flare

Research Report

The Typology of Illicit Telegram Channels

Table Of Contents

Cybercriminals seem to always be looking for new and innovative ways to commit their crimes more efficiently. In the past, the dark web and parts of the deep web were some of the most common places where you can find cybercriminals committing their schemes. However, many criminals have moved over to more secure online messaging apps, such as Telegram, in order to continue their illicit activities publicly.

In recent years, Telegram has become increasingly popular for cybercriminals to create channels for individuals and groups to engage in criminal activity. This is due in part because Telegram allows for users to have end-to-end encrypted messaging capabilities, providing it is a secure platform to connect and communicate with others freely. Telegram also provides its users with more anonymity than other online messaging apps which makes it an attractive and easy avenue for illicit activities to occur without the ramifications of being caught by law enforcement.

The result of this increased criminal activity on secure messaging apps like Telegram has made it harder for authorities to proactively monitor and regulate illicit activities and content shared openly in these illicit communities. In this post we will cover why illicit Telegram channels are a growing issue, the common types and characteristics of these channels, risks and challenges related to these channels, and ways to mitigate the impact of these growing illicit communities.

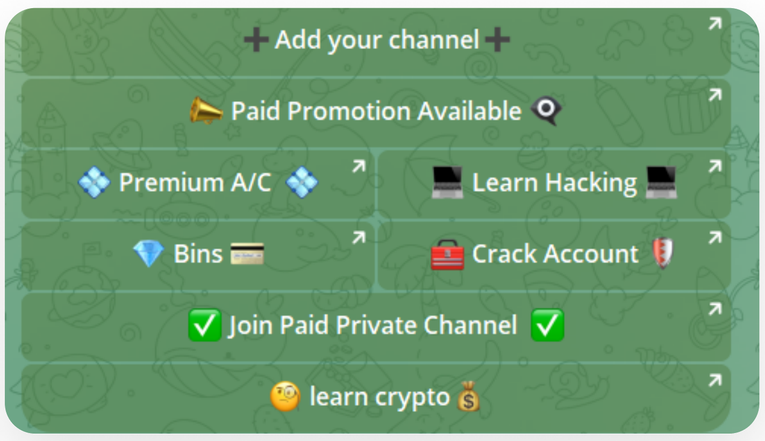
Illicit Telegram Channels: Why are they a Growing Issue?

The rise of Telegram and similar style encrypted messaging platforms have allowed countless users to connect and message others with more anonymity. While there are many channels on the platform that are used for legitimate communication possibilities to build private communities, a lot of channels have also been created for more nefarious reasons. The privacy of Telegram messaging has allowed more criminals and other malicious actors to grow **illicit Telegram channels** and communities specifically to conduct criminal activities.

One of the main reasons that Telegram has become a large hub for illicit activities is due to the ease of use and accessibility for users to locate and join many of these channels quickly. Although many of the illicit channels researched did require approval to join, there were numerous others that required no approval and were easily searchable once the app was downloaded successfully. For example, users can search for the criminal activity group they want to join of their choice and search the results to join the channels that fit their results successfully.

Another reason that illicit Telegram channels have been growing in popularity, is due in part to the rise in cryptocurrencies and other forms of digital currencies. Many cryptocurrencies offer users a greater level of anonymity and untraceability when it comes to exchanging payments between individuals and malicious groups regularly. Cryptocurrencies such as Bitcoin and Etherum are often some of the most commonly used on illicit Telegram channels since they are the most adopted forms of cryptocurrency used globally.

Many illicit Telegram channels also have increased in popularity given they often allow criminals to collaborate and share latest exploits with one another. The rise of online messaging apps, like Telegram, have allowed cybercriminals to connect and create more communities from all over the world. Additionally, many of these individuals and groups are more than willing to assist those new to cybercrime the ability to learn how to conduct attacks, hack, or conduct criminal activities themselves with the help of those more seasoned and experienced in these activities.



Screenshot from an illicit Telegram channel that shows buttons linked to various services.

Common Types and Characteristics of Illicit Telegram Channels

On Telegram there are many different types of channels that users can search for on the platform. Some of these channels can be fully legitimate and others nefarious. The illicit type of channels that can be found on the app can range from everything regarding financial fraud to radical organizations communicating their latest extremist activities and content.

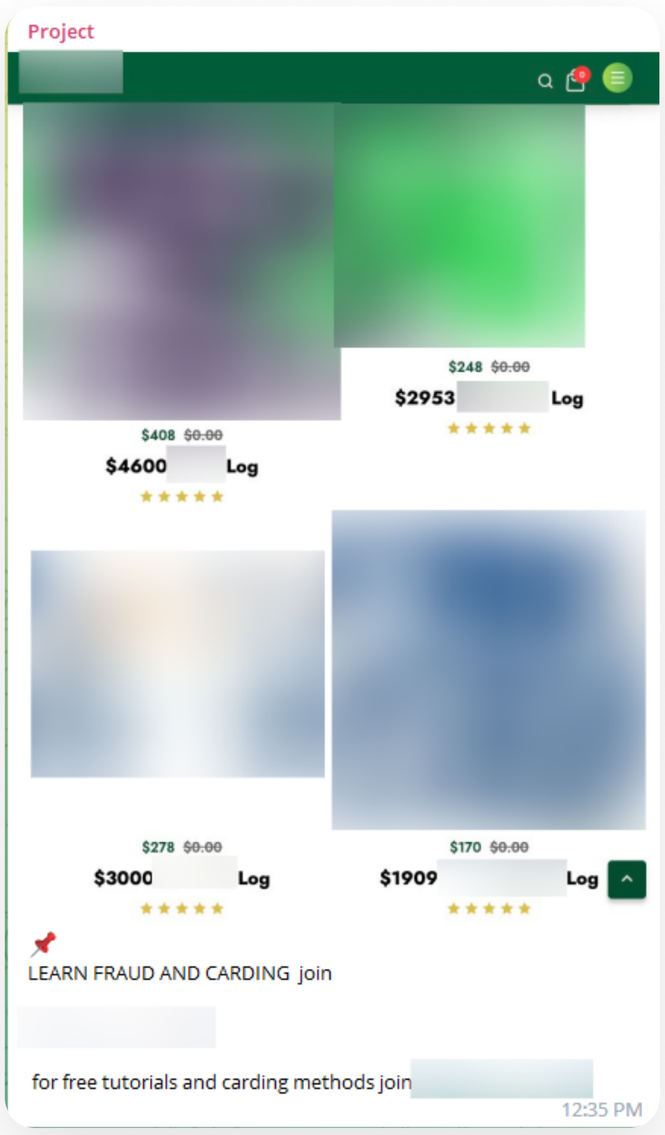
Many of these channels we studied in our in-depth research uncovered several different types of common criminal activity found to be popular on Telegram. The following are several of the most common types of illicit channels found on Telegram and the tactical characteristics surrounding the criminal activity that can be found on them.

1. Carding

Carding is one of the most commonly found illicit activities that is conducted on Telegram. Carding is essentially the practice of stealing credit card information from victims through various methods that can include phishing, skimming, and data breaches. Criminals will then take that information and sell it within the Telegram channel for a small fee.

What makes carding so lucrative, profitable, and popular among these illicit communities is the ease of use on the app and the accessibility. More seasoned hackers can sell their payload from a data breach or multiple successfully phishing attacks to others. For example, if a hacker is able to steal information from a large batch of victims then they can sell that data for a small profit.

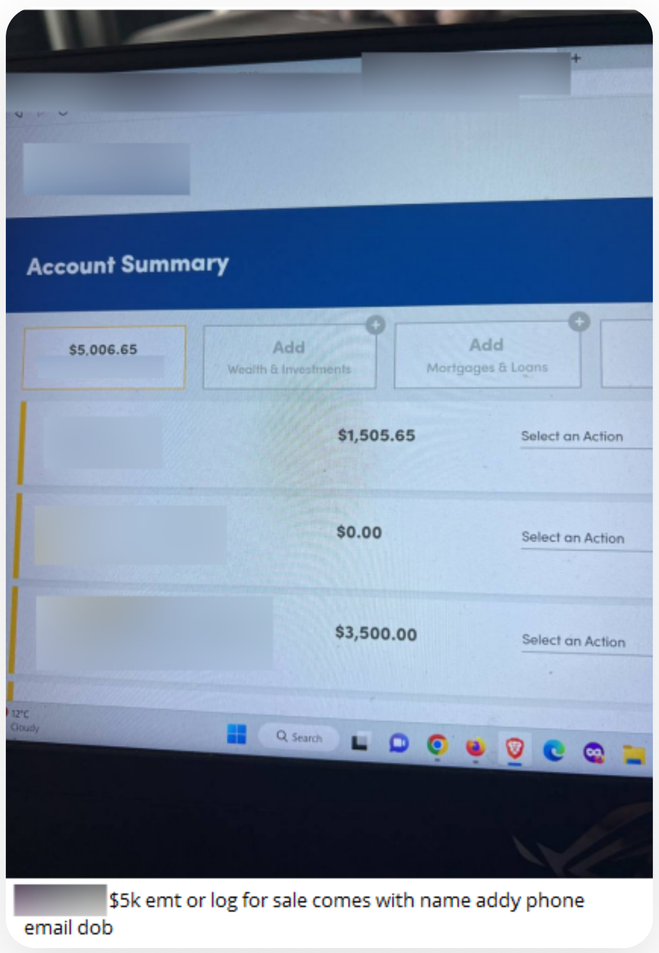
A threat actor sells stolen banking credentials for accounts with balances that range **from $221.78-$1,638.81 for $10-$40.**



A threat actor sells stolen credentials or logs for multiple bank accounts.

Many cybercriminals can also employ and program bots to post credit card information across multiple channels, increasing their profitability. Additionally, these channels can also allow criminals to easily share, collaborate, and sell carding tools, guides and training to help other malicious users conduct their own schemes successfully.

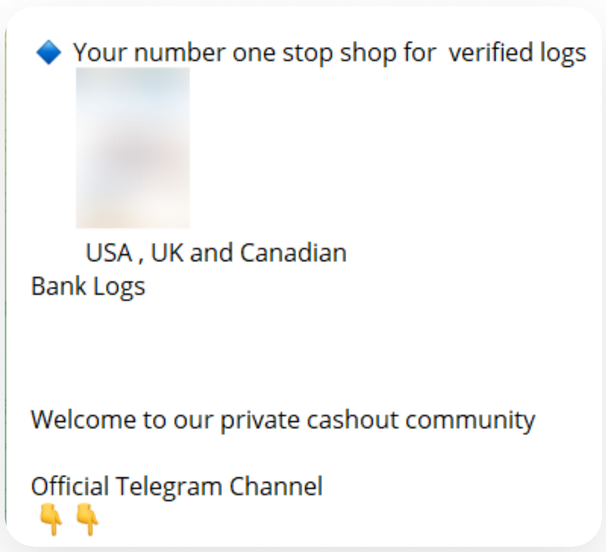
2. Bank Account Logins



A threat actor sells bank account information for an account with about a **$5,000** balance.

Bank account logins are another popular type of illegal activity that can be seen on many of the **Telegram fraud** channels found on the app regularly. Similar to carding, selling victim bank account information on Telegram can result in a high payout for criminals. This is due to the ease of access to stolen funds with minimal effort from purchasers on the channel.

Criminals that sell bank account logins often will find this type of malicious activity in high demand and low risk for getting caught by law enforcement. This can equal the seller to make a good profit on the payload successfully. Many of these cybercriminals often will acquire the information from phishing attacks or through large data breach batches acquired from hacking.



Selling bank account logins on illicit Telegram channels is also not limited to just bank account information. Several of the illicit Telegram channels we researched also offered account logins for payment apps. Users on the channels can also purchase account logins for other applications as well, like streaming services.

Screenshot of an advertisement for an illicit Telegram channel offering stolen credentials for various financial accounts.

3. DDoS

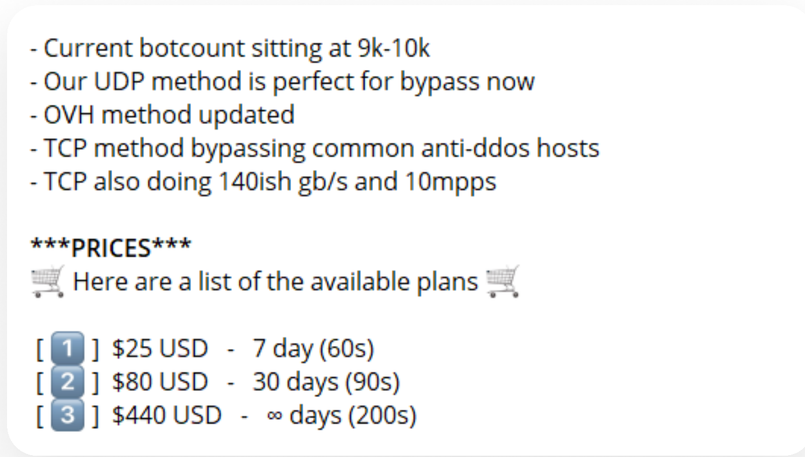
Over the past few years, secure messaging apps like Telegram have also been host to illicit channels that connect threat actors from all over the world without selling any stolen data. These channels are often made up of hackers that join together to conduct distributed denial of service (DDoS) attacks. While they may not be selling victim information like in the illicit channels that conduct carding or sell bank logins, these types of channels can still be dangerous to organizations around the world.

Screenshot of a DDos attack Telegram channel with links for other threat actors to join DDoS attacks on the multiple German organizations.

Due in part to the security and anonymity of Telegram messaging within channels is that it can allow for multiple parties to participate in active attacks against nation-states along organizations and businesses more effectively. These DDoS illicit Telegram channels allow hackers to also utilize bots to aid in the orchestration of their attacks.

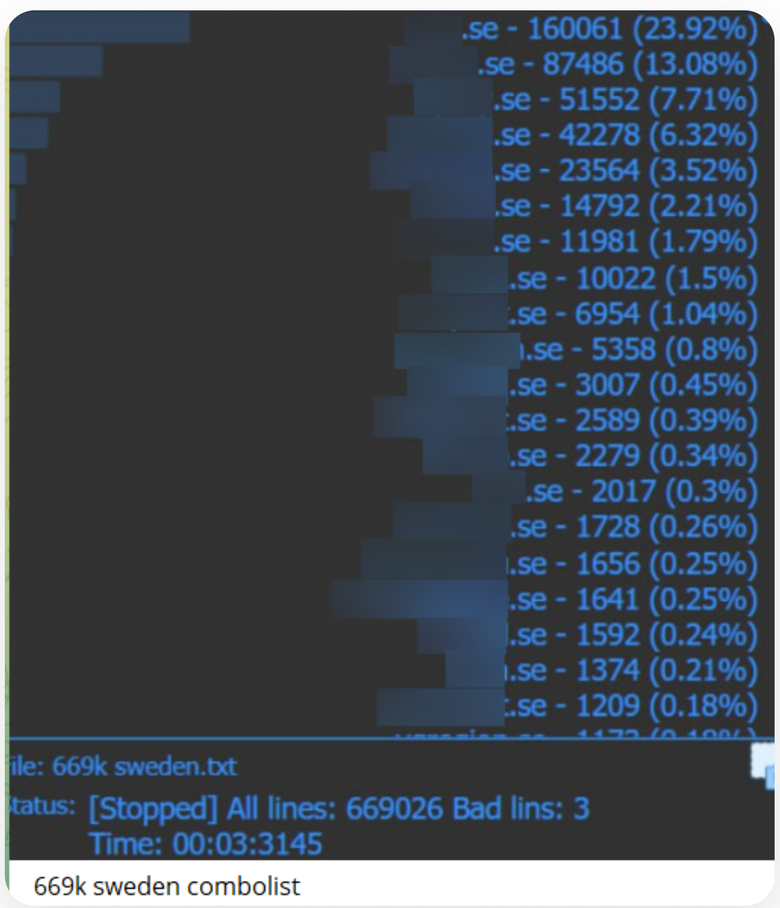
4. Botnets

Botnets have been used on illicit Telegram channels for a variety of reasons. Oftentimes botnets involve a network of compromised devices that are controlled and commanded by centralized servers. The administrators of these botnets, commonly known as botmasters, can then carry out a multitude of attacks against targets. These attacks can often include DDoS attacks, spamming, phishing attacks, credential stuffing, and other malicious activities.



A threat actor advertises subscriptions to their botnet channel.

Botnets are attractive to cyber attackers given that they can yield more anonymity plus also allow for increased reach and flexibility with the infected devices when deployed appropriately. Many botmasters will also often sell other botnets within illicit Telegram channels in order to help other criminals increase their own attack vectors successfully.



669k sweden combolist

A threat actor shares a combolist of stolen information from Swedish accounts.

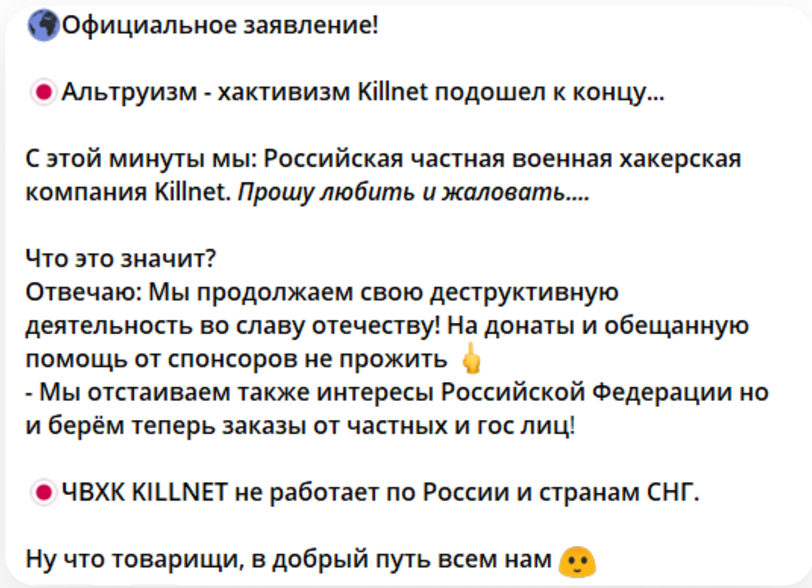
These combolists are often constructed with a large amount of sensitive user data that can include email addresses, usernames, passwords, security questions and answers, and access token information or API keys for bypassing authentication security on websites or applications. Combolists often are sold, shared, or traded on illicit Telegram channels in large amounts of data sets which can allow criminals to receive the information in bulk.

Combolists can be lucrative to acquire on illicit Telegram channels given they can provide cybercriminals widespread access to unauthorized access capabilities to conduct further attacks on organizations. They also provide a large amount of easy distribution in bulk and return on the purchase or trade given if some of the user data is not pliable to gain access to, there may still be a large amount of other combos that hackers can still steal from within the greater combolist they acquired.

5. Russian Hacktivism

Over the past few years hacktivism has been a growing issue Telegram due to the ease of access between multiple hacker groups. Among many of the illicit Telegram groups researched, Russian hacktivism was the most prominent. Many of the present Russian hacktivist groups that use Telegram do so in order to communicate, recruit, and share resources and tools with other hackers with the goal of joining their cause.

The issue with the Russian hacktivism on illicit Telegram channels is that it allows these groups to increase their attack vector and reach, causing more damage to targets. It can allow for more rapid information dissemination and radicalization among groups looking to share, train, and recruit more hackers to join their cause.

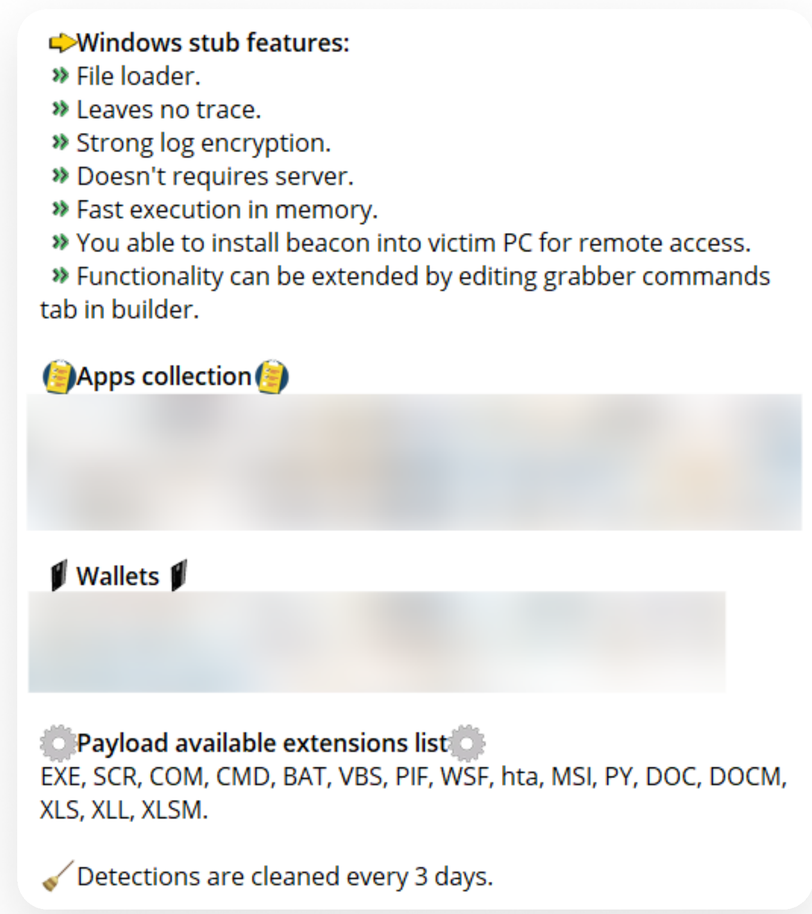


Russian hacktivist group recruits other threat actors.

More threat actors can then create more successful attacks against targeted organizations. This can also open up targeted organizations and businesses to the possibility of cross-border attacks for multiple different countries and hacker groups. Ultimately making the attack surface harder to manage against threat actors that join in these hacktivist groups.

6. Stealer Logs

Stealer logs are often another valuable item that is commonly sold on illicit Telegram channels. Many times these stealer logs can also contain data that includes passwords, usernames, credentials, credit card numbers, and other PII. In contrast to combolists, stealer logs are often data that has been collected via malware disruption from the victims of infected devices. These logs are then sold and distributed to other criminals for their own malicious use which can include conducting their own attacks against organizations.



Threat actor sells stealer logs and outlines various features.

Challenges Related to Illicit Telegram Channels

As the rise of criminal activity and illicit channels on Telegram continues to increase, the app has attempted to take measures to mitigate these issues more effectively. Within their **Terms of Service** agreement, Telegram states that by joining users agree to not engage in illicit activity. Users are often encouraged to report any criminal channels or activity on the app directly. Although Telegram has stated that it does not support or condone any illicit activity on the app, **many countries have enforced bans** from using the app legitimately.

Many individuals and companies have continued to be targeted by cybercriminals using Telegram due to the illicit channel activity that can occur on the app regularly. Here are some of the risks and challenges that many organizations continue to face from the online criminal activity still occurring on Telegram:

1. **Data breaches** – countless illicit Telegram channels often will sell user data, personally identifiable information (PII), account logins, credit card information, and other confidential information obtained through various methods to the other criminals for a profit.

2. **Reputational damage** – organizations can face the ramifications of malicious content or data shared on illicit Telegram channels. This can cause brands to lose profits, shareholders, and stock values due to reputational damage.

3. **Difficulty in monitoring criminal activity** – Telegram's purpose is to provide end-to-end encrypted messaging for users of the platform. Although it can be a secure way to communicate with others, the lack of stored metadata, such as IP addresses, associated with the app can make it challenging for organizations to proactively mitigate the criminal activity targeted at them when conducted on the platform.

4. **Operational disruptions** – the amount of malware and DDoS attacks that can be spread and shared within many illicit Telegram communities can cause operational damages to companies. For instance, some criminally motivated DDoS groups can promise to take an organization's website offline for up to 24 hours or more. This can cause disruptions to daily operations, systems, and supply chains.

5. **Intellectual property piracy** – in addition to data leaks, cybercriminals can leak confidential data from organizations within illicit Telegram channels regularly. This malicious content can be shared openly about organizations which can include their copyrighted content, trade secrets, controlled data, and other confidential information pertaining to that organization. It can lead to brand damage, financial losses, and more.

6. **Legal fines and penalties** – the malicious content that can be shared with others on illicit Telegram channels can ultimately cost businesses legal fines and penalties. Even organizations who have enlisted practical cybersecurity measures can still become a target victim within some of these illicit communities.

About Flare

Flare is the proactive external cyber threat detection solution for organizations. Our AI-driven technology constantly scans the online world, including the dark and clear web, to discover unknown events, automatically prioritize risks and deliver actionable intelligence you can use instantly to improve security.

Want to learn about how Flare can support dark web monitoring for leaked credentials?

flare.io • hello@flare.io

Free Trial **Book a Demo**

flare