

# A WEB OF SURVEILLANCE

UNRAVELLING A MURKY NETWORK OF  
SPYWARE AND SURVEILLANCE EXPORTS TO  
INDONESIA

---

VirusBulletin Oct 2024

**AMNESTY**  
INTERNATIONAL



# SECURITY LAB

We are a multi-disciplinary team of researchers, hackers, coders, campaigners and advocates.

We work to protect civil society from unlawful digital surveillance, spyware and other human rights abuses enabled by technology.

Previously, Pegasus Project, Predator Files and other research.

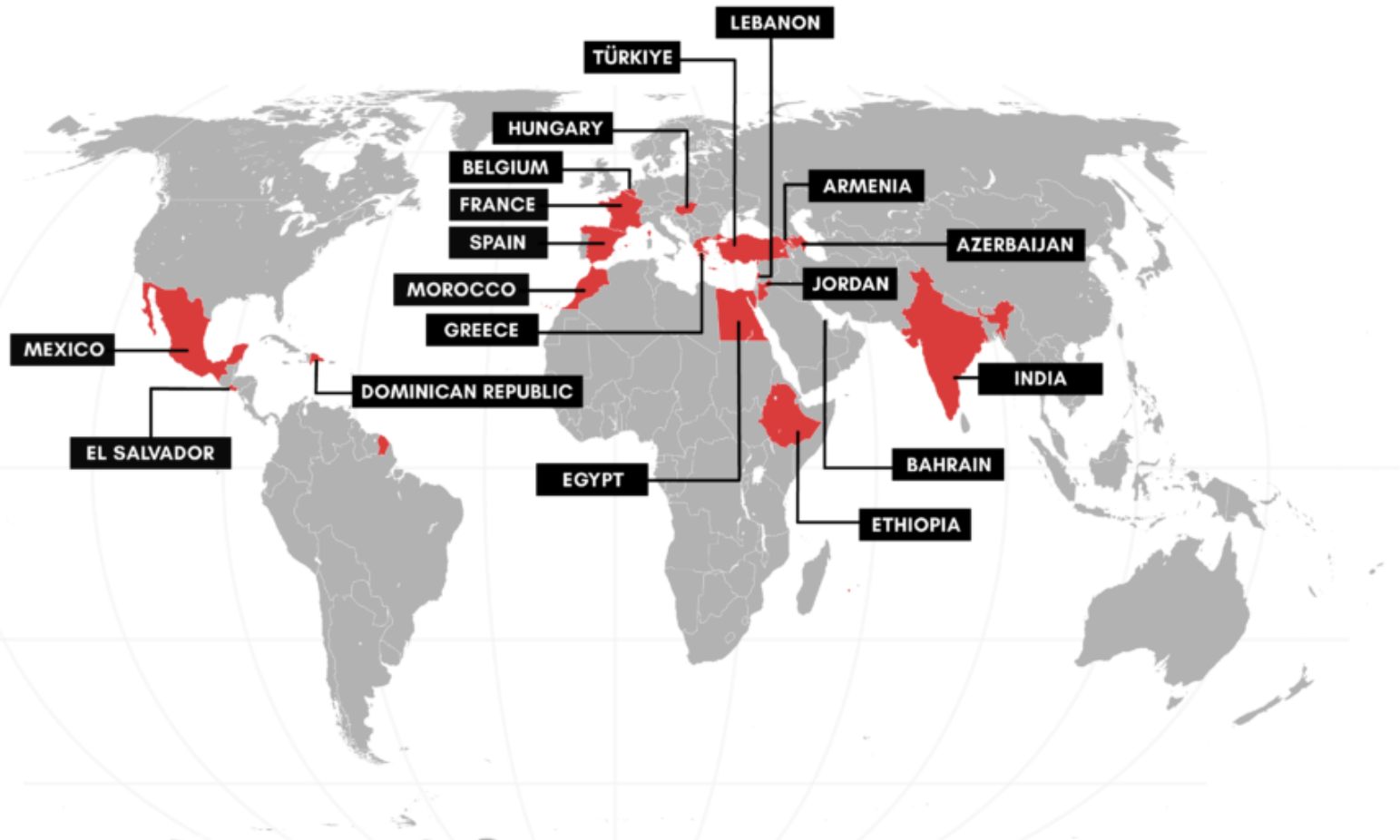
The screenshot shows the homepage of the Amnesty International Security Lab. At the top left is the Amnesty International logo and the text "SECURITY LAB" and "ENGLISH". To the right are navigation links: "ABOUT US", "RESOURCES", "PUBLICATIONS", "CONTACT US", and "GET HELP". The main header features the "SECURITY LAB" title in a dark box, followed by "at Amnesty International" and a yellow "WHAT WE DO" button. A large circular graphic in the background depicts people working at computers with various icons around it. Below the header is a grey banner with the text "We campaign for a world where human rights are enjoyed by all" and a sub-headline: "The Security Lab at Amnesty International is a multi-disciplinary team of researchers, hackers, coders, campaigners and advocates working to protect civil society from unlawful digital surveillance, spyware and other human rights abuses enabled by technology." A yellow button below this banner says "GET HELP FOR DIGITAL SECURITY THREATS". The "Latest news" section contains three articles: "Apple threat notifications: What they mean and what you can do" (with an illustration of a hand holding a smartphone), "Partner research update: new cases of Pegasus in Jordan and Togo" (with a photo of protesters holding signs), and "Support from the Spyware Accountability Initiative" (with an illustration of people protesting).

# WHAT IS SPYWARE

*Spyware* is malicious software which enables a spyware operator to gain covert access to information from a target computer system or device.

# SCALE OF SPYWARE THREAT

Targeting of journalists forensically confirmed in at least 19 countries.



# SCALE OF SPYWARE THREAT

We only see the tip of the iceberg. Scale of abuse is much higher.



Spyware systems are sold for **millions of euros**.

Each successful attack may cost the customer **10-20+ thousand euro** according to leaked Intellexa quotes.

# SALES OF SPYWARE AND SURVEILLANCE TECHNOLOGIES



# INVESTIGATION

- **Collaborative investigation between Amnesty International and key media:** Security Lab, Tempo (Indonesia), Haaretz (Israel), WAV research group, Woz (Switzerland) and Inside Story (Greece)



## Investigation: Israeli Surveillance Technology and Spyware Sold to Indonesia

A joint investigation by Amnesty International and Haaretz has revealed that Indonesia, which has no diplomatic ties with Israel, imported Israeli spy tech. Then Singapore found out about it

# INVESTIGATION

- **Challenge:** Murky ecosystem of brokers, suppliers and resellers, making research and transparency, accountability and oversight exceedingly challenging.
- **Methodology and sources:**
  - Commercial trade databases (Panjiva, Volza, and 52wmb)
  - Indonesian tender database
  - Mapping of spyware companies and subsidiaries
  - Open-source intelligence (subsidiaries, internet, GetContact)
  - Spyware infrastructure mapping
  - Previously published research (IndonesiaLeaks, Citizen Lab, Access Now)



# INVESTIGATION - SUBSIDIARIES

- Opencorporates.com

Found 3 officers

Tal Dilian GO

exclude inactive Advanced Options

**TAL JONATHAN DILIAN** *secretary*,  ERSIENDIA LTD (Cyprus, 14 Jun 2024- )

**TAL JONATHAN DILIAN** *director*,  ERSIENDIA LTD (Cyprus, 14 Jun 2024- )

**inactive** TAL JONATHAN DILIAN *director*,  **inactive** PASSITORA LTD (Cyprus, 23 Jan 2013-22 Nov 2022)

# INVESTIGATION - SUBSIDIARIES

- <https://aleph.occrp.org>

The screenshot shows a profile for a person named Mr Tal Jonathan Dilian. Below the name, there are two tabs: 'Info' and 'Assets and shares'. The 'Assets and shares' tab is selected and has a blue circle with the number '1' next to it. Underneath the tabs, the word 'Asset' is displayed. A dropdown menu is open, showing a building icon and the text 'MANUFUTURE LTD'.

Person

**Mr Tal Jonathan Dilian**

Info Assets and shares 1

Asset

MANUFUTURE LTD

# INVESTIGATION - SUBSIDIARIES

- Buying company extracts can reveal shareholders

2	STANLEY THIRTABRATA	X008075 /INDONESIAN 1b821836137caf1a4e98c28be3d5cd017f9a2c5545bb4178d39496a7bb2656a2	SINGAPORE, DOLLARS	Ordinary	20
				Preference	
				Others	
3	SASTRAWAN KAMTO	X062785 /INDONESIAN	SINGAPORE, DOLLARS	Ordinary	20
				Preference	
				Others	
4	SOEHERMAN DJAJA	X169441 /INDONESIAN	SINGAPORE, DOLLARS	Ordinary	20
				Preference	
				Others	

# INVESTIGATION - SUBSIDIARIES

Name of undertaking	Registered office	Principal activities	Class of shares held	% Held Direct
Intellexa Limited	Ireland	Provide intelligence products for law enforcement agencies.	Ordinary	100.00
Feroveno Limited	Greece	Development and licensing of data analysis software products	Ordinary	100.00
Intellexa Limited	British Virgin Islands	Provide intelligence products for law enforcement agencies.	Ordinary	100.00
Thalestris (Switzerland) SA	Switzerland	Provide intelligence products for law enforcement agencies.	Ordinary	100.00
Intellexa Single Member .S.A	Greece	Design and development of information technologies for applications.	Ordinary	65.00
Mistrona Limited	Cyprus	Development and licensing of	Ordinary	100.00

# INVESTIGATION – TENDER DB

Skor	Judul	Penyedia	LPSE	Tanggal Pengumuman	Nilai Kontrak
50	PERALATAN DAN MATERIIL KHUSUS DIT INTELKAM (ZERO CLICK INSTRUKSION SYSTEM) POLDA METRO JAYA BERIKUT PENGIRIMAN	PT. RADIKA KARYA UTAMA	LPSE Kepolisian Republik Indonesia	22 September 2017	Rp 98.912.000.000,00

# TRADE DATABASES

## Passitora Ltd

Viewed

Switzerland | 15 Transactions



Active Value 61

Trading: spear head bricface lenovoyoga 730 laptop 13"

Data updated to 2022-06-19

Buyers	<a href="#">Bendahara Badan Siber Dan Sandi Negara</a>
Supplier	White Global Holdings Pte Ltd.
Import area	Indonesia
Export area	Singapore
Product description	PROPRIETARY ANDROID ONE CLICK INSTALLATION MODULE BAIK , BARU <a href="#">翻译</a>

# SHAKING THE TREE



# FINFISHER

- Amnesty identified a hardware shipment on 7 August 2021 from Malaysia based Raedarius m8 to Indonesian Digital Solusi Prima
- Unclear if this hardware was spyware or another surveillance product
- Unclear who the intended end-user recipient is.



**FINFISHER™**  
EXCELLENCE IN  
CYBER INVESTIGATION



## PARTICULARS OF SHAREHOLDER

### CORPORATE INFORMATION

Name : RAEDARIUS M8 SDN. BHD.  
Last Old Name : Nil  
Date of Change : Nil  
Registration No. : 201501041916 (1167237-D)  
Incorporation Date : 26-11-2015

### CURRENT SHAREHOLDERS

<u>ID/Passport/ Registration No</u>	<u>Name/Address</u>	<u>Total Share</u>
-	RAEDARIUS M8 GMBH SAPPOROBOGEN 6-8, C/O OFFICE HPH, 80637, MUNICH GERMANY FOREIGN	1,000,000

# FINFISHER

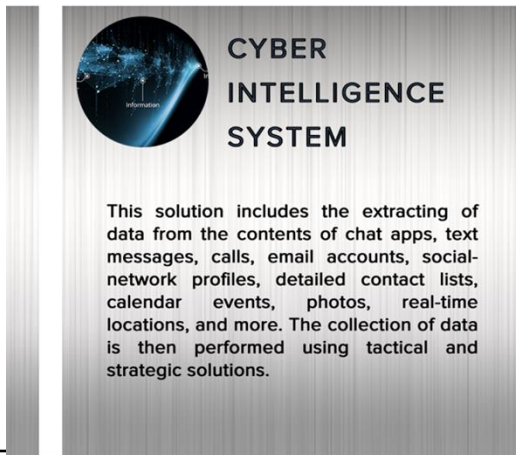


# SHAKING THE TREE



# WINTEGO

- Wintego Systems is an Israeli based company
- Not a lot is known publicly about their product offerings.
- Amnesty International found: malicious domains targeting Indonesia and two companies in Singapore, Ataka Enterprises and ESW Systems involved in a sale on Wintego products to the Indonesian National Police.
- Unclear if this was one deal or multiple deals.



**CYBER INTELLIGENCE SYSTEM**

This solution includes the extracting of data from the contents of chat apps, text messages, calls, email accounts, social-network profiles, detailed contact lists, calendar events, photos, real-time locations, and more. The collection of data is then performed using tactical and strategic solutions.



**CYBER INTELLIGENCE SYSTEM**

**WINTEGO**

This solution includes the extracting of data from the contents of chat apps, text messages, calls, email accounts, social-network profiles, detailed contact lists, calendar events, photos, real-time locations, and more. The collection of data is then performed using tactical and strategic solutions.

# WINTEGO

- A WINT system was shipped from ESW Systems to Indonesian National Police in 2019.
- WINT is advertised as being able to extract data through WiFi from target devices.

Date	Product description	Shipper	Receiver	Declared value
9 September 2019	WINT SYSTEM ADVAN C/W ACCESSORIES BAIK,BARU	ESW Systems PTE LTD	Slog Polri	5,594,053.87 USD

# WINTEGO

- Communication media surveillance systems and integrated control centers
- OSINT system
- Android-Based Investigation System and Web Information Collection System
- Wi-Fi Based Information Collection System
- IPDR Solution
- Social Media Analysis System

Perusahaan ini bernama **Ataka Enterprise Pte. Ltd.** adalah perusahaan yang bergerak di bidang jasa keamanan "Cyber Security" khususnya di bidang jasa penyedia layanan keamanan pada dunia maya, dengan kantor pusat berlokasi di 217 Henderson Road #02-09 Henderson Industrial Park Singapore 159555, dengan 2 kantor perwakilan di Rm 706 Yu Sung Boon Building, 107-111 Des Voeux Road Central, Hong Kong, dan DBS Bank Tower 28/F Room 2810, Ciputra World 1, Jl Prof Dr Satrio Kav. 3-5, Jakarta 12940, Indonesia. Perusahaan ini sudah terdaftar sebagai salah satu mitra nasional dari Indonesian National Police, Criminal Investigation Unit, Economic & Special Crime Directorate CID INP, Dit Tipideksus Bareskrim Polri Dalam kemitraan ini, Ataka Enterprise Pte. Ltd. dituntut untuk menyediakan Produk Keamanan berbasis Teknologi Informasi (IT) dalam dunia maya yaitu "the **Helios Android and Tactical Web Intelligence**" secara berkelanjutan dan tepat waktu, tepat kualitas sesuai dengan standarisasi yang diatur dalam ketentuan kontrak kemitraan dan CIQS (Certified Insurance Quality System).

# WINTEGO

## Resource

### Path

Primary Request /

Show response

tribunnews.org/

abcdefgh

www.coolbrandlabs.com/ Frame 3F64

- Internet scanning found tribunnews.org
- Coolbrandlabs.com once resolved to 31.168.34[.]139
- One of their sysadmins had a publicly accessible folder that listed the IP of a Fortinet firewall on 31.168.34[.]138 called wint.txt.
- From those IP's we were able to find more domains and were able to pivot from to find others mimicking domains targeting EU and Senegal.

# SHAKING THE TREE





# INTELLEXA

- Intellexa spyware sold under various names: Predator, Helios & Arrows
- Amnesty International found malicious domains that imitate legitimate Indonesian news websites.
- Through internet scanning we found a server in Indonesia that matches a fingerprint for Intellexa Predator backend servers.
- Amnesty International has not been able to determine who the end-user is.

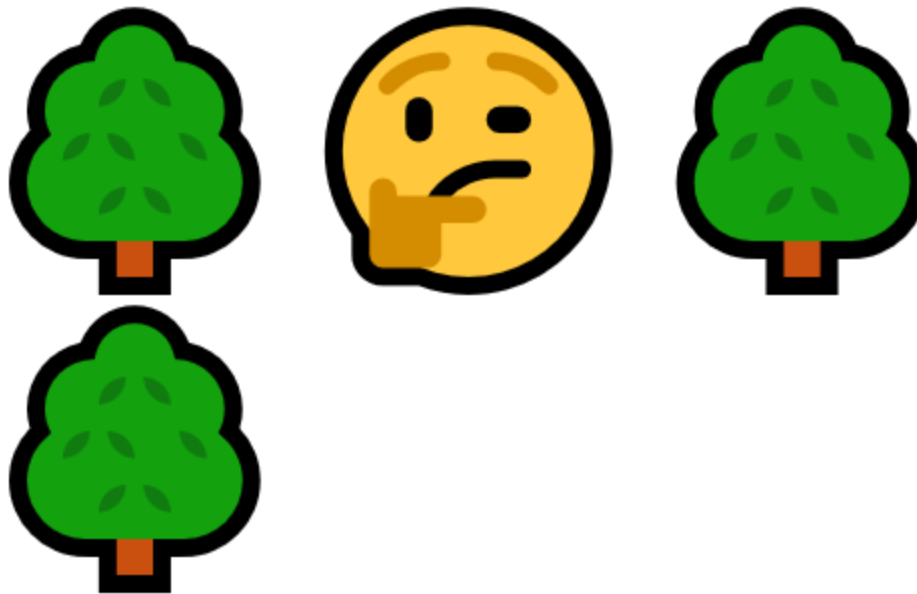
# INTELLEXA - SCANNING

- December 2021 Oopsie! a backend server (103.106.174.99) exposed!
- March 2022 Predator domains: ewestpapua[.]org and nindonesia[.]news.
- 2023: Intellexa Predator infection domain geloraku[.]id, registered in, may refer to either the Gelora News website or the Gelora political party.

**INTELLEXA**

# Treasury Sanctions Enablers of the Intellexa Commercial Spyware Consortium

# SHAKING THE TREE



# CANDIRU (SAITO TECH)

CYBER INTELLIGENCE INFILTRATION SYSTEM SOFTWARE SYSTEM MAIN SYSTEM

CYBER INTELLIGENCE INFILTRATION SYSTEM SOFTWARE SYSTEM AGENTS CONCURRENCY

CYBER INTELLIGENCE INFILTRATION AND EXFILTRATION SYSTEM SOFTWARE SYSTEM AGENTS CONCURRENCY

---

## Main Modules

- > System SW modules supporting the following platforms:
  - **Windows** (see Appendix A for full technical details)
  - **iOS** (see Appendix C for technical details)
  - **Android** (see Appendix D for technical details)
- > Vulnerability chains embedded to support the platform
- > Gathering of EPD (End Point Device) metadata
- > Intelligence gathering from social media applications

# CANDIRU (SAITO TECH)

- **May/July 2020/January 2021:** Shipments from *Heha* to Indonesia National Police
- **November 2020:** Amnesty International identified new domains being registered which we associate with the Candiru spyware
- **July 2021** reports by CitizenLab and Microsoft identified a suspected Candiru customer located in Indonesia based on internet scan data.
- Their report also identified a suspected Candiru infection domain `indoprogress[.]co`, which imitated the left-leaning Indonesian news website IndoPROGRESS.
- **2022:** We spotted more possible Candiru domains being registered.

# CANDIRU (SAITO TECH)

NSO Group and Candiru were added to the Entity List based on a determination that they developed and supplied spyware to foreign governments that used this tool to maliciously target government officials, journalists, businesspeople, activists, academics, and embassy workers.

# SHAKING THE TREE





# NSO GROUP

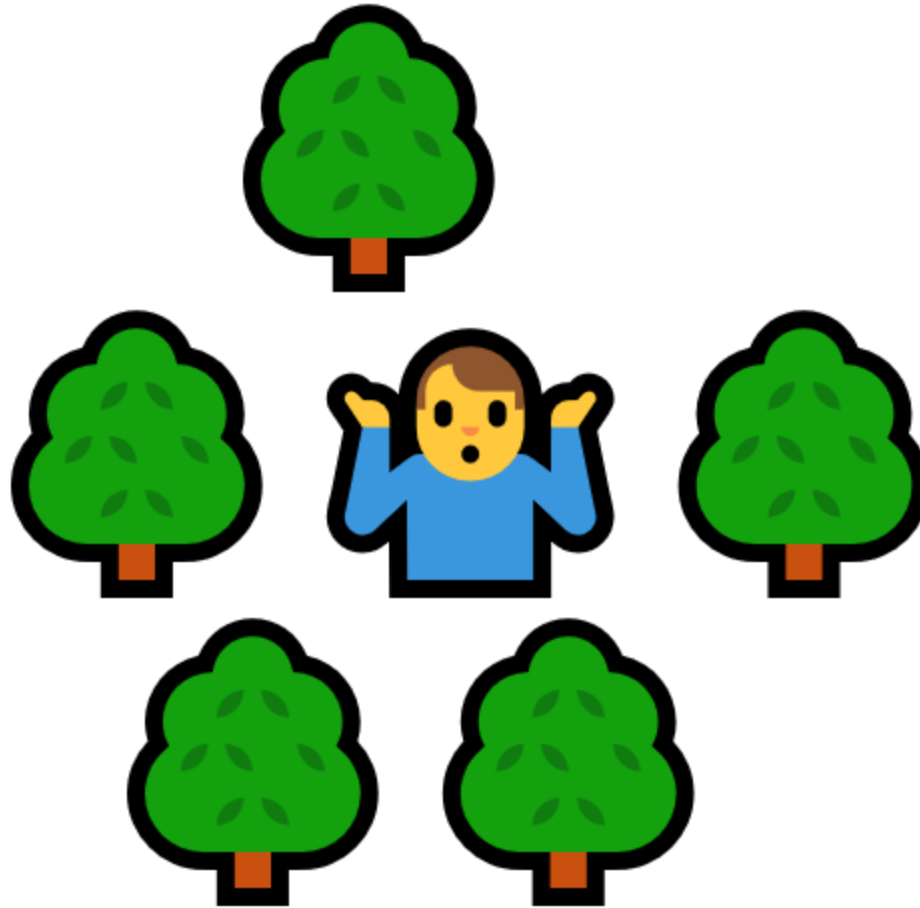
## Indonesia

Client Name	Possible Identity	Seen in Scan	Firewall IPs
		2018/9/11 – Present	203.142.69.82 – 84
		2018/9/4 – Present	117.102.125.50 – 52

```
inetnum: 203.142.69.80 - 203.142.69.87
netname: BIZNET-RADIKA-KARTA-UTAMA-BLOCK
country: ID
descr: RADIKA KARTA UTAMA
```

Date	HS Code	Product Description	Consignee	Shipper	Quantity	Unit	Gross Weight	Unit Rate \$	Value \$	Country of Origin	Country of Destination	Port of Destination	Port of Origin	Bill of Lading
15-Dec-2020	84715090	DELL SERVER KOND.BAIK/BARU	<a href="#">PT MANDALA WANGI KREASINDO</a>	<a href="#">Q CYBER TECHNOLOGIES SARL</a>	1	PCS	-	10,000	10,000	Japan	Indonesia	Soekarno-hatta Apt/jakarta	Heathrow Aptlondon	345164
15-Dec-2020	84715090	CISCO ROUTER KOND.BAIK/BARU	<a href="#">PT MANDALA WANGI KREASINDO</a>	<a href="#">Q CYBER TECHNOLOGIES SARL</a>	1	PCS	-	6,000	6,000	Japan	Indonesia	Soekarno-hatta Apt/jakarta	Heathrow Aptlondon	345164

# SHAKING THE TREE



# CONCLUSION

Indonesia authorities have spent tens of million on spyware products from numerous surveillance vendors with little transparency or oversight.

Full extent of sales is likely to be even higher as we lack numbers for total imports for several of the spyware systems we've seen active in Indonesia.

Unclear who the targets are, not a focus of this investigation. Even when we know spyware is used, it can still be difficult to find and forensically confirm cases.

Amnesty International wrote to authorities including the Indonesia National Police and intelligence bodies for comment but did not receive responses to detailed questions about these surveillance sales.

# CONCLUSION

- Lots of opportunities to strengthen threat intel research with OSINT approaches!
- NSO/Candiru entity listed in the U.S
- Intellexa companies and executives sanctioned by the U.S and unknown individual has criminal charges in Switzerland
- FinFisher is insolvent and dead 🎉
- Wintego's office firewall just dropped offline on the 28<sup>th</sup> Sept, dead?
- The EU is still 🤔
- Ireland and Intellexa 🤔?

# THANK YOU!

[HTTPS://SECURITYLAB.AMNESTY.ORG](https://securitylab.amnesty.org)

[JURRE.VANBERGEN@AMNESTY.ORG](mailto:jurre.vanbergen@amnesty.org)

---

Amnesty International, October 2024

**AMNESTY**  
INTERNATIONAL

