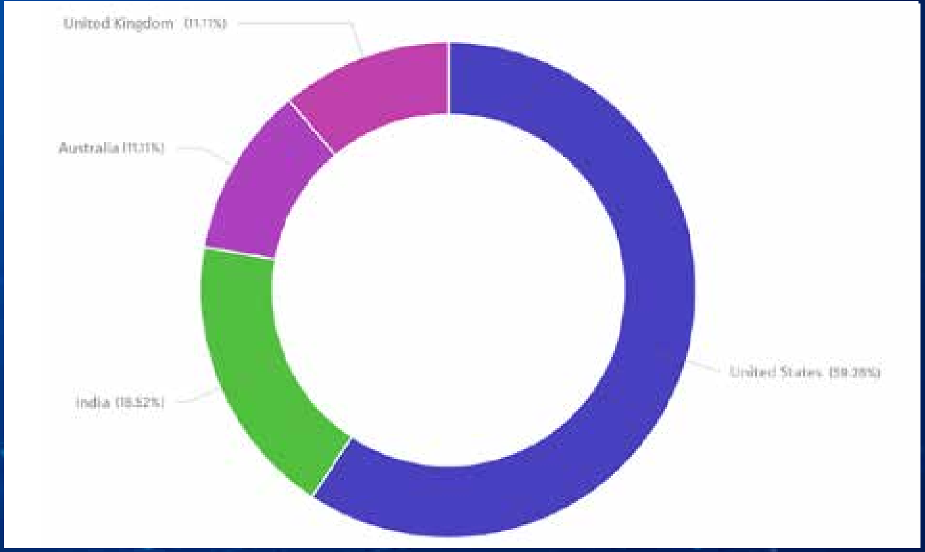
Ransomware remains one of the most prevalent and impactful cyber threats globally. By collecting and analysing samples, Lab52 is able to draw a reliable representation of the presence of each of the different ransomware families in the current landscape.

Based on the data obtained by Lab52, a graph has been created representing the countries most affected by ransomware during the first quarter of 2023.

Moreover, analysis of the sectors most affected by cybercrime campaigns reveals that the finance and banking sectors are the main targets of cybercrime campaigns.



12. Top ransomware families seen in incidents during Q1 2023.



13. Top countries most affected by ransomware.

Snake Keylogger, Guloader y Formbook

Throughout the first quarter, many campaigns against Spain and Latin America have been observed, especially with themes associated with banking and financial issues. It is interesting to note the proliferation of the use of Telegram as a method of exfiltration of information, as well as the use of dynamic domains. Among the most impersonated organisations are the Spanish banks Santander, BBVA and Sabadell.

Keyloggers

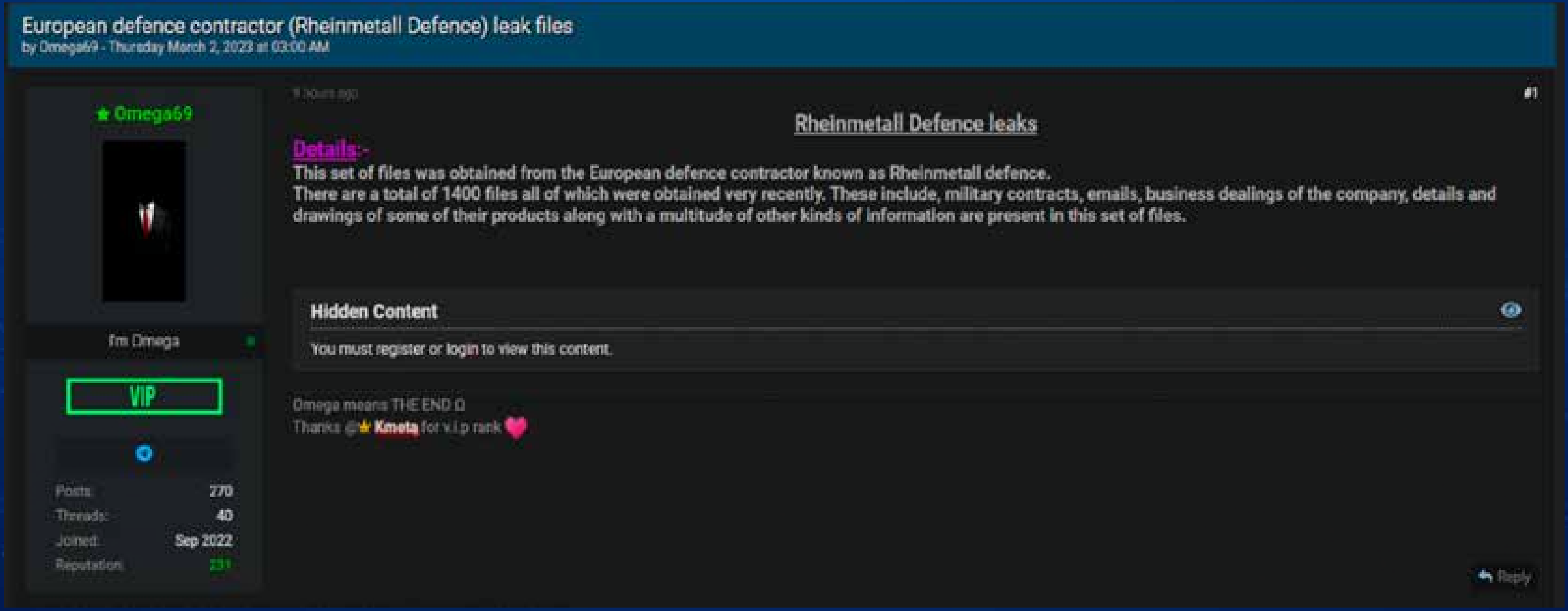
A very high percentage of cybercrime campaigns deploy keyloggers on compromised machines. In one campaign analysed by Lab52, a PowerShell-based keylogger was detected that aimed to record the user's clipboard activity. Upon detecting the combination CTL+C or CTL+V it sent the information to a Discord server via a webhook.

Deep Web

In terms of Deep Web leaks, there has been a particular increase in those associated with defence issues. Among the leaks are the following:

Rheinmetall

In early March, an actor named Omega69 was detected selling exfiltrated Rheinmetall Defence company files on a well-known dark web forum.



European defence contractor (Rheinmetall Defence) leak files
by Omega69 - Thursday March 2, 2023 at 03:00 AM

★ Omega69

I'm Omega

VIP

Posts:	270
Threads:	40
Joined:	Sep 2022
Reputation:	231

9 hours ago

#1

Rheinmetall Defence leaks

Details:-
This set of files was obtained from the European defence contractor known as Rheinmetall defence.
There are a total of 1400 files all of which were obtained very recently. These include, military contracts, emails, business dealings of the company, details and drawings of some of their products along with a multitude of other kinds of information are present in this set of files.

Hidden Content

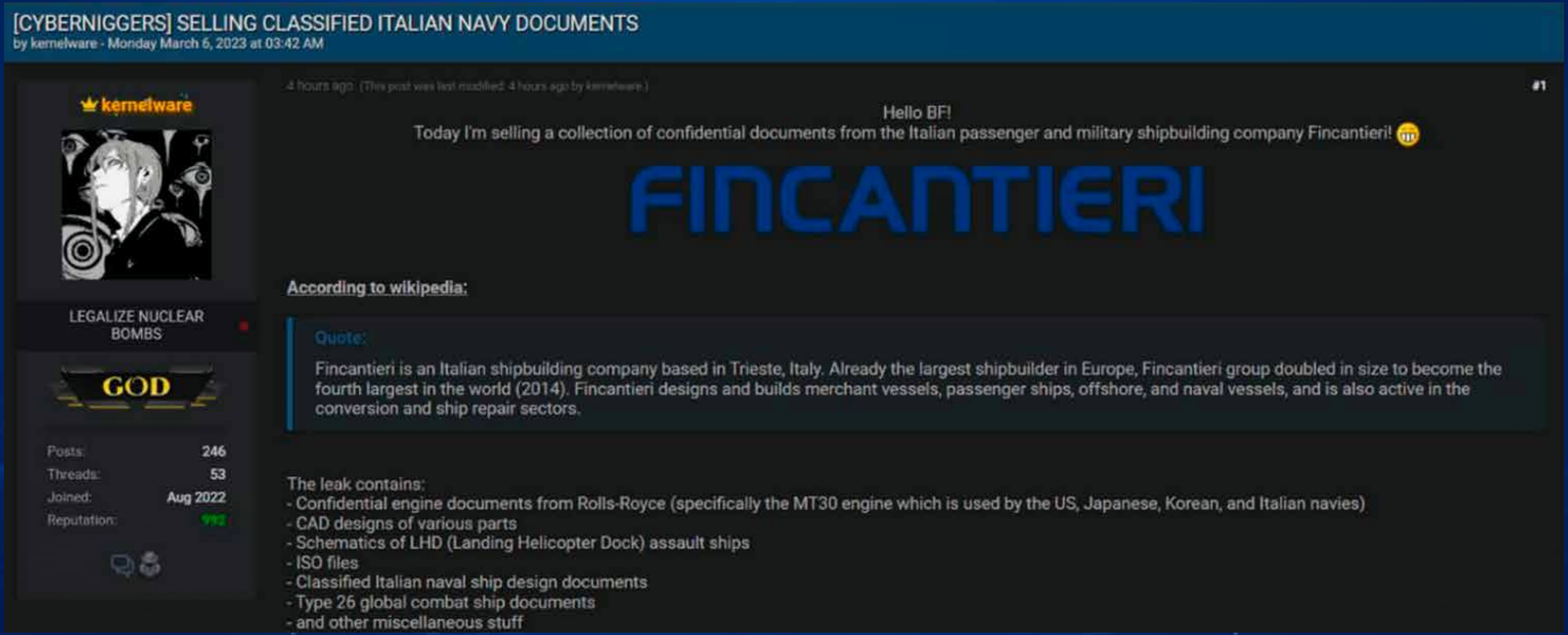
You must register or login to view this content.

Omega means THE END Ω
Thanks @★ Kmeta for v.i.p rank

14. Rheinmetall Defence data leak.

Ficantieri

Just days after the Rheinmetall Defence compromise, an actor called kernelware appeared on the same dark web forum offering information about the Italian shipping company Fincatieri. Among the data it was selling were confidential data on Rolls-Royce engines, schematics of LHD assault vessels and documents on the Type 26 global combat ship.



[CYBERNIGGERS] SELLING CLASSIFIED ITALIAN NAVY DOCUMENTS
by kernelware - Monday March 6, 2023 at 03:42 AM

kernelware

LEGALIZE NUCLEAR BOMBS

GOD

Posts:	246
Threads:	53
Joined:	Aug 2022
Reputation:	992

4 hours ago (This post was last modified: 4 hours ago by kernelware.) #1

Hello BF!
Today I'm selling a collection of confidential documents from the Italian passenger and military shipbuilding company Fincantieri! 😁

FINCANTIERI

According to wikipedia:

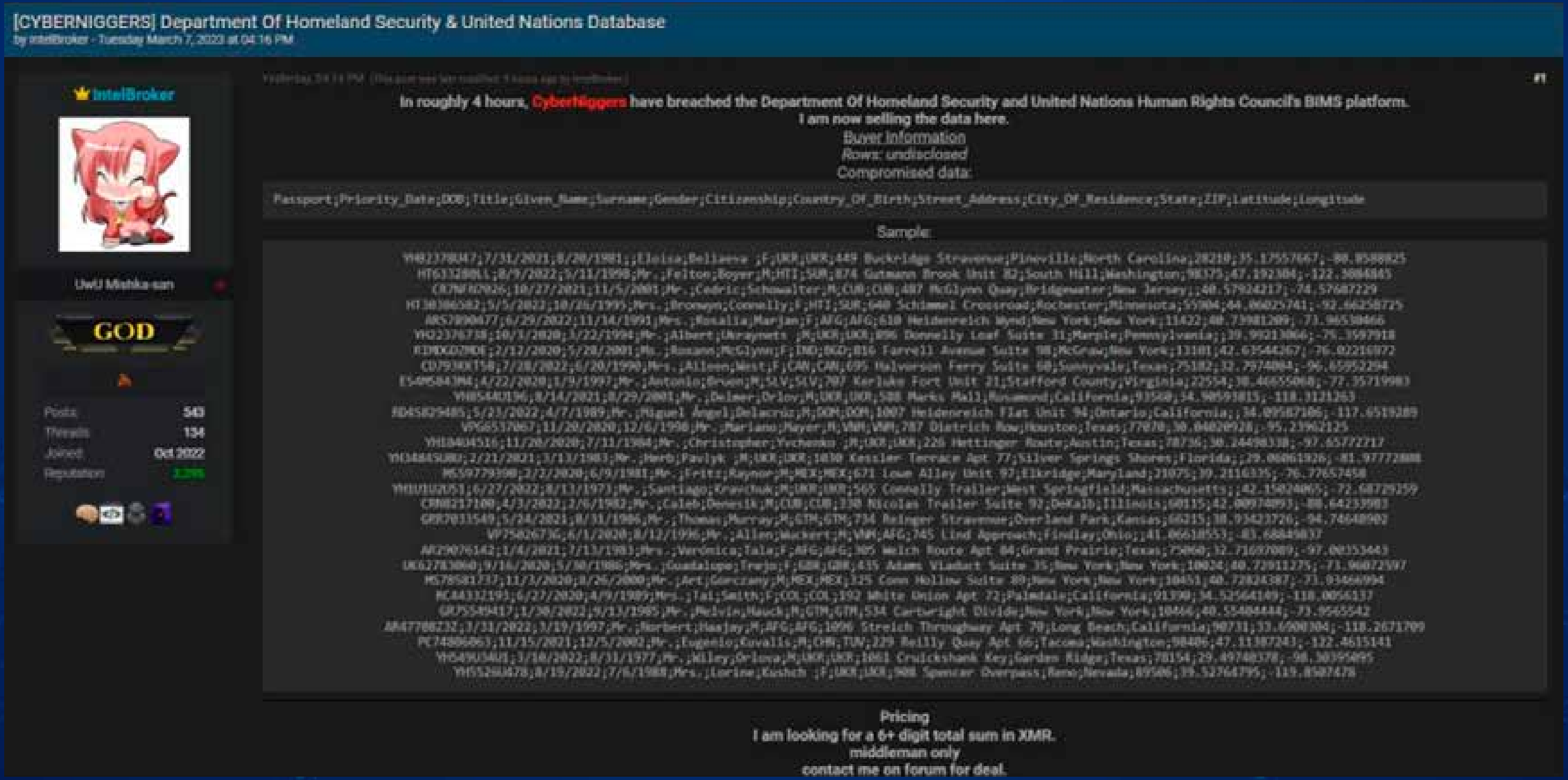
> Quote:
> Fincantieri is an Italian shipbuilding company based in Trieste, Italy. Already the largest shipbuilder in Europe, Fincantieri group doubled in size to become the fourth largest in the world (2014). Fincantieri designs and builds merchant vessels, passenger ships, offshore, and naval vessels, and is also active in the conversion and ship repair sectors.

The leak contains:
- Confidential engine documents from Rolls-Royce (specifically the MT30 engine which is used by the US, Japanese, Korean, and Italian navies)
- CAD designs of various parts
- Schematics of LHD (Landing Helicopter Dock) assault ships
- ISO files
- Classified Italian naval ship design documents
- Type 26 global combat ship documents
- and other miscellaneous stuff

15. Fincatieri data leak.

US Department of Homeland Security

On 7 March, an announcement was posted on a Deep Web forum about the sale of the US Department of Homeland Security and United Nations database containing detailed personal information relating to both US Department of Homeland Security employees and civilians.



[CYBERNIGGERS] Department Of Homeland Security & United Nations Database
by IntelBroker - Tuesday March 7, 2023 at 04:16 PM

Yesterday, 04:16 PM (This post was last modified: 5 hours ago by IntelBroker.) #1

In roughly 4 hours, CyberNiggers have breached the Department Of Homeland Security and United Nations Human Rights Council's BIMS platform.
I am now selling the data here.
Buyer Information
Rows: undisclosed
Compromised data:

```
Passport;Priority_Date;DOB;Title;Given_Name;Surname;Gender;Citizenship;Country_Of_Birth;Street_Address;City_Of_Residence;State;ZIP;Latitude;Longitude
```

Sample:

```
YH82378U47;7/31/2021;8/20/1981;;Eloisa;Bellaeva ;F;UKR;UKR;449 Buckridge Stravenue;Pineville;North Carolina;28210;35.17557667;-80.8588825
HT6332800LL;8/9/2022;5/11/1998;Mr.;Felton;Boyer;M;HTI;SUR;874 Gutmann Brook Unit 82;South Hill;Washington;98375;47.192304;-122.3084845
CR7NF07026;10/27/2021;11/5/2001;Mr.;Cedric;Schowalter;M;CUB;CUB;487 McGlynn Quay;Bridgewater;New Jersey;;40.57924217;-74.57687229
HT30306582;5/5/2022;10/26/1995;Mrs.;Bronwyn;Connelly;F;HTI;SUR;640 Schimmel Crossroad;Rochester;Minnesota;55904;44.06025741;-92.66258725
ARS7890477;6/29/2022;11/14/1991;Mrs.;Rosalia;Marjan;F;AFG;AFG;610 Heidenreich Wynd;New York;New York;11422;40.73981209;-73.96530466
YH22376738;10/1/2020;3/22/1994;Mr.;Albert;Ukraynets ;M;UKR;UKR;896 Donnelly Leaf Suite 31;Marple;Pennsylvania;;39.99213066;-75.3597918
KIMDGD2MDE;2/12/2020;5/28/2001;Ms.;Roxann;McGlynn;F;IND;BGD;816 Farrell Avenue Suite 98;McGraw;New York;13101;42.63544267;-76.02216972
CD79300T58;7/28/2022;6/20/1990;Mrs.;Alleen;West;F;CAN;CAN;695 Halvorson Ferry Suite 60;Sunnyvale;Texas;75182;32.7974084;-96.65952294
ES4M5043N4;4/22/2020;1/9/1997;Mr.;Antonio;Bruen;M;SLV;SLV;707 Kerluke Fort Unit 21;Stafford County;Virginia;22554;38.46655068;-77.35719983
YH85440196;8/14/2021;8/29/2001;Mr.;Delmer;Orlov;M;UKR;UKR;588 Marks Mall;Rosamond;California;93560;34.90593815;-118.3121263
RD45829485;5/23/2022;4/7/1989;Mr.;Miguel Ángel;Delacruz;M;DOM;DOM;1007 Heidenreich Flat Unit 94;Ontario;California;;34.09587186;-117.6519289
VPG6537067;11/20/2020;12/6/1998;Mr.;Mariano;Mayer;M;VNM;VNM;787 Dietrich Row;Houston;Texas;77070;30.04020928;-95.23962125
YH10404516;11/20/2020;7/11/1984;Mr.;Christopher;Yvchenko ;M;UKR;UKR;226 Hettinger Route;Austin;Texas;78736;30.24490338;-97.65772717
YH34445U8U;2/21/2021;3/13/1983;Mr.;Herb;Pavlyk ;M;UKR;UKR;1030 Kessler Terrace Apt 77;Silver Springs Shores;Florida;;29.06061926;-81.97772888
MS59779390;2/2/2020;6/9/1981;Mr.;Fritz;Raynor;M;MEX;MEX;671 Lowe Alley Unit 97;Elkridge;Maryland;21075;39.2116335;-76.77657458
YH1U1U2U51;6/27/2022;8/13/1971;Mr.;Santiago;Kravchuk;M;UKR;UKR;565 Connelly Trailer;West Springfield;Massachusetts;;42.15024065;-72.68729259
CRN8217100;4/3/2022;2/6/1982;Mr.;Caleb;Denesik;M;CUB;CUB;330 Nicolas Trailer Suite 92;DeKalb;Illinois;60115;42.00974093;-88.64233983
GRR7031549;5/24/2021;8/31/1986;Mr.;Thomas;Murray;M;GTM;GTM;734 Reinger Stravenue;Overland Park;Kansas;66215;38.93423726;-94.74648902
VP75026736;6/1/2020;8/12/1996;Mr.;Allen;Wuckert;M;VNM;AFG;745 Lind Approach;Findlay;Ohio;;41.06618553;-83.68849037
AR29076142;1/4/2021;7/13/1983;Mrs.;Verónica;Tala;F;AFG;AFG;305 Welch Route Apt 04;Grand Prairie;Texas;75060;32.71697089;-97.00353443
UK62783060;9/16/2020;5/30/1986;Mrs.;Guadalupe;Trejo;F;GBR;GBR;435 Adams Viaduct Suite 35;New York;New York;10024;40.72911275;-73.96072597
MS78581737;11/3/2020;8/26/2000;Mr.;Art;Gorczany;M;MEX;MEX;325 Conn Hollow Suite 89;New York;New York;10451;40.72824387;-73.93466994
MC44332193;6/27/2020;4/9/1989;Mrs.;Tai;Smith;F;COL;COL;192 White Union Apt 72;Palmdale;California;91390;34.52564149;-118.0056137
GR75549417;1/30/2022;9/13/1985;Mr.;Melvin;Hauck;M;GTM;GTM;534 Cartwright Divide;New York;New York;10466;40.55404444;-73.9565542
AR47708232;3/31/2022;3/19/1997;Mr.;Norbert;Haajay;M;AFG;AFG;1096 Streich Throughway Apt 70;Long Beach;California;90731;33.6900304;-118.2671709
PC74806063;11/15/2021;12/5/2002;Mr.;Eugenio;Kuvalis;M;CHN;TUV;229 Reilly Quay Apt 66;Tacoma;Washington;98406;47.11387243;-122.4615141
YH54903401;3/10/2022;8/31/1977;Mr.;Wiley;Orlova;M;UKR;UKR;1061 Cruickshank Key;Garden Ridge;Texas;78154;29.49740378;-98.30395095
YH55260478;8/19/2022;7/6/1988;Mrs.;Lorine;Kushch ;F;UKR;UKR;908 Spencer Overpass;Reno;Nevada;89506;39.52764795;-119.8507478
```

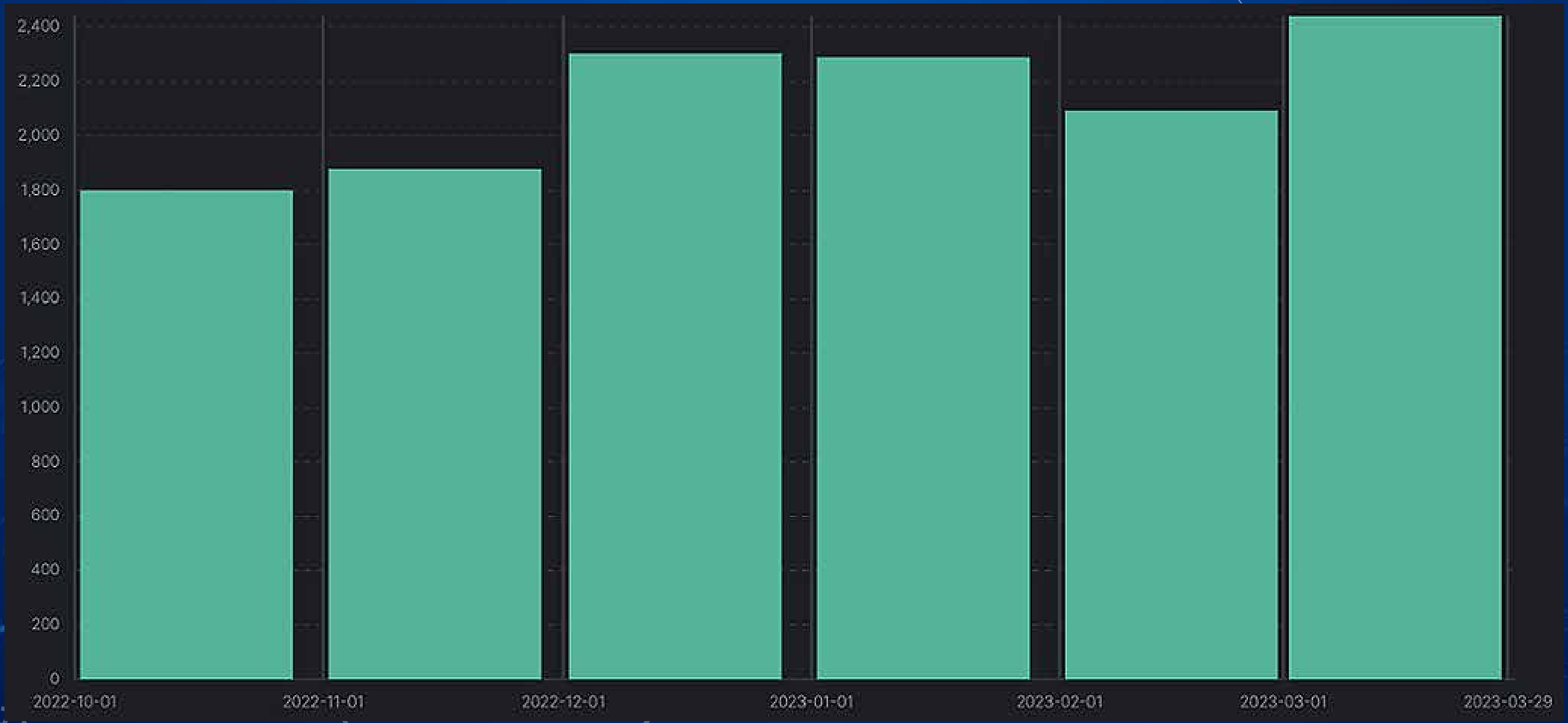
Pricing
I am looking for a 6+ digit total sum in XMR.
middleman only
contact me on forum for deal.

16. US Department of Homeland Security and United Nations database data leak.

Vulnerabilities

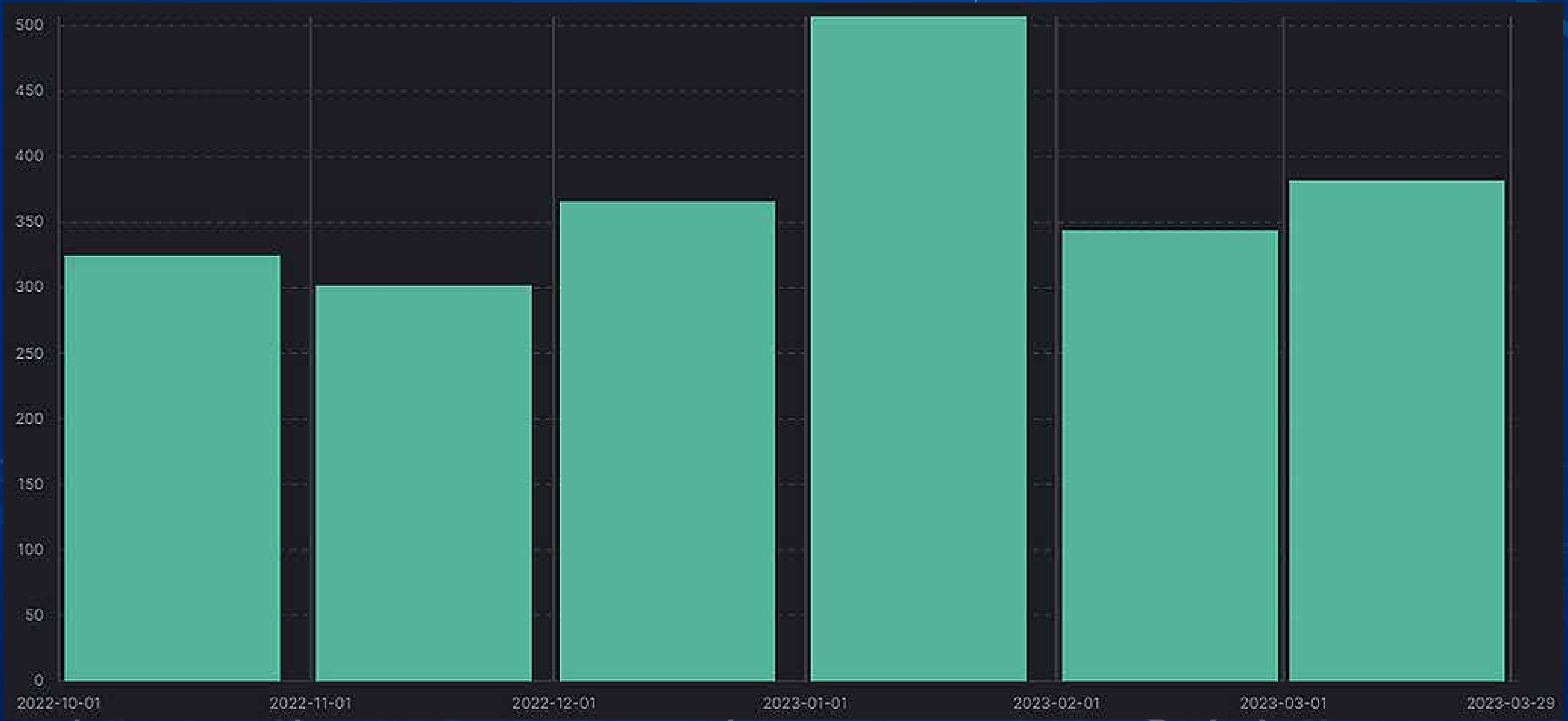
Vulnerability data and statistics

The graph below represents the total number of vulnerabilities published between October 2022 and March 2023. The total number of vulnerabilities in the first quarter of 2023 has increased compared to the last quarter of 2022. This peak in vulnerabilities is the result of the publication of 80 highly critical vulnerabilities for the Hub of Insteon.



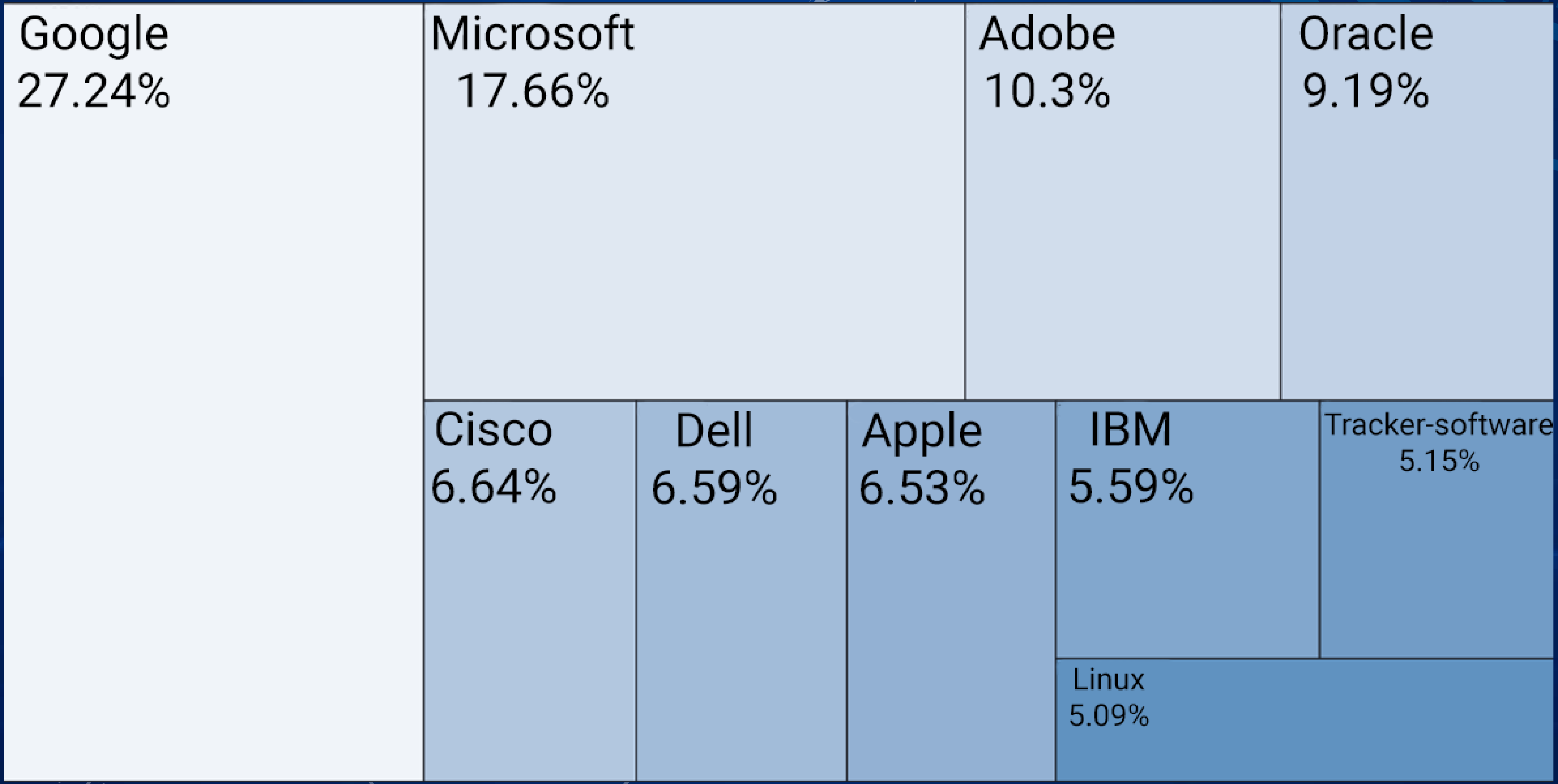
17. Number of vulnerabilities per month.

The monthly distribution of the number of published critical vulnerabilities reveals a peak during the month of January, which represents an increase of about 25% compared to the other months.



18. Number of critical vulnerabilities per month.

The top 10 firms affected by vulnerabilities during the period are as follows:



19. Percentage of vulnerabilities by vendor in Q1.

Noteworthy vulnerabilities

Microsoft Office/Outlook CVE-2023-23397

An attacker successfully exploiting this vulnerability could access a user's Net-NTLMv2 hash which could be used as the basis of an NTLM Relay attack against another service to authenticate as the user.

Microsoft Windows11/Windows Server2022 CVE-2023-23392

An unauthenticated attacker could send a specially crafted packet to a target server that uses the HTTP protocol stack (http.sys) to process packets.

Fortinet-FortiOS CVE-2023-25610

A buffer overflow vulnerability in the administrative interface of FortiOS and FortiProxy can allow an unauthenticated remote attacker to execute arbitrary code on the device and/or perform a denial of service on the GUI, via specifically crafted requests.

GOOGLE-Android CVE-2023-20946

In onStart of BluetoothSwitchPreferenceController.java, there is a possible permission bypass due to an attachment. This could lead to remote privilege escalation of the Bluetooth configuration without the need for additional execution privileges. User interaction is not required for exploitation.

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

The vulnerability allows a remote attacker to execute arbitrary code on the target system. The vulnerability exists due to a type confusion bug when parsing web content in WebKit. A remote attacker can trick the victim into visiting a specially crafted website, trigger a type confusion error and execute arbitrary code on the target system. Note, the vulnerability is being actively exploited in the wild.

Conclusions

The Western bloc's pro-Ukrainian involvement in the Russian-Ukrainian conflict increases the risk of an escalation of tensions and the possibility of an extension of the armed conflict internationally. In this scenario of instability, China is positioning itself as the mediating figure between the two blocs, which could have a major impact on its power of influence at the international level over the coming decades.

Data collected by Lab52 during the first quarter of the year 2023 reveals that strategic and critical sectors of Western countries such as governments, public administrations and defence have been recurrently attacked by advanced threat actors. The analysis of attacks, threats and victims seems to indicate that there is a direct link between these incidents and the Russian-Ukrainian conflict. Hacktivist groups stand out as the most active groups during the first quarter.

In terms of the malware used in the incidents recorded during the first quarter, the RedLineStealer, Mirai and Agent Tesla malware families were predominant. On the other hand, Chinese infrastructure is the most used by threat actors to conduct their cyber-attacks.

The number of published vulnerabilities has increased compared to the previous quarter, with high criticality vulnerabilities in widely used products from Google, Microsoft, and Cisco, among others.

The information published in this report has been generated from the analysis of data collected by Lab52 from internal and external sources as part of the cyber intelligence service provided by S2 Group.

S2 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