The Dark Side of Digital Connection: Panel Data Breach

An analysis of the massive personal data leak on platforms like Discord and Telegram, its origins, and the resulting ethical and security crisis.

The Pandemic's Digital Shift

Retreat from Social Life

Early 2020s: People, especially youth, moved social activity online due to confinement.

Rise of Online Gaming

Increased activity on game servers led to a demand for better moderation and rule-enforcement.

Need for Real Identity

Server owners, unable to access anonymous players' real details, started seeking personal data to detect cheaters.

What began as a need for safer gaming quickly escalated into a demand for personal data.

Escalation: From Cheating to Crime

First Breach

A server owner used an insurance agency contact to identify a cheating player.

Realizing Data Power

Other server owners recognized the power of personal data for exposure and bullying.

Demand for Doxxing

The harmless request turned into a demand for data to commit crimes and expose others.

The Panel Software and Data Acquisition

Targeting Government Systems

Admins, seeking more data for their "panel" software, began attacking government-linked systems holding nationwide records.

- Targets included MHRS and e-Devlet.

- Admins, often under 20, successfully breached these systems.

- Result: Personal data of about 101 million people was stolen.
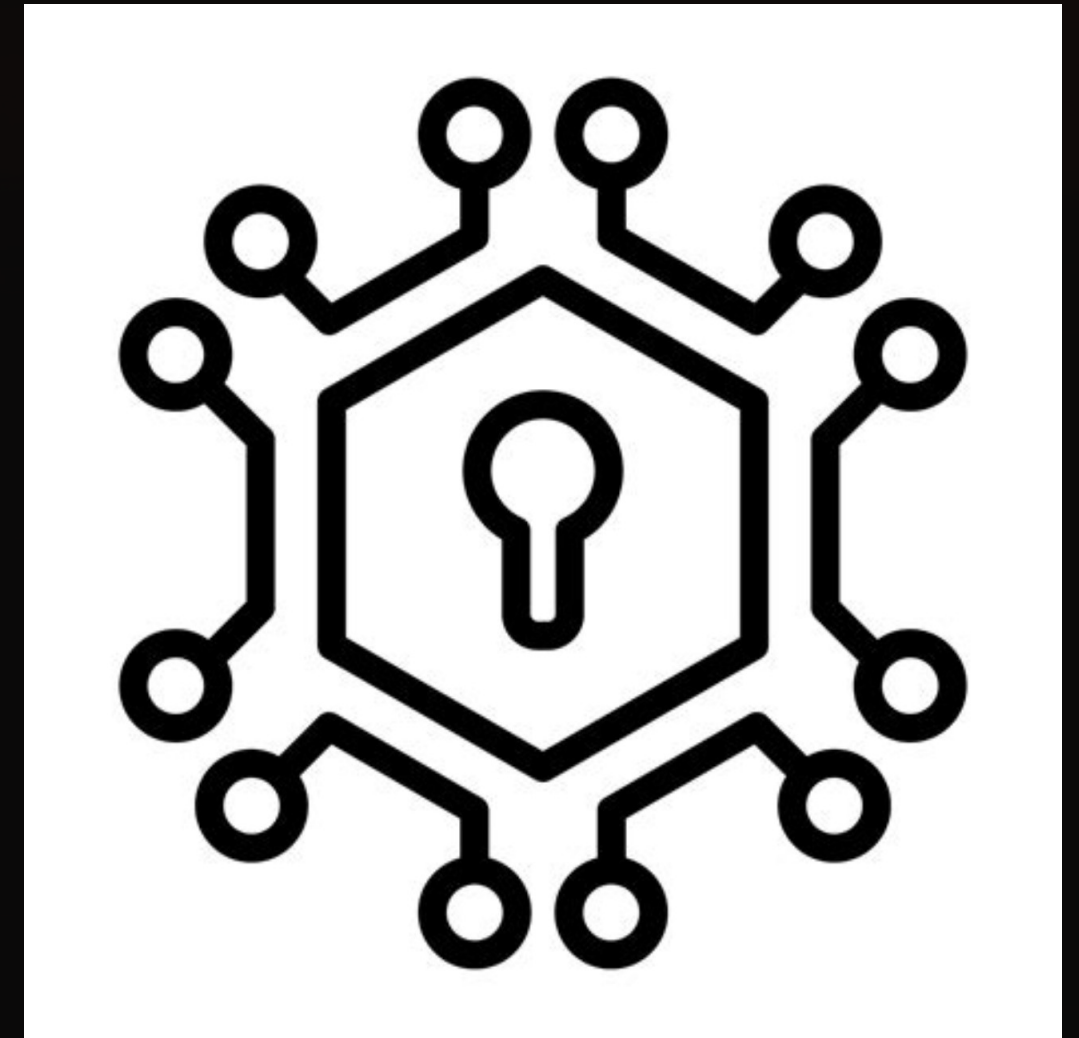
Scope of the Stolen Records

The data stolen was extensive, going far beyond basic contact information.

Personal Details

Names, addresses, and phone numbers.

Medical Information

Sensitive hospital records.

Family Connections

Details about family members.

The stolen data was uploaded to the "panel" software and monetized by the administrators.

The Human Cost: Abuse and Blackmail

Blackmail on Discord

Servers, with average user age around 15, used the data to blackmail victims for revenge or personal gain.

Psychological Trauma

Perpetrators demanded unethical images, leading to severe psychological problems and constant fear for victims.

Tragic Consequences

Some victims, unable to confide in family, were driven to attempt suicide due to the abuse.

Ethical Failure: Government and Platform Accountability

Government Failure

Government-linked applications (MHRS, e-Devlet) failed to adequately protect personal data, causing a major ethical issue.

Discord's Refusal

Discord refused to share information about perpetrators or servers with authorities, citing data protection laws, despite ongoing criminal activity.

1   **2**   **3**   **4**

Platform Complicity

Discord and Telegram played a significant role in the widespread distribution of the stolen data and subsequent crimes.

Market Ban

The government responded by imposing an indefinite ban on Discord within the Turkish market.

Preventive Measures: Building Digital Resilience

A multi-faceted approach is required to prevent future data breaches and abuse.
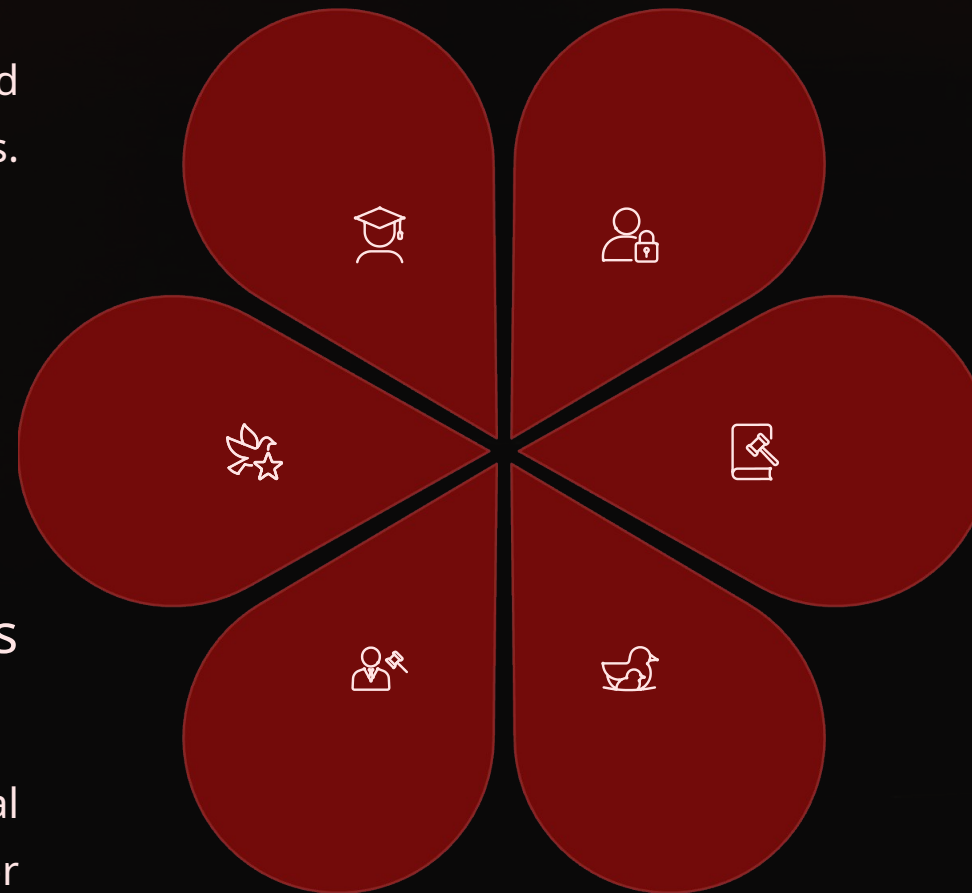
Digital Ethics Education

Teach young people about data privacy and cybersecurity awareness in schools.

Promote Ethical Culture

Platforms must encourage ethical behavior and quickly ban users involved in misuse.

Support & Reporting Systems

Provide easy access to psychological counseling and safe reporting channels for victims.

Stronger Cybersecurity

Invest in advanced security and regular data protection audits for institutions.

Stricter Laws & Penalties

Enforce tougher laws for data theft, cyberbullying, and privacy violations.

Monitoring & Parental Control

Parents must monitor online activity and educate children on safe internet use.

THANKS FOR LISTENING !!!

022290015 Arda yılmaz

022190017 Abdulsamet Akdemir