Cybercriminal market in Telegram

Positive Technologies

ptsecurity.com

Cybercriminal market in Telegram

Over the past few years, we've seen major cybercrime marketplaces disappear or lose the trust of their users. Some forums, such as RaidForums and DarkMarket, were shut down by law enforcement. Others, like BHF, Carding Mafia, Nulled, and Maza, were hacked by competitors. Some cybercrime forums changed ownership, as was the case with DarkMoney. Such events can result in user data being compromised, leading cybercriminals and their customers to fear that their identity and location could be revealed and their connections to illegal websites exposed.

With users losing confidence in the anonymity offered by forums, illicit marketplaces are increasingly turning to Telegram. The Telegram messaging platform is easy to use and is perceived as more secure. Cybercriminals are expanding their reach by using Telegram as their communication platform and cybercrime marketplace.

In this study, we analyzed the current state and maturity level of the market for cybercriminal services in Telegram channels and groups.

Materials and methods

Our study analyzed 323 public channels and groups on Telegram with over 1 million subscribers in total. We included not only explicitly criminal channels and groups, but also legitimate IT communities that can potentially be abused by cybercriminals.

The number of channels and groups hosting cybercriminal content has been growing since the second half of 2019. Most of the channels and groups in the sample (73%) have existed for less than two years, which may indicate both their short lifespan and the recent transition of criminal communications to the messaging app.

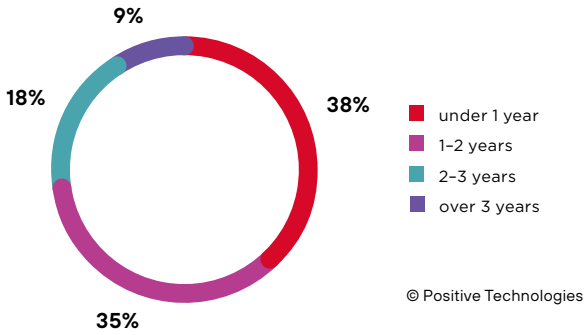

Figure 1. Age of channels and groups

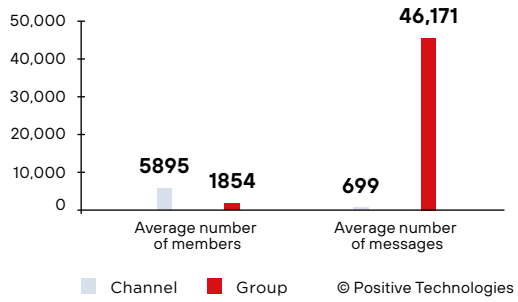

Figure 2. Average number of messages by type

We selected messages and posts (from here on we'll refer to them collectively as messages) published from early 2019 through Q2 2022 that discuss malware, vulnerabilities and exploits, access to corporate networks, user data, and cybercrime services such as hacking (for example, hacking websites, email accounts, and social media accounts), cash-out services, malware distribution, spamming, and DDoS services. The final sample includes more than 120,000 messages in Russian and English.

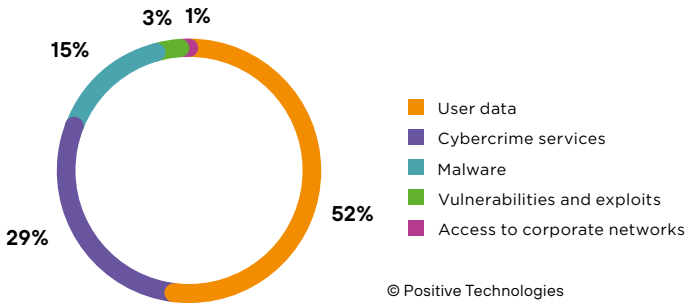

Figure 3. Message topics

From criminal forums to messaging apps

Messaging apps are easy to use, provide a fair degree of anonymity and have a simple registration process, making them a viable medium for cybercriminals to expand their market and reach new customers.

Starting from Q2 2020, we can see a boost in the number of cybercrime-related Telegram messages; in 2021, user activity increased manifold. The timing of this mass migration to Telegram coincides with the discovery in 2020 of many critical vulnerabilities in a number of forum engines including vBulletin, XenForo, and IPB, and the hacking of several major cybercriminal forums in 2021. This may have damaged the credibility of the forums and caused the transition to Telegram. At that time there was a lot of advertising for new channels, groups, and individual users providing various criminal services. For this reason, the total number of messages increased considerably at the end of 2021, but then user activity returned to previous levels.

By the end of Q1 2022, a spate of hacks and leaks prompted a new wave of advertising for Telegram groups and channels offering cybercriminal services. Q2 2022 saw a record number of over 27,000 messages.

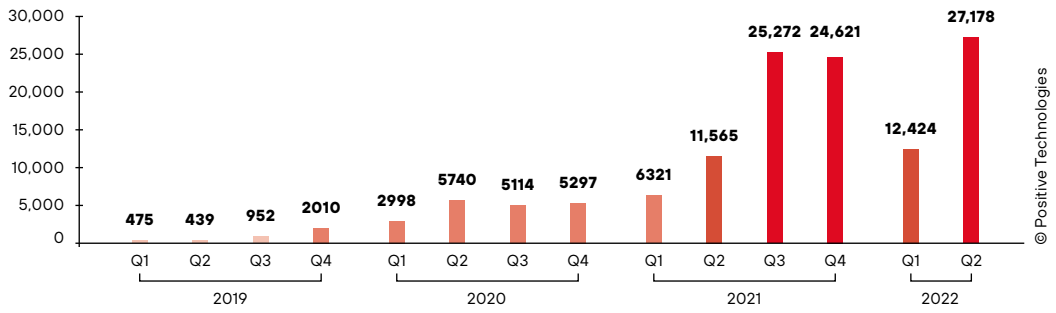

Figure 4. Total number of messages

Malware

According to the messages analyzed, the most popular malware types were remote access trojans (RAT) and various types of infostealer spyware.

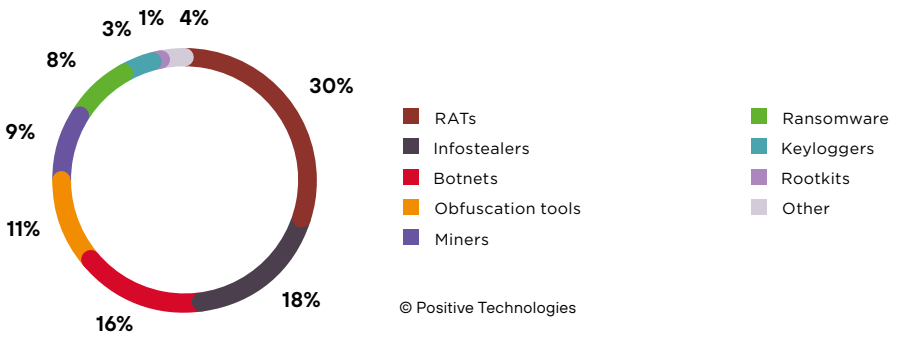

Figure 5. Malware types mentioned in messages

Ransomware was mentioned in just 8% of the messages, although the number of ransomware attacks has been at a record high in recent years. One reason for this might be that ransomware is distributed mostly through partner programs, on specialized darkweb forums and websites, or in closed groups. This would explain why the messaging app, being in the public domain, has so few ads for buying and selling ransomware tools, most of which are quite basic and sell for as little as $10.

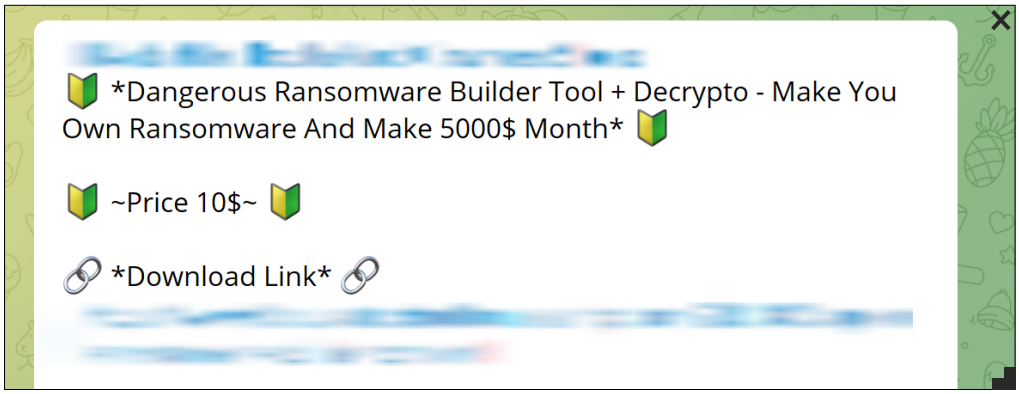

Figure 6. Ransomware tool ads

Although RATs are the most widely discussed malware in messages, their overall prevalence has dropped by 10 percentage points since the beginning of 2021. They accounted for 42% of all malware-related messages in Q1 2021, falling to 32% by the end of Q2 2022. This is partly due to other categories gaining momentum: Q3 2021 saw infostealers (23%) and botnets (22%) rising in popularity, while miners were among the leaders in Q4 2021 at 19%.

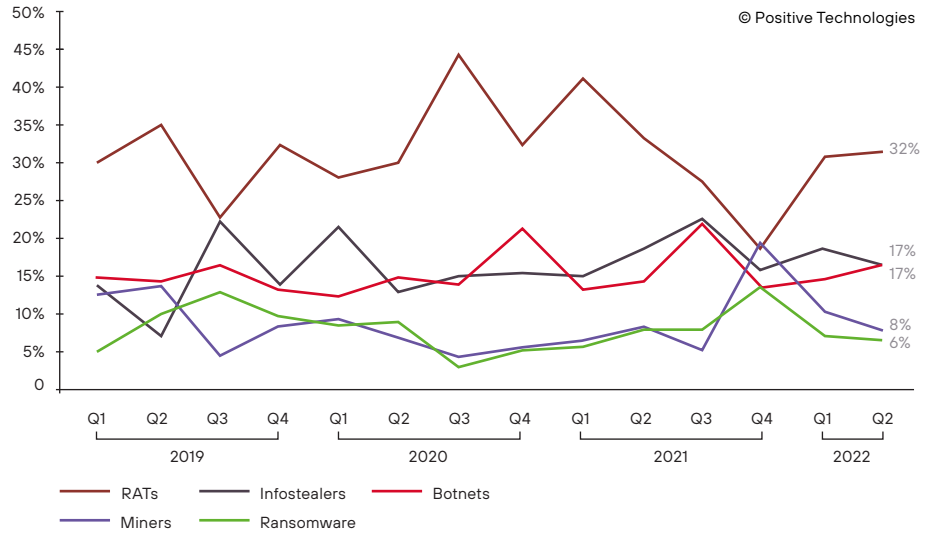

Figure 7. Most popular malware types by percentage of messages

Of all the messages, 11% were ads for selling malware, 10% offered malware for free, and 7% were offers to buy. Development services and cooperation initiatives are in the least demand on Telegram; cybercriminals go to specialized websites and forums for such purposes. This is understandable, as there is no rating system in Telegram to establish trust between users. Telegram allows users to easily change their nicknames, which makes it more difficult to track down dishonest sellers and buyers and gives fraudsters more opportunities to cheat. That is why 31% of purchase-related messages mention an escrow agent—a person trusted by both parties who acts as an intermediary in the transaction.

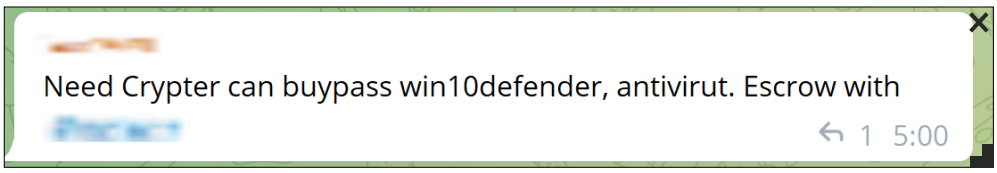

Figure 8. Messages about malware deals involving an escrow agent

Discussions about malware functionality, its use and distribution, as well as news about malware releases and updates accounted for 70% of the messages.

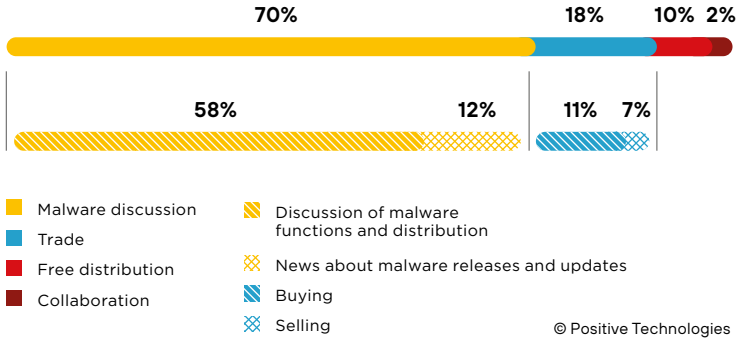

Figure 9. Categories of malware messages

Prices for ready-to-use malware depend on the type of malware, its functionality (the more features, the higher the price), and the usage time: a lot of malware is offered with a limited usage or support period. Tools for obfuscating malware code to evade detection can cost in the range of $20 to $100, while a botnet or a guide to building botnets can sell for up to $750.

Messages about miners have the highest proportion of sales offerings (27%), most of them being in the form of adverts. The price range spans from $10 for a simple malware tool with limited capabilities to $1,000 for the source code of a miner with many features, including antivirus bypass and the ability to infect systems without administrator privileges.

Figure 10. Miner advertisement

Remote access tools and infostealers

Among the most popular RATs are SpyMax (8% of all messages mentioning RATs), SpyNote (5%), and Mobihok (4%). All of them are for Android devices. Overall, RATs for Android account for almost a quarter of all messages in this category. The price depends on the feature set and can range from $10 to $500.

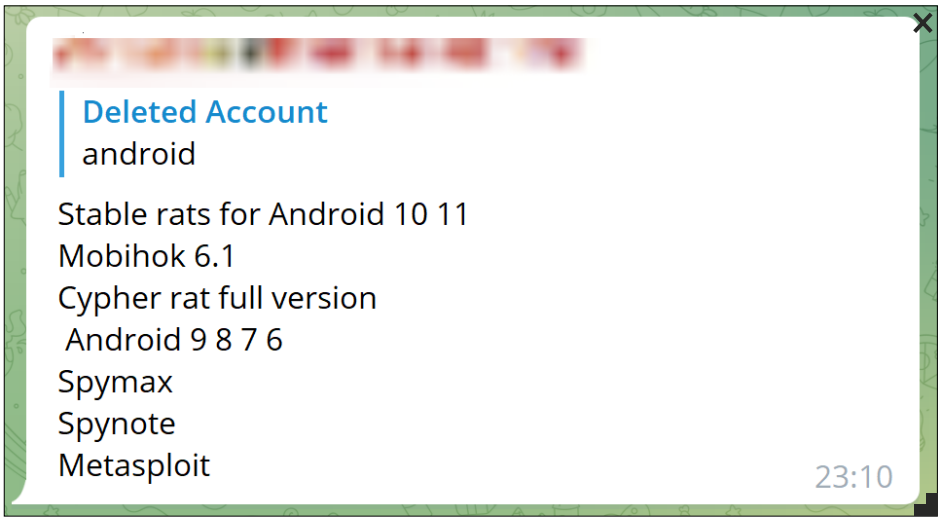

Figure 11. Discussion of most common RATs for Android

The most popular infostealer turned out to be RedLine, which featured in our Q1 2022 cybersecurity threatscape study. It is mentioned in more than 18% of messages related to infostealers, with many discussions about its features, sale and distribution of its source code, as well as information collected with its help. Other infostealers available in Telegram include Anubis, SpiderMan, Oski Stealer, and Loki Stealer. Infostealer prices range from $10 to $3,500.

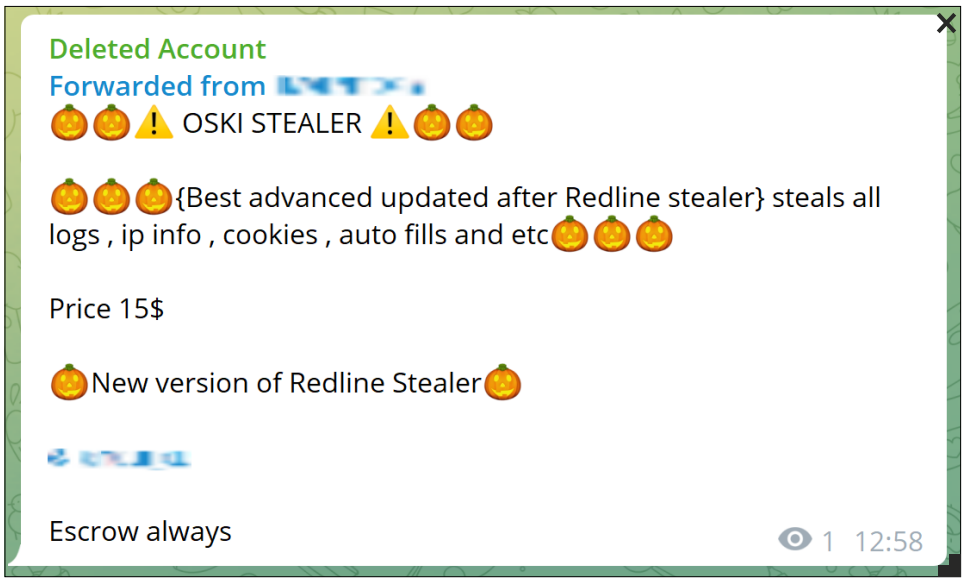

Figure 12. Infostealer advertisement

Infostealers typically collect user information from the victim's device: usernames and passwords, banking details, webcam and microphone recordings, and geolocation data. Most infostealers can also collect cryptowallet credentials and secret keys.

Vulnerabilities and exploits

The most popular topics among messages relating to exploits are zero-day vulnerabilities (29% of exploit-related messages), previously disclosed vulnerabilities (25%), and remote code execution (RCE) and local privilege escalation (LPE), which together comprise 24%. RCE and LPE are the most dangerous vulnerabilities and the most popular among attackers.

Figure 13. Distribution of messages relating to exploits

Most messages about operating system vulnerabilities and their exploits concern Windows, with Linux taking second place. Android ranks third: there is increasingly more malware being developed and circulated that targets this operating system.

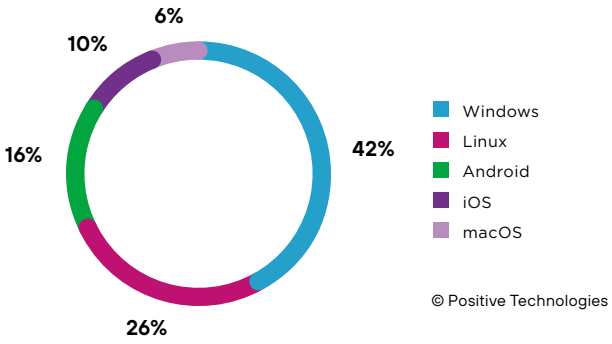

Figure 14. Messages about operating system exploits

In most cases (22%) exploits were distributed free of charge in the form of links to source code. There are far fewer buy and sell offers (4% and 3% respectively); most of these offers relate to exploits that are not widely available in the public domain. The majority are for zero-day vulnerabilities, recently published vulnerabilities, and the most dangerous types of vulnerabilities (RCE and LPE). An RCE exploit for a website can cost up to $4,500, while one buyer offered to pay $30,000 for a zero-day LPE for Windows.

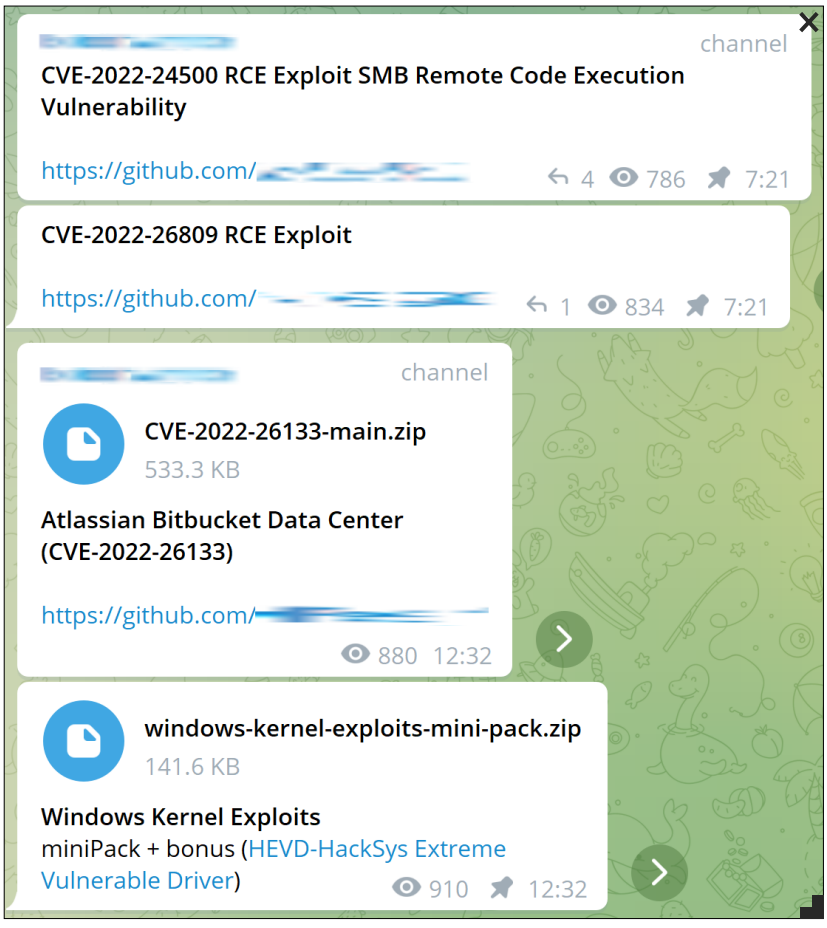

Figure 15. Free distribution of exploit source code

There are also comprehensive exploit tools that can detect and exploit not just one, but multiple vulnerabilities. Usually they are designed for a specific software product or framework. Tools for scanning Laravel-based websites (around 600,000 websites run on Laravel) are especially popular, featuring in 9% of exploit-related messages.

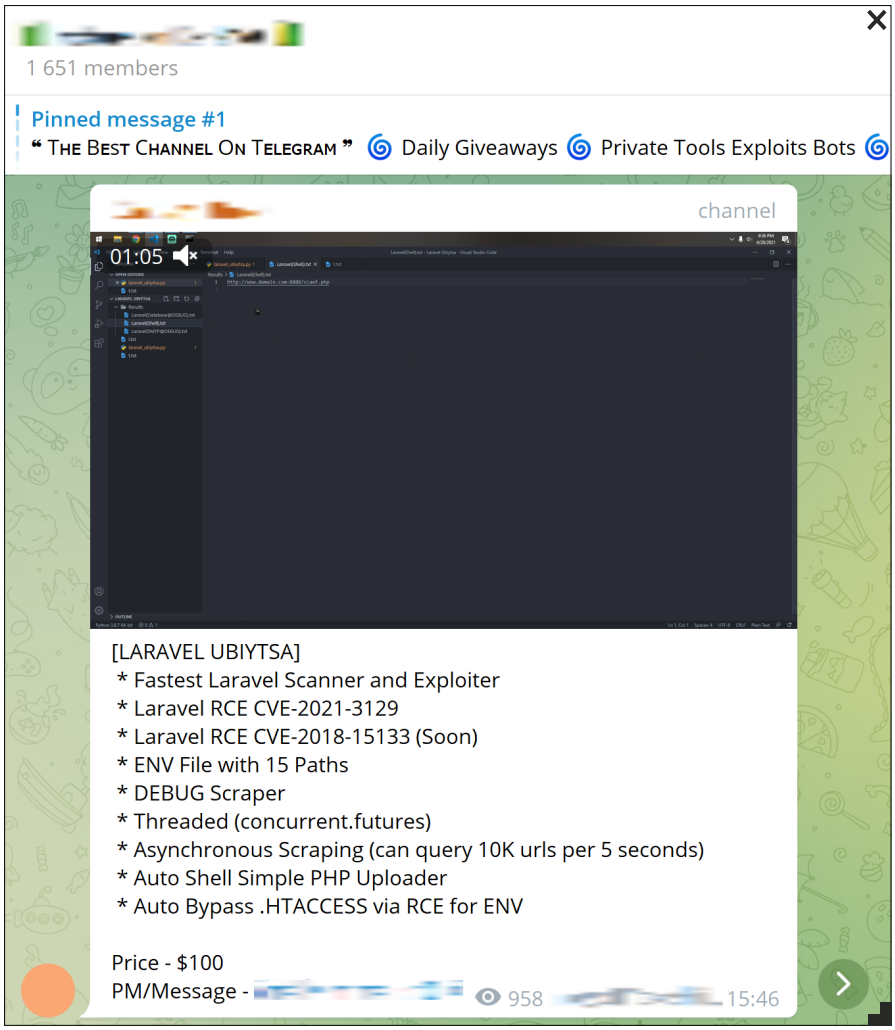

Figure 16. Vulnerability exploit tool for sale

In 17% of cases, exploits began to appear in messaging apps within 24 hours after a vulnerability was disclosed, but on average exploits for known vulnerabilities started appearing 13 days after publication. The most popular vulnerabilities in the first half of 2022 were:

- CVE-2022-26809 in Microsoft RPC
- CVE-2022-22965 (Spring4Shell) in Java Spring Framework
- CVE-2022-0847 (Dirty Pipe) in Linux
- CVE-2022-26134 in Atlassian Confluence
- CVE-2022-26133 in Atlassian Bitbucket Data Center

In addition, some flaws discovered a long time ago are still popular: for example, an RCE exploit for CVE-2017-9841 in Laravel was actively distributed at the end of June 2022.

Data

A significant share of all messages in this category is related to documents and personal data (43%), as well as user accounts (42%).

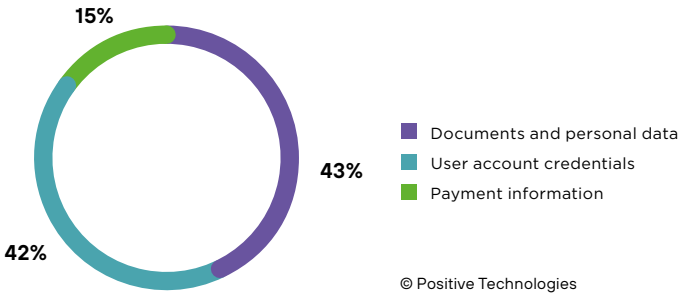

Figure 17. Messages related to data compromise

In 2021, user accounts were the subject of nearly half of all messages, but the predominant subjects in the first six months of 2022 were documents, personal data, and related services (71%). After numerous attacks and data breaches in Q1 2022, the number of services involving documents leaked from various institutions surged in Q2 2022.

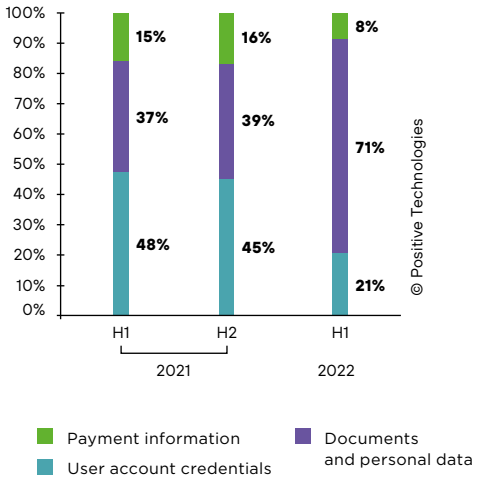

Figure 18. Messages related to data compromise

A significant portion of all messages on this topic (28%) are offers to sell data and data-related services (for example, forged documents and digital signatures), and about 10% of messages are offers to buy.

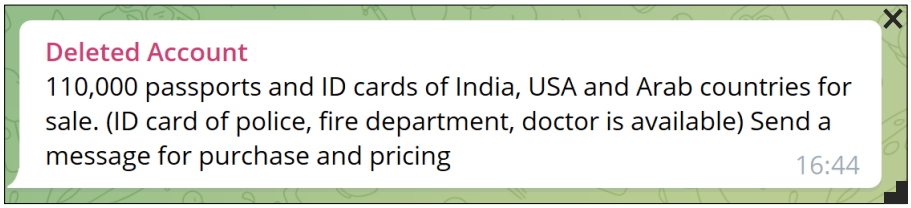

Figure 19. Message offering documents and personal data for sale

Cash-out services are gaining popularity, along with document forgery services. Forged documents are used, for example, to create and verify accounts, including bank accounts and crypto exchange accounts. The increasing level of demand may be due to the fact that many online services are now unavailable or only partially available to Russian users.

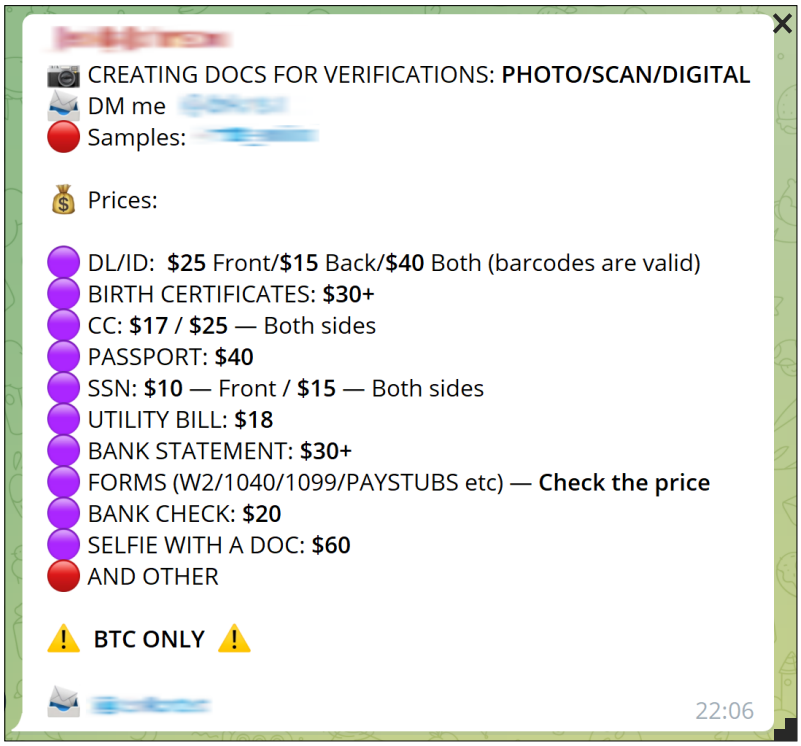

Figure 20. Message offering document forgery services

Most messages advertising user accounts for sale offer access to online services such as streaming platforms, social networks, crypto exchanges, and betting websites. A Spotify account can be purchased for $5, and a Netflix premium account with a year's subscription can sell from $10 and upwards. Crypto exchange accounts and accounts on betting platforms are much pricier, as they typically require government-issued ID for registration, and some accounts may already have some money deposited in them.

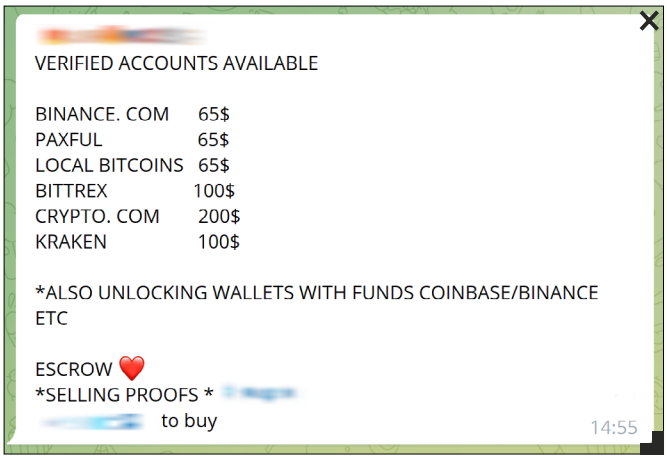

Figure 21. Message offering crypto exchange accounts for sale

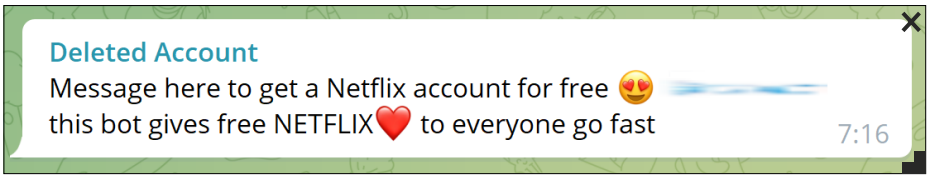

Figure 22. Netflix accounts offered for free

In Q1 2022 we reported an increase in the market for VPN accounts, and this tendency is reflected in Telegram activity. Compared to early 2020, the number of VPN-related messages more than tripled by 2022. NordVPN accounts, which are harvested by the infostealers mentioned in the malware section, are the most widely offered for sale.

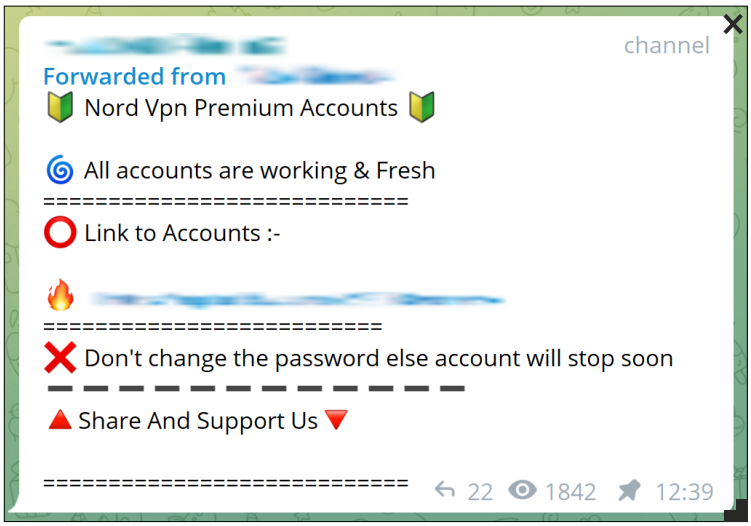

Figure 23. Message offering VPN accounts for sale

Corporate access

[1]A web shell is a file that an attacker can upload to a server and then use to execute OS commands through its web interface and gain access to other files.

This category includes messages offering access to corporate networks, for example user accounts for connecting to networks via remote access protocols and web shell accounts.[1] Such messages accounted for only 1% of the messages included in this analysis, but individual messages in this category can offer multiple accounts for access to networks of various companies. The volume of trade in corporate access accounts in public Telegram groups and channels still lags behind the volume observed on forums.

Most adverts offer to sell RDP, VPN, and web shell access, with prices starting at $7.

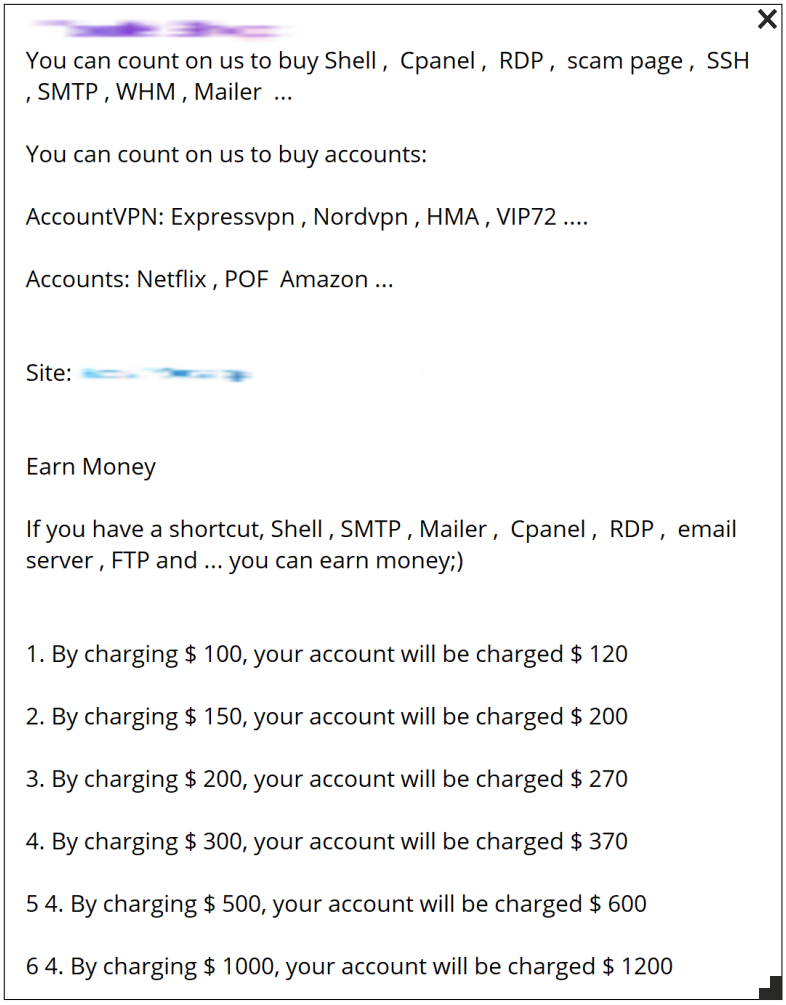

Figure 24. Message offering account access and soliciting cooperation

Cybercriminal services in messaging apps

Discussions relating to cash-out services account for 66% of all messages relating to criminal services. DDoS attacks rank second in popularity at 16%. About 9% of messages offer hacking services, including compromise of email and social media accounts, as well as hacking into websites and servers.

Among other offers are mass installation of malware (2%), traffic redirect from advertising networks (1%), targeted advertising, and services via other communication channels that can be used to direct victims to phishing websites or malware-infected websites.

Malware can be installed on victim's phones or computers by means of malicious attachments in messages, through botnets, or via watering hole attacks. This service is often provided as an option when criminals sell malware (for example, stealers and miners).

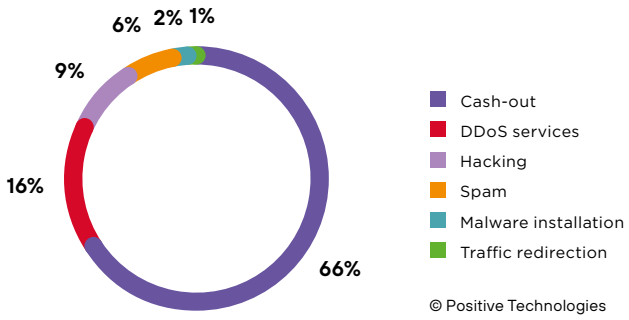

Figure 25. Messages about cybercriminal services

Execution of DDoS attacks

Every fifth message about DDoS attacks offers DDoS as a service, with prices depending on the attack duration: $8 for an hour, $40 for 24 hours, and at least $200 for a week. DDoS attack tools are distributed in the same way.

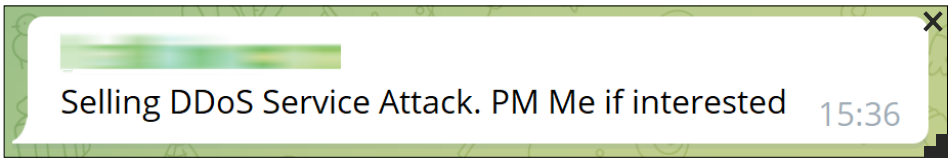

Figure 26. Advert offering DDoS services

The number of messages related to DDoS increased significantly in Q1 2022. This correlates with an increase in attacks against corporate websites in the same quarter.

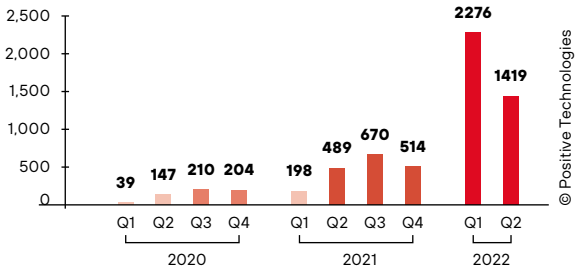

Figure 27. Volume of DDoS-related messages per quarter

This growth in the number of attacks can be attributed to the increased distribution of free DDoS attack tools in Q1. Some messages from that period called for attacks against particular servers.

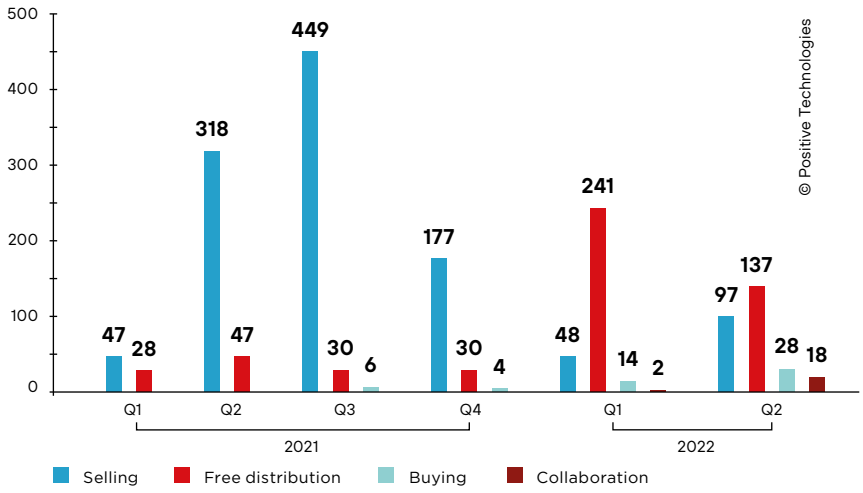

Figure 28. Categories of DDoS-related messages

In Q2 there were fewer messages about free DDoS tools, but the number of cooperation offers increased slightly: some cybercriminal groups switched their focus from distributing source code to looking for new recruits among their subscribers.

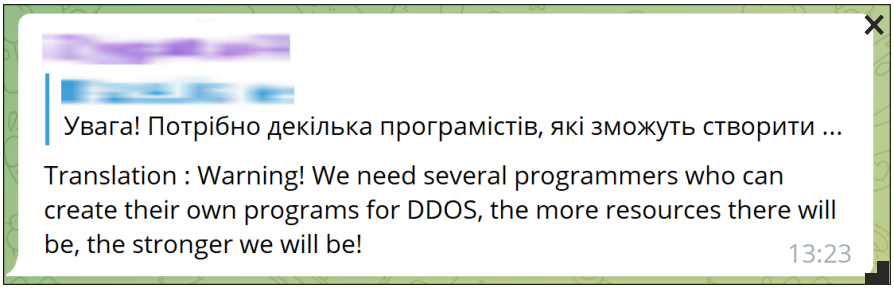

Figure 29. Recruitment advert

Hacking services

Most messages in this category (72%) offer hacking into social media and messaging app accounts like VKontakte, Telegram, WhatsApp, and Viber.

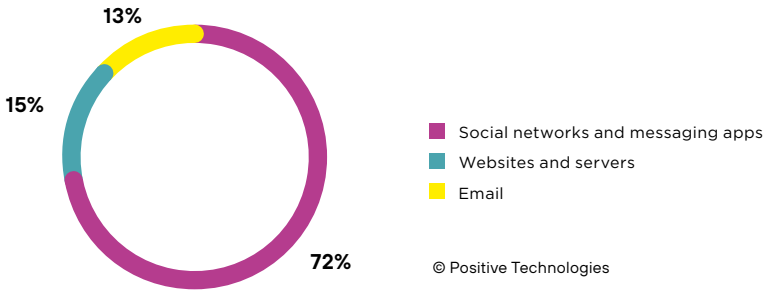

Figure 30. Hacking-related messages

Prices for hacking messenger accounts are much higher than for hacking social media accounts. Prices for hacking an account on the social network VKontakte range from $10 to $50, while prices for hacking a Telegram, Viber, or WhatsApp account start from $350.

Hackers charge $100 for breaking into a private email account and at least twice as much for a corporate email account.

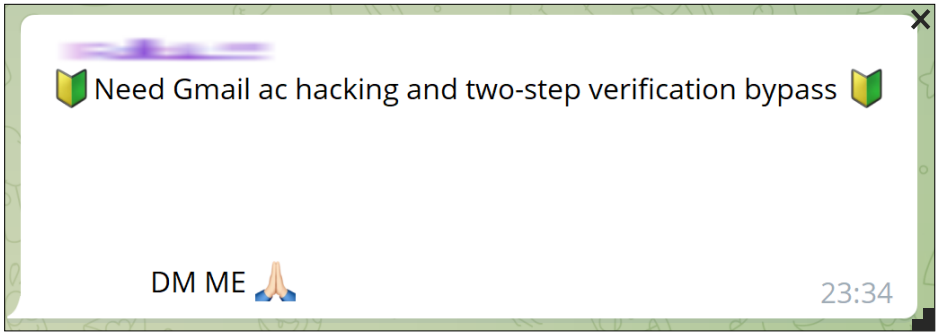

Figure 31. Message about email account hacking

Cash-out

Cash-out services are widespread and gain in popularity every quarter. The number of cash-out offers declined in Q1 2022 as a result of a crackdown in which many groups with illegal content were blocked, but in Q2 it returned to 2021 levels.

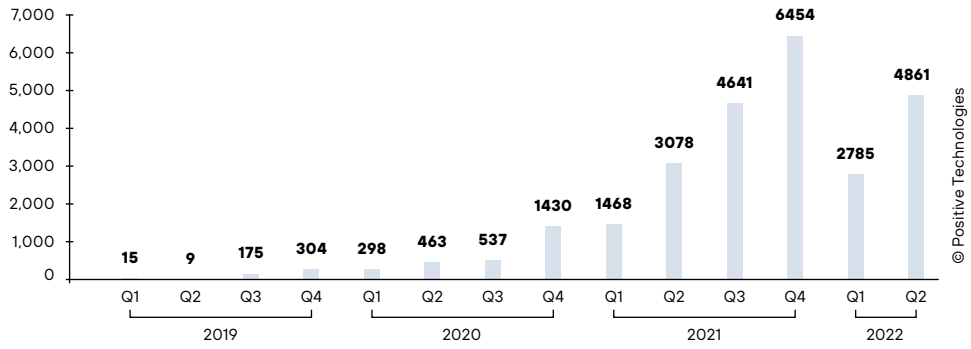

Figure 32. Number of messages about cash-out services

Sales adverts and service offerings make up 60% of all messages about cash-out services. Another 16% are offers to buy, and 3% solicit long-term cooperation.

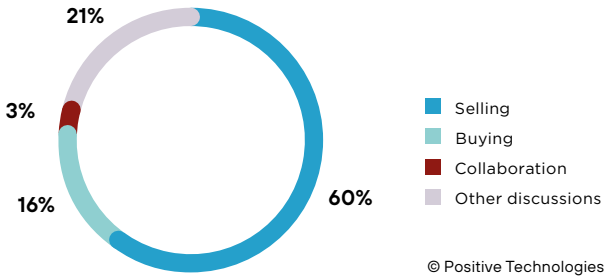

Figure 33. Cash-out service categories

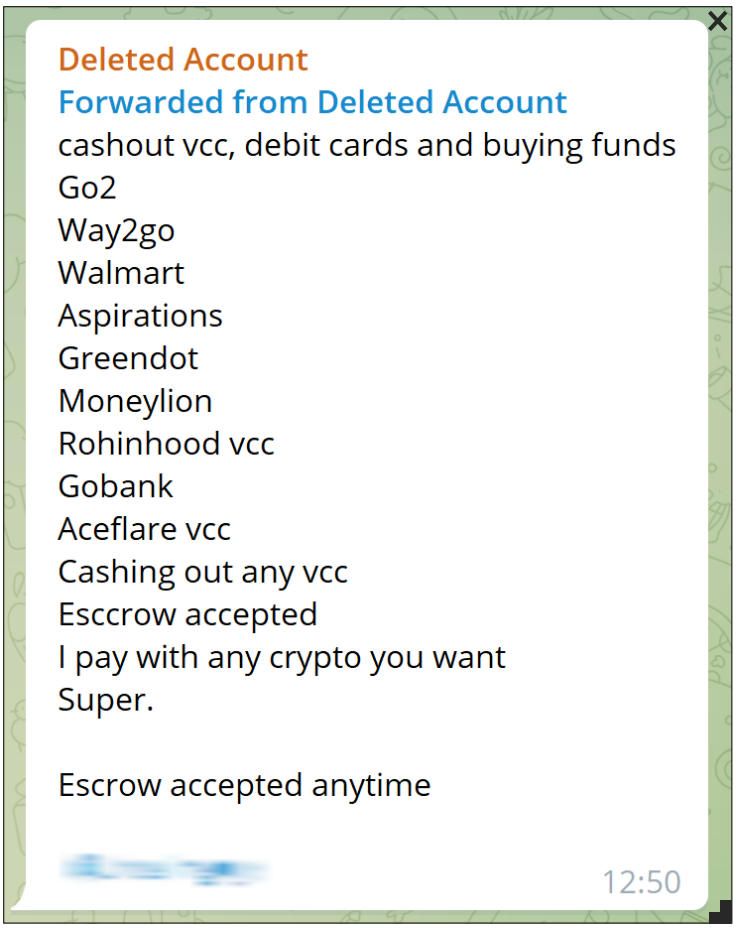

Figure 34. Message offering cash-out services

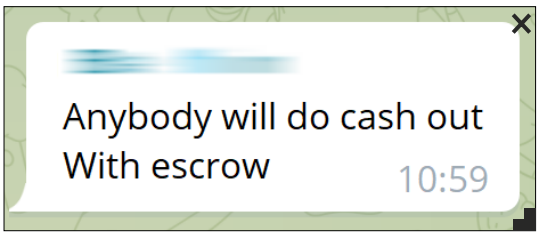

Figure 35. Message requesting cash-out services

Spam

Spamming services, including mass texting and mailing, account for 6% of service-related messages in Telegram. SMS spam is offered in 54% of messages, followed by email spam with 32%.

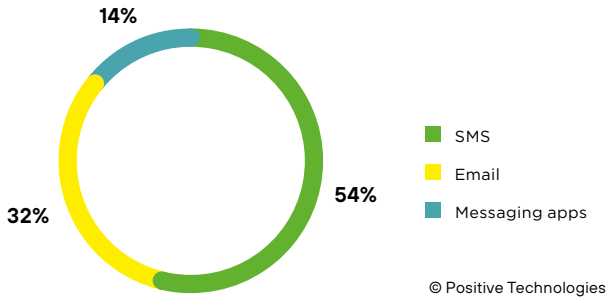

Figure 36. Types of spam tools in messages

SMS spamming services are often offered in combination with spam calls. Telegram is the most popular messaging platform for spamming.

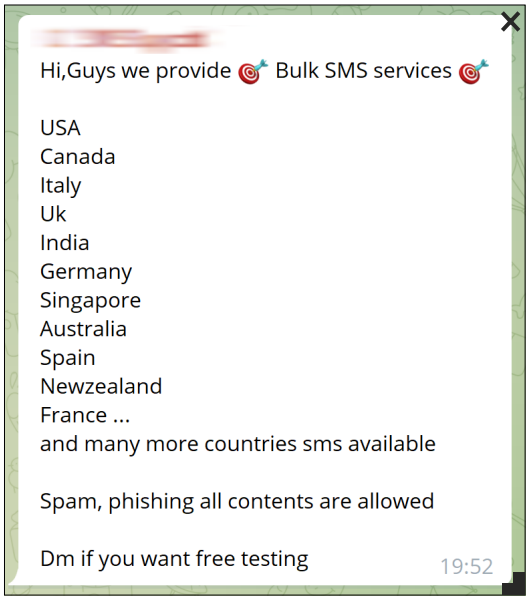

Figure 37. Message offering spamming services

Prices for spamming services usually depend on the campaign duration or the number of spam messages sent. Email flooding services for one email address cost about $1 per hour or per 1,000 emails.

Conclusion

The number of unique cyberattacks is constantly growing, and the market for cybercriminal services is expanding and moving into ordinary social media and messaging apps, thereby significantly lowering the entry threshold for cybercriminals. Our study reflects the current state of the cybercrime market in Telegram and gives reason to consider this messaging app as a valid source of information for cyberintelligence and cyberthreat forecasts that can be used in establishing information security processes. Timely responses to messages about upcoming attacks (for example, DDoS campaigns), new exploits, and compromised data can help organizations take preventive actions and avoid events that could lead to unacceptable consequences.

Cybercriminal_market_in_Telegram_A4.ENG.0004.03.NOV.09.2022