Tomorrow's Affairs
Analysis of today
Assessment of tomorrow

By: The Editorial Board

How Russian services gain access to encrypted conversations without breaking the encryption

On 26 June, the FBI and CISA released an updated public warning about a campaign in which Russian intelligence actors continue to compromise accounts on commercial encrypted communications applications. The document follows up on the March warning but reveals that Russian intelligence has improved its tactics in the meantime.

In the earlier phase of the campaign, attackers mainly relied on extracting verification codes and PINs. In the new pattern, their goal is increasingly to obtain keys for recovering message backups. At first glance, this may appear to be a technical detail that concerns only how applications store data. In practice, it is a far more serious shift.

The attack is no longer just about taking over accounts or accessing future communications. It is aimed at the user's past, at the archive of conversations spanning months or years of private and group communication, which is often much more valuable than anything yet to be written.

This warning shows that Russian intelligence services are adapting not only to technological changes, but also to the habits of their targets. Politicians, diplomats, military officials, journalists, and members of the security services now use encrypted applications every day to share sensitive information, believing that these are more secure than email or other communication channels.

That is why Russian actors are not trying to break the encryption of those applications. It is much easier to get the user to provide access to a backup of their conversations and thereby obtain what is far more difficult to access technically.

Who are the real targets of Russian services?

The FBI and CISA alert identifies a clear group of targets: current and former US and international government officials, military personnel, political figures, journalists, and key officials in Ukraine. According to US agencies, thousands of accounts have been compromised so far.

US services track this activity under the designations UNC5792 and UNC4221. According to their assessment, members of the Russian Federal Security Service (FSB), including officers assigned to the FSB Border Service, as well as operatives linked to Russian military intelligence structures, are participating in the operation.

The choice of targets is not random. People involved in decisions about support for Ukraine, planning on NATO's eastern flank, military assistance, political coordination, or public reporting on the war have a value that is not measured solely by the positions they formally hold.

> The user does not feel that they are doing something risky

Their conversations often reveal institutional mindsets, gaps between public attitudes and private assessments, the degree of trust between partners, weaknesses in coordination, and the limits of political readiness for certain decisions.

For an intelligence service, the record of such conversations can be more valuable than an individual classified document. It enables the reconstruction of relationships, decision-making rhythms, and the informal channels through which information is transmitted.

A compromised account can reveal not only what the account owner knew, but also whom he spoke to, who trusted him, which groups he joined, and how attitudes changed over time.

This is why the specific emphasis in the US warning is important. Attackers are not trying to break the encryption of the applications themselves; they exploit the human factor, user trust, and features designed to protect data.

This is precisely why this method is much

more dangerous than phishing. The user does not feel that they are doing something risky. On the contrary, they are convinced that they are further protecting their account, while in reality they are giving the attacker access to a backup copy of their conversations.

The new target is backup

Special attention is drawn to the way the campaign was designed. The FBI and CISA have released examples of messages that attackers use to gain the trust of their targets.

One pattern appears as an urgent warning about possible data loss and asks the user to enable backup and submit a recovery key. The second mimics a notification from the app itself, claiming that the attacks were carried out by hackers from Iran and post-Soviet countries, and advising the user to activate backup to save their messages.

> Messages are aimed at people who already live in a high-risk environment

Such messages are not ordinary spam. They are aimed at people who already live in a high-risk environment, follow news about cyber-attacks and understand that they can be targets.

Therefore, the attacker does not present themselves only as technical support; they also try to tap into the user's realistic fears. A message does not have to be perfect to be effective; it only needs to arrive at the moment when the user believes they are acting pre-emptively.

Why the archive is more important than instant access

In high-risk communication, the biggest mistake is to assume that the only thing that matters is protecting what is happening now.

In intelligence work, the past often has greater value. It shows how a decision was made, who influenced it, who opposed it, who hesitated, and where there were gaps in coordination. One message may be interesting; thousands of messages can form a map of relationships.

That is why switching to backup keys is important. An attacker who gains access to message history does not just obtain content; they obtain context.

In group conversations, they can see who takes the initiative, who remains silent, who passes on information from other circles, who has access to political or military assessments, and how internal thinking changes after certain events. Such a picture cannot easily be obtained from public statements, press conferences or formal documents.

> An attacker who obtains an archive of conversations does not just see the messages; they see the process

The problem is even more serious because the subsequent reaction does not undo the damage. The FBI and CISA emphasise that generating a new recovery key invalidates the old one for future downloads but does not delete any copies that have already been downloaded.

In other words, the user can reduce future risk but cannot recover what has already been lost. From an intelligence perspective, that is enough. Once downloaded, the archive continues to exist in the hands of the attacker and can be analysed for months.

This makes this type of compromise particularly dangerous for institutions that use encrypted applications as informal but permanent work channels. In many state and international structures, such applications are no longer just auxiliary tools. They are spaces where coordination is accelerated, positions are checked, drafts are exchanged, meetings are arranged, and policy assessments are tested before they become formal documents.

An attacker who obtains an archive of those conversations does not just see the messages; they see the process.

The Russian method is adaptation, not improvisation

The campaign reveals a pattern that is important for understanding Russian intelligence work in the digital space. When one method becomes known, the actors do not give up; they change their approach.

After warnings about extracting codes and PINs, the focus shifted to a feature users perceived as protective. The backup was introduced as a precaution, then became a point of penetration.

Russian actors apparently monitor not only the technical capabilities of apps, but also how they are used by people in political, military and media circles. They understand that many users have learned not to share verification codes.

Therefore, the pressure shifts to more complex functions, where the user is not always sure what is a normal procedure, what is a warning from the application itself, and what is an attempted compromise.

> The new tactic asks users to do something that seems responsible

This change also has a psychological dimension. Phishing asks the user to do something obviously risky. The new tactic asks them to do something that seems responsible: saving messages, activating backups and protecting data.

That is its strength. It does not rely solely on ignorance among technically illiterate users. It exploits fatigue, haste, constant pressure, and the normalised sense that attacks are possible every day.

For people working on Ukraine, NATO, military issues or sensitive political files, such a message may seem credible precisely because the threat is not fabricated. They really can be a target.

The attacker therefore does not have to construct a false reality from scratch; it is enough to embed the attack within the existing climate of caution.

A problem for governments and newsrooms

Individuals whose accounts have been compromised are not the only ones at serious risk. The risk extends to the entire networks in which these individuals participate.

A journalist's account can reveal sources, editorial conversations, communications with officials and unpublished assessments.

An official's account can reveal consultations with allies, internal dilemmas and the names of people not publicly associated with a particular process.

A single account from a military or security official can reveal the rhythm of coordination, even when it does not contain formally classified information.

Therefore, it is mistaken to view such incidents as a problem of individuals' digital hygiene. In institutions that work with sensitive information, a private account on an encrypted application is often not truly private; it becomes an extension of professional communication.

For newsrooms, especially those covering war, intelligence issues or international relations, this risk is just as serious

If meetings are arranged through it, assessments shared, contacts exchanged or decisions commented on, then compromising it has institutional consequences.

For newsrooms, especially those covering war, intelligence issues or international relations, this risk is just as serious. Journalists often protect the trust of sources through encrypted applications. If an attacker gains access to the communication history, the damage does not affect only the journalist.

It can endanger people who spoke under conditions of confidentiality, reveal the direction of future texts, and allow the opposing side to prepare a reaction or a discrediting campaign in advance.

For governments, the problem is even greater. Formal communication systems may be well protected, but real work often moves faster than formal procedures.

Encrypted applications fill the space between official channels and the urgent need for coordination, and this is exactly where the weakness arises: the more useful the channel, the more valuable the target becomes.

What must change

For institutions that use encrypted applications every day, the biggest challenge is no longer which application to choose, but how to manage it.

The warning from the FBI and CISA shows that even a secure platform can become a serious source of risk if an organisation does not have clear rules for backing up messages, recovering accounts and retaining communication history.

This is precisely why backup can no longer be left solely to the user. If official or professional communication is conducted through a particular application, the way backups are stored must form part of the institution's security procedures. Otherwise, a single employee's decision can jeopardise the communication of an entire team or organisation.

> The archive that remains accessible for years on a single user account is exactly what is most valuable to an attacker

In closed groups, it is often assumed that an account is the same as the person using it. Such campaigns rely on this assumption. Any unusual request involving verification codes, recovery keys, backups, device changes or account reconnection should be confirmed through another communication channel. This is not an expression of distrust, but a basic security procedure.

Institutions and newsrooms should also review how much sensitive data is stored in these applications. The larger the archive and the longer it is kept, the more value a successful attack can yield.

It is therefore important to define clearly what information should be exchanged through these channels, how long it should be stored, and when communication should be moved to more secure systems. The archive that remains accessible for years on a single user account is exactly what is most valuable to an attacker.

The wider significance of the campaign

This campaign comes at a time when communications about Ukraine, NATO's eastern flank and European security are of high intelligence value. Public statements reveal political positions. Private conversations show how firm those positions are, where any doubts lie, and how far partners are prepared to go beyond what is publicly stated.

For Russia, access to such exchanges can help it assess Western resolve, plan pressure, identify divisions among allies, and guide propaganda or diplomatic activity.

That is why it is not just about account theft; it is an attempt to penetrate the everyday nervous system of political and security coordination.

The campaign comes at a time when communications about Ukraine, NATO's eastern flank and European security are of high intelligence value

In modern crises, much of the decision-making does not take place in a single formal document or a single meeting. It happens through a series of quick messages, reactions, consultations and checks. Whoever sees that flow sees far more than the final decision.

Russian actors understand this. Instead of spending resources on a frontal attack on encryption, they target the points where users themselves equate security with convenience.

Backup, account recovery and message history transfer exist because people do not want to lose data. In the intelligence context, this same need to preserve continuity becomes a weakness.

Further development of the campaign will likely follow the same logic. Messages will become more credible, better tailored to the applications the targets use, and more closely linked to current security incidents.

The focus may also shift to other functions that users perceive as protective or administrative. Any feature that relies on user trust can become an entry point.

For security services, this warning confirms that protecting confidential communication will depend less on the technology itself and more on the organisation of work.

The weakest point is no longer the encryption algorithm, but the day-to-day procedures that determine how accounts, backups, and user identities are managed.

This is precisely why, in the coming years, most competition between intelligence services will be driven by the human factor rather than by attempts to break encryption.