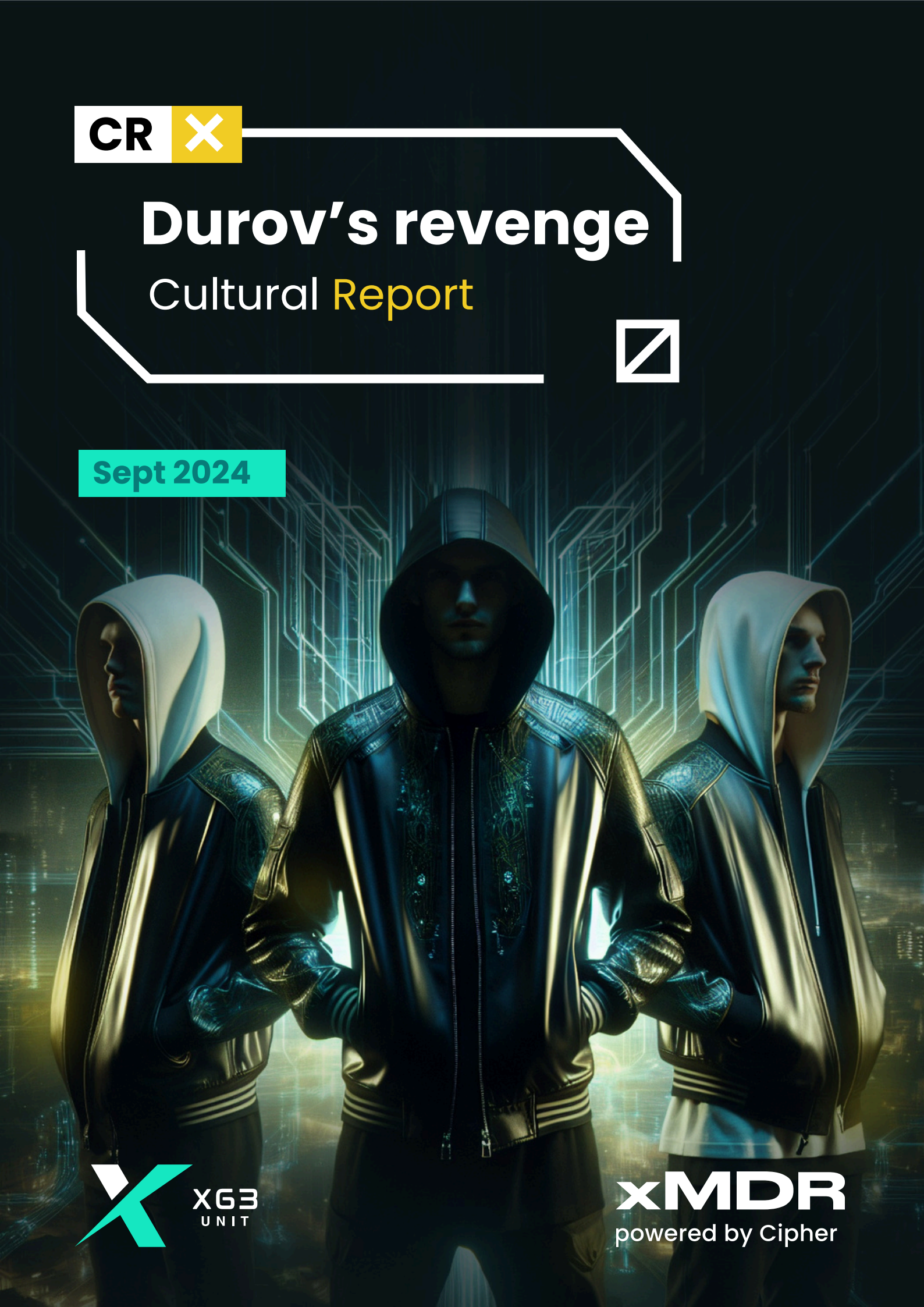
CR X

Durov's revenge

Cultural Report

Sept 2024



XG3 UNIT

xMDR powered by Cipher

Introduction

Last weekend, 24th augoust, French authorities arrested Telegram CEO Pavel Durov during a trip to Paris. He was arrested in connection with an investigation into the lack of moderators on Telegram, something he had previously denied. Durov is accused of failing to take action to curb criminal use of Telegram. The app is accused of failing to cooperate with authorities on drug trafficking, child sexual content and fraud. The judge finally charges Durov, founder of Telegram, and releases him on €5 million bail, he must also report twice a week to the police station and may not leave the country.

On the other hand, Durov's defenders consider his arrest a political arrest. Even the Russian authorities have not been granted access to Durov, in another power play between the West and Russia. The Russian government requested his extradition, but France rejected the request.

About Pavel Durov

Pavel Durov is a Russian entrepreneur and programmer best known as the founder of Telegram and the social network VKontakte. Nicknamed 'the Russian Mark Zuckerberg,' Durov is known for his strong stance in favour of freedom of expression and online privacy, principles that have guided Telegram's development. After facing political pressures in Russia, he left the country and became a digital nomad, devoting himself fully to Telegram's global growth.

About Telegram

Telegram is an instant messaging app that is distinguished by its focus on privacy, security and the ability to create large communities of users. Launched in 2013, Telegram allows the exchange of text messages, images, videos and files up to 2 GB, as well as offering features such as secret chats with end-to-end encryption, and the option to self-destroy messages. Its flexibility, coupled with its cloud-based architecture, has made Telegram a popular tool for both personal and professional use.

However, these same features that prioritise privacy and security have made Telegram an attractive platform for cybercriminals. Telegram groups and channels are used by malicious actors to coordinate illegal activities, such as selling stolen data, distributing malware, organising DDoS attacks, and spreading extremist propaganda. The ability to create channels and groups with thousands of members, often under pseudonyms and with minimal oversight, facilitates the coordination and expansion of these illicit activities. In addition, the use of bots on Telegram enables the automation of criminal tasks, such as running illegal shops or distributing phishing on a large scale.

Revenge: The hacktivist motivation

The recent arrest of Telegram founder Pavel Durov has triggered a series of cyber attacks against sites in France by hackers and hacktivist groups.

Hacktivist groups are usually driven by a set of ideals, often linked to defending freedom of expression, privacy and opposition to what they perceive as authoritarianism or government repression. The arrest of Durov, a symbol of resistance against state surveillance and an advocate for digital privacy, is interpreted as a direct attack on these core values. For hacktivists, Telegram's lack of cooperation with the authorities, which possibly influenced Durov's arrest, represents a stance they themselves take in their fight against state control.

Influential factors

Several factors influence the nature and scale of the hacktivist response:

Symbolism of the Affected Figure: Pavel Durov is not just a tech entrepreneur, but a symbol of resistance against state surveillance. His arrest has a significant impact on the perception of injustice among hacktivists, intensifying the need for a response.

Perception of Injustice: The narrative of the arrest as an unjust act by the French state generates a strong emotional response, mobilising hacktivists to act in defence of their ideals.

Solidarity within the Cyber Community: The often dispersed but ideologically aligned hacktivist community tends to unite quickly in the face of what they perceive as a shared threat. This solidarity amplifies the response, resulting in coordinated and larger-scale attacks.

Publicity and Outreach Strategies: Hacktivists use attacks not only to cause harm, but also to attract media and public attention, amplifying their message and gaining support for their cause.

Historical Grievances and Long-standing Animosities: Hacktivists often act on accumulated grievances, not just immediate events. Long-standing tensions between certain groups and state actors can exacerbate responses, leading to more intense and widespread actions. The arrest of Durov could have reignited old conflicts or feelings of oppression, prompting a stronger and more widespread hacktivist retaliation.

Groups involved in revenge

So far, two main hacktivist groups have carried out attacks in response to Pavel Durov's arrest:

RipperSec: This hacker group is known for its focus on hacktivism, using cyberattacks as protest tools against government and corporate entities. RipperSec conducts defacement campaigns and DDoS attacks, motivated by political or social causes, and has gained notoriety for its aggressiveness and technical prowess in cyberspace.

Usersec: A hacktivist collective that organises itself to carry out cyber attacks motivated by political, social or ideological reasons. They are characterised by their use of DDoS attacks and website defacement, seeking to draw attention to issues of global concern and challenge institutions they consider oppressive or corrupt.

Cyberdragon: A hacker group that specialises in targeted attacks against critical infrastructure and high-security systems, using advanced cyber-espionage methods. This group operates in the shadows and is known for its ability to infiltrate sensitive networks and extract valuable information, often acting for geopolitical purposes.

Russian Army Cyber Team: This group is aligned with Russian interests and is known for carrying out sophisticated cyber-attacks in support of pro-Russian causes and policies. They have been linked to operations that seek to destabilise Western entities and support state agendas, using a hybrid warfare approach in cyberspace.

CgpIlnet: An emerging group on the dark web, specialises in selling hacking tools and illicit cyber services. Although less well known than others, its focus on trading exploits and malware makes it a relevant player in the online criminal ecosystem.

VulcanSec: VulcanSec is a hacker collective that focuses on breaching security systems by exploiting vulnerabilities and developing malware. They are known for their advanced technical capabilities and have been involved in multiple cyber-attack campaigns, often for financial or sabotage purposes.

EvilWeb: Cybercriminal group that carries out attacks for financial gain, mainly through data theft and extortion. Their activities include the development of ransomware and other forms of malware, and they have been responsible for incidents that have caused significant financial damage to their victims.

GraveNet: GraveNet specialises in the development and distribution of advanced malware, and is a key player in large-scale cybercrime campaigns. This group not only creates malicious tools, but also distributes them to other criminal actors, facilitating a wide range of illicit activities on the dark web.

Implications and Consequences

The arrest of Pavel Durov and the subsequent response by hacktivist groups highlight the **growing tension** between governments seeking to exert control over digital platforms and collectives that perceive this surveillance as a violation of fundamental rights. This conflict is not an isolated phenomenon, but reflects a global trend in cyberspace, where the actions of states can trigger immediate and amplified responses by non-state actors, further complicating cyber security globally.

The cyber attacks that followed Durov's arrest not only highlight the technical and organisational capacity of these groups, but also the depth of their ideological convictions. **Revenge and the defence of digital freedom** emerge as the main drivers of these actions, which seek to challenge the power and authority of states in a space where traditional borders are meaningless.

This phenomenon is representative of a **new era in cyberwarfare**, where hacktivists act as ideological warriors, armed not with traditional weapons, but with digital tools capable of causing significant impact on critical infrastructures and people's daily lives. Durov's figure becomes a symbol of resistance against what many perceive as the invasion of privacy and online censorship, intensifying the conflict between state power and individual freedom in the digital age.

In conclusion, Pavel Durov's arrest has served as a **catalyst for hacktivist groups** to unleash retaliatory attacks, motivated primarily by revenge and the defence of their ideological principles. This event highlights the importance of understanding hacktivism not only as a criminal activity, but as an ideological movement with deep roots in the defence of digital freedom. Moreover, the swift and coordinated reaction of these actors underlines the growing influence that hacktivist movements can exert on global politics and power dynamics in cyberspace.

Data Digital Adversary

Threat Actors 6

Top Most Relevant

- DarkSalmon Cosmos Taurus
- Darkred Cosmos Taurus
- Black Masker Army

Tools 1

Top Most Relevant

- ShrinkLocker

TTP'S 36

Top Most Relevant

- Exploit Public-Facing Application
- Ingress Tool Transfer
- Phishing

xMDR

Durov's revenge

Cultural Report

SEPT 2024

xMDR
powered by Cipher