



Making Sense of Data Dumps & Data Leaks in Times of War & Peace

*Stefan Soesanto, Senior Cyber Defense Researcher & Lead - Cyber Defense Project
Center for Security Studies (CSS), ETH Zurich*

Swiss Cyber Storm - October 24, 2023, Bern

5 hours ago (This post was last modified: 5 hours ago by gosh.)

gosh

ISRAEL MINISTRY OF DEFENSE DATABASE

aks

Source: CheckPoint

Target: Ono Academy College

Malek Team

Code	Surname	ProfName/Passport	Institution_Name	Address_Street_and_Number	Zip_Code	City	Home_Telephone_Number	Work_Telephone_Number	Fax_Number	Email_External	Cellular_Phone_Number	Home_email_External
JAN00001	YU	0	0	0	0	0	00-000000				00-000000	000000@000000.com
JAN00002	YU	0	0	0	0	0	00000000			000000@000000.com	000-000000	000000@000000.com
JAN00003	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00004	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00005	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00006	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00007	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00008	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00009	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00010	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00011	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00012	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00013	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00014	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00015	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00016	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00017	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00018	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00019	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00020	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00021	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00022	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00023	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00024	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00025	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00026	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00027	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00028	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00029	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00030	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00031	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00032	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00033	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00034	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00035	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00036	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00037	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00038	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00039	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00040	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00041	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00042	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00043	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00044	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00045	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00046	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00047	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00048	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00049	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com
JAN00050	YU	0	0	0	0	0	00-000000			000000@000000.com	000-000000	000000@000000.com

Looks real



Rami Tamam
Co-Head of the Cyber Security and Forensics Program

Contact me : @ [redacted]
My Channel : https://t.me/[redacted]
My Backup Channel : https://t.me/[redacted]



More than **250 000** Personal Identities are available , wait for Leak

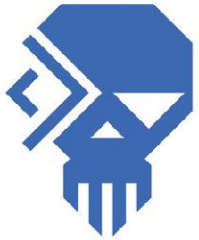
Posts: 83
Threads: 22
Joined: Jun 2023
Reputation: 185



Wartime

Why does it matter?

“Peacetime”



Kyber Sprotyv (UKR) is not Phineas Fisher



Nemez1da (RU) is not RaidForums



(new) Anonymous is not Vice Society



DDoSecrets is not Wikileaks



**Losing data/information/PII in wartime
can get people killed**

In everyday interaction,
the terms “data dumps” and “data leaks”
are used synonymously

General Definitions

- Dumps are large amounts of data transferred from one system or location to another.
- Leaks are sensitive data that is unknowingly exposed.



General Differences

/ Information Density:

Dumps = Generally information poor (random files and sheets)

Leaks = Generally information rich (PII, financial data etc.)

/ Dissemination Vector:

Dumps = Usually dumped into the public domain with little specifics on its origin, content, how it was exfiltrated, who it is addressed to, and its overall purpose. (ex. Random X account posts link to a huge .rar file)

Leaks = Usually released via a trusted intermediary, contextualized in origin, content, who found it, how it was exfiltrated, who it was given to, and why. (ex. Snowden leaks – we don't call it the Snowden dump)

Peacetime data leaks: Suisse Secrets (February 2022)

Q SZ | Meine SZ | SZ Plus | Ukraine | Israel | Polen | Politik | Wirtschaft | Meinung | Panorama

Suisse Secrets

Suisse Secrets enthüllen heikle Konten bei Schweizer Großbank

21. Februar 2022, 10:36 Uhr | Lesezeit: 3 min



SZ | Meine SZ | SZ Plus | Ukraine | Israel | Polen | Politik | Wirtschaft | Meinung | Panorama

Suisse Secrets

Suche nach dem Whistleblower

5. Februar 2023, 18:28 Uhr | Lesezeit: 1 min



OCCRP | SUISSE SECRETS | DONATE | f

Q SZ | Meine SZ | SZ Plus | Ukraine | Israel | Polen | Politik | Wirtschaft

Statement der Quelle

"Warum ich es getan habe"

20. Februar 2022, 17:50 Uhr | Lesezeit: 2 min



SUISSE SECRETS

 Suisse Secrets





Who's in the Suisse Secrets Leak?

SUISSE SECRETS

The Suisse Secrets data leak includes dozens of corrupt government officials, criminals, and alleged human rights abusers who have been clients of the Swiss banking giant.

There is nothing inherently wrong with having a Swiss bank account. But banks are supposed to avoid clients who earned money illegally or were involved in crimes. Despite their notoriety - which, in some cases, would have been obvious from a quick Google search - Credit Suisse maintained relationships with some of these clients for years, though it is possible that some accounts were ordered frozen by law enforcement.

Peacetime data leaks



Search for an account

Or browse the archive below

Region

Category

On Jan 1st 2022 100 CHF = 110 USD

Person of Interest	Category	Country	Max balance	
 Abdelaziz Bouteflika	Political	Algeria	CHF 1,483,528	view the profile
 Abdul Halim Khaddam	Political	Syria	CHF 89,795,788	view the profile

STORIES FROM THE VAULTS



Sons of Azerbaijani Strongman Vasif Talibov Received Millions From Money Laundering Systems

Having opened bank accounts with Credit Suisse, Barclays, and other foreign banks, Rza and Seymur Talibov received over \$20 million in suspicious wire transfers, even as the people of the Azerbaijani exclave of Nakhchivan suffered under their father's dictatorial rule.

30 FEBRUARY 2022 [READ THE ARTICLE](#)



Credit Suisse Account Played Role in Scheme That Destroyed Ukrainian Agriculture Firm

Mriya Agro Holding collapsed after its Ukrainian owners, members of the Guta family, siphoned over \$100 million of the company's money into shell companies. SuisseSecrets

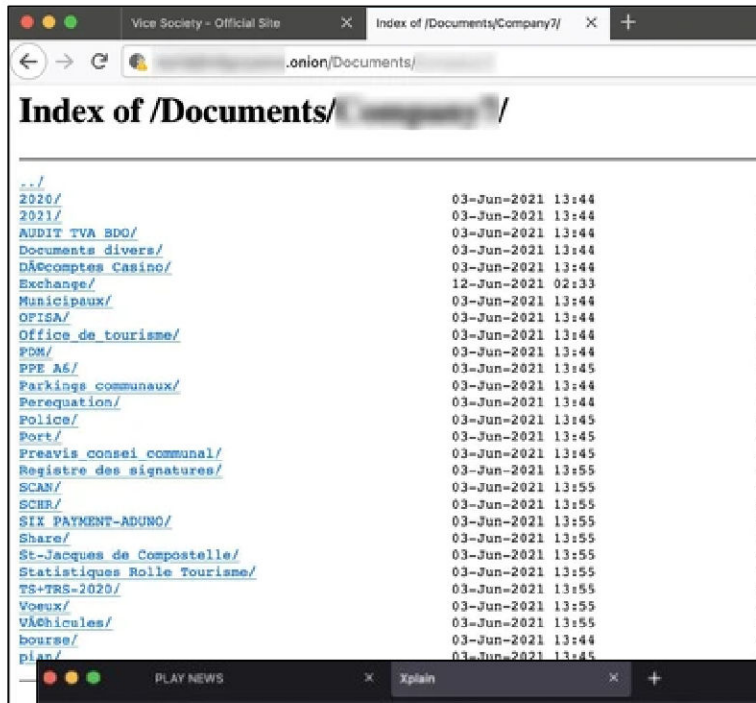


Credit Suisse Banked And Financed Zimbabwean Fraudster In Deal That Saved Mugabe

Details from the Suisse Secrets leak cast new light on Credit Suisse's role in financing Robert Mugabe's regime.

Source: <https://cdn.occrp.org/projects/suisse-secrets-interactive/en/>

Peacetime data leaks: Rolle & Xplain



LE TEMPS

SWISS ECONOMY OPINIONS CULTURE COMPANY SCIENCE SPORT DATA EVENTS

“If we have access to other Swiss cities than Rolle, we will attack them too”

When contacted, the hackers who targeted the town of Rolle claimed that there had been no negotiation with the authorities. They also say that they will not be the ones to exploit the data posted online on the darknet

Xplain

Switzerland
www.xplain.ch
views: 60
amount of data: 907 gb
added: 2023-05-23
publication date: 2023-06-01

information: Xplain AG is a company that operates in the Consumer Services industry.
comment: Private and personal confidential data, finance, taxes, clients private information.

Hackerangriff auf die Firma Xplain: Auch die Bundesverwaltung ist betroffen

Bern, 08.06.2023 - Vom Ransomware-Angriff auf das Unternehmen Xplain, bei dem ein Teil der entwendeten Daten im Darknet publiziert wurde, könnten nach aktuellem Kenntnisstand auch operative Daten der Bundesverwaltung betroffen sein. Die vertieften Analysen laufen derzeit noch.

Die Firma Xplain, eine Schweizer Anbieterin von Behörden-Software, ist Opfer eines Ransomware-Angriffs geworden. Nachdem die entwendeten Daten verschlüsselt worden waren und die Firma erpresst worden war, stellten die Angreifer einen Teil der entwendeten Daten ins Darknet.

What happens in the space in-between?

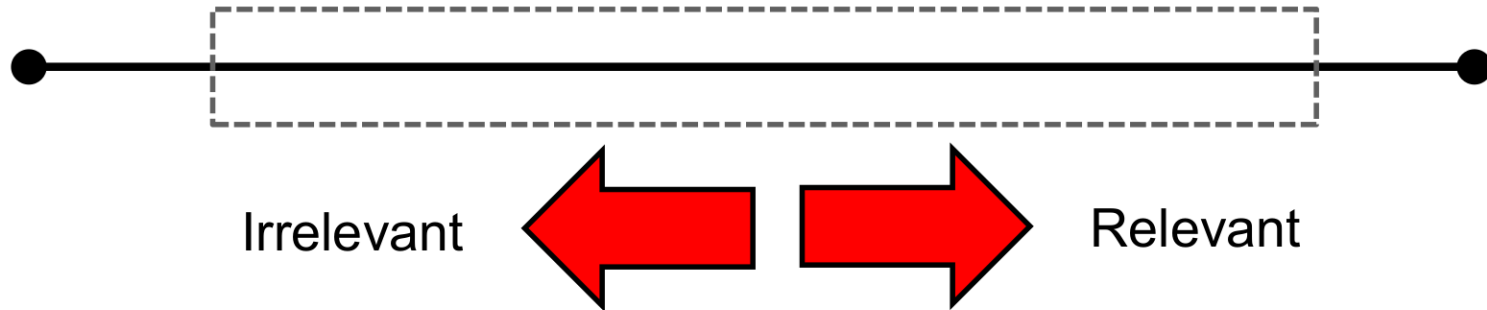
Some Information

Perfect Dump

No information

Perfect Leak

Perfect Information



In peace time, the space in-between is an academic problem.

Cases naturally become either relevant or irrelevant depending on the overarching ecosystem

(ex. data availability, journalistic/research interest (fake/real), public/company reaction, threat intel)

For this to function appropriately, there needs to be an ecosystem

Ex. What if there is a massive data dump/leak and literally nobody cares?



In Wartime: new ecosystems pop-up

- New/resurfacing actors enter the playing field
- Anything becomes a target for whatever reason
- Anything can get dumped/leaked
- These ecosystems develop their own internal dynamics

One part:

Oldschool Hacktivism & Wargifting (chasing headlines)

Other part:

state-encouraged, state-shaped, state-coordinated,
state-ordered, state-controlled groups

The attribution line is very blurry

Problem

- ! People are interested in secrets, they are interested in conflict dynamics, and they interested in news.
(trying to discouraging these traits by saying “don’t download this” is counter-productive)
- ! Very few have the time and resources to investigate a dump/leak for its veracity (cost-benefit calculation / few dumps/leaks are investigated)
- ! The general differences to discern a dump from a leak do not matter in wartime (anything could be sensitive information)
- ! Journalists, academics, youths etc. need **shortcuts** to navigate this environment

- Hosting Choices:** Why do groups use certain hosting providers to upload their dumps/leaks?
- Data Availability:** Do they provide mirror links and re-upload the dump/leak?
- Language:** Does the group have the language skills necessary to analyze the dump/leak itself?
- Size:** Generally, an inverse relationship - the larger the data dump, the less valuable the information
- Origin:** The more detailed the information on where the data was exfiltrated from and how, the higher the likelihood it is legit
- Etc.**

Another “Shortcut” is to look at the Ecosystem

WSJ PRO

Nestlé's Data Leak Shows War-Related Hacktivism Risks

Food giant denied being hacked, says exposed data was related to information that was unintentionally posted on a business test website

By *Nicolle Liu*

April 5, 2022 5:30 am ET | WSJ PRO

B

PRIVACY AND SECURITY

Nestlé: Anonymous Didn't Hack Us, We Leaked Our Own Data

After a hacker group claimed to have stolen the conglomerate's data, a company spokesman told Gizmodo that the info had actually been leaked by Nestlé itself.

By **Lucas Ropak** Published March 23, 2022 | Comments (22)



Nestlé denies cyberattack, says stolen data came from business test website

Multinational food conglomerate Nestlé has denied that it suffered a cyberattack after a Twitter account associated with hacking group Anonymous **leaked a 10GB trove** of information that allegedly included emails, passwords and client information.

A Nestlé spokesperson told The Record that the data came from a situation that happened in February.

Jonathan Greig

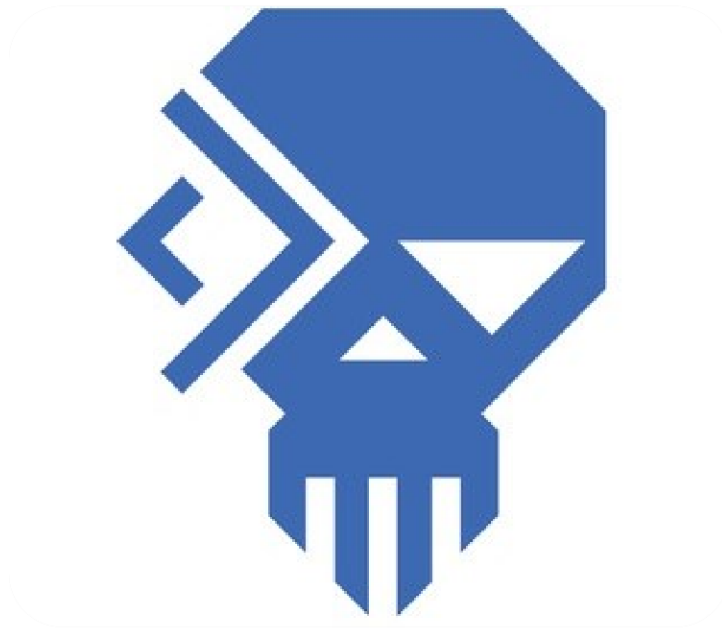
March 23rd, 2022

Briefs

Cybercrime



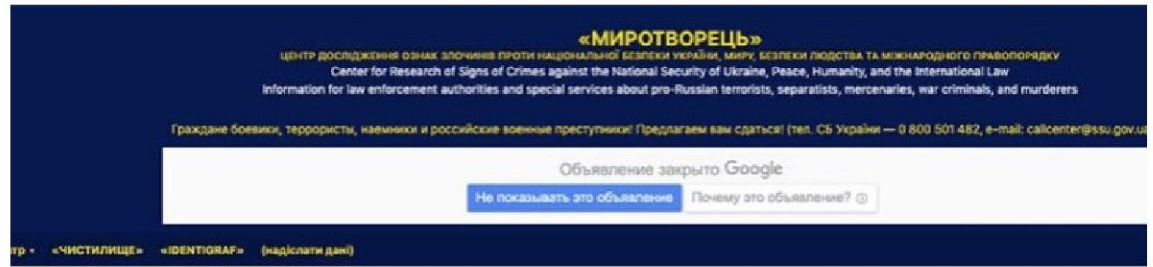
Kyber Sprotyv (Cyber Resistance)



Features | Media

Peacemaker: The Ukrainian website shaming pro-Russia voices

Being blacklisted on Peacemaker can have serious consequences, including the risk of being killed.



Peacemaker has blacklisted thousands of people, including pilots, journalists, a priest, rocker Roger Waters and Nobel Prize-winner Svetlana Alexievich [Screengrab from myrotvorets.center]

By Mansur Mirovalev
27 Aug 2019



To the



оловна Про Центр «ЧИСТ

3509
день війни з
російсько-
фашистськими
загарбниками

Наші проекти

Центр
«Миротворець»

«DentigrAF»
система
розпізнавання

MYROTVORETS
NEWS

Радіо
Миротворець

Будуємо країну разом!
Ukraine NOW

Про безпеку України
НАШ ЗАХИСТ

SEA
KRIME

ORDILO
Сховище дампи

Law
Derers

ПІДТРИМА

Тягати
у розвитку

СУВЕНІРИ

ДрукАрмія

ДА

ЗАБЕ

д
дпо

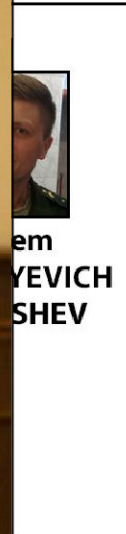
Поскаржитись

Поскаржитись



WANTED

Example



Aleksandr Vladimirovich Osadchuk and Anatoliy Sergeyeovich Kovalev, are charged with a separate conspiracy to commit computer crimes, relating to hacking into the computers of U.S. persons and entities responsible for the administration of 2016 U.S. elections, such as state boards of elections, secretaries of state, and U.S. companies that supplied software and other technology related to the administration of U.S. elections. The United States District Court for the District of Columbia in Washington, D.C. issued a federal arrest warrant for each of these defendants upon the grand jury's return of the indictment.

-
- (1) There is an educational need/demand when it comes to understanding and categorizing data dumps/leaks.**
(this is more pressing the more instable geopolitics become)
 - (2) There is a general need to clearly explain the ecosystems in which a dump/leak is released into.**
(contextualization & conflict dynamics)
 - (3) There is an ongoing evolution in how data dumps/leaks are being released** (personalization)

Thank you :)