FORTINET | FortiRecon

REPORT

Threat Intelligence Report

Darknet Trends for Q2 2022

TABLE OF CONTENTS

About This Report and FortiRecon

This FortiGuard Labs Darknet Trends Report leveraged the Fortinet FortiRecon service to provide a deep dive into what adversaries are seeing, doing, and planning, enabling organizations to better understand the threats posed by the growth of criminal forums and markets operating on the darknet. The report covers global, regional, and industry/sector threat landscape perspectives as well as protection recommendations for IT and OT organizations for darknet activity observed during Q2 2022.

FortiRecon is Fortinet's Digital Risk Protection (DRP) service. This SaaS-based service combines three powerful technologies and services—External Attack Surface Management, Brand Protection, and Adversary Centric Intelligence—to protect critical digital assets and data from external threats. By looking into open web, social media, mobile app stores, the dark web, and deep web sources, FortiRecon provides organization-specific, expert-curated, and actionable external attack surface intelligence on exposed assets, threat actor activity, and their tools, and tactics. The service also identifies brand infringement and monitors ransomware data leaks to proactively help remediate and execute takedowns on an organization's behalf.

FortiRecon provides organization-specific, expert-curated, and actionable external attack surface intelligence on exposed assets, threat actor activity, and their tools, and tactics.

1. Executive Summary

Lurking in the shadows of the internet, there is a hidden, fast-growing threat of adversaries using newfound ways of committing crimes for their financial, political, or reputational gain. FortGuard Labs, leveraging the FortiRecon service, tracks these cybercriminals and their activities to protect organizations from imminent threats. This report presents an overview and related data of the cybercrime trends we witnessed during Q2 2022.

Cybercriminals gravitate to the darknet because of its anonymity and lack of accountability. For the same reason, many adversaries are now starting to use instant messaging apps, such as Telegram, Tox, QQ, WeChat, and Discord. Others may use Threema or Jabber to offer a Tor redirection.

These platforms provide numerous features, including end-to-end encryption and auto-deleted messages, making tracking more difficult. Messaging apps are also being used to place bids on marketplace orders and host chat groups known as "channels" to send messages to an unlimited number of anonymous subscribers. Responses to group messages can be private encrypted conversations about illicit job offers, stolen documents, or hacking tools. The safer threat actors feel they can communicate, the more likely they are to share these tools and cybercrime opportunities—and the harder they'll be to track.

Below is a summary of darknet activities observed by the FortiGuard Labs using the FortiRecon team service during Q2 2022:

- Financial services was the most targeted industry sector, followed by manufacturing, government, and technology.
- The Top Victim organizations operate in North America, followed by South Asia, Western Europe, and East Asia.
- FortiGuard Labs promoted 24 threat actors to be credible, meaning they had been sufficiently observed and their activity confirmed for the reports to be treated as genuine.
- Rising ransomware activity was observed, where the operators of LockBit ransomware were particularly active, naming 252 victims and outperforming all other ransomware groups.

- Credential Stealer logs were a powerful weapon among initial access brokers, specifically, an actor that uses the handle "Pirat-Networks" advertised maximum access to a victim's network by leveraging malware logs.
- Ransomware operators continue to buy initial access from access brokers. The team observed network access to organizations being advertised that were later listed as victims on multiple ransomware blog sites.
- Chatter on the darknet about vulnerabilities, their exploitation, and the sale of exploits continues to be of high interest among threat actors, where Microsoft and VMware product vulnerabilities appear to be the most popular.
- The widely exploited Follina MSDT RCE (CVE-2022-30190) and Atlassian RCE Confluence Server and Data Center vulnerabilities (CVE-2022-26134) received significant attention among threat actors on the darknet.
- The team observed cybercrime threat actors joining forces with hacktivist groups to support cyber events, such as the Russia–Ukraine Conflict and #OpsPatuk.
- Darknet forums that had previously not been particularly active have seen recent growth and may be attributed to the shutting down of the infamous RAID forum back in Q1 2022.

2. Notable Darknet Trends

2.1. Overview

This statistics presented in this section were collected by FortiGuard Labs using FortiRecon. It highlights the distribution of industry sectors being targeted in Q2 2022 as well as their geographical distribution.

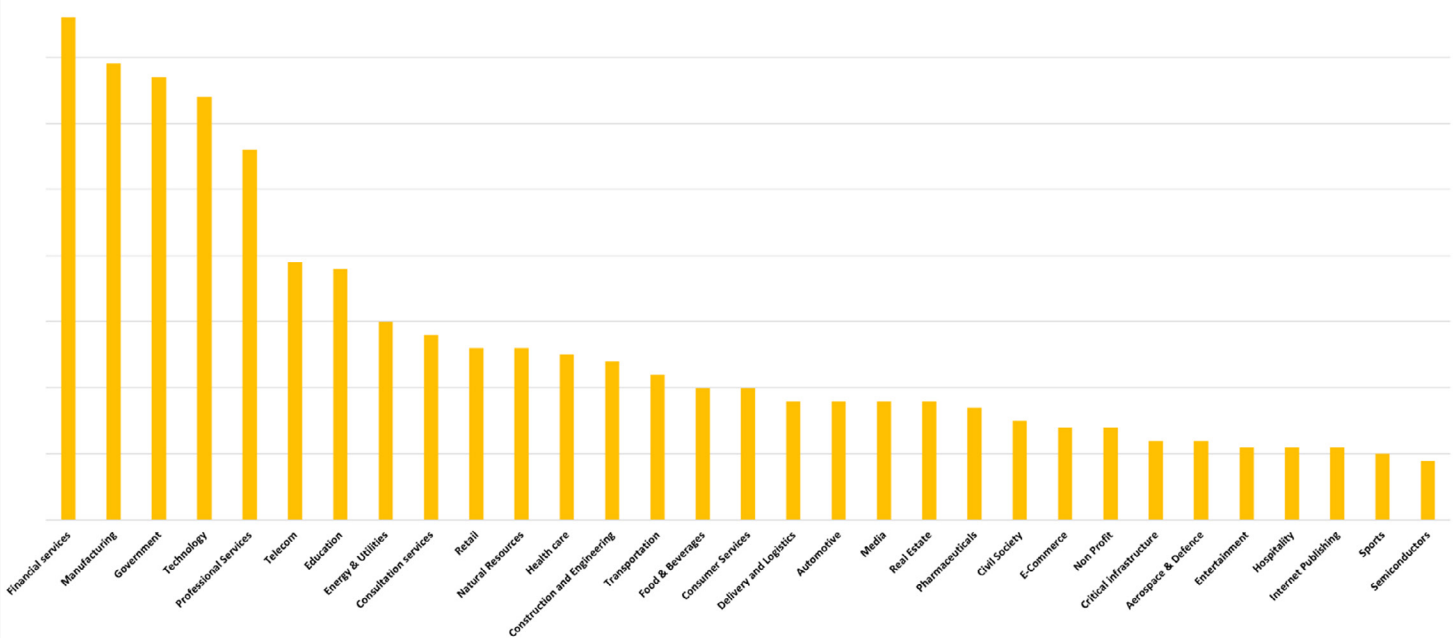

Figure 1: Distribution of sectors targeted in Q2 2022

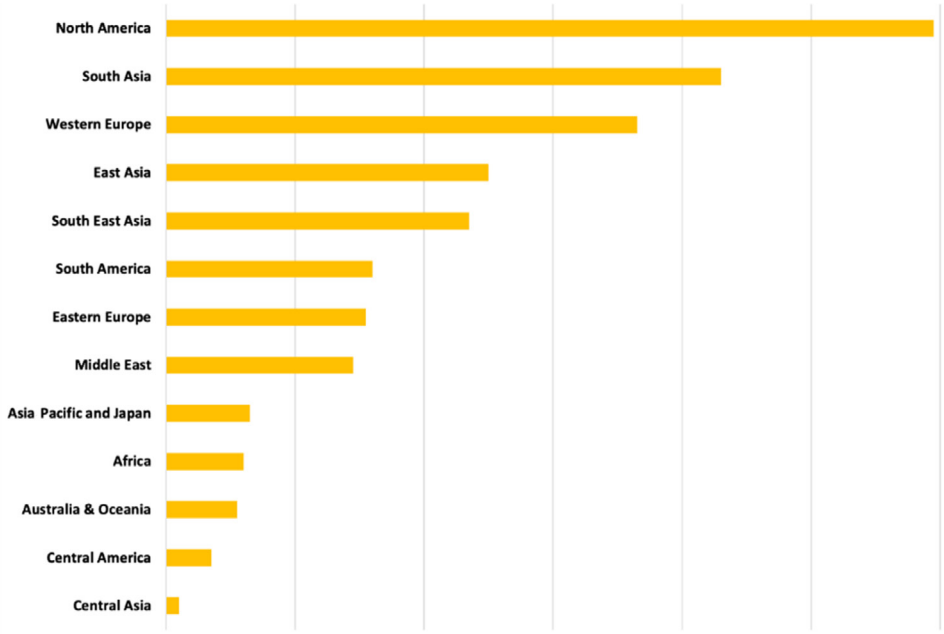

Figure 2: Geographical distribution of target organizations in Q2 2022

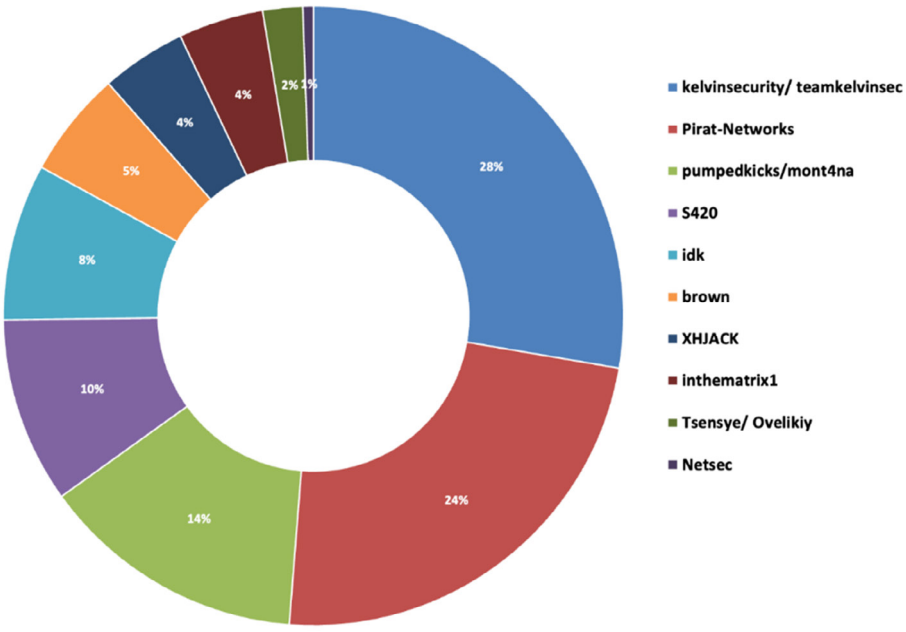

Figure 3: Distribution of the top threat actors active in Q2 2022

2.2. Targeted organizations and their top hackers by geo/industry

The following section covers the geographical distribution of target organizations by industry sector and the top 10 threat actors targeting each respective sector.

2.2.1. Financial Services

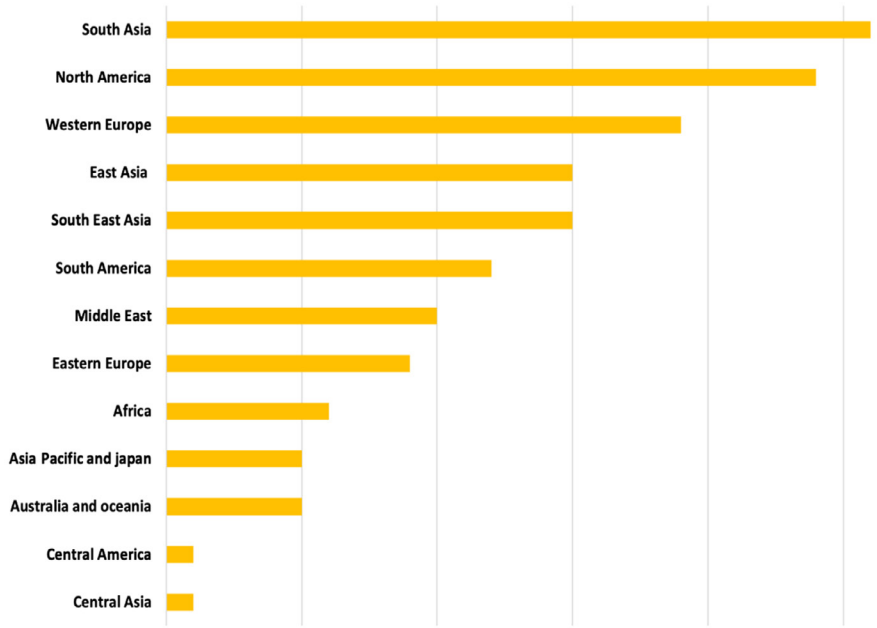

Figure 4: Geographical distribution of target organizations within the financial services sector

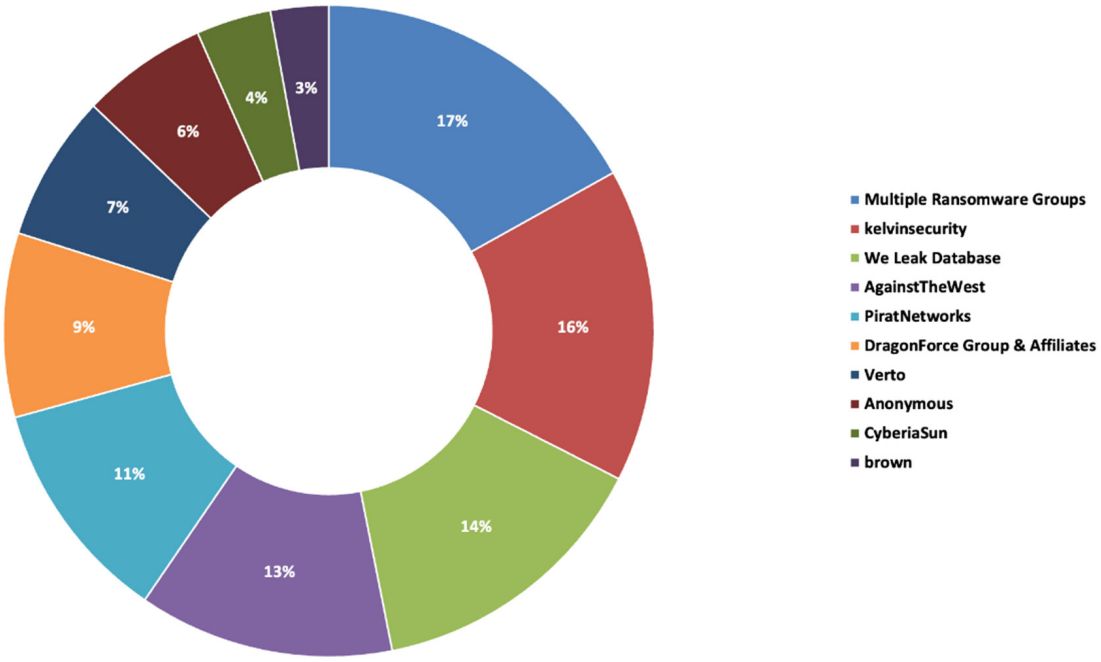

Figure 5: Top 10 threat actors targeting the financial services sector

2.2.2. Manufacturing

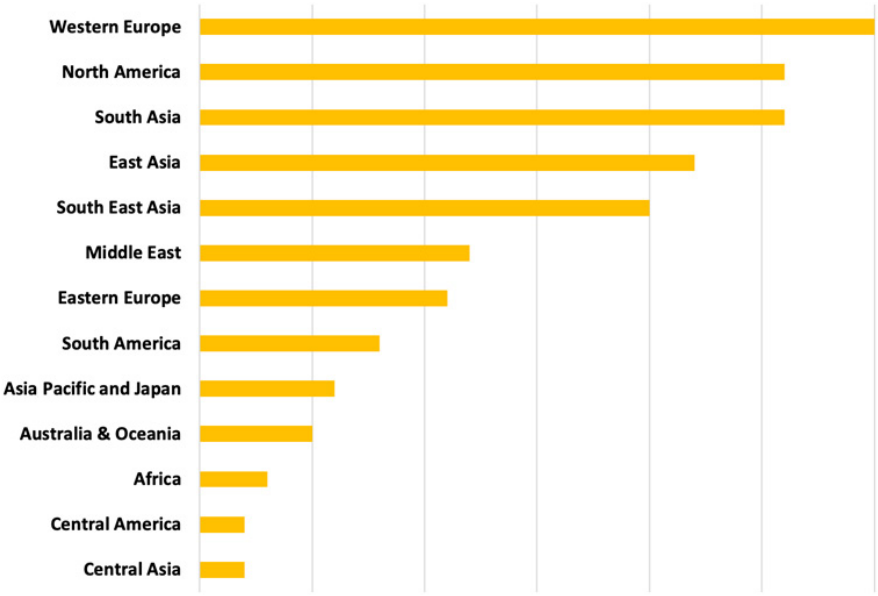

Figure 6: Geographical distribution of target organizations within the manufacturing sector

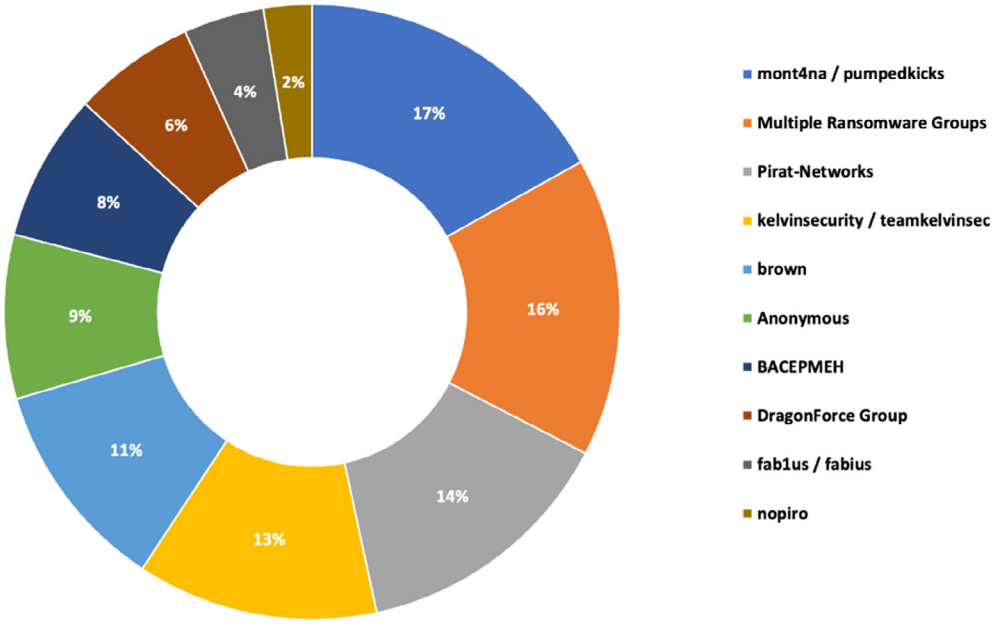

Figure 7: Top 10 threat actors targeting the manufacturing sector

2.2.3. Government

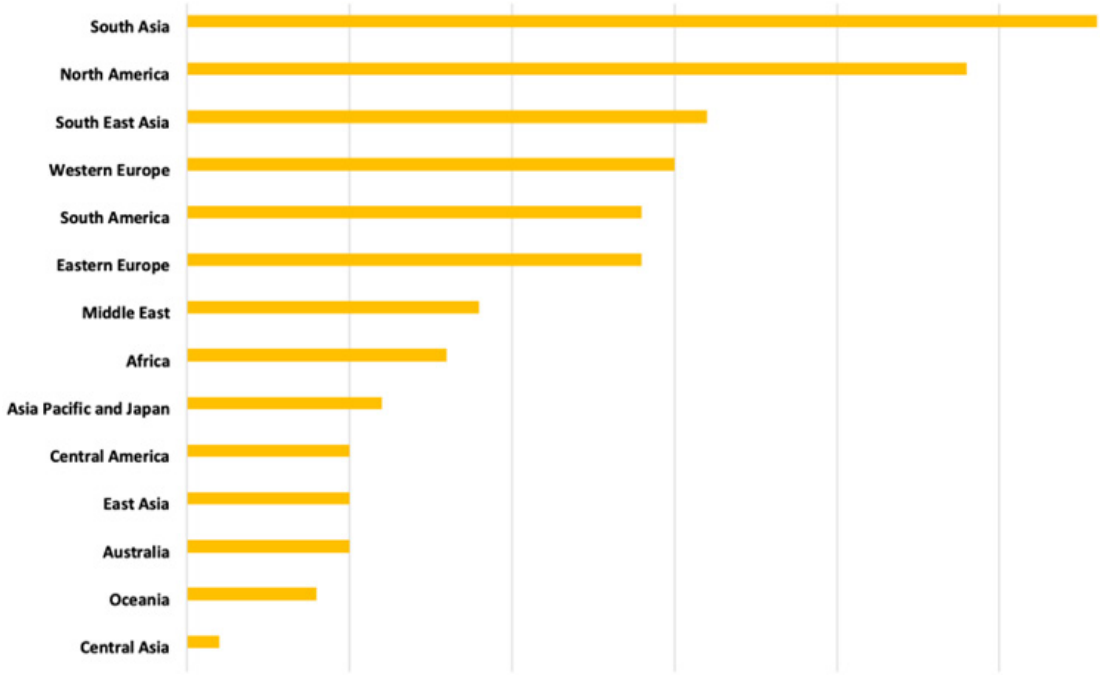

Figure 8: Geographical distribution of target organizations within the government sector

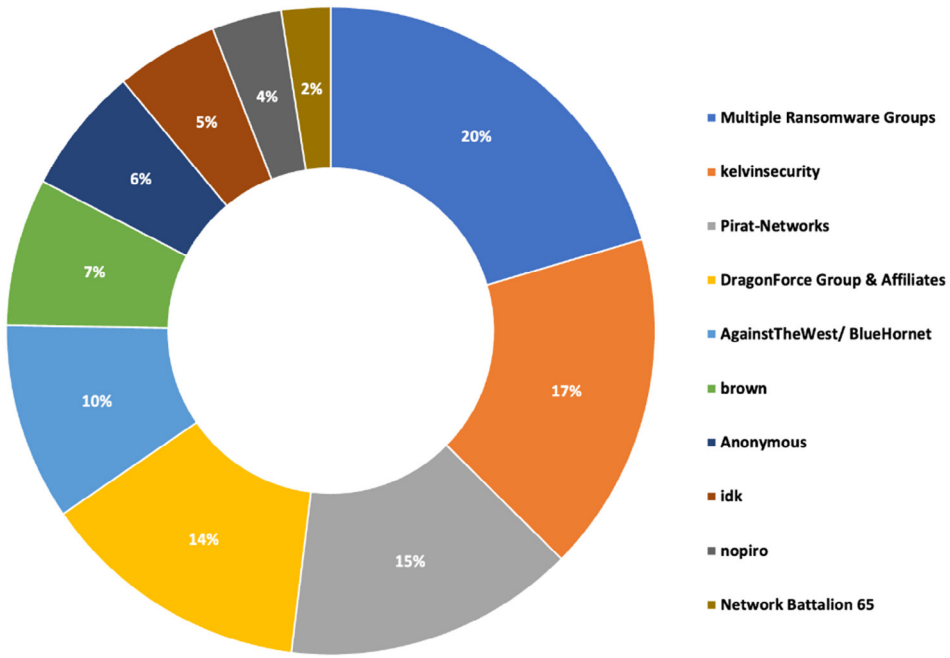

Figure 9: Top 10 threat actors targeting the government sector

2.2.4. Technology

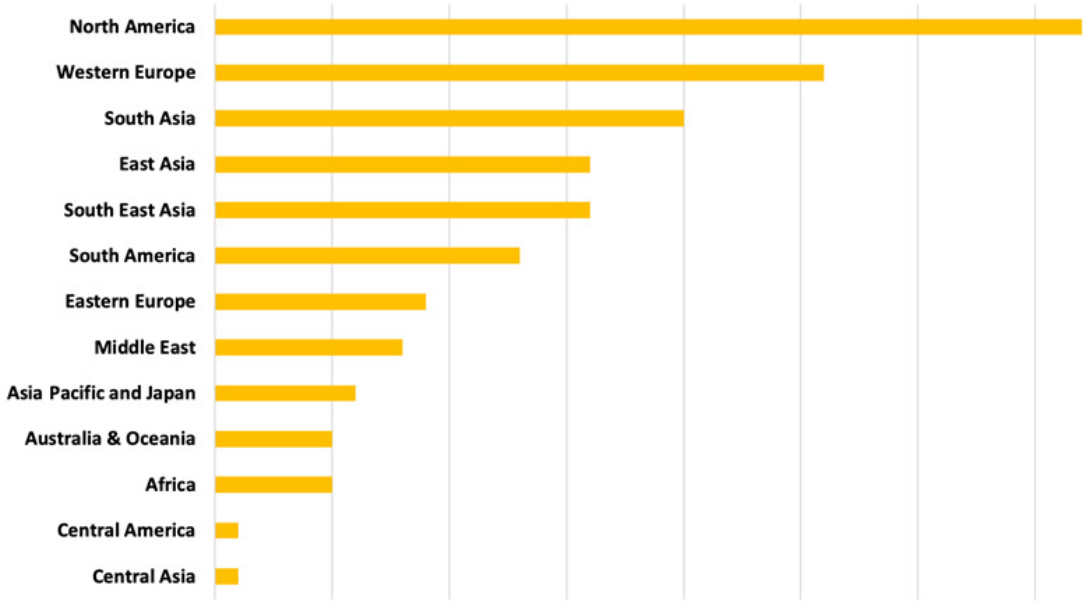

Figure 10: Geographical distribution of target organizations within the technology sector

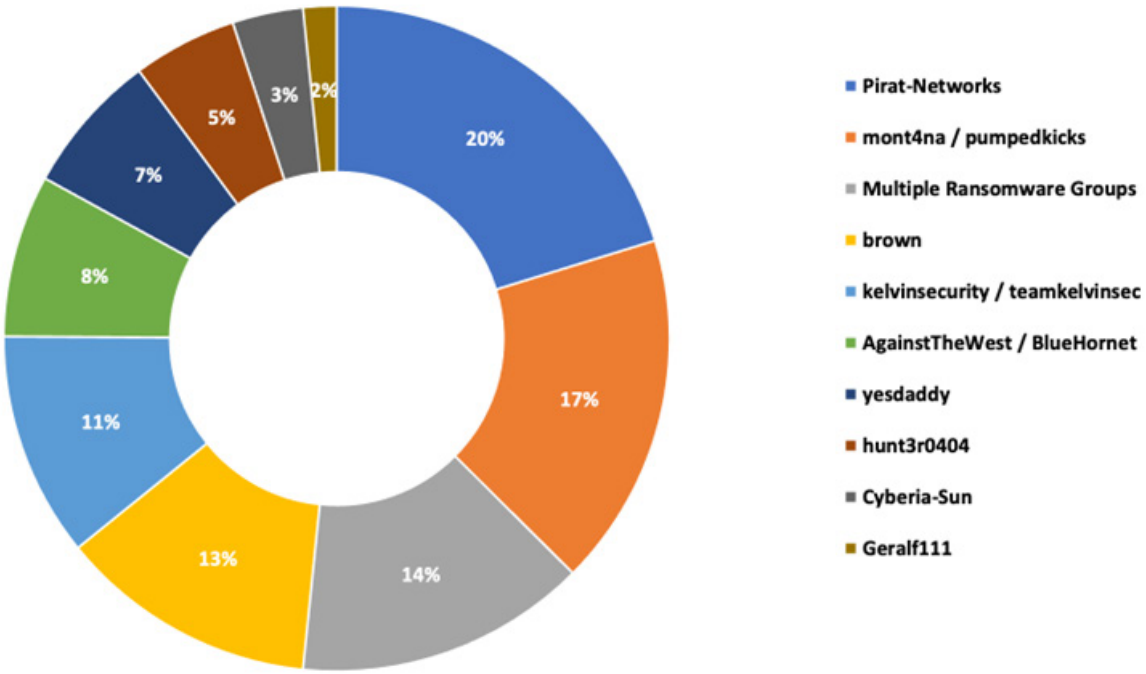

Figure 11: Top 10 threat actors targeting the technology sector

2.2.5. Professional Services

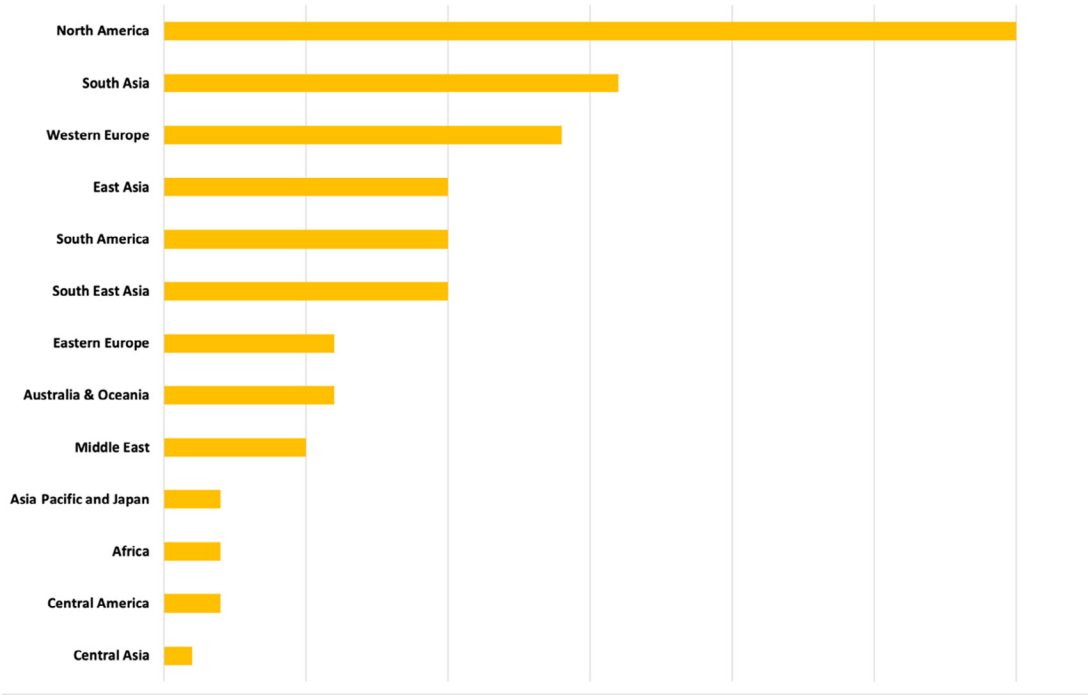

Figure 12: Geographical distribution of target organizations within the professional services sector

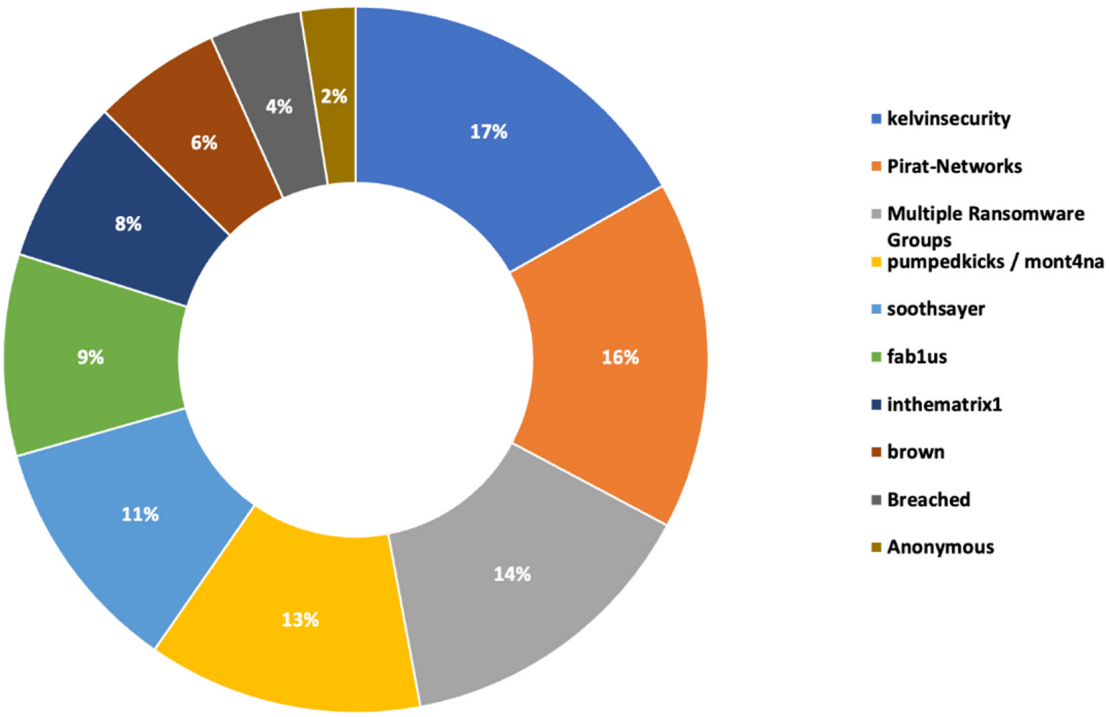

Figure 13: Top 10 threat actors targeting the professional services sector

2.2.6. Telecommunications

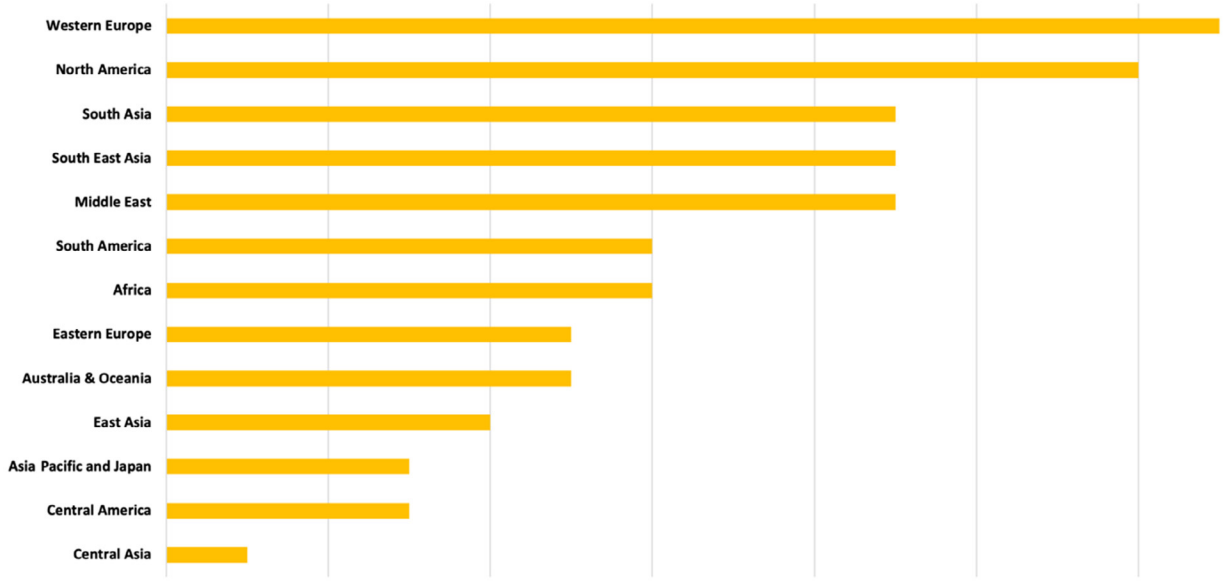

Figure 14: Geographical distribution of target organizations within the telecommunications sector

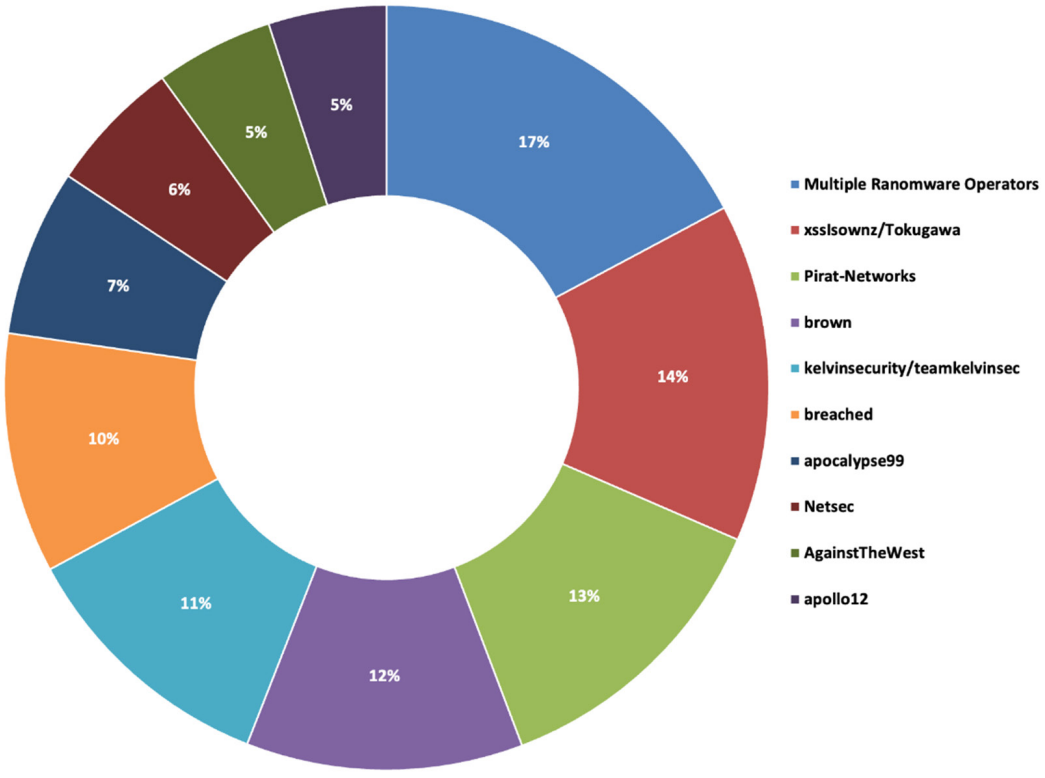

Figure 15: Top 10 threat actors targeting the telecommunications sector

2.2.7. Education

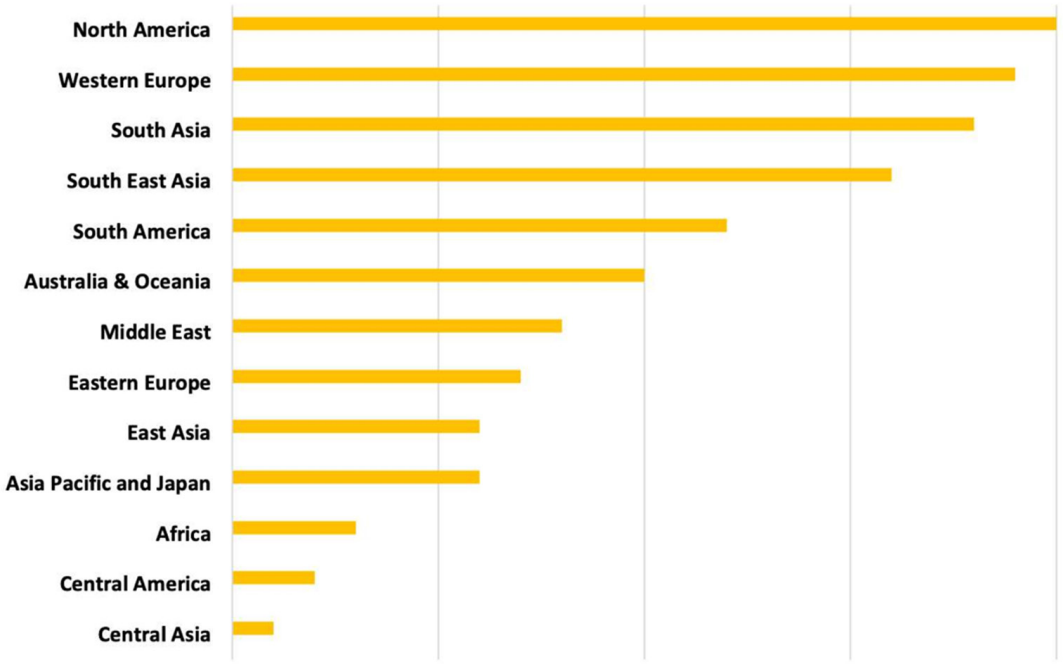

Figure 16: Geographical distribution of target organizations within the education sector

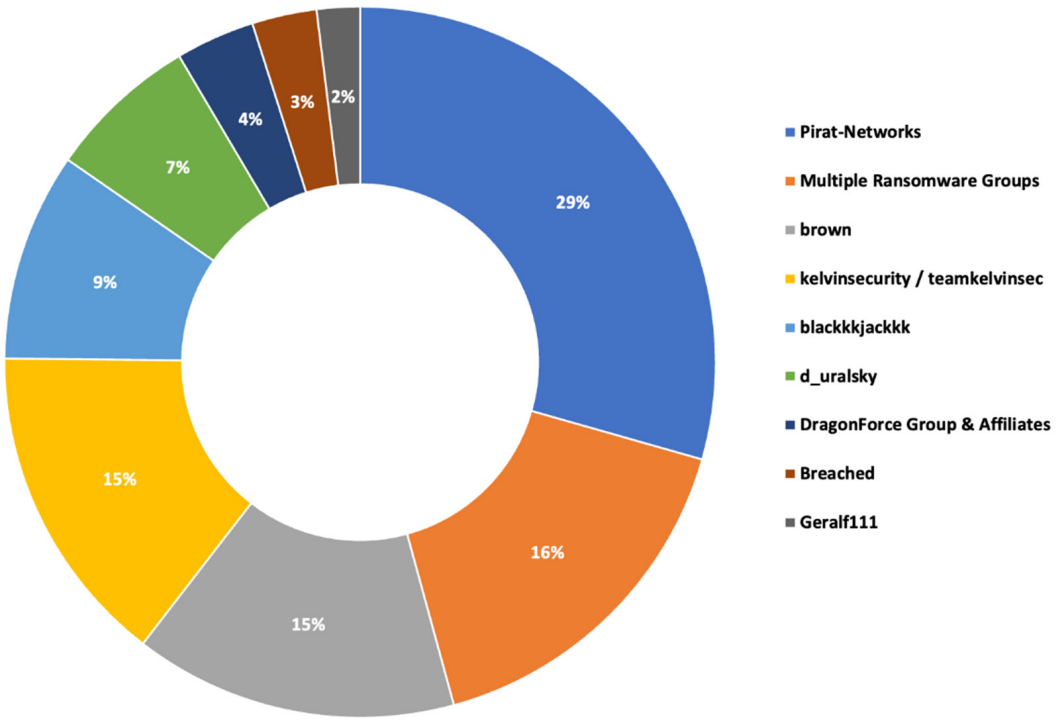

Figure 17: Top 10 threat actors targeting the education sector

2.2.8. Energy and Utilities

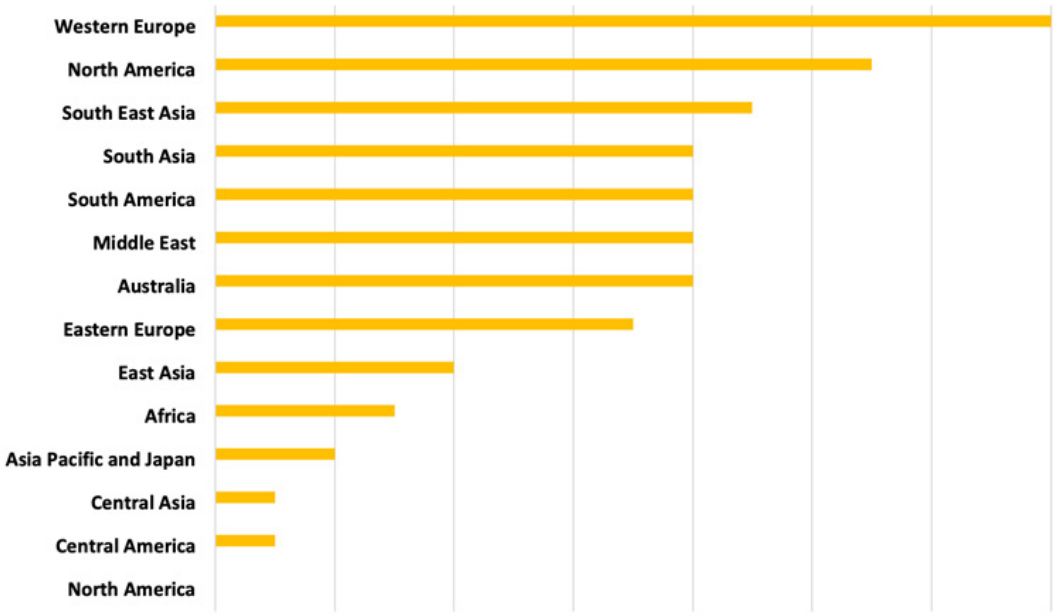

Figure 18: Geographical distribution of target organizations within the energy and utilities sector

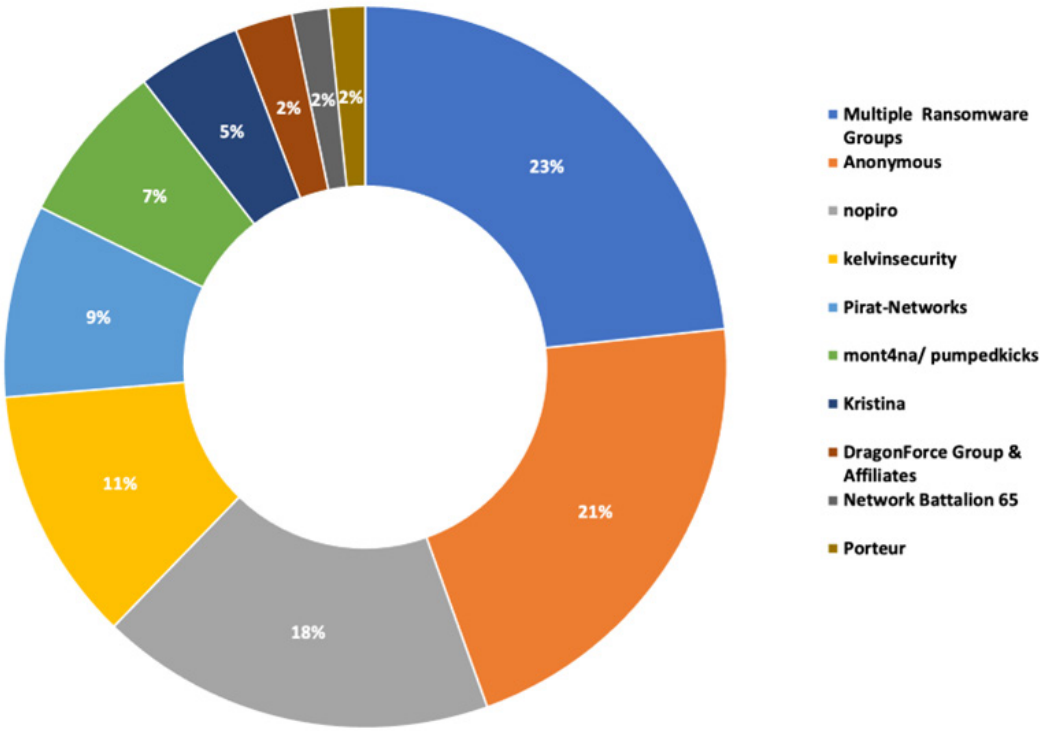

Figure 19: Top 10 threat actors targeting the energy and utilities sector

2.2.9. Consultation Services

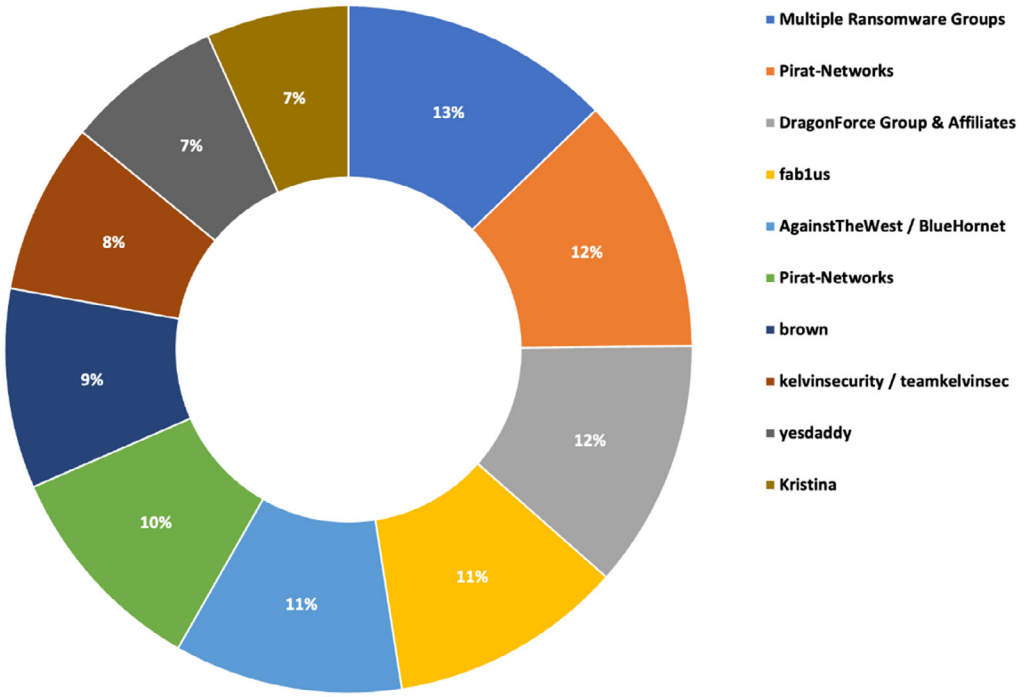

Figure 20: Geographical distribution of target organizations within the consultation services sector

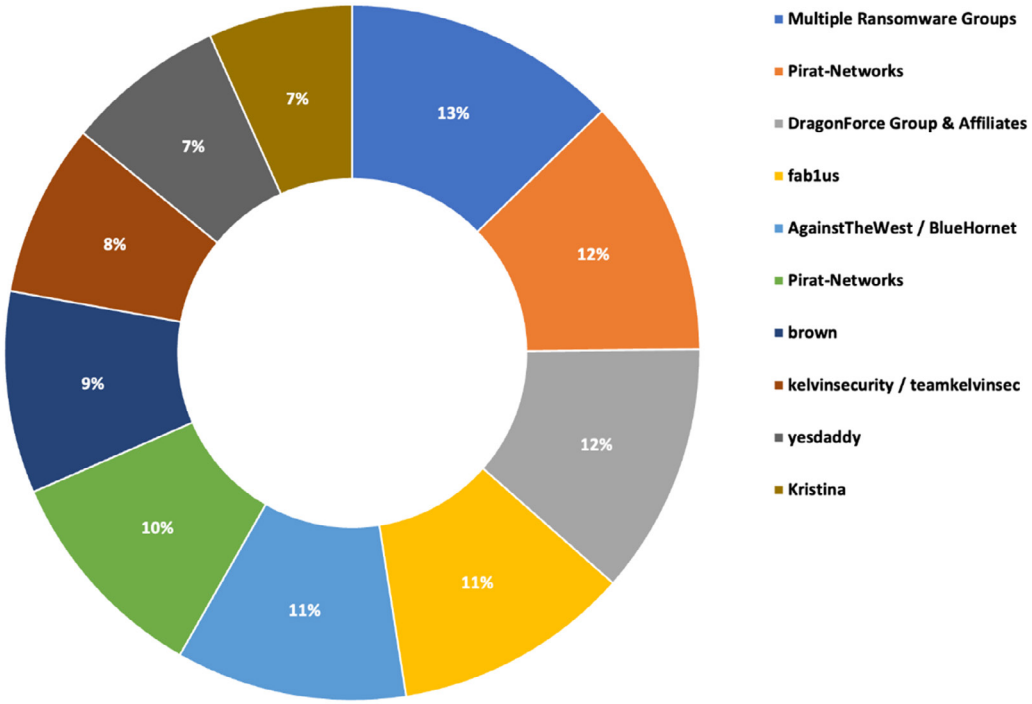

Figure 21: Top 10 threat actors targeting the consultation services sector

2.2.10. Retail

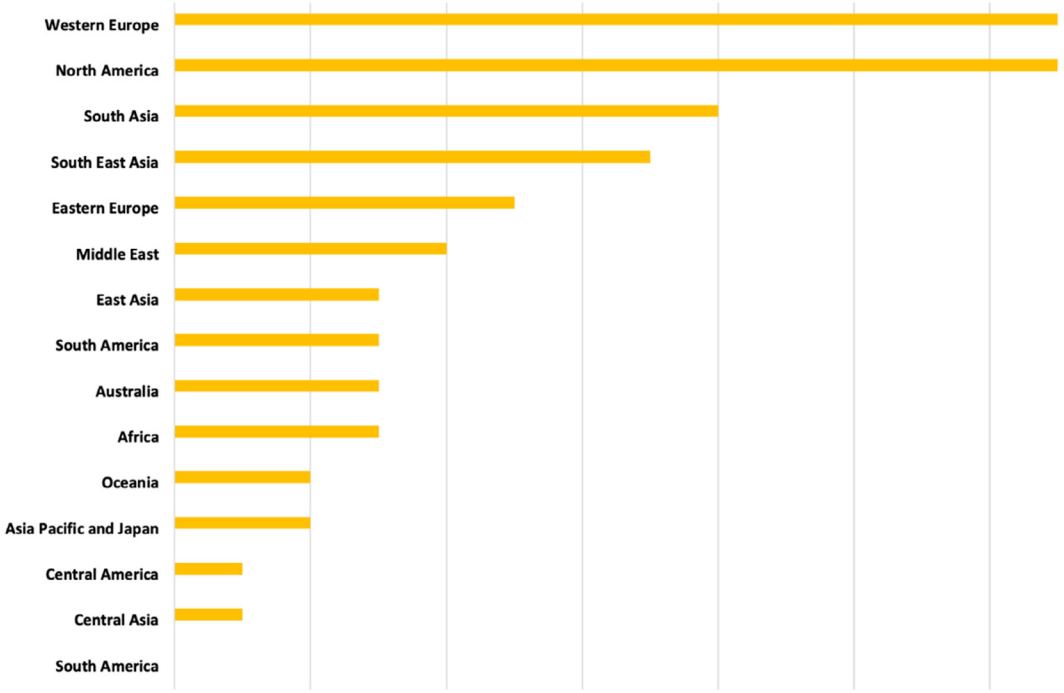

Figure 22: Geographical distribution of target organizations within the retail sector

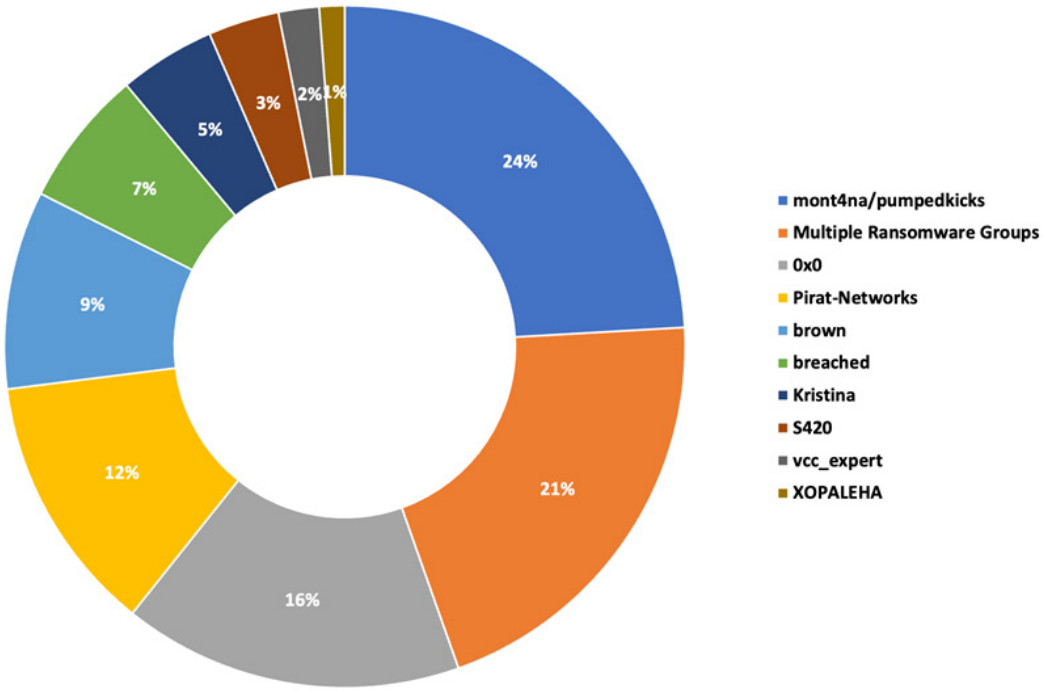

Figure 23: Top 10 threat actors targeting the retail sector

2.2.11. Natural Resources

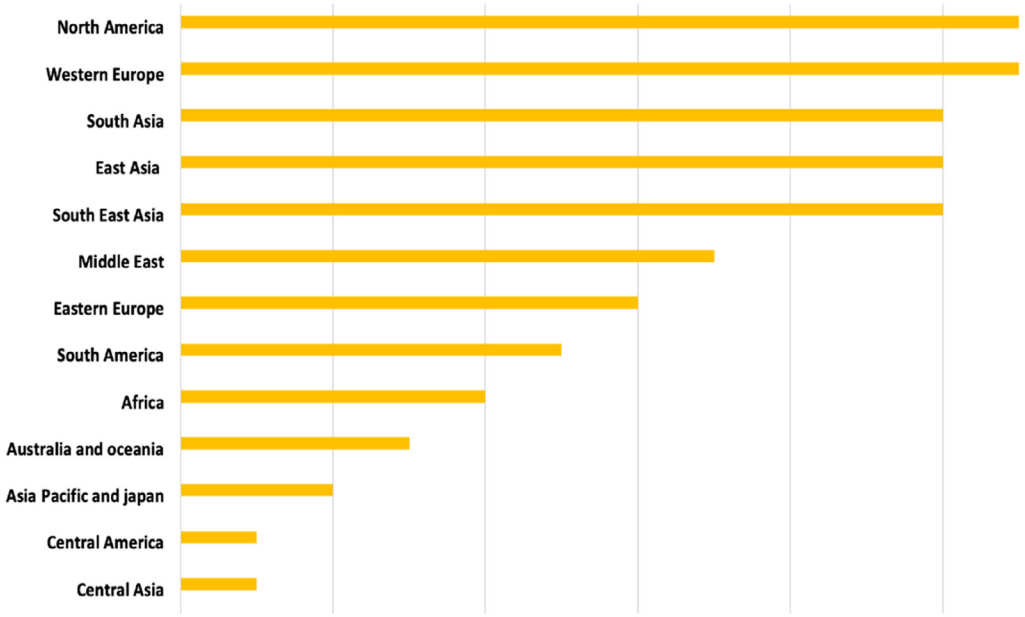

Figure 24: Geographical distribution of target organizations within the natural resources sector

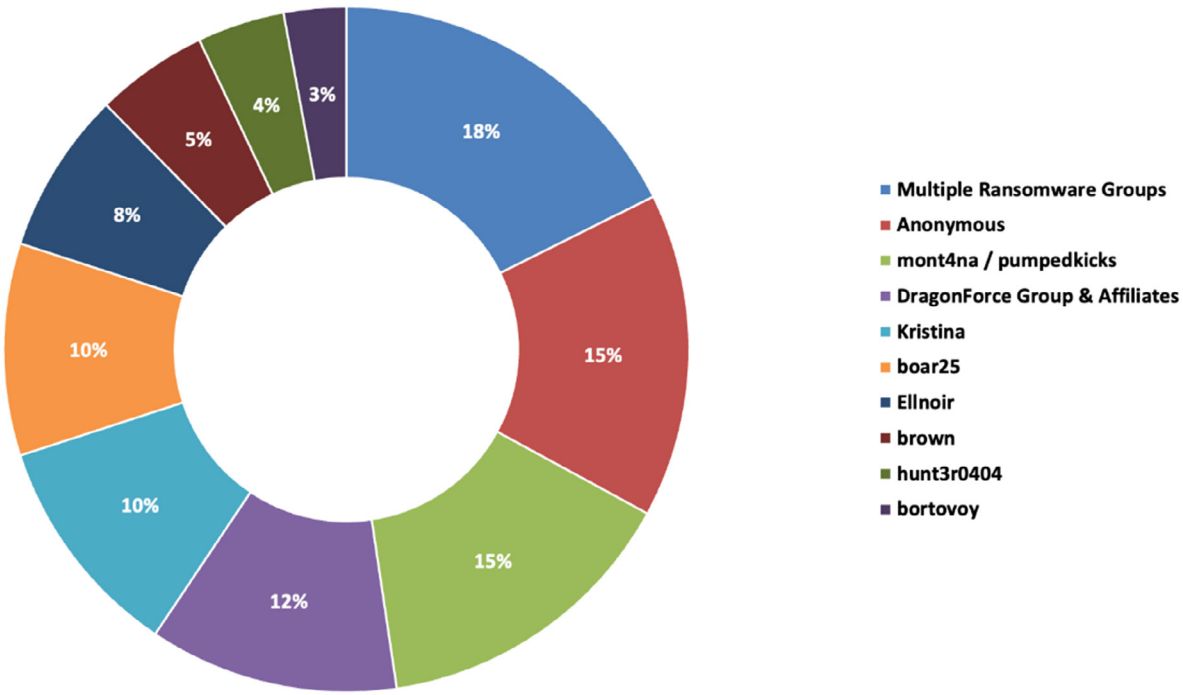

Figure 25: Top 10 threat actors targeting the natural resources sector

2.2.12. Healthcare

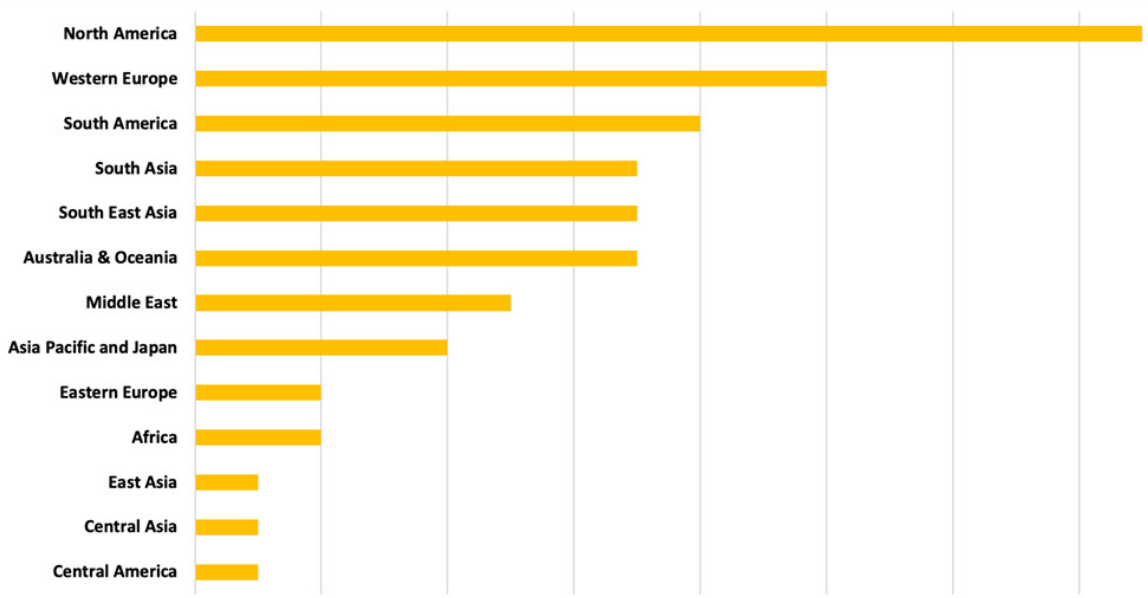

Figure 26: Geographical distribution of target organizations within the healthcare sector

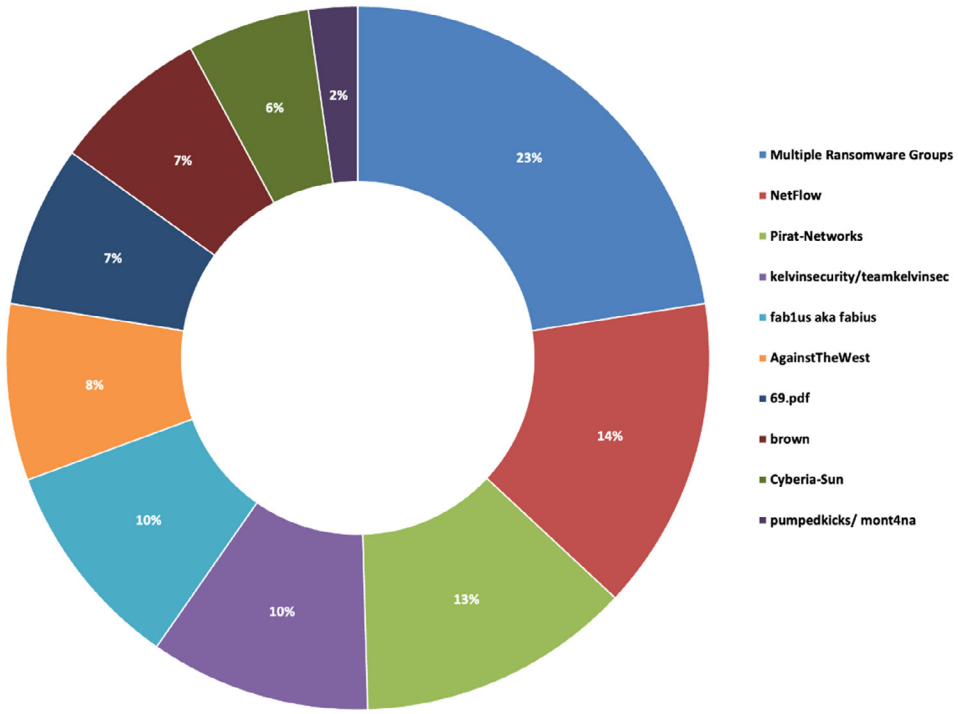

Figure 27: Top 10 threat actors targeting the healthcare sector

2.2.13. Construction and Engineering

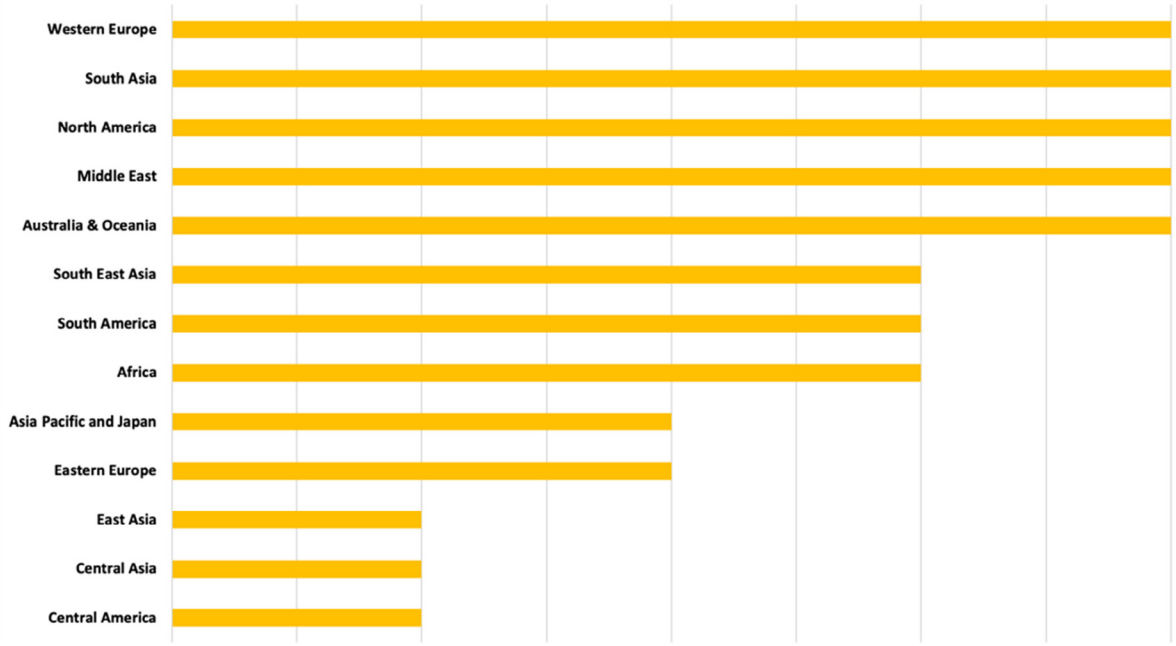

Figure 28: Geographical distribution of target organizations within the construction and engineering sector

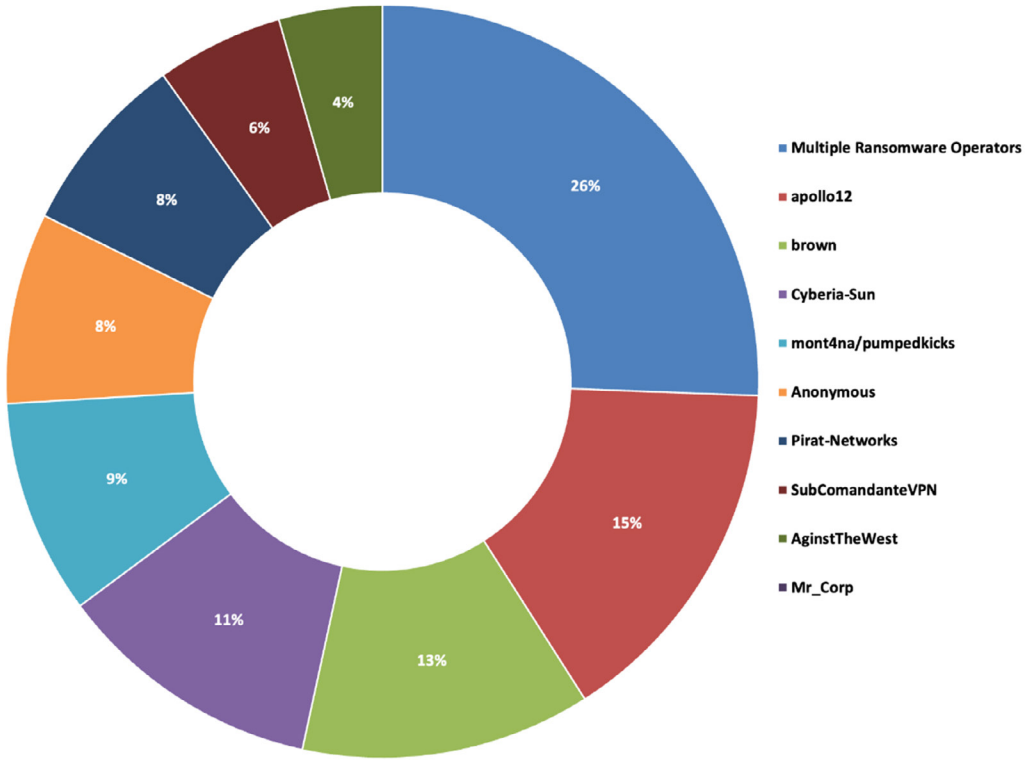

Figure 29: Top 10 threat actors targeting the construction and engineering sector

2.2.14. Transportation

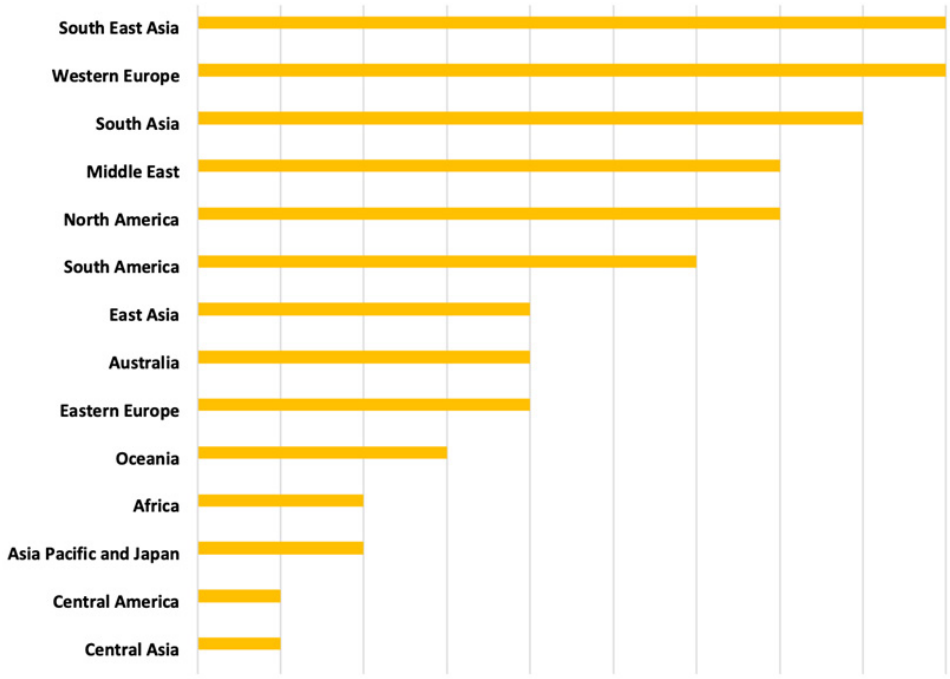

Figure 30: Geographical distribution of target organizations within the transportation sector

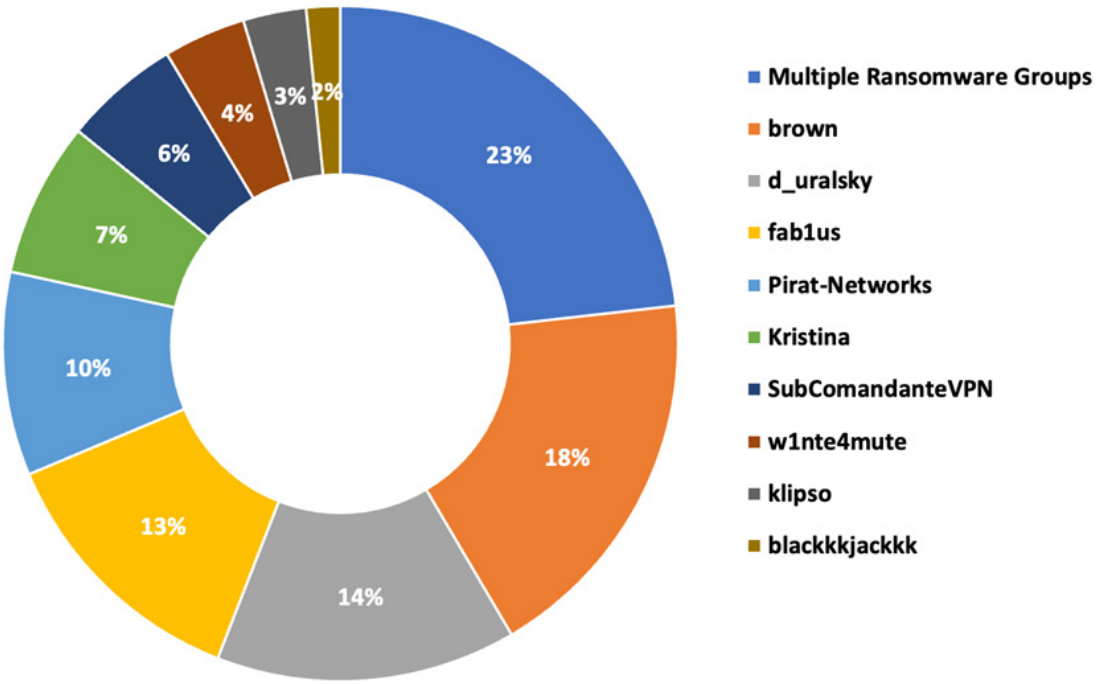

Figure 31: Top 10 threat actors targeting the transportation sector

2.2.15. Food and Beverages

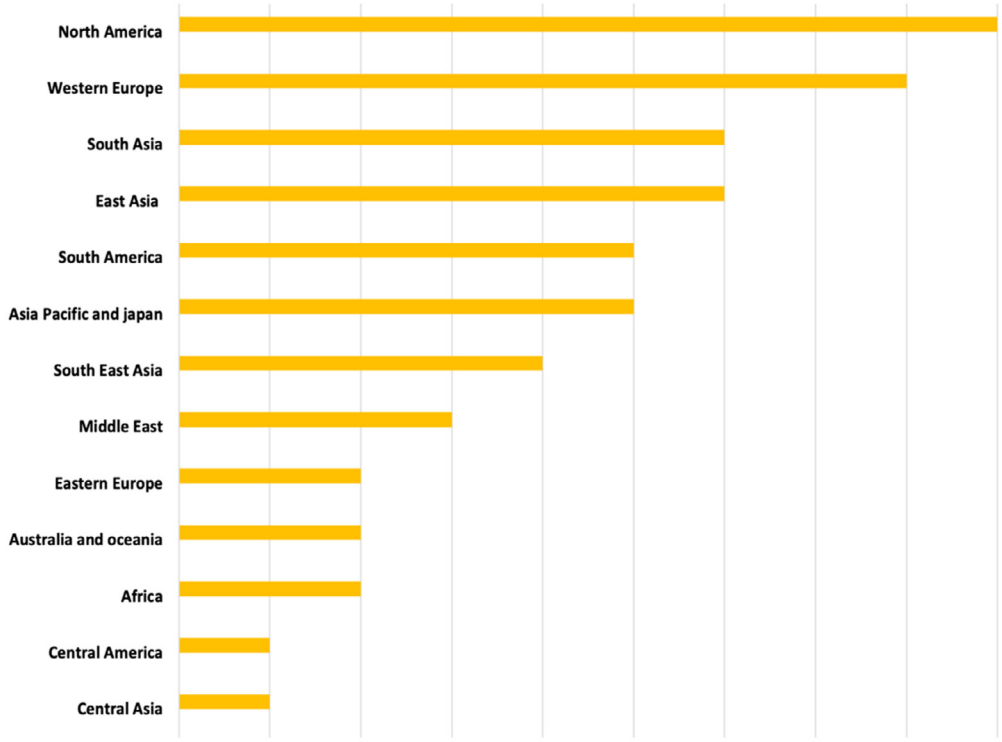

Figure 32: Geographical distribution of target organizations within the food and beverages sector

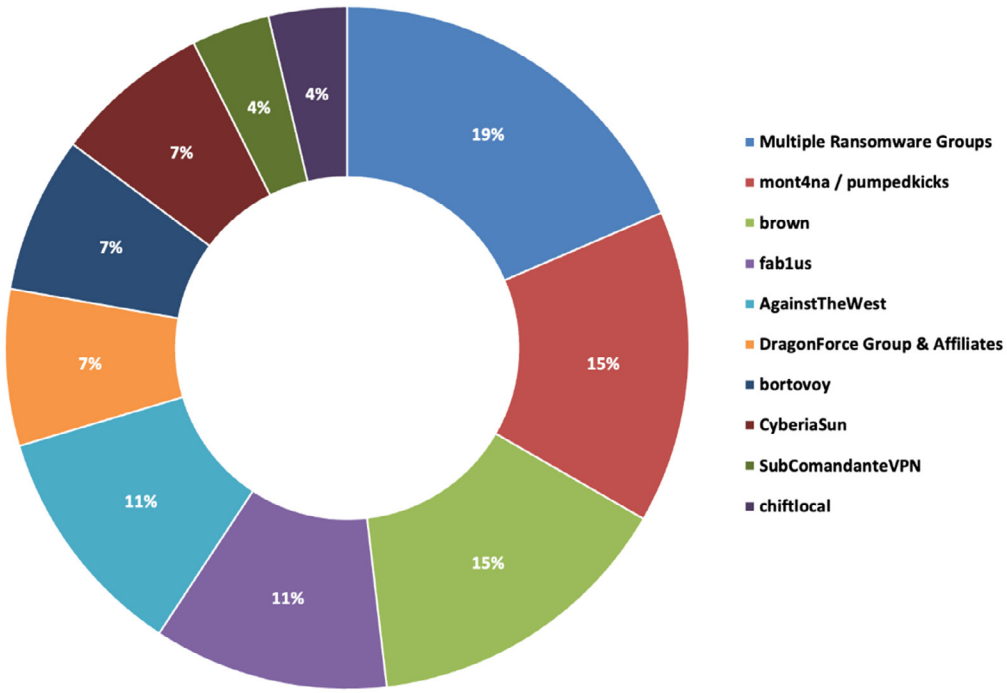

Figure 33: Top 10 threat actors targeting the food and beverages sector

2.2.16. Consumer Services

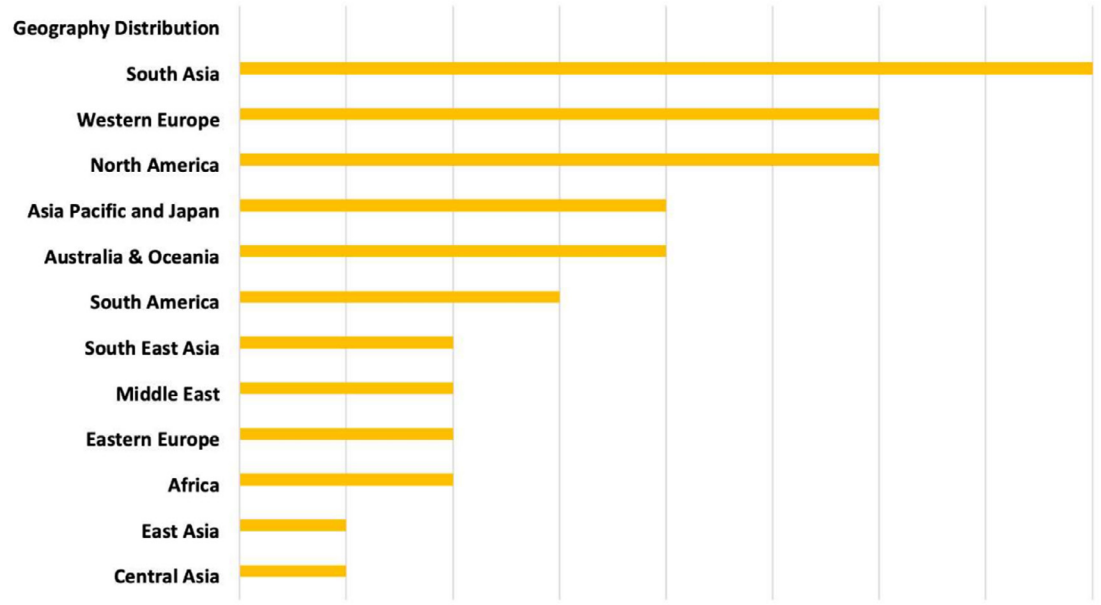

Figure 34: Geographical distribution of target organizations within the consumer services sector

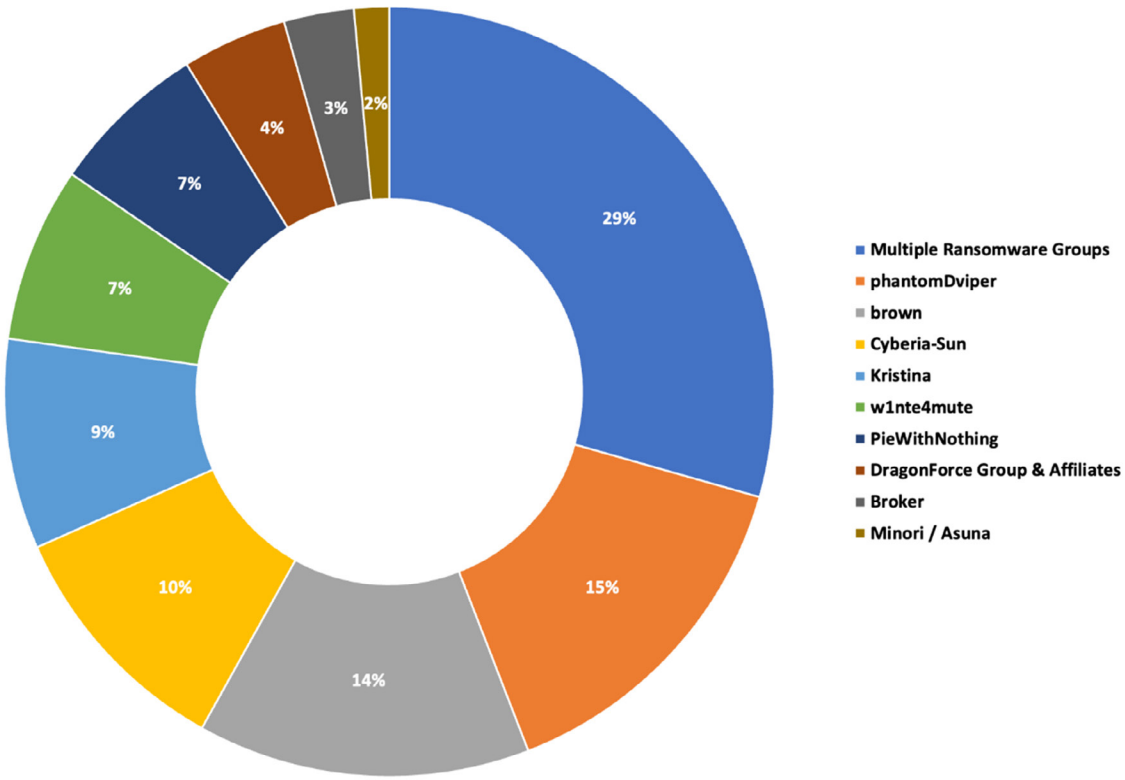

Figure 35: Top 10 threat actors targeting the consumer services sector

2.2.17. Delivery and Logistics

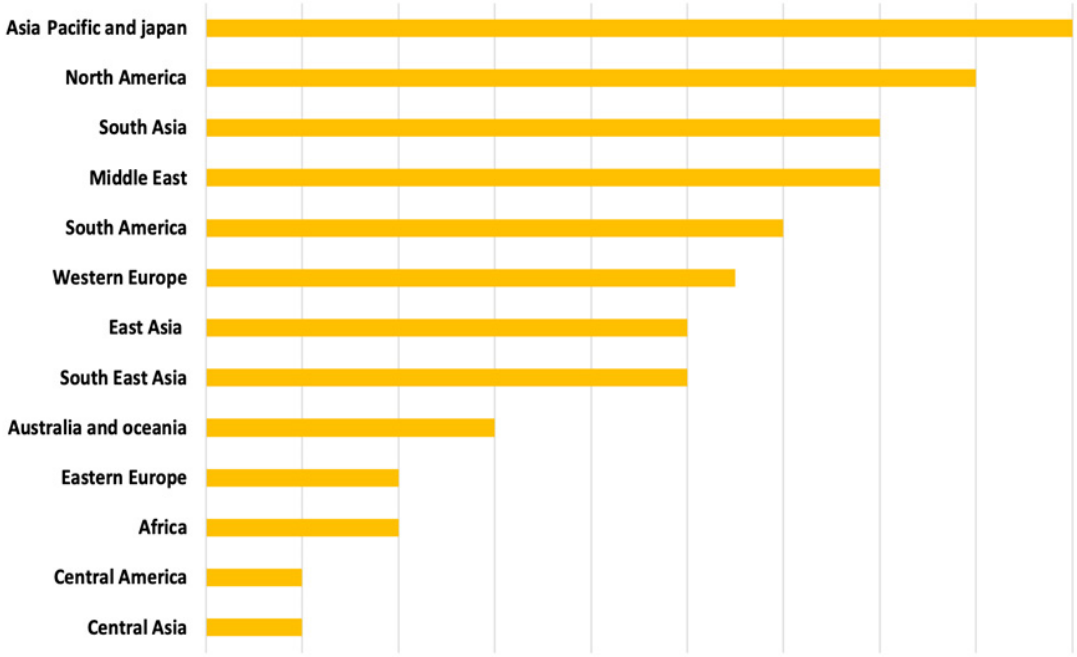

Figure 36: Geographical distribution of target organizations within the delivery and logistics sector

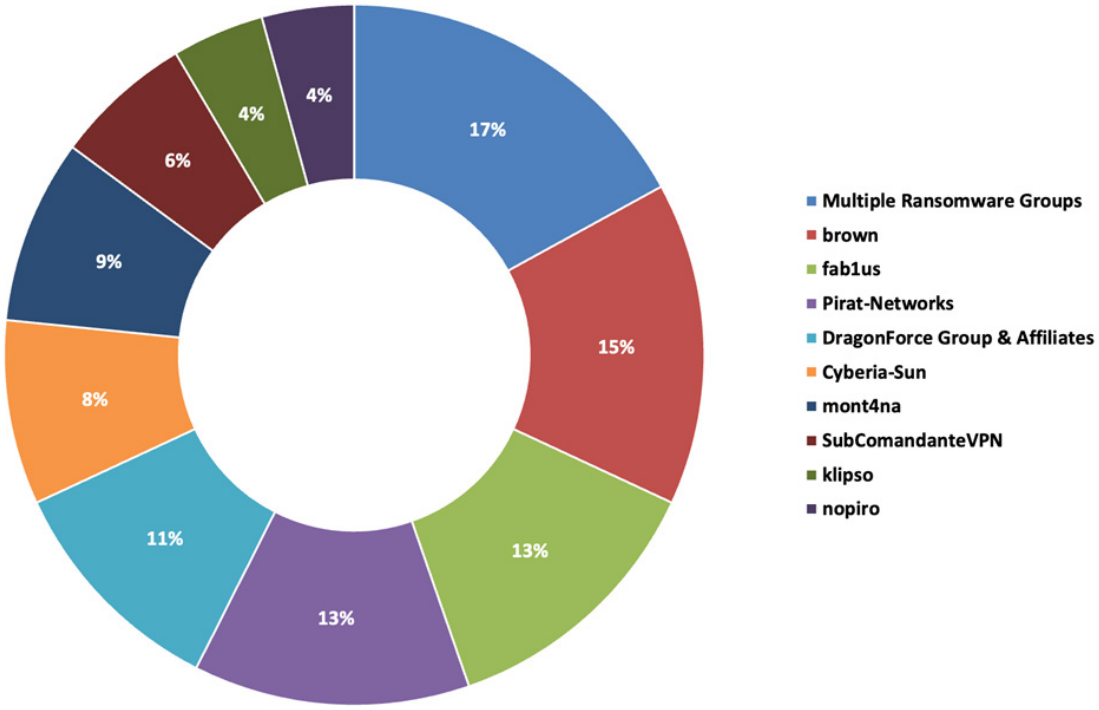

Figure 37: Top 10 threat actors targeting the delivery and logistics sector

2.2.18. Pharmaceuticals

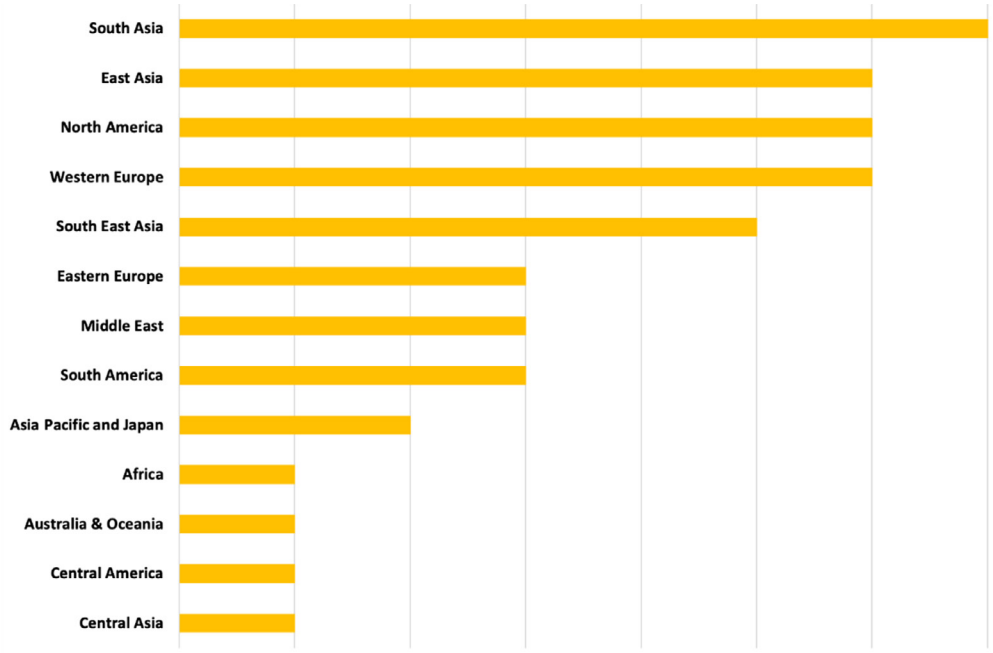

Figure 38: Geographical distribution of target organizations within the pharmaceuticals sector

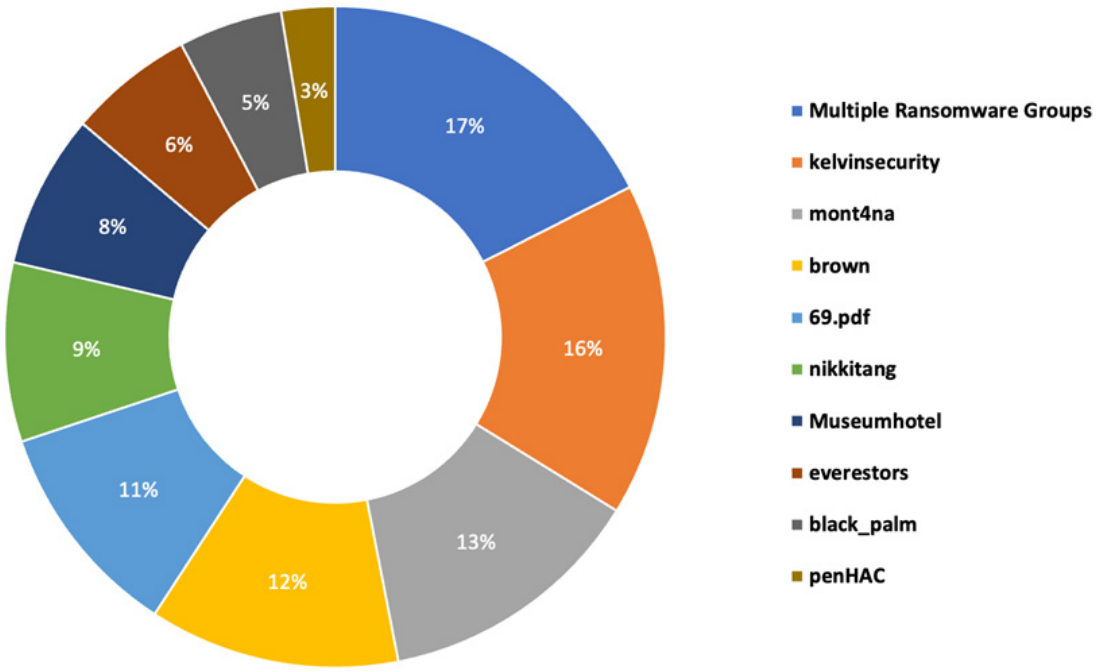

Figure 39: Top 10 threat actors targeting the pharmaceuticals sector

2.2.19. E-Commerce

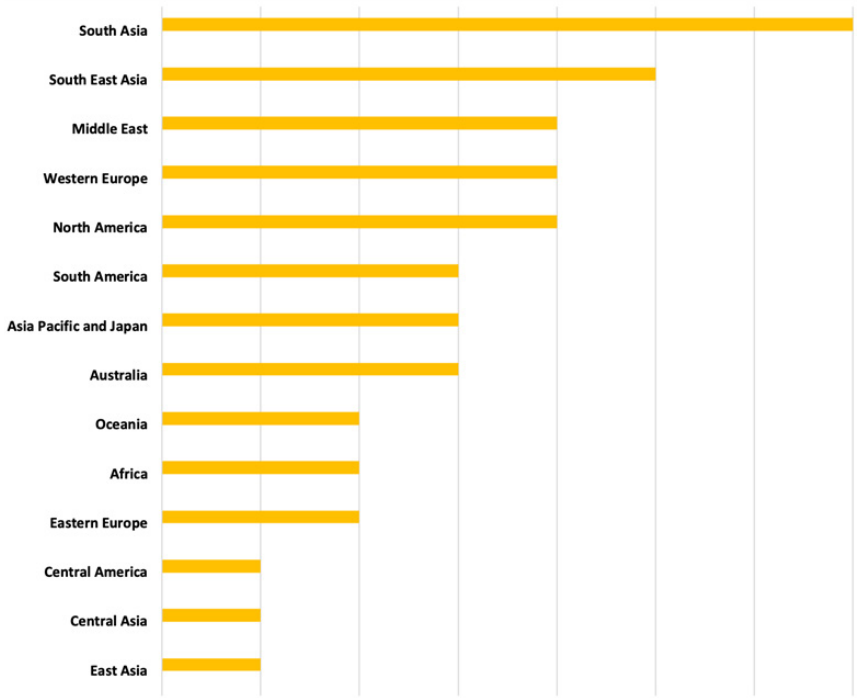

Figure 40: Geographical distribution of target organizations within the e-commerce sector

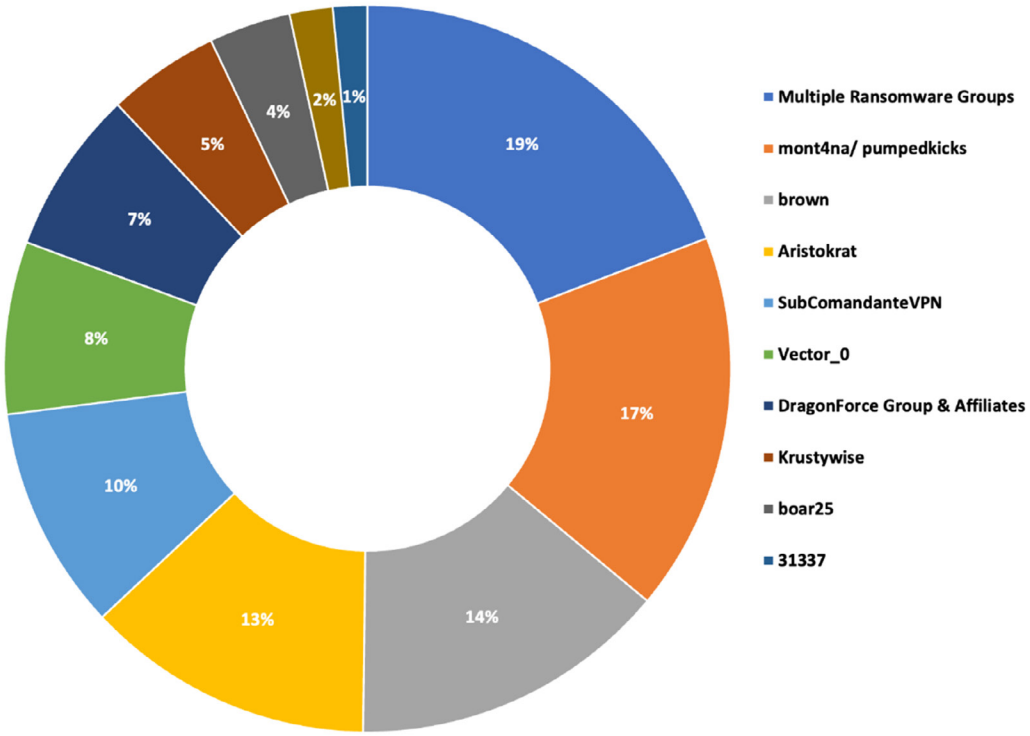

Figure 41: Top 10 threat actors targeting the e-commerce sector

2.2.20. Automotive

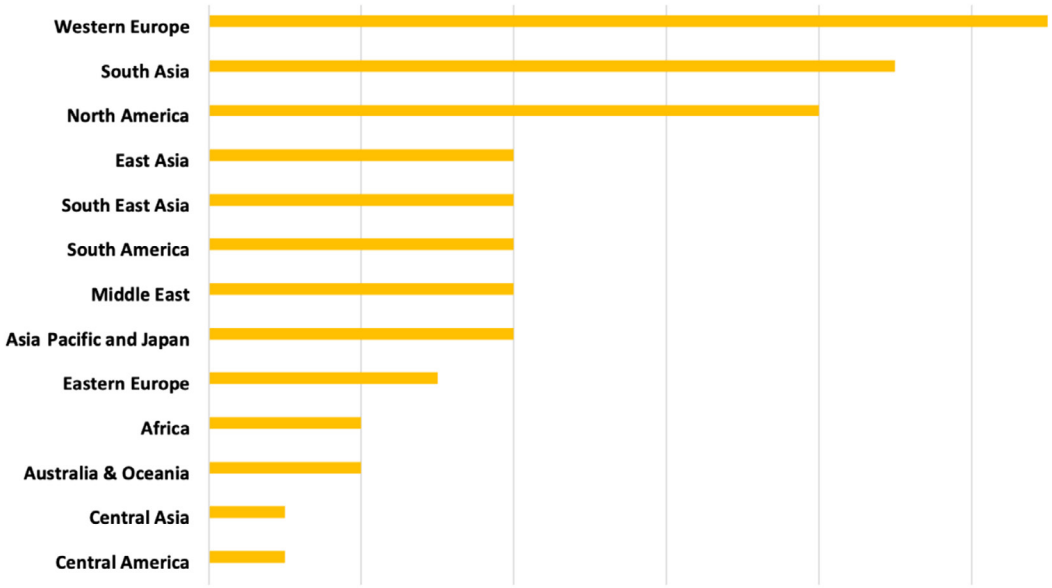

Figure 42: Geographical distribution of target organizations within the automotive sector

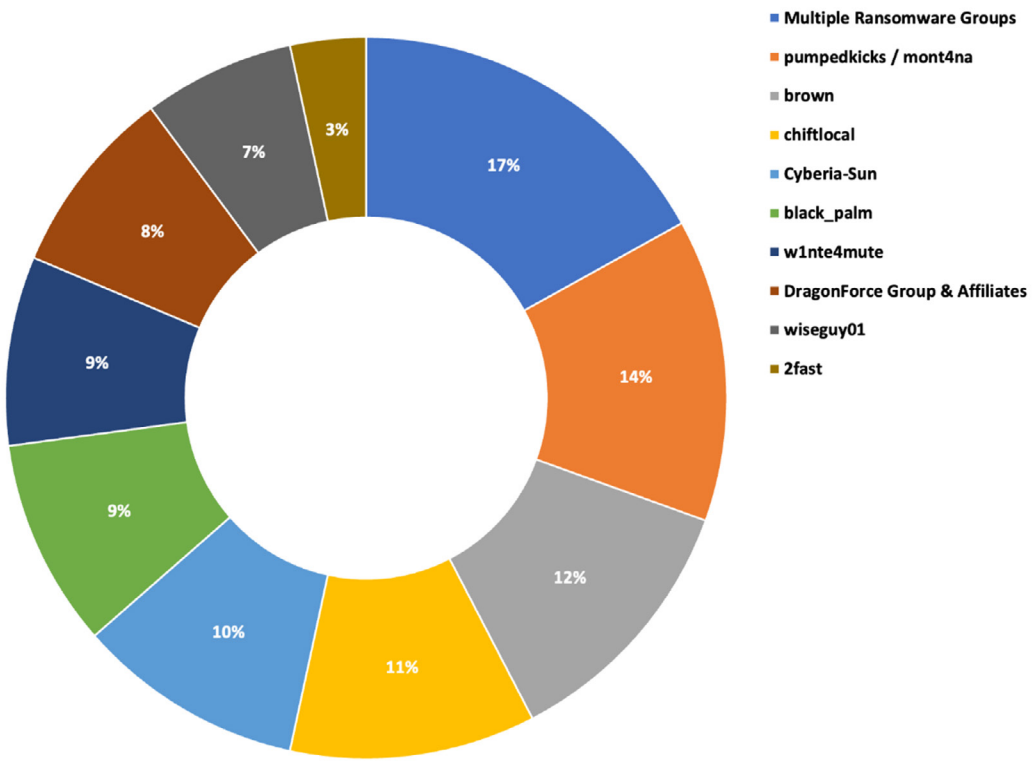

Figure 43: Top 10 threat actors targeting the automotive sector

2.2.21. Media

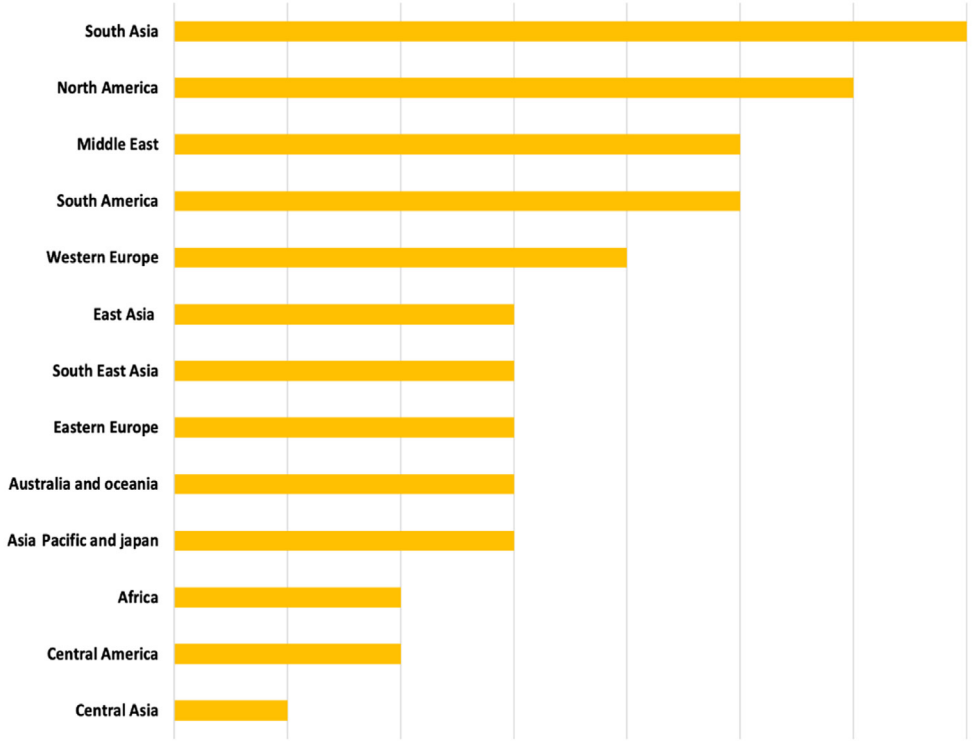

Figure 44: Geographical distribution of target organizations within the media sector

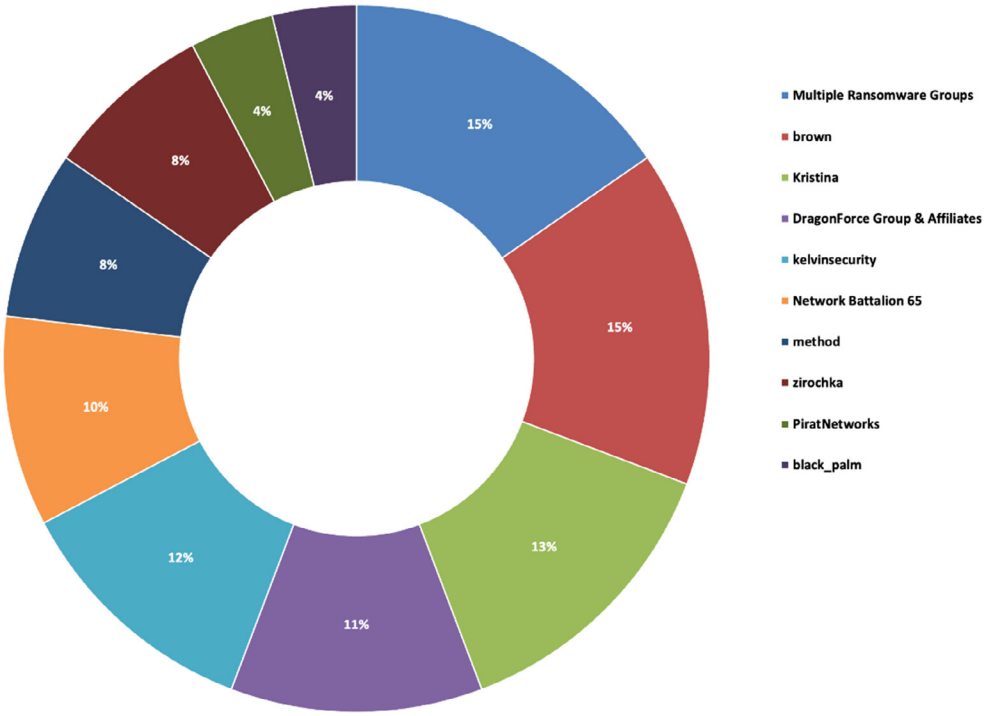

Figure 45: Top 10 threat actors targeting the media sector

2.2.22. Real Estate

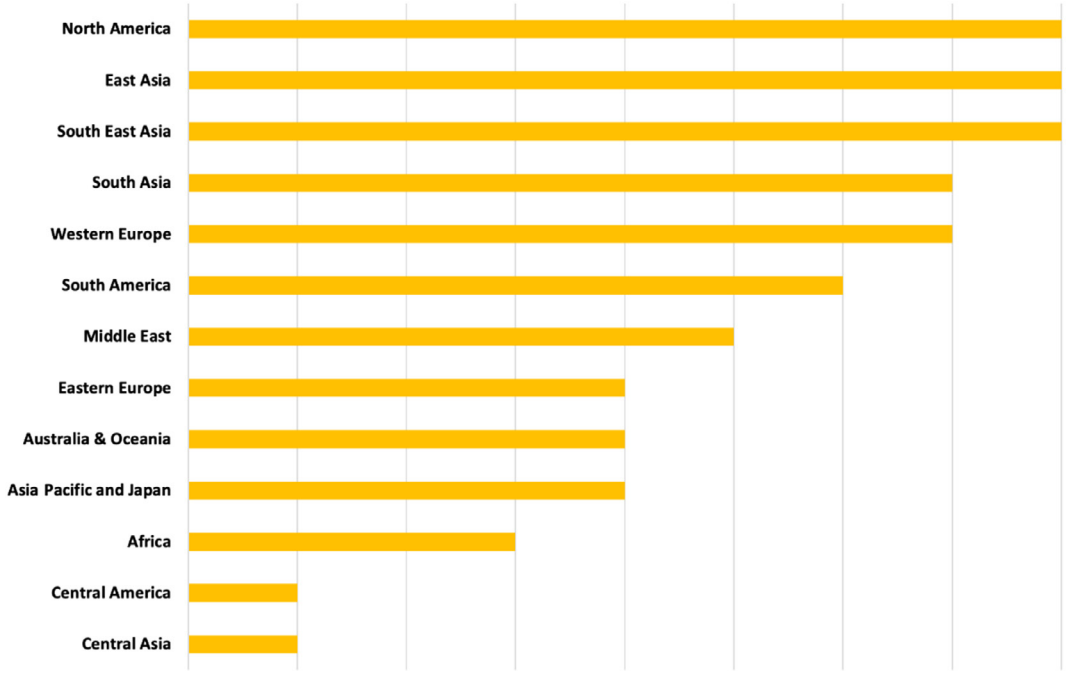

Figure 46: Geographical distribution of target organizations within the real estate sector

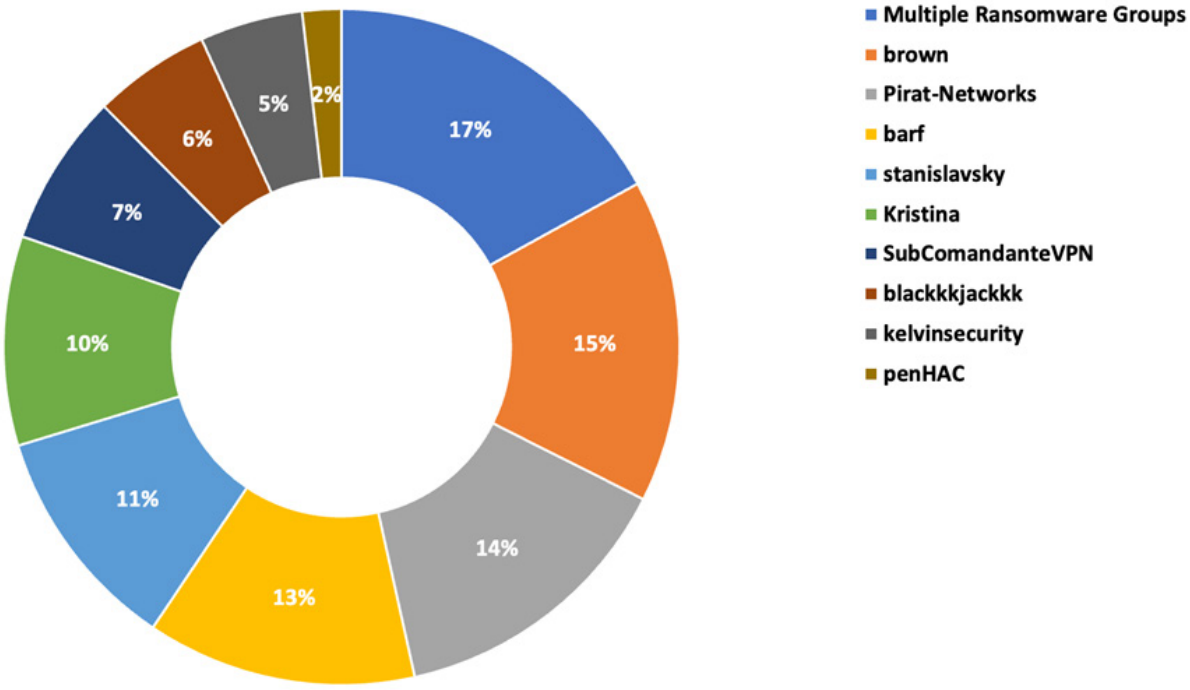

Figure 47: Top 10 threat actors targeting the real estate sector

2.2.23. Non-Profit

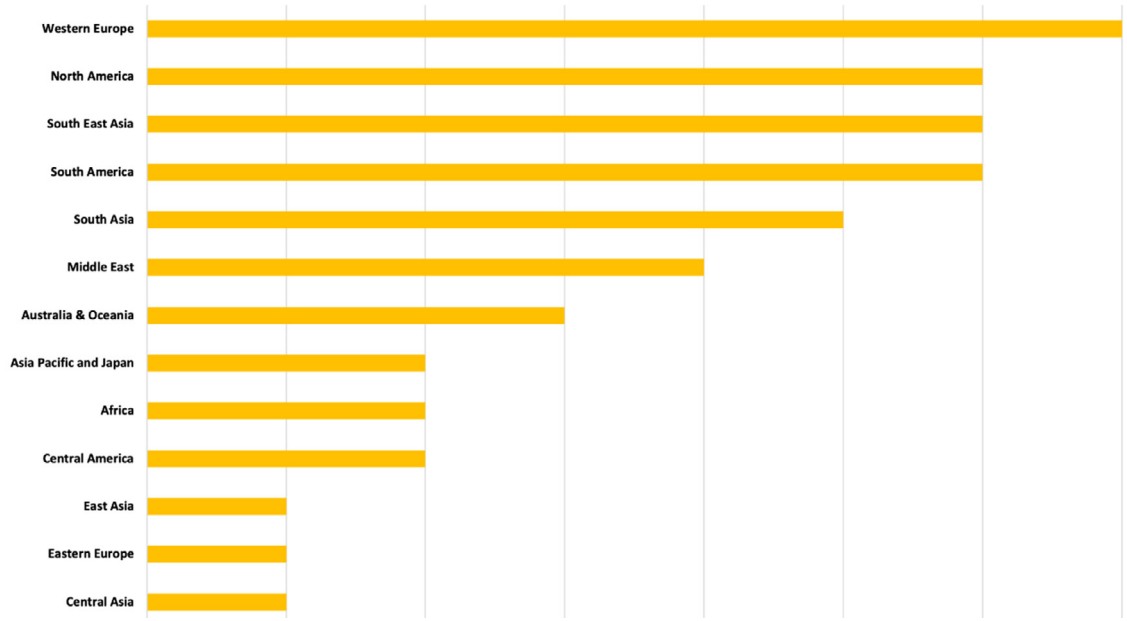

Figure 48: Geographical distribution of target non-profit organizations

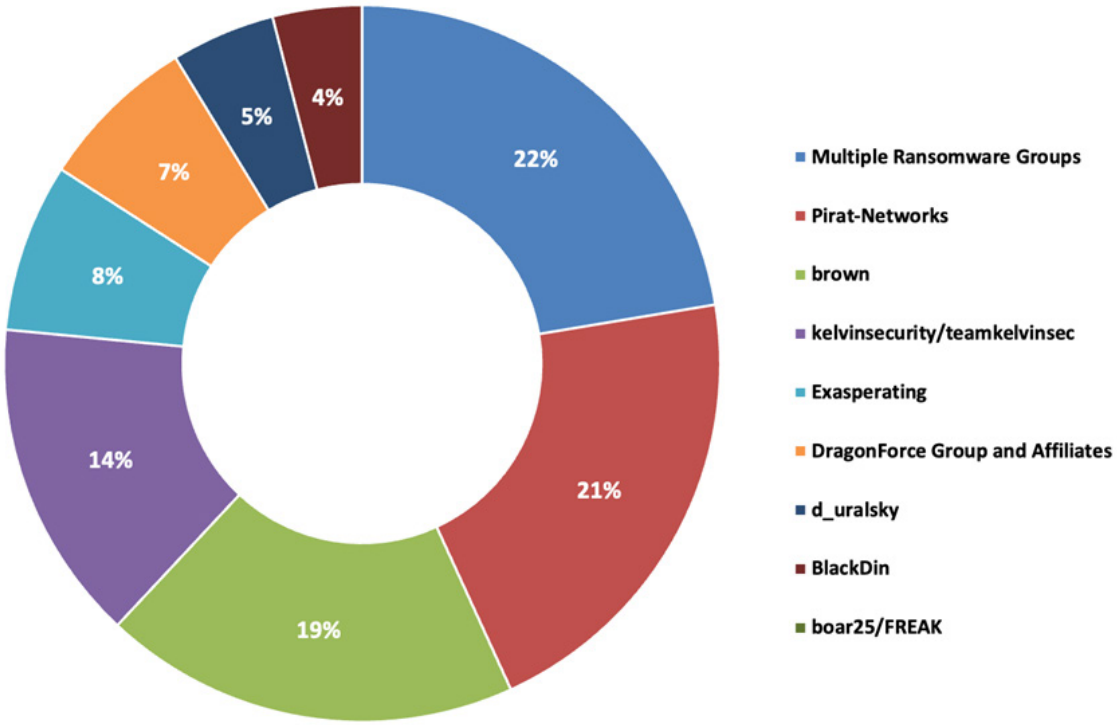

Figure 49: Top 10 threat actors targeting non-profit organizations

2.2.24. Critical Infrastructure

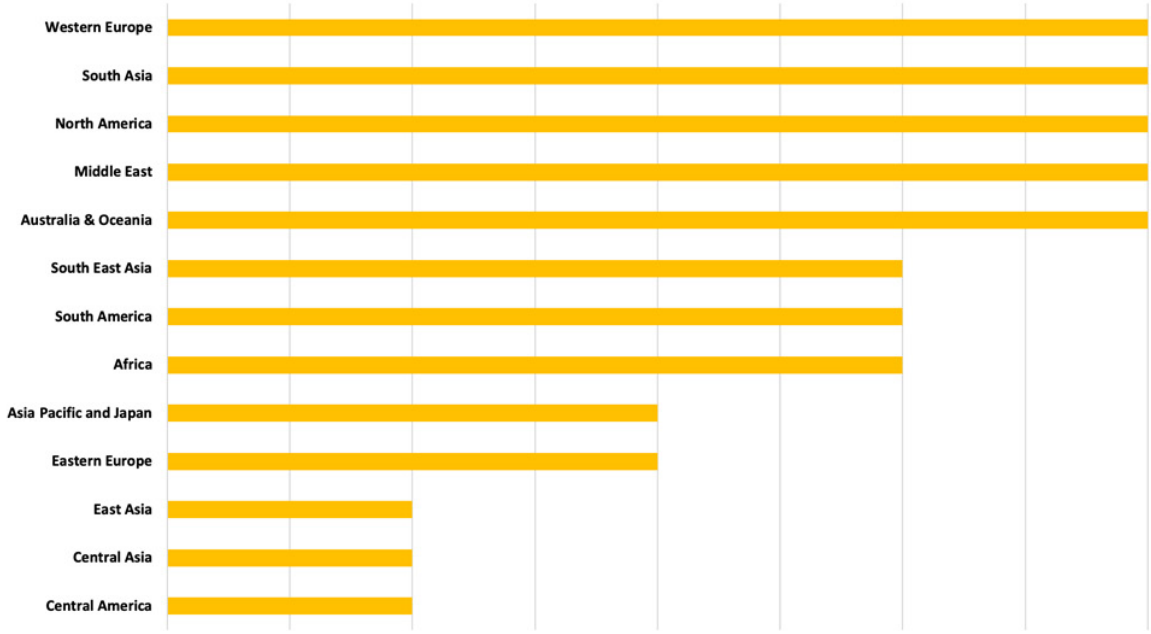

Figure 50: Geographical distribution of target organizations within the critical infrastructure sector

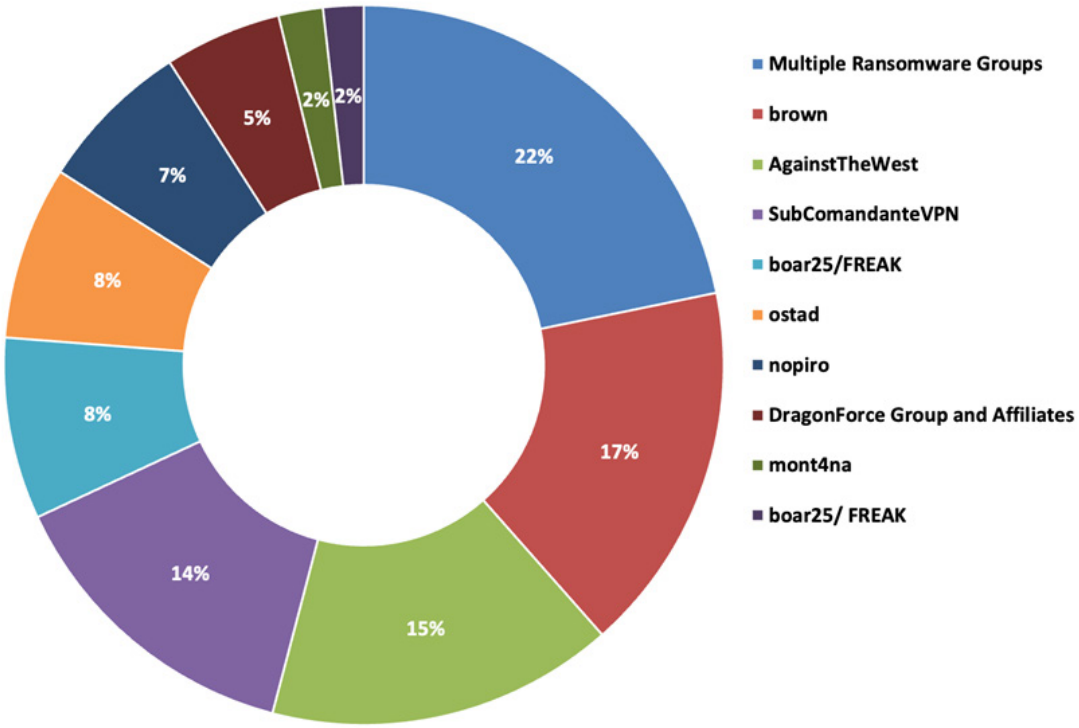

Figure 51: Top 10 threat actors targeting the critical infrastructure sector

2.2.25. Aerospace and Defense

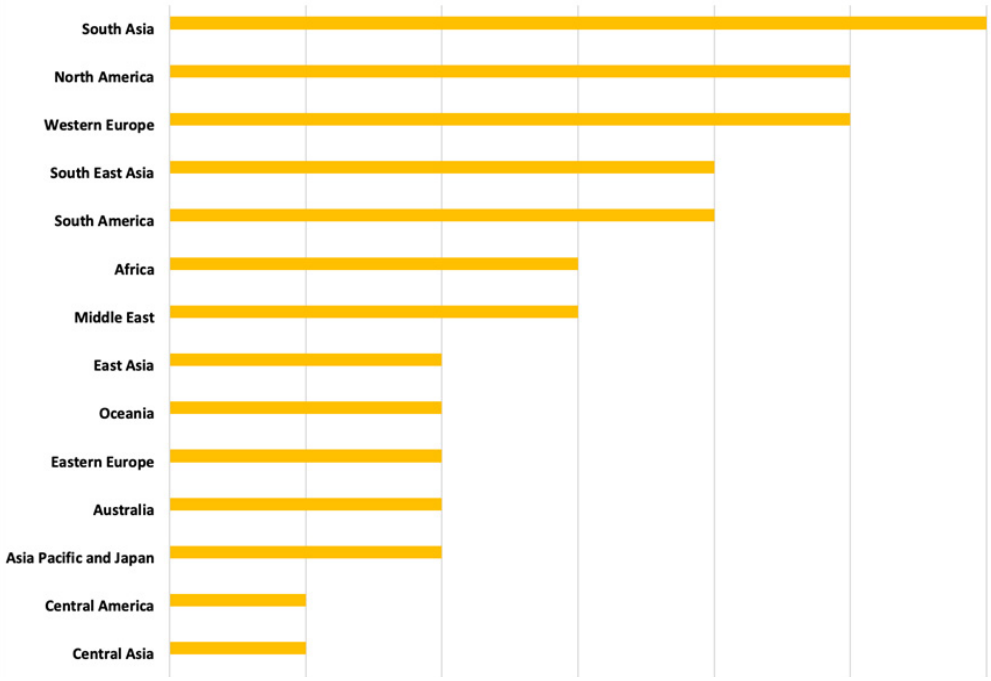

Figure 52: Geographical distribution of target organizations within the aerospace and defense sector

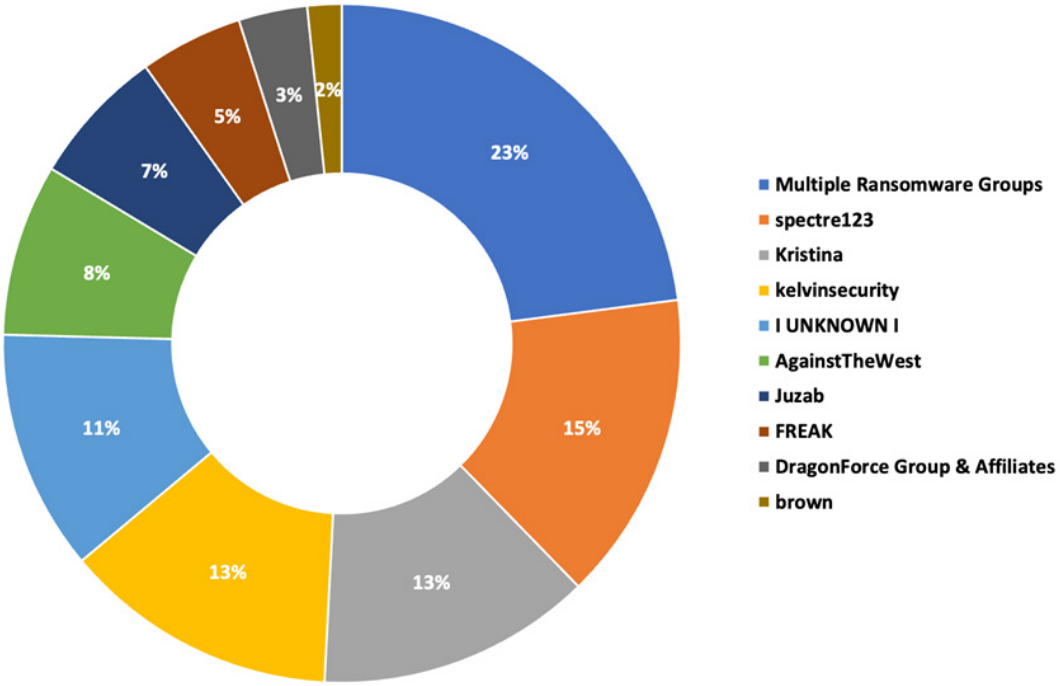

Figure 53: Top 10 threat actors targeting the aerospace and defense sector

2.2.26. Entertainment

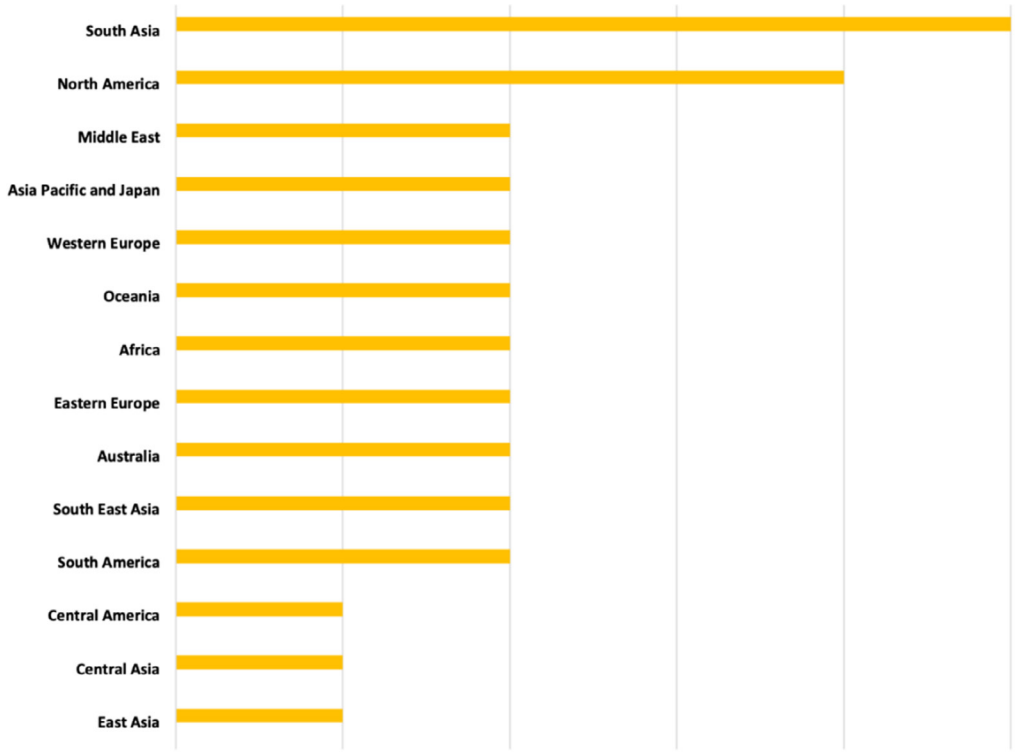

Figure 54: Geographical distribution of target organizations within the entertainment sector

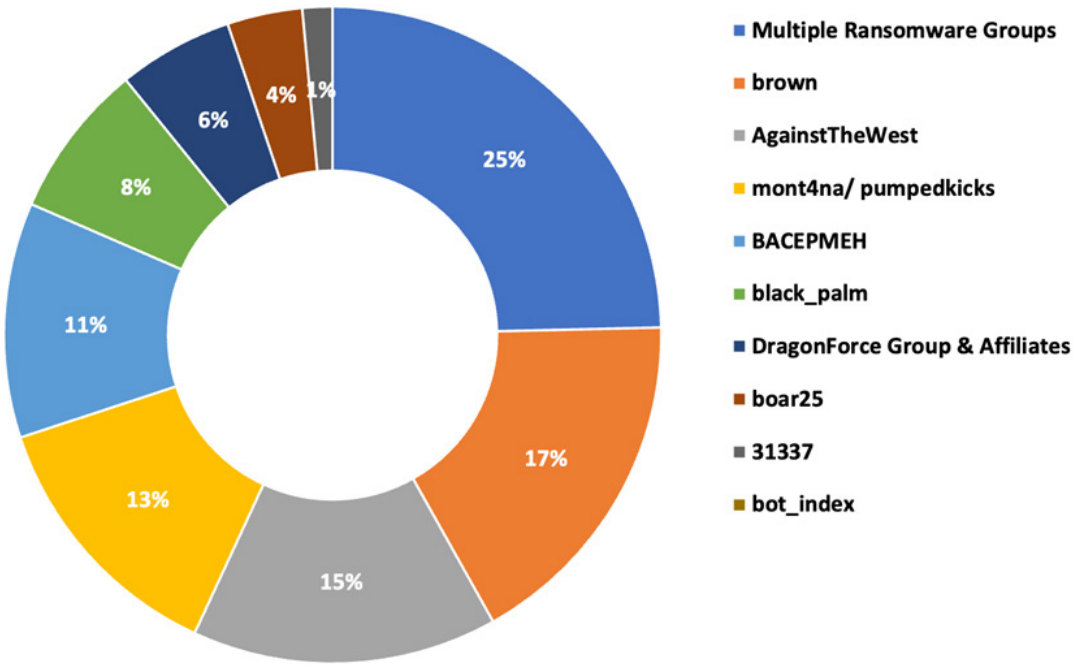

Figure 55: Top 10 threat actors targeting the entertainment sector

2.2.27. Hospitality

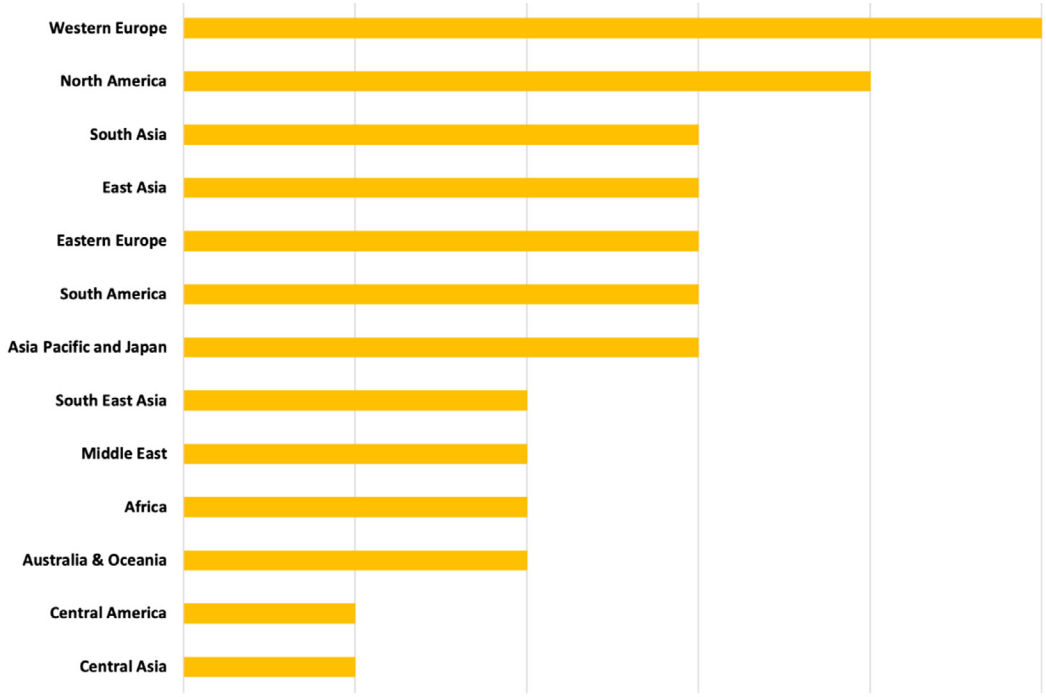

Figure 56: Geographical distribution of target organizations within the hospitality sector

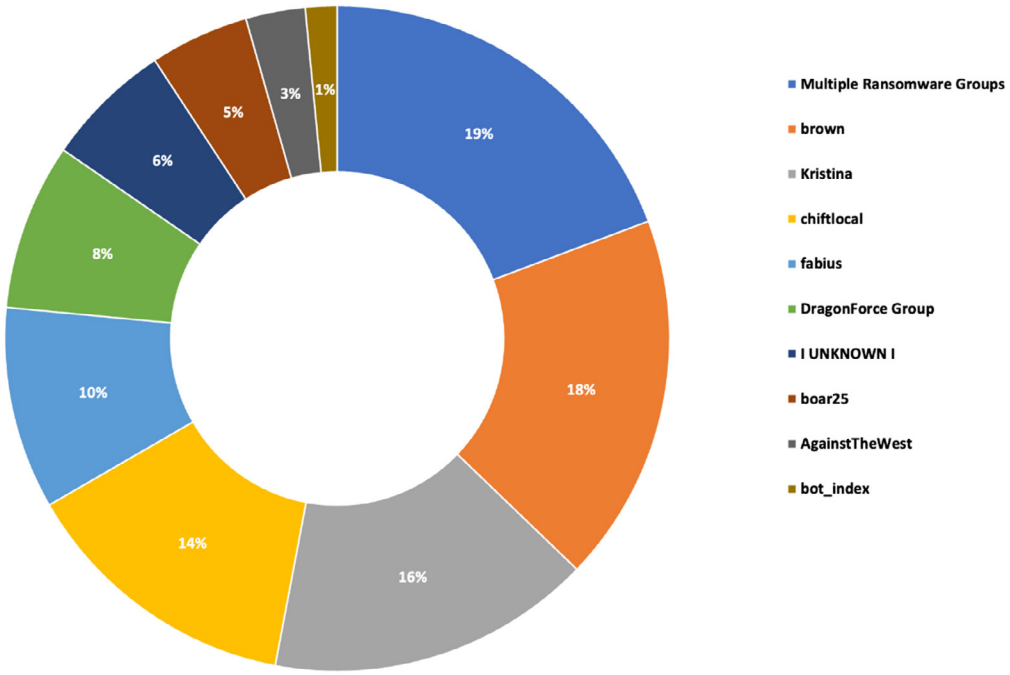

Figure 57: Top 10 threat actors targeting the hospitality sector

2.2.28. Internet Publishing

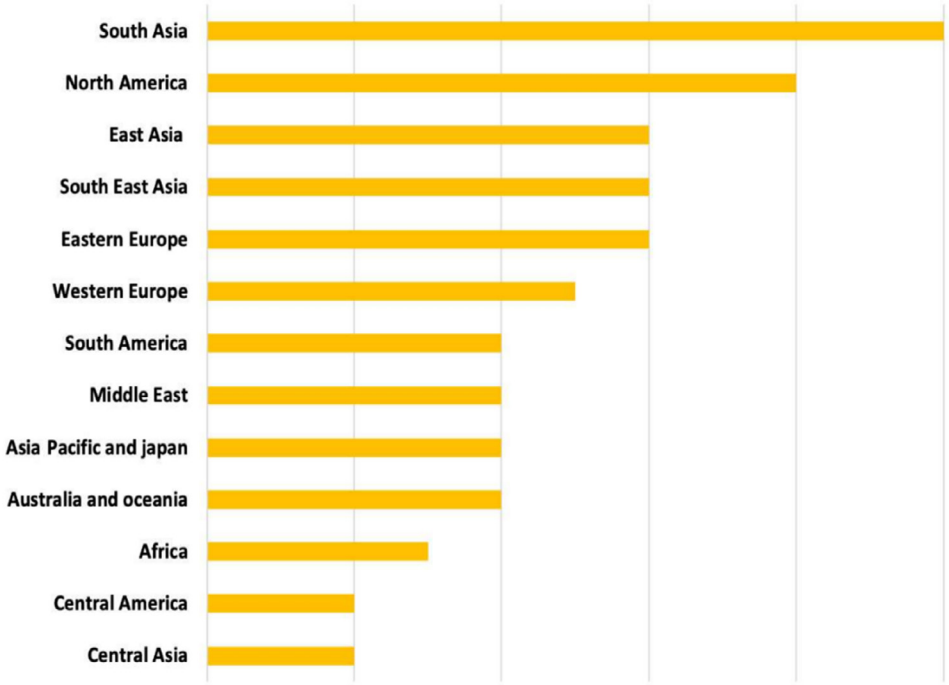

Figure 58: Geographical distribution of target organizations within the internet publishing sector

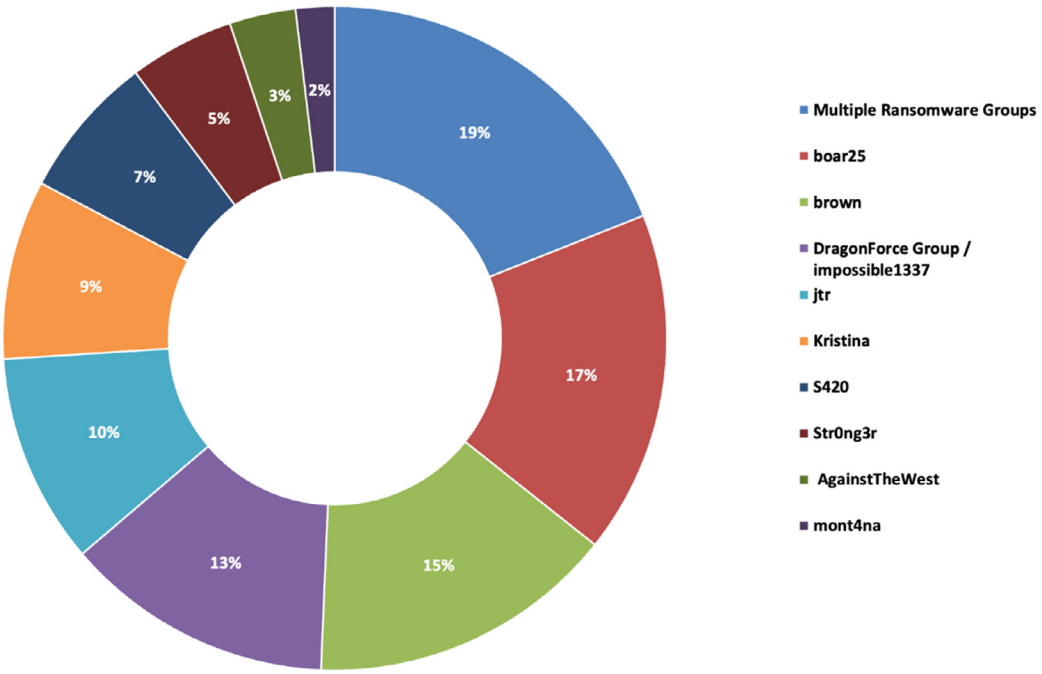

Figure 59: Top 10 threat actors targeting the internet publishing sector

2.2.29. Sports

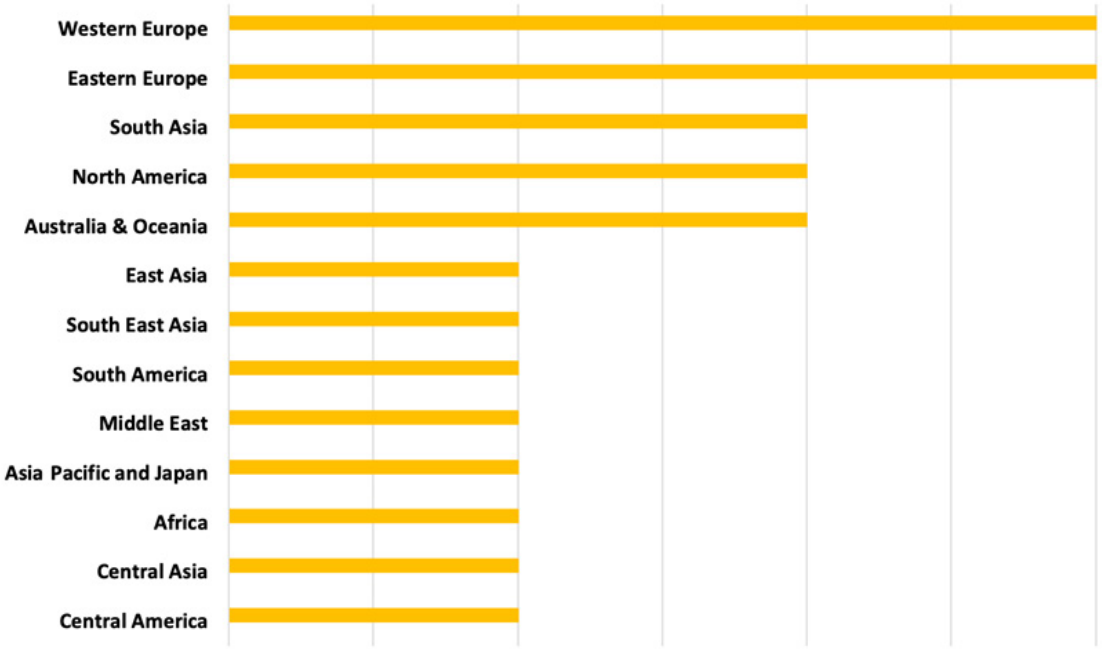

Figure 60: Geographical distribution of target organizations within the sports sector

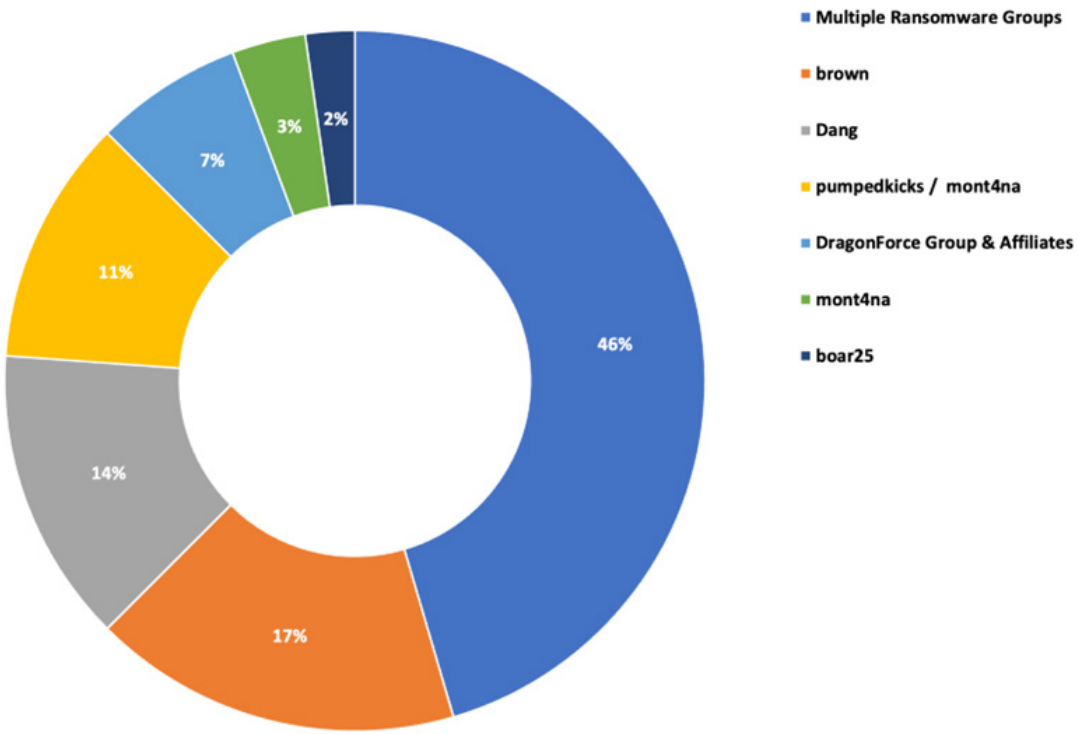

Figure 61: Top 10 threat actors targeting the sports sector

2.2.30. Semiconductor

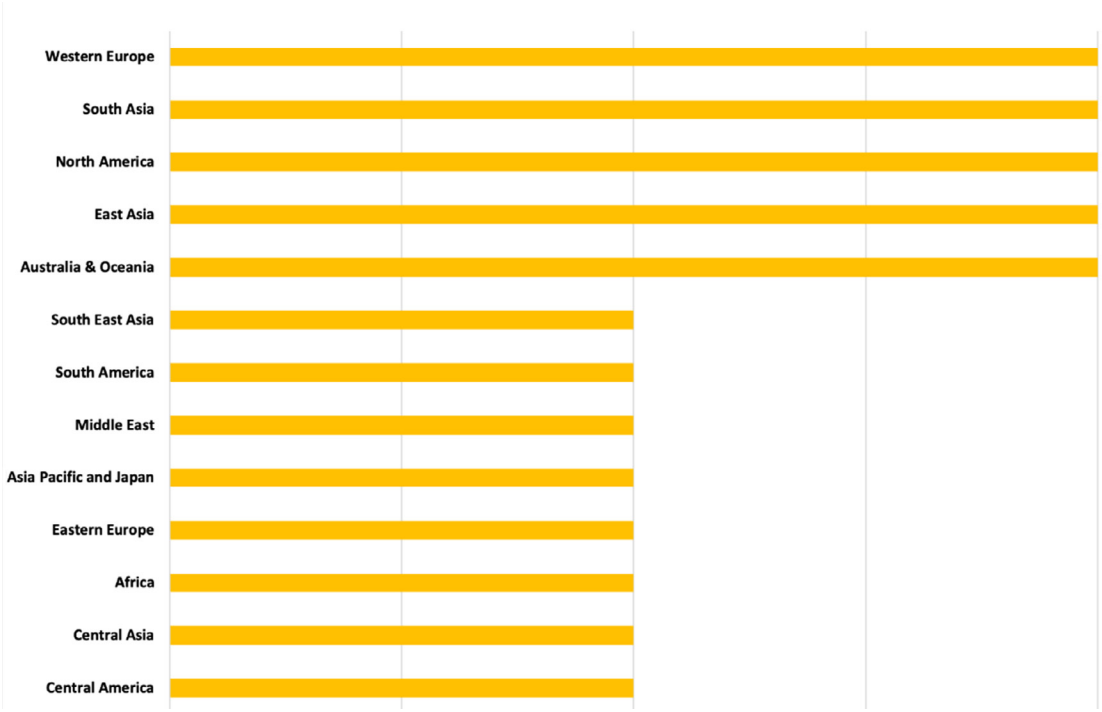

Figure 62: Geographical distribution of target organizations within the semiconductor industry

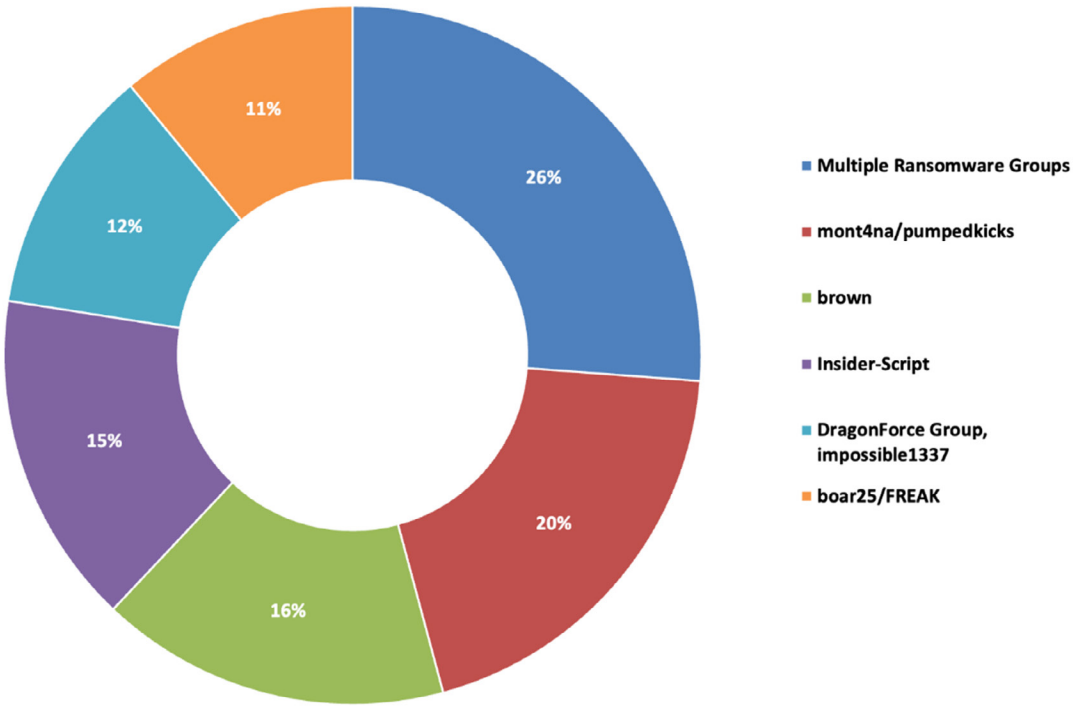

Figure 63: Top 10 threat actors targeting the semiconductor industry

3. Threat Actors Promoted to Credible in Q2 2022

During Q2 2022, FortiGuard Labs used FortiRecon to validate the reliability of threat actors, identifying 24 of these adversaries as being credible.

- inthematrix
- Pirat-Networks
- Mont4na, pumpedkicks
- Yesdaddy
- NetFlow
- spectre123
- kelvinsecurity, teamkelvinsec
- Network Battalion 65
- Breached
- Netsec
- RedLineVIP
- PieWithNothing
- SebastianPereiro
- TopFuel
- zanko
- pompompurin
- zirochka
- pixe1
- black_palm
- We Leak Database, GuntherMagnuson
- Weaver
- DragonForce Group, impossible1337
- Krustywise
- r1z

4. Ransomware Trends

In Q2 2022, the team observed continuous growth in the frequency of ransomware attacks. One of the primary reasons may be an ill-prepared response to such attacks. Ransomware attacks can have devastating effects on an organization, as well as entities associated with the victim. Further, the team observed more ransomware gangs buying initial access from access brokers and advertising network access to organizations that were later listed as victims on multiple ransomware blog sites.

The LockBit ransomware group, in particular, was the most active, followed by Conti. Incidentally, Conti claimed to have ceased operations, although time will tell if this is true. During this period, the team also observed that LockBit upgraded its malware and branding by releasing a new malware version, LockBit 3.0.

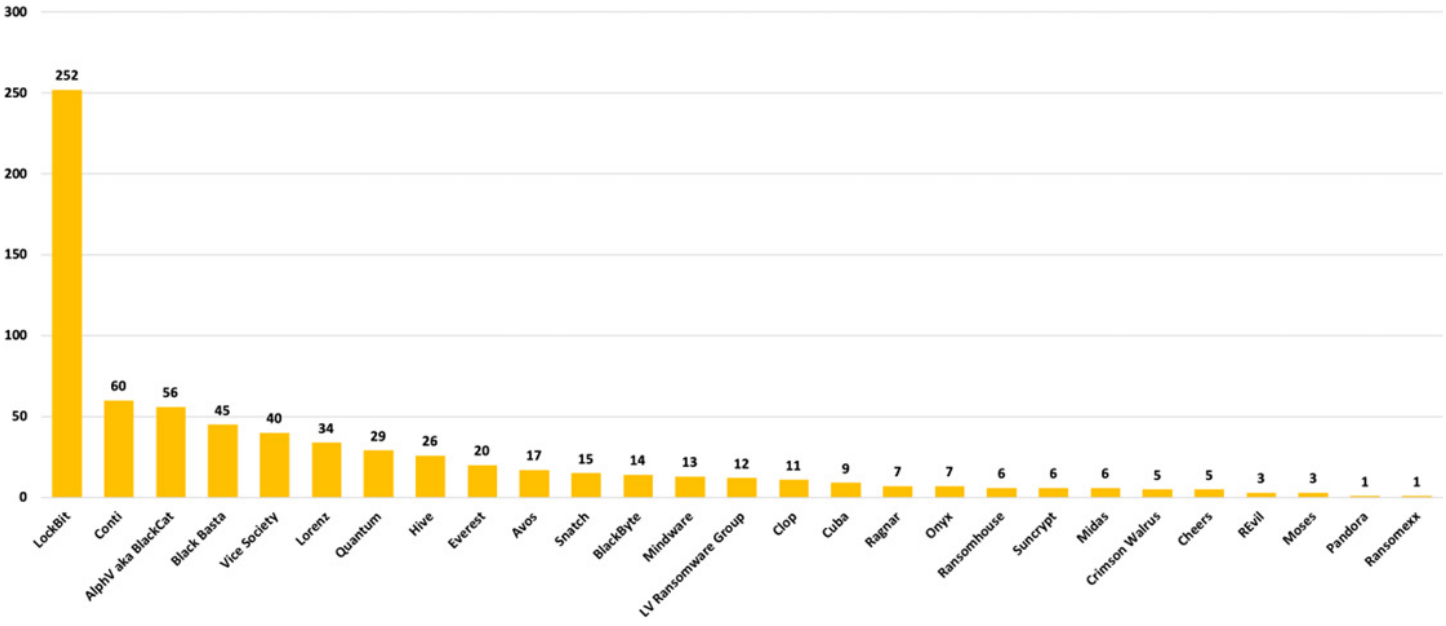

Figure 64: Ransomware victims by group

5. Actors Leveraging Credential Stealer Logs

The FortiGuard Labs team used FortiRecon to observe an increasingly close relationship between access brokers and ransomware, ultimately streamlining their operations to maximize profits. The team also documented a surge in credential stealer malware logs used by actors operating in underground forums. These logs were used to access VPN portals from organizations such as Citrix, Cisco, Pulse Connect Secure, and Fortinet's own solutions.

Access brokers often purchase credential stealer logs from darknet marketplaces and forums. These logs enable an actor to access the target organizations' internal infrastructure, including their web apps, systems, servers, and other sensitive data/documents stored on the systems.

Another notable observation was that network access to some organizations was advertised for sale on underground forums. These same organizations were later found to be victims of ransomware. This indicates a growing reliance by ransomware groups on access brokers, who depend on credential stealer malware to gain initial access to organizations. The team also observed credential stealer malware developers update their functionality by offering the ability to encrypt infected systems and demand ransoms. These new features allow access brokers to control large botnets to perform their own ransomware attacks to maximize profits, rather than selling access to ransomware groups at a lower price—moving themselves up the food chain.

Ransomware operators are increasingly changing tactics and switching to easier ways to acquire credentials. Initial infection vectors have been transformed from complex exploits to cybercriminals simply purchasing credential stealer logs from underground markets, as illustrated in Figure 65 below, where credentials are stolen using a wide range of TTPs (tactics, techniques, and procedures). This compromised data has a variety of uses, including enabling attackers to breach organizations and steal sensitive information. In fact, all it takes is one good username/password combination to gain access to an organization's infrastructure and cause damage.

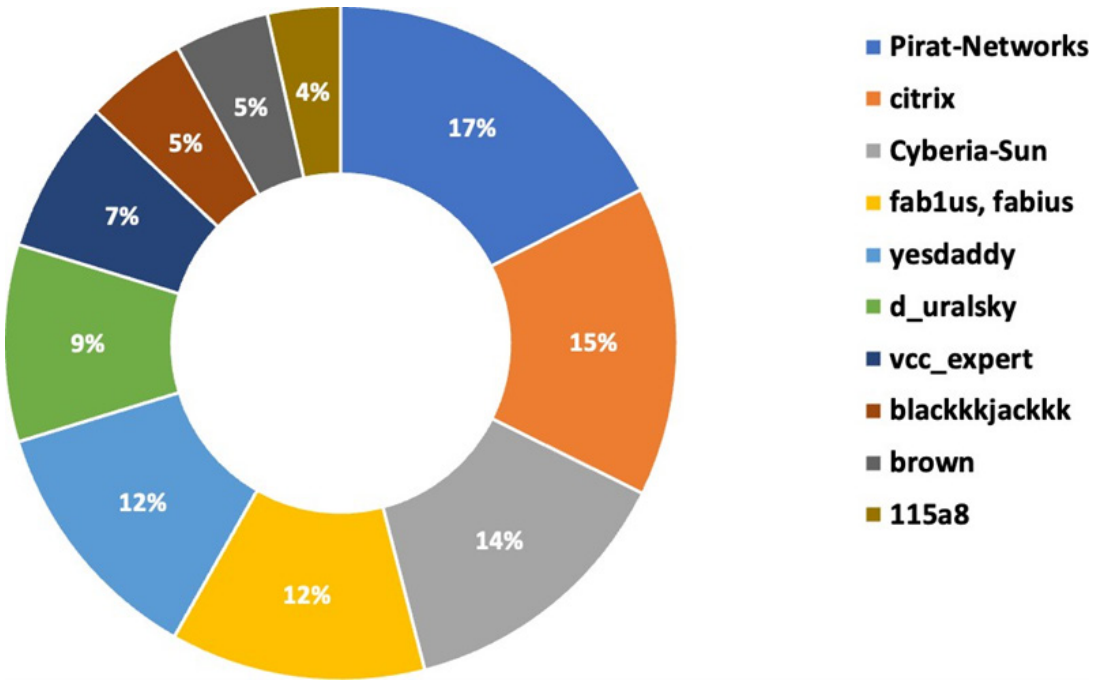

Figure 65: Distribution of actors leveraging credential stealer logs

6. Vulnerabilities Chatter

Threat actors continue to target known vulnerabilities and find ways to exploit them to complete their mission. The table below illustrates the vulnerabilities discussed on darknet forums in Q2 2022:

CVE Number	Vendor	CVE Title	Description	CVSS (v3)	Severity	Vendor/ Security Advisory
CVE-2022-30525	Zyxel	An OS command injection vulnerability in the CGI program	An OS command injection vulnerability in the CGI program of Zyxel USG FLEX 100(W) firmware versions 5.00 up to and including 5.21 Patch 1, USG FLEX 200 firmware versions 5.00 up to and including 5.21 Patch 1, USG FLEX 500 firmware versions 5.00 up to and including 5.21 Patch 1, USG FLEX 700 firmware versions 5.00 up to and including 5.21 Patch 1, USG FLEX 50(W) firmware versions 5.10 up to and including 5.21 Patch 1, USG20(W)-VPN firmware versions 5.10 up to and including 5.21 Patch 1, ATP series firmware versions 5.10 up to and including 5.21 Patch 1, VPN series firmware versions 4.60 up to and including 5.21 Patch 1, which could allow a malicious user to modify specific files and then execute some OS commands on a vulnerable device.	9.8	Critical	Advisory
CVE-2022-30190		Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability.	A remote code execution vulnerability exists when MSDT is called using the URL protocol from a calling application such as Word. An attacker who successfully exploits this vulnerability can run arbitrary code with the privileges of the calling application. The attacker can then install programs, view, change, delete data, or create new accounts in the context allowed by the user's rights.	7.8	High	Advisory
CVE-2022-29464	WSO2	Unrestricted arbitrary file upload and remote code to execution vulnerability	Due to improper validation of user input, a malicious actor could upload an arbitrary file to a user-controlled location of the server. By leveraging the arbitrary file upload vulnerability, it is further possible to gain remote code execution on the server. By leveraging the vulnerability, a malicious actor may perform Remote Code Execution by uploading a specially crafted payload.	9.8	Critical	Advisory
CVE-2022-26925		Microsoft Windows LSA Spoofing Vulnerability	Microsoft Windows Local Security Authority (LSA) contains a spoofing vulnerability where an attacker can coerce the domain controller to authenticate to the attacker using NTLM.	5.9	Medium	Advisory
CVE-2022-26923		Active Directory Domain Services Elevation of Privilege Vulnerability	An authenticated user could manipulate attributes on computer accounts they own or manage and acquire a certificate from Active Directory Certificate Services that would allow the elevation of privilege.	8.8	High	Advisory
CVE-2022-26809		Remote Procedure Call Runtime Remote Code Execution Vulnerability	Remote Procedure Call Runtime Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-24492 and CVE-2022-24528.	9.8	Critical	Advisory

CVE Number	Vendor	CVE Title	Description	CVSS (v3)	Severity	Vendor/ Security Advisory
CVE-2022-26134	Atlassian	Remote code execution via OGNL injection in Confluence Server and Data Center	In affected versions of Confluence Server and Data Center, an OGNL injection vulnerability exists that would allow an unauthenticated attacker to execute arbitrary code on a Confluence Server or Data Center instance. The affected versions are from 1.3.0 before 7.4.17, from 7.13.0 before 7.13.7, from 7.14.0 before 7.14.3, from 7.15.0 before 7.15.2, from 7.16.0 before 7.16.4, from 7.17.0 before 7.17.4, and from 7.18.0 before 7.18.1.	9.8	Critical	Advisory
CVE-2022-24706	Apache	Apache CouchDB Remote Privilege Escalation	In Apache CouchDB versions prior to 3.2.2, an attacker can access an improperly secured default installation without authenticating and gain admin privileges. The CouchDB documentation has always recommended properly securing an installation and using a firewall in front of all CouchDB installations.	9.8	Critical	Advisory
CVE-2022-24086	Adobe	Arbitrary Code Execution	Adobe Commerce versions 2.4.3-p1 (and earlier) and 2.3.7-p2 (and earlier) are affected by an improper input validation vulnerability during the checkout process. Exploiting this issue does not require user interaction and could result in arbitrary code execution.	9.8	Critical	Advisory
CVE-2022-22965	VMware	Spring FrameworkRCE via Data Binding on JDK 9+	A Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding. The specific exploit requires the application to run on Tomcat as a WAR deployment. If the application is deployed as a Spring Boot executable jar, i.e., the default, it is not vulnerable to the exploit. However, the nature of the vulnerability is more general, and there may be other	9.8	Critical	Advisory

Table 1: Vulnerabilities discussed on darknet forums

Note: We have mentioned only the "Top 10" vulnerabilities. A comprehensive list of 23 vulnerabilities is available via the FortiRecon Service.

The team also assessed a pattern in the vulnerabilities that threat actors were discussing. The chart below shows the distribution of vulnerabilities from various disclosure years being discussed on darknet forums. Our team also observed a general shift in focus from vulnerabilities discovered in 2021 to those found in 2022, as would seem normal now that we are in mid-2022. This trend may also be due to two major vulnerabilities found this year, the Atlassian Confluence vulnerability (CVE-2022-26134) and the Microsoft MSDT RCE vulnerability (CVE-2022-30190), also known as Follina.

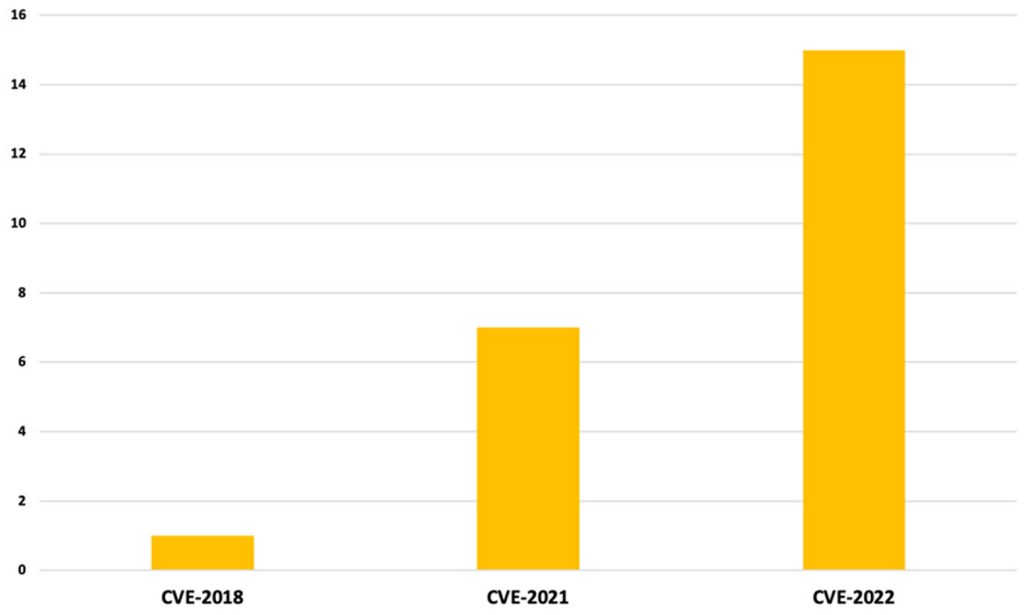

Figure 66: Distribution of vulnerabilities from different disclosure years being discussed on the darknet

7. Significant Cyber Events

During Q2 2022, the team tracked several cyber events. Some warrant separate mentions to highlight their importance in shaping the current cybersecurity landscape. The events detailed below had an extraordinary effect on the threat landscape during these three months.

7.1. Ongoing Russia–Ukraine Conflict

AgainstTheWest, aka BlueHornet, continued attacks and leaks in support of Ukraine after Russia's invasion. The group's activities began in Q1 and continued into Q2. Notable actions by the group in Q2 include:

- The attacker group accused China of supporting Russian aggression and shared the source codes of multiple Chinese government entities and organizations as retribution.
- The attacker group also revealed the identities and shared the personal information of individuals allegedly working as part of Russian, Chinese, and North Korean Nexus APT groups.
- AgainstTheWest also shared and advertised the alleged source codes of multiple Chinese organizations, along with access to a platform they claim belongs to a Chinese ministry.

The data leaks website, DDoSecrets, has been active since 2018. However, it has recently shifted its focus to publishing data related to Russian organizations. The site grew to a prominent position during Q2 with leaks from groups such as Anonymous, NB65, and BB00da. Of the 11 DDoSecrets leaks the team reported on, the following are of particular interest:

- Pro-Ukrainian hacktivist group Anonymous claims to have breached three Russian organizations within the oil and gas and manufacturing sectors and stolen over 425 GB of data, allegedly containing more than 400,000 emails. All this data was released on the DDoSecrets website.
- DDoSecrets also published data claimed to have been taken from several Russian organizations and the Nauru state police force. This data was also allegedly sourced from the hacktivist group Anonymous.

7.2. #OpsPatuk

In Q2 2022, the #OpsPatuk campaign led to attacks on Indian companies and government entities. The operation was directed by a group using the name "DragonForce" That has compromised Indian websites, primarily government, technology, financial services, manufacturing, and education sectors. Attackers have publicly released sensitive information about numerous organizations on its official website.

Our team's extensive reporting on the operation covered 13 reports, with the most notable findings below:

- The Malaysian-based hacktivist group defaced over 70 Indian websites.
- DragonForce also exploited a critical unauthenticated RCE vulnerability (CVE-2022-26134) to impact Confluence servers in India, in addition to sharing a Shodan query for identifying vulnerable instances.
- DragonForce admin, "impossible1337," targeted Indian educational websites and a government website with DDoS and defacement attacks. A forum member operating as "JustM" claims to have targeted the State Bank of India with a DDoS attack.

7.3. Notable Vulnerabilities

Confluence CVE-2022-26134 is a critical RCE (Remote Code Execution) vulnerability in Atlassian Confluence Server and Confluence Data Center solutions. In Q2 2022, numerous PoC exploits were shared on underground forums for the vulnerability. This same vulnerability was also leveraged in attacks during the #OpsPatuk campaign that targeted vulnerable Indian entities, as noted herein.

Key Findings:

- Multiple actors on Russian language forums, Club2crd and XSS, shared an exploit for a critical unauthenticated remote code execution vulnerability found in Confluence Server and Data Center solutions, tracked as CVE-2022-26134.
- Actor "r1z" advertised access to 50 vulnerable Confluence servers acquired by exploiting the critical Confluence unauthenticated RCE vulnerability, tracked as CVE-2022-26134, and claimed to be in possession of a list of over 10,000 vulnerable Confluence servers.

Follina CVE-2022-30190, is a high-severity RCE vulnerability in the Microsoft Support Diagnostic Tool (MSDT), widely reported in May 2022. The team received several reports on PoC exploits and builders as the issue progressed, including:

- Several actors on the XSS forum shared exploits, payload generators, and POCs for CVE-2022-30190, a remote code execution vulnerability impacting Microsoft Support Diagnostic Tool (MSDT) (dubbed "Follina") that was being actively exploited.
- Actors "aion" and "Crux" advertised a private exploit for the Follina zero-day (CVE-2022-30190), which allows remote code execution without user interaction utilizing malicious Rich Text File (.rtf) files.
- Actor "3xp1r3" advertised a builder to generate undetectable Microsoft documents and HTML files to exploit Follina (CVE-2022-30190).

7.4. U.S. Supreme Court Overturns Roe v. Wade

The overturning of Roe v. Wade in June 2022, a Supreme Court decision originally made in a 1973 ruling that said the U.S. Constitution guaranteed the right to an abortion, led to abortion bans across the U.S. that made global headlines. The team observed darknet activity in relation to Roe v. Wade to dox U.S. Supreme Court justices.

The team's research showed that all the details in underground forum posts were either publicly available or incorrect, proving the doxing effort to be of little importance. However, the threat does show a clear and present risk from hacktivists targeted at those in high-ranking decision-making positions. The team published a comprehensive report of its findings, "Actor paksiban2 shares publicly available personally identifiable information (PII) of four Associate Justices of the U.S. Supreme Court, intending to condemn the recent Supreme Court ruling on abortion rights."[1]

8. Recommendations

8.1. Defending Against Ransomware Attacks

While ransomware targets small businesses, mid-sized companies, and large enterprises across every industry, some industries are more vulnerable than others. To help protect networks against ransomware and other cyberattacks, the team recommends that organizations:

- **Continuously monitor the external attack surface to detect vulnerable, exposed assets and leaked credentials.** The discovery of external facing assets that may be vulnerable to an attack poses a critical risk for your organization. We typically see attackers selling RDP access and databases obtained by abusing misconfigurations on web servers. Solutions such as Fortinet FortiRecon continuously monitor an organization's external attack surfaces, enabling security admins to discover unknown/known externally exposed and vulnerable assets. In addition, FortiRecon monitors the dark web, underground and invite-only adversary forums, open-source intelligence (OSINT) sources, and more to detect and alert on data/credential leaks, allowing you time to proactively respond to prevent or minimize attack impact. What's more, you can take advantage of FortiRecon and FortiGuard Labs' in-depth knowledge and expertise to acquire leaked credentials and other data on behalf of your organization to help you take earlier and faster action on imminent cyber threats.
- **Monitor your organization's digital footprint and conduct takedowns to maintain brand integrity and protect customer trust.** We often see attackers leveraging an organization's brand reputation to deceive employees and customers into providing sensitive data/credentials via fake websites, mobile apps, or even social media accounts, which the attackers will then use to penetrate the organization. The FortiRecon service closely monitors and looks for brand-infringing domains, mobile apps, and social media accounts, and once found, can take them down at your command.
- **Implement multi-factor authentication (MFA) and a strong password policy.** We continuously monitor the darknet for leaked credentials of corporate portals used by employees, and we regularly find them having been compromised and put up for sale on the darknet. Organizations can reduce their risk from such exposure by enforcing MFA combined with a strong password policy across all user accounts.
- **Limit access rights.** Implement least privileges for all users and admins, only granting them the rights they need to complete their daily tasks.
- **Make regular data backups.** Backups should be tested for malware and maintained offsite and offline, where attackers cannot access the data. Demanding a ransom only works because a business has no other way to access its data.
- **Patch early and patch often.** Ransomware, such as WannaCry and NotPetya, relied on unpatched vulnerabilities to spread around the globe. Organizations should also lock down RDP (remote desktop protocol) and even turn it off if it's not required.
- **Ensure tamper protection is enabled.** Ryuk and other ransomware strains attempt to disable endpoint protection.
- **Protect your endpoints.** Even the best-trained employees occasionally make mistakes. Installing antivirus and antimalware software on computers adds an extra layer of protection, especially against phishing attacks and credential stealers. However, the best antivirus and antimalware programs are only as good as their latest patches. Regularly installing patches will prevent hackers from exploiting system weaknesses.
- **Replace end-of-life software.** Organizations unable to perform rapid scanning and patching of internet-facing systems should consider moving these services to mature, reputable cloud service providers (CSPs) or other managed service providers (MSPs). Reputable MSPs can patch applications, such as webmail, file storage, file sharing, chats, and other employee collaboration tools for their customers.
- **Develop (and test) an incident response plan.** A robust incident response plan helps in assessing a threat and minimizing damage. Organizations should always have a fully equipped incident response team, whether staffed internally or contracted through an MSSP.

- **Threat Intelligence.** Cyber threat intelligence (CTI) helps enterprises collect data about current and potential cyber risks. It also helps organizations determine whether a cyberattack can threaten their particular security. A darknet threat intelligence solution, such as FortiRecon, can also help organizations monitor darknet chatter related to the organization or data leaks that can result in financial losses before they are even made public. Such crucial and time-sensitive data can help organizations handle incidents appropriately and take all necessary legal steps.

8.2. Stolen Credentials

To protect their systems and stored data and decrease the risk of falling victim to credential stealers, such as RedLine and Vidar Stealer, organizations need to deploy an antivirus solution, such as FortiClient. Following is a list of Fortinet's recommendations to protect your organization's systems from stealer attacks:

- **Security awareness training.** Critical in helping your employees recognize and be suspicious of unsolicited emails and phishing campaigns, as well as suspicious social media, including messages with embedded links or file attachments that might lead to the distribution of further malicious payloads.
- **Multi-factor authentication.** MFA should always be used to reduce the effectiveness of any stolen credentials. Your organization should also mandate strong password policies for all employees.
- **Email security.** Ensure precautions are taken to prevent end-users from receiving potentially malicious email attachments or links, as well as configuring protocols and security controls, such as DKIM, DMARC, and SPF. Secure email gateway solutions should also be able to detect, disarm, redirect, or remove emails with malicious attachments,
- **Abnormal endpoint behavior.** Continuously monitoring abnormal endpoint behavior, such as requests to domains with a low reputation score, helps detect intrusions early and allows admins to take appropriate and preemptive action.

Appendix A: Darknet Forums

Following is the description of the most popular and active darknet cybercrime forums.

XSS

xss[.] was previously known as damagelab.org (stylized as DaMaGeLaB) and was one of the first and most popular Russian-language forums, dating back to at least 2013. Following the arrest of one of its administrators in 2017, the site was rebranded as xss[.] and relaunched in September 2018. It derives its name from cross-site scripting, a security vulnerability in web applications that bypasses access controls. It is a popular Russian language forum, hosting discussion topics including hacking, programming, and technology and a marketplace section where users can directly purchase primarily digital products.

XSS also provides custom groups on the forum, listed below:

Legend Group: Members operating on the forum for a long time or who share very sensitive information can be a part of this group.

Premium Group: Members get access to all hidden links, can change nicknames, have no limit on editing messages, etc. The cost of a premium account is $100 per year.

PR Group: These members are responsible for posting new content on the forum. The forum's moderators provide this account after the member's credibility has been proven.

Member Group: Members who join using free registration are a part of this group.

Exploit

Exploit is an invitation-only cybercrime forum that can also be joined with a paid registration. Because of this, actors with low count positive reputation points can be considered fairly reliable. To register on exploit without paying a registration fee, users need to fit at least one of the below-listed criteria:

- Have their own service on other reputable forums. The service must be older than a year and have more than ten positive reviews. They must also be a member of the Administration or the forum team.
- They must be a specialist in C/C++, Assembler, Delphi, Pascal, Visual Basic, .NET, Kylix, Python, etc. They can also be a specialist in web-based languages, such as PHP, Perl, ASP, JavaScript, XML, XSL, MySQL, MsSQL, and others.
- Their account on any similar forum must be older than two years.
- They must specialize in malware, exploits, bundles, crypto, or automated transfer systems. Their account on any similar forum must be older than two years.

Breached Forums (aka BreachForum)

Breached Forums have been mentioned a handful of times in the Telegram group chat "LAPSUS$ Chat," owned and managed by the data breach and extortionist group "LAPSUS$." Since Breached Forums is relatively new, it has nowhere near the user base and popularity that Raid Forums once held. However, given the incentives offered to former Raid Forums users, the site's near-identical appearance and functionality to Raid Forums, and Breach Forums being owned and operated by the well-known and reputable former Raid Forums user pompompurin, Breach Forums has the potential to become a proper replacement for Raid Forums. In time, the site could reach or exceed its predecessor as the most popular clearnet hacking forum.

About Forum Account Upgrades:

Similar to Raid, Breached Forums also provides three types of upgraded accounts:

- **VIP account**, where the user gets 30 forum credits, a higher post limit, more storage for messages, and more. The cost of a VIP account is 10 EUR.
- **MVP account**, where the user gets 60 forum credits, a higher post limit, more storage for messages, advertisement bypass, and more. The cost of an MVP account is 20 EUR.
- **GOD account**, where the user gets 120 forum credits, a higher post limit, more storage for messages, advertisement bypass, graphical changes, and more. The cost of a GOD account is 50 EUR.

Helium Forum

Helium is a cybercrime forum offering free registration for all. According to the moderators, the forum was started with the goal of ensuring everyone in the community is given a platform to learn, share, and exchange goods and services. The operators charge 3% of the total transaction amount for every item sold on the forum.

Appendix B: Credential Stealers

Credential theft is a cybercrime involving unlawfully obtaining an organization's or individual's password(s) to access and abuse/exfiltrate critical data and information. Often an early stage of a cyber-based attack, credential theft enables attackers to operate undetected throughout a network, reset passwords, and wreak havoc within an organization. A few of the more popular credential stealers mentioned or advertised by threat actors are listed below:

RedLine

First revealed in 2020, RedLine stealer has been increasingly advertised on the underground forums as a Malware-as-a-Service (MaaS) threat. It is available for $150-200 for a monthly subscription or standalone sample. RedLine is one of the most widely deployed information stealers. It can grab Windows credentials, browser information, cryptocurrency wallets, FTP connections, banking data, and other sensitive information from infected hosts. Apart from its data dumping capabilities, the malware was recently upgraded with additional features that allow its operators to load second-stage malicious payloads and run commands from the attacker's command-and-control (C&C) server.

Raccoon

Raccoon is a classic InfoStealer distributed as Malware-as-a-Service that gathers autofill data, login credentials, and cookies from an infected system. The Raccoon InfoStealer is very popular among cyber threat actors even though it is not a sophisticated or advanced malware. It has infected over 100.000 devices and continues to spread. In 2019, Raccoon became one of the most mentioned malware on the darknet forums.

FormBook

Initially called Babushka Crypter, FormBook is an InfoStealer distributed as a Malware-as-a-Service capable of keylogging, webform hijacking, and clipboard monitoring. It first began its activity on the 1st of January, 2016. FormBook is still an active and dangerous trojan, recently adding the latest Microsoft Office zero-day vulnerability (CVE-2021-40444) into its capabilities. It is used mainly by inexperienced threat actors.

Vidar

Vidar InfoStealer, an evolved version of the Arkei InfoStealer, is a commonly-used InfoStealer used by cyber attackers. Vidar is believed to have been created in a Russian-speaking country because the InfoStealer is programmed to stop if the system is located in one of the ex-USSR countries. Vidar's capabilities include collecting browser cookies and history, taking screenshots, gathering two-factor authentication data, and collecting information about digital wallets. After Vidar collects data from the system, the InfoStealer erases itself and sends its compressed data to the threat actor.

8.2. Azorult

Created by the threat actor Gorgon Group, Azorult InfoStealer was first discovered in 2016. The Azorult InfoStealer is believed to have originated in one of the former USSR countries. Primarily bought in Russian Darknet forums, Azorult's capabilities include collecting browser cookies and history, stealing login credentials, and collecting system information such as the username and operating system version. Some newer versions of Azorult InfoStealer include setting up a Remote Desktop Protocol (RDP) connection for the threat actor to take control of the system.

[1] This report is available via the FortiRecon Service.

November 22, 2022 1:54 PM

1783739-0-0-EN