Cyberwar Data Leaks Related to the Russian Invasion of Ukraine

July 19, 2022

A global cyberwar emerged in the wake of the Russian invasion of Ukraine in February of 2022, with targets spanning from private government agencies to large commercial enterprises. DarkOwl analysts have identified critical leaks across major key sectors, including those amongst cyber hacktivists and threat actors themselves.

The data contained in these leaks is comprised of crucial information such as network and server records, sensitive military documentation and the PII of key political leaders. Such exposed information is likely to be exploited to target and execute subsequent cyberattacks against supply chain and third party vendors.

Key Detected Leaks*

GOVERNMENT AGENCIES

- mil.ru & gov.ru
- Roscosmos FTP Server
- GLONASS Satellite Data
- Ministry of Foreign Affairs
- Ministry of Economy
- Duma.gov.ru
- Ministry of Finance
- Ministry of Internal Affairs
- Russian Science Academy
- Mosreg.ru - rocket chat logs
- Republic of Crimea (SUDAK)
- FSB
- Tver Governor's Office
- Polar Branch of RU Fisheries & Oceanography
- Achinsk City Government
- Public Chamber of Kranoyarsk
- Federal State Statistics Service
- Nauru Police Force
- Dept of Education – Strezhevoy
- Blagoveshchensk City Administration
- Gov of the Sverdlovsk Region
- RU Hydrometerology & Env Agency
- Joint Institute Nuclear Research (JINR)
- Russian Federal institute of Science
- St. Petersburg Military Training Ctr

TRANSPORTATION

- UtAir Air Carrier Service
- Metrospetstekhnika (Train ASTOP)
- Port & Railway Services (JSC UMMC)
- RZD & Moscow Rail Infrastructure Monitoring Service

MEDIA & PROPAGANDA

- Roskomnadzor Agency
- State Television and Radio Broadcasting (VGTRK)
- Ministry of Culture
- Department of Information
- Oblgazeta State Media
- Vyberi Radio

ENERGY INFRASTRUCTURE

- PromEngineering
- Gazprom
- Rosseti Centre Electric
- OMEGA Company
- MashOil
- Petrofort
- Aerogas
- TechnoTec
- Gazprom Linde Engineering
- Gazregion
- Neocom Geoservice
- Enerpred
- ALET
- Elektrocentromontazh (ECM)
- McLanahan Russia
- SOCAR Energeoresource
- Novonor (Oderbrecht)
- Rosatom/TENEX

RUSSIAN PERSONS

- Oligarchs Dox Including List of Physical Assets
- Pravda Leak of 120,000 Soldier Identities
- Russian Air Force Officers & 300K Residents
- Russian Police Force Identities
- 620 FSB Agents Identities & Passport Numbers
- Identities of the 64 Motor Rifle Brigade in Bucha
- Kremlin Staff Registry & RU Embassy Diplomats
- Belarusian Gov Database
- 2.5M RU Citizens Cred Stuffing Database
- EPAM Employees

FINANCIAL / INVESTING

- Sberbank Account Data
- Central Bank of Russia
- Tendertech (fintech proc)
- Worldwide Invest
- Accent Capital
- Capital Legal Services
- Marathon Group
- OJSC Ak Bars Holding
- Thozis Corp Private Equity
- Petersburg Social Commercial Bank (PSCB)
- LLC Capital
- CorpMSP
- QiWi Payment Processor

IT / TELECOMMUNICATIONS

- QTECH
- Naumen Cloud
- Synesis & Kipod
- Unique Fiber Devices
- RAS-AS Supercomputers
- Nauchnyy Tsentr Prikladnoy Elektrodinamiki
- Moscow Internet Exchange
- NPO VS IT
- ComTron
- Sipteco
- Convex.ru
- Domain.ru
- Tensor.ru
- Lars.tech
- Telderi

MILITARY SUPPLIERS

- GUOV i GS - Troops & Civil Construction Dept
- RostProekt
- Forest Logging
- Almaz-Antey – Missile Manufacturer
- DNPP - Dolgoprudnenskoe Plant
- Lipsetsk Mechanical Plant
- Korolevskiy Rations
- ORF Monitor
- Kronshtadt
- NPKTAIR
- Metprom Group
- Polymery.ru

DARKNET DRAMA

- CONTI RaaS Source Code
- CONTI Dox & Jabber Chats
- Trickbot Team Dox
- DATABASE MARKET PMs Leak
- 136K Russian Telegram Usernames
- Rocketchat Logs
- Trickbot Chat Logs
- Bazaar Botnet Loader
- Xaknet DDoS Team
- Killnet Dox
- Team Hydra Hacking Dox

RETAIL & COMMERCIAL

- Yandex Eats
- Berega Retail
- CDEK Post Shipping
- Magnit.ru
- Vkontakte Social
- Mail.ru User Database
- Continent Express Travel
- Miltor.ru
- Pickabu.ru
- Sawatzky Property
- Shambala Joker Poker Club
- Nestle
- Mosekspertiza

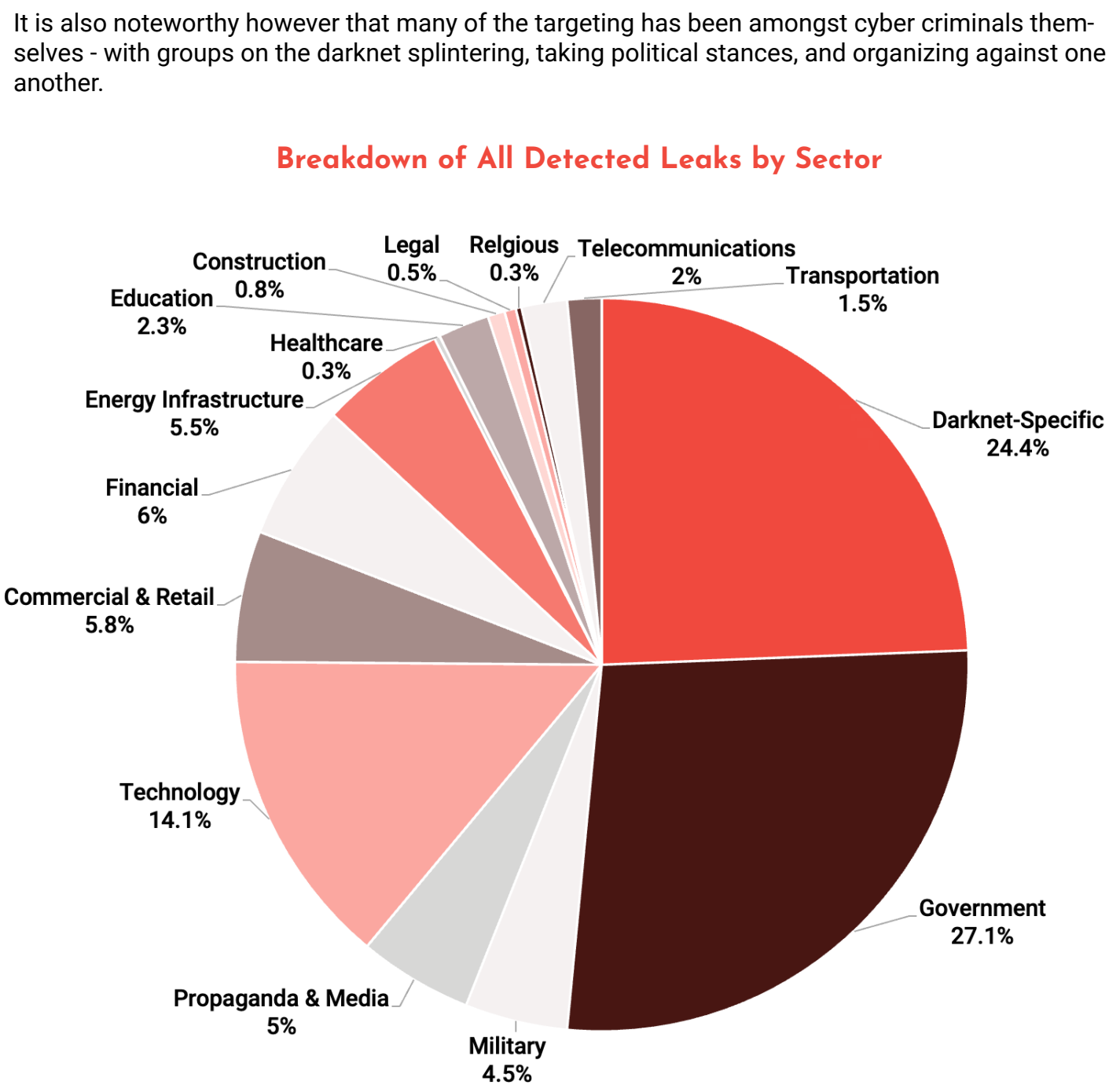
* These are leaks that have been deemed particularly noteworthy by DarkOwl analysts due to their size, the nature of the target, or propensity for future exploitation.

Sectors with Key Data Leaks Since the Onset of the Global Cyberwar as a Result of the Ukrainian Invasion

Considering the geo-political kinetic events that sparked this cyberwar, it is unsurprising that the majority of cyberattacks have been against government entities.

It is also noteworthy however that many of the targeting has been amongst cyber criminals themselves - with groups on the darknet splintering, taking political stances, and organizing against one another.

Breakdown of All Detected Leaks by Sector



As this cyberwar continues, it is more important than ever to monitor the darknet for indicators of compromise. By assessing and having visibility into leaked data, preparations can be made against potential future attacks such as ransomware or espionage.

DarkOwl uses machine learning to automatically, continuously, and anonymously collect, index and rank darknet, deep web, and high-risk surface net data that allows for simplicity in searching. Our platform collects and stores data in near realtime, allowing darknet sites that frequently change location and availability, be queried in a safe and secure manner without having to access the darknet itself.

Visit www.darkowl.com to learn more.