



Stayin' Alive: How Global Stolen Data Markets Thrive on Telegram

Tina Marjanov, Taro Tsuchiya, Konstantinos Ioannidis

Jack Hughes, Nicolas Christin, Alice Hutchings



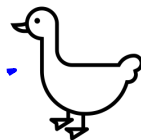
UNIVERSITY OF
CAMBRIDGE



Carnegie Mellon University
Security and Privacy Institute



What happens to my data after the breach?



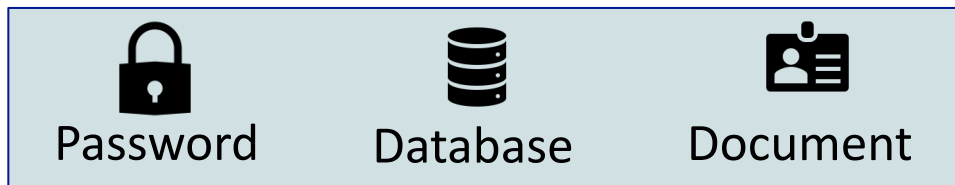
Data Breach Notification

Dear Taro

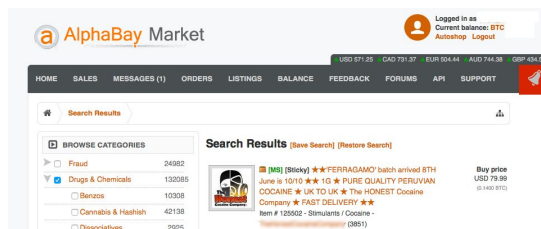
....the data security incident that
may have affected your personal
information. ...

Stolen data markets are moving to Telegram

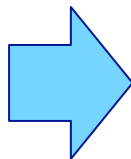
Stolen data



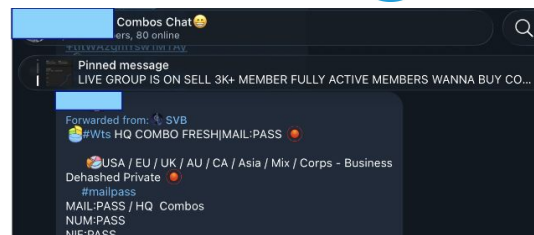
Darknet Marketplaces



Structured
(listings + reviews)



Telegram Messenger



Unstructured
(group + private chats)

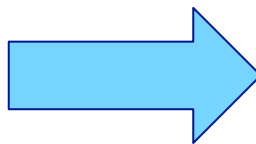
RQ: How can we moderate stolen data communities on this new infrastructure?

Collect stolen data channels, messages, files

Experts' Keywords
(e.g., "combo")

Darkweb forum links

+ Snowball



Manual curation



1,500+ groups



14+ million messages



3.6+ million files

Stolen data communities thrive on Telegram

Main findings

1: Expand the operation globally

Many non-English channels (e.g., Chinese, Spanish)

Many credit cards from Argentina

2: Deploy evasion techniques

Gateway channels → Private channels

Takeaways

1) Stolen data are the global problem

2) Telegram requires different interventions