Threat actors targeting telecom companies

ENISA Telecom & Digital Infrastructure Security Forum

Alexandre De Oliveira, 24 May 2023
alexandre.deoliveira@post.lu

POST
CYBERFORCE
« Smart security enabling the digital society »

enisa
EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

POST
LUXEMBOURG

Threat Actors are making the news

SURVEILLANCE

Ghost in the network PUBLISHED MAY 10, 2023

How a Swiss tech expert runs a global phone surveillance system

Vulnérabilités des réseaux télécoms : révélations sur un « courtier » de la surveillance

La discrète société suisse d'Andreas Fink est l'un des acteurs principaux d'un marché de la surveillance utilisant une faille dans les réseaux des opérateurs mobiles. Celle-ci permet de géolocaliser ou d'intercepter les communications des téléphones. Le collectif de journalistes Lighthouse Reports a enquêté durant un an sur ce marché des plus opaques.

How a Secretive Swiss Dealer Is Enabling Israeli Spy Firms

The international mobile system is exposed and a loophole allows hackers, cybercriminals and states to geolocate targets and even hijack email and web accounts. Israelis can be found among the victims - and the attackers

"TEAM JORGE": IN THE HEART OF A GLOBAL DISINFORMATION MACHINE

February 15, 2023

In Part 2 of the "Story Killers" project, which continues the work of assassinated Indian journalist Gauri Lankesh on disinformation, the Forbidden Stories consortium investigated an ultra-secret Israeli company involved in manipulating elections and hacking African politicians. We took an unprecedented dive into a world where troll armies, cyber espionage and influencers are intertwined.

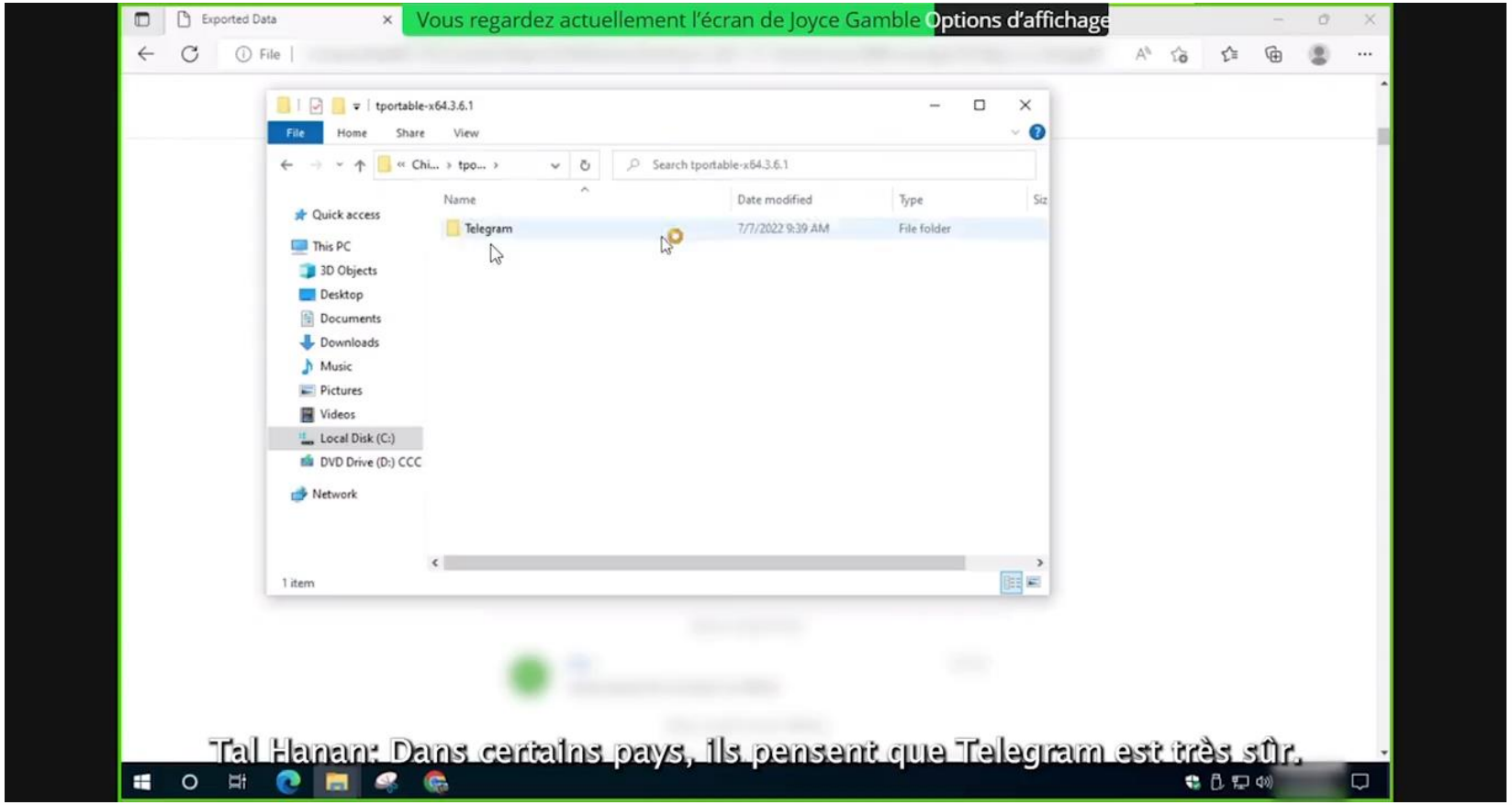
Handy-Spähattacken

S+ Wie ein Schweizer IT-Unternehmer weltweite Überwachung ermöglicht

Sicherheitslücken im Telefonnetz gefährden die Daten von Millionen Handynutzern weltweit. Die Infrastruktur für die Angriffe der Hacker liefert oft ein Basler Unternehmer mit einem bizarren Geschäftsmodell.

Real capabilities – Telegram Takeover

Speciality in campaign manipulation “33 presidential campaigns, 27 of which were successful”



https://forbiddenstories.org/story-killers/team-jorge-disinformation/

Tracking threat actors – Fink Telecom

From 2018 to 2023

- End 22-23 : Using 50+ SS7 & Diameter entry points in 7 countries
  - Switzerland, Sweden, Namibia, Russia, Turkey, Italy & UK
  - Even registered as an official operator in CH & SE
- Using GT leasing makes it complex to trace and to identify attackers
- Up to 80% of critical attacks in some operators
- Relying on a full ecosystem, many MVNE, MVNO supporting

Attack methods from Threat Actors

- Information Gathering
  - The first stage for spyware companies (Pegasus, Predator…)
  - Phone numbers, IMSI, IMEI
- Location Tracking
  - Permanent gathering of Cell-ID & Triangulation phones in real-time
- Interception SMS, Call & Data
  - Used to intercept 2FA SMS on Telegram & Co
  - For calls, various methods, from 2G to VoLTE calls

Further Support from Autorities

- Discussions with autorities is sometimes complex
- Subject gets quickly technical, often the actors are international
- Idea for the future: Creation of a “reporting” framework for misusage of these surveillance technologies by ENISA / Europol
- Wild competition is this sector, means multiplication of malicious actors
- Regulations might help but **inteligence coordination** is the key to take down these actors

Threat Intel published

GSMA Telecommunication ISAC

- Check the GSMA T-ISAC MISP events:
  - **3752** Synchronised Diameter & SS7 Location Tracking attempts from Limitless Mobile
  - **3751** SS7 Information Gathering campaigns on Mobile Networks
  - **3689** Tykelab GTs targeting SS7 infrastructures via Location tracking & Info Gathering
  - **3565** Fink Telecom (FTS) GTs targeting SS7 networks (Interception/Info Gathering/Location Tracking)

- Advice: Block the GTs and nodes of these actors
  - If possible ask Carriers to not route anymore trafic from threat actors towards you

- Today FTS is way less active and companies started disconnecting it

Thank you!

alexandre.deoliveira@post.lu

If you are not monitoring, you are one of their target.

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

POST LUXEMBOURG