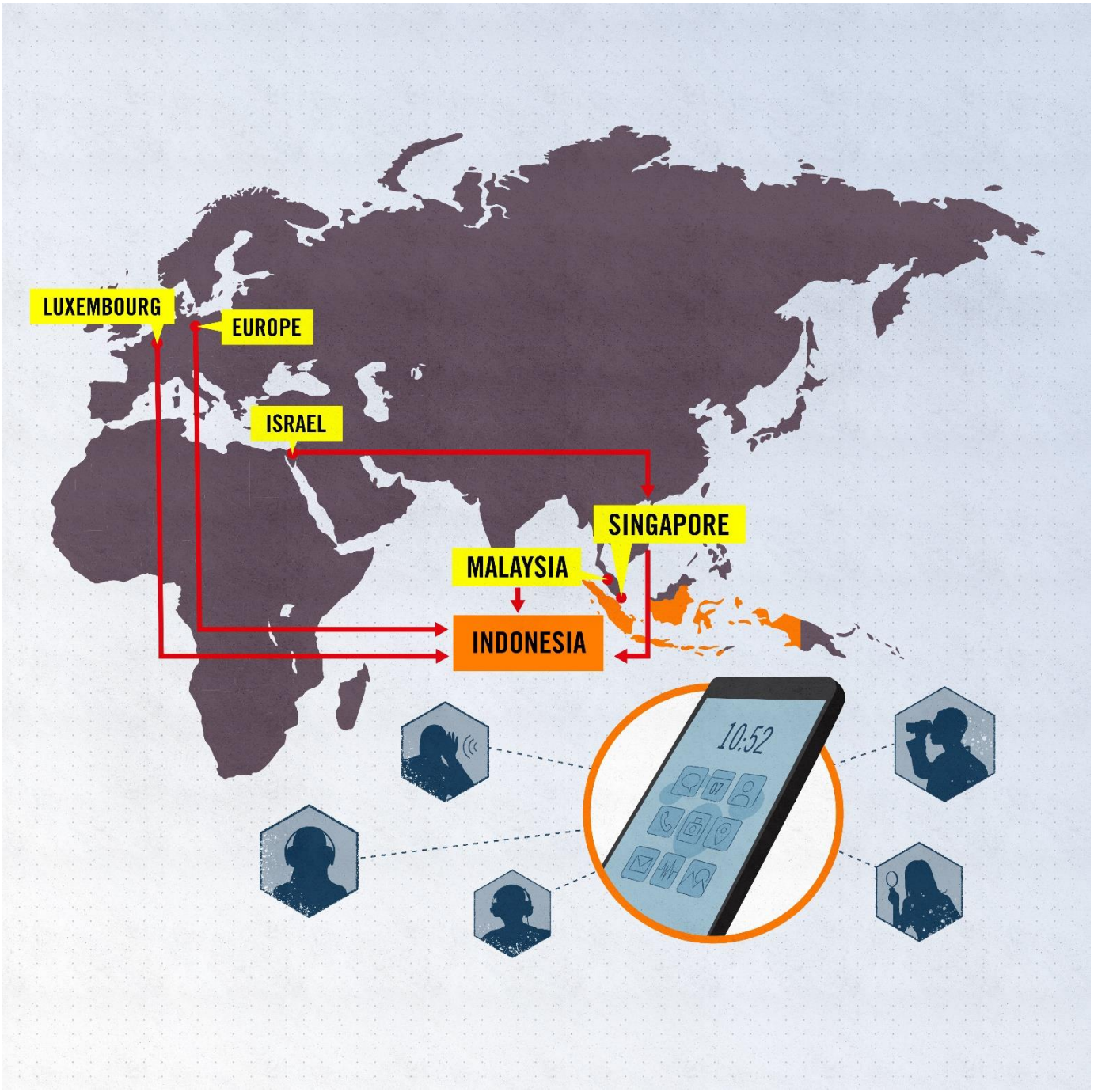


A WEB OF SURVEILLANCE

UNRAVELLING A MURKY NETWORK OF SPYWARE EXPORTS TO INDONESIA

RESEARCH BRIEFING

AMNESTY INTERNATIONAL

Cover image © Colin Foo 2024

1. EXECUTIVE SUMMARY

Highly invasive spyware and other rights-threatening surveillance technologies have been used to target human rights defenders, journalists and other members of civil society worldwide, as documented by an ever-growing body of research. Unfortunately, technical obstacles inherent in forensic investigations and a culture of secrecy surrounding the sale and transfer of surveillance tools keeps civil society and human rights defenders in the dark about the full extent of their deployment or use.

This research provides a case study on how one country, Indonesia, is relying on a murky ecosystem of surveillance suppliers, brokers and resellers that obscures the sale and transfer of surveillance technology. The investigation also showcases the continued failure of multiple countries to regulate and provide transparency on the exports of dual-use technologies, such as spyware, and the non dual-use hardware that hosts the spyware or surveillance technology which pose serious human rights risks.

This months-long investigation by Amnesty International's Security Lab, in collaboration with Haaretz, Inside Story, Tempo, WAV research collective and Woz into the global surveillance trade has found evidence of extensive sales and deployment of highly invasive spyware and other surveillance technologies in Indonesia sourced from Israel, Greece, Singapore and Malaysia between 2017 and 2023. Surveillance suppliers whose products are identified in Indonesia in this research include Q Cyber Technologies (linked to NSO Group), the Intellexa consortium, Saito Tech (also known as Candiru), FinFisher and its wholly-owned subsidiary Raedarius M8 Sdn Bhd, and Wintego Systems.

These findings build on existing research into the sale of surveillance technologies to Indonesia. In 2023, the IndonesiaLeaks consortium reported that NSO Group supplied surveillance products to authorities in Indonesia. In February 2022, Reuters reported that QuaDream had pitched its spyware product to the government of Indonesia, but "couldn't determine if Indonesia became a client". A later article from Reuters indicated that a range of senior Indonesian government officials and military officials were notified by Apple in November 2021 that their devices had been targeted by a "state-sponsored attacker". The November 2021 round of Apple threat notifications also included individuals whose devices were targeted by Quadream customers, as confirmed by Citizen Lab. It is unclear if the targeting reported by Reuters originated from Indonesia or was a result of cross-border targeting by a customer of Quadream or another mobile spyware product located outside Indonesia.

Through open-source intelligence, including commercial trade databases and spyware infrastructure mapping, Amnesty International has uncovered numerous spyware imports or deployments between 2017 and 2023 by companies and state agencies in Indonesia, including the Indonesian National Police (Kepala Kepolisian Negara Republik) and the National Cyber and Crypto Agency (Badan Siber dan Sandi Negara). As this research shows, several of these imports have passed through intermediary companies located in Singapore, which appear to be brokers with a history of supplying surveillance technologies and/or spyware to state agencies in Indonesia. Records show that many of these intermediary companies have been established with nominal company secretaries. These secretaries are recorded as owners of the company's registry documents or of the company shares, therefore making it difficult to identify the beneficial owner is of the company, especially in jurisdictions that do not provide these details to the public. By covering the beneficial owner in this way, verification of end-to-end supply chains for dual-use goods becomes close to impossible, making public procurement oversight challenging.

The research also documents numerous malicious domain names and network infrastructure linked to multiple advanced spyware platforms, seemingly aimed at targeting individuals in Indonesia. These malicious spyware domains include domains that mimic the websites of opposition political parties and major national and local news media outlets, including media from Papua and West Papua with a history of documenting human rights abuses.

While Amnesty International and its media partners have uncovered significant evidence about the spyware and surveillance systems sold to Indonesia, Amnesty International has little visibility into who was targeted with these systems. Highly invasive spyware tools are designed to be covert and to leave minimal traces. This built-in secrecy can make it exceedingly difficult to detect cases of unlawful misuse of these tools against civil society, and risks creating impunity-by-design for rights violations. Numerous investigations by Amnesty International and other civil society researchers have demonstrated how governments worldwide have used spyware to target civil society and journalists.

This is of special concern In Indonesia, where civic space has shrunk as a result of the ongoing assault on the rights to freedom of expression, peaceful assembly and association, personal security and freedom of arbitrary detention.

This investigation does not focus on forensic investigations to identify individual spyware targets. As such, Amnesty International does not have evidence that the surveillance technologies described have been used to target specific members of civil society in Indonesia. Rather, the research focuses on the opaque sale and transfer of several highly invasive spyware tools, which are inherently incompatible with human rights and should be permanently banned.

The current research provides material evidence to inform further research and accountability efforts to ensure that civil society in Indonesia can operate in an environment free from the fear of unlawful surveillance.

2. RESEARCH METHODOLOGY

Amnesty International has used a variety of methodologies to research the murky surveillance market and to lift a veil of secrecy around the sale and use of spyware. This investigation stretches multiple jurisdictions, each posing its own unique challenges in accessing information.

Surveillance technologies, including spyware, are considered 'dual-use' items, meaning they can have both civilian and military applications. There is a clear human rights interest in monitoring the sale and export of dual-use items, but in practice it is extremely challenging because most states do not publish reports of exports of such items and even in cases where they do, company names are not typically included. Accessing this information is therefore complicated and often requires freedom of information requests, if possible in the jurisdiction.

In the specific case of Indonesia, the ecosystem of spyware and surveillance brokers, suppliers and resellers to and in Indonesia is murky, making research, and transparency, accountability and oversight at the domestic and international level exceedingly challenging. For example, some of the business entities involved in spyware shipments identified by Amnesty International are set up by corporate secretarial service companies, rendering the beneficial owners and how these companies relate to each other difficult to decipher as only the nominee company secretary will appear on Singaporean corporate documents. For example, many of the Singaporean business entities identified in this research were established by corporate services companies with a nominee company secretary rather than a beneficial owner listed on the corporate documents. Only in one case, was it possible to identify previous shareholders for a company listed on older corporate registry records. None of the broker companies in Singapore or Indonesia replied to detailed questions from Amnesty International about their corporate ownership or sales activity. In light of these corporate transparency challenges, Amnesty International relied on a variety of other research methods to document spyware and surveillance technology sales to Indonesia.

Firstly, Amnesty International used commercial trade databases to identify shipments that indicated spyware sales to Indonesia. As a result, Amnesty International uncovered various transfers of hardware and software through Singapore-based companies acting as intermediaries for spyware or surveillance technology suppliers from countries including Israel and Malaysia. Trade databases referenced as part of this research include Panjiva, Volza and 52WMB.

Through this detailed analysis of shipment records and import declarations, supported by open-source research, Amnesty International identified specific shipment descriptions such as "one-click Android installation module" and "CYBER INTELLIGENCE INFILTRATION; EXFILTRATION SYSTEM" which suggested the purchase of spyware and formed the basis of the investigation.

Amnesty International cross-referenced identified shipments with open-source materials, such as leaked surveillance product brochures published by previous investigations by media outlets. Other open-source information, including archived web pages from broker companies and resellers, was also used to identify the suppliers of the spyware and surveillance technology. Amnesty International also relied on previously published research by Citizen Lab and Access Now which tracked FinFisher's FinSpy deployments in Indonesia.

Through this detailed analysis of shipment records and import declarations, supported by open-source research, Amnesty International identified specific shipment descriptions such as "one-click Android installation module" and "CYBER INTELLIGENCE INFILTRATION; EXFILTRATION SYSTEM" which suggested the purchase of spyware and formed the basis of the investigation.

Amnesty International also performed continuous internet scanning and network measurements to identify the deployment of attack servers and other infrastructure linked to highly invasive spyware. Spyware infrastructure from all different spyware vendors each have distinct fingerprints on how webservers are enabled, the locations where internet domains are purchased and how intermediary servers are setup. This has allowed Amnesty International to build visibility into the testing and deployment of spyware systems in multiple countries around the world. This methodology has also, at

times, allowed for the identification of spyware backend systems deployed on networks, by linking the spyware infrastructure networks to a specific government in a country, but not to a specific agency. These technical measurements provide insights into the deployment of such spyware systems. In the case of Indonesia, the network measurements have been used extensively to confirm findings first identified in trade data.

Lastly, Amnesty International sent letters to the twenty-one entities mentioned in the briefing, including companies, government agencies responsible for export controls and end-users requesting their responses to the research findings. Of the twenty-one entities contacted, companies Candiru (Saito Tech) and NSO Group (Circles and Cyber Technologies SARL) and exporting agencies Swiss State Secretariat for Economic Affairs (SECO) and Israeli Defense Exports Control Agency (DECA) responded to our request for confirmation and clarifications. The Indonesian National Police responded to acknowledge our letter but declined to answer our questions. The responses have been summarised and incorporated in this publication.

3. CIVIC SPACE AND LEGAL FRAMEWORK IN INDONESIA

3.1SHRINKING CIVIC SPACE IN INDONESIA

The use of surveillance technologies, such as spyware, gives rise to a risk not only of real-time violations of the right to freedom of peaceful assembly, but also to the deterrence of people from exercising their rights in the future. Spyware is a type of malicious software that collects information from a device without alerting the user and sends it to another unauthorised entity. Highly invasive spyware allows unlimited access to a device by default and leaves minimal traces, making it almost impossible for the user to know what data was taken (for more information on what spyware is, please check Amnesty International's spyware explainer).

The number of identified sales and deployments of highly invasive spyware to Indonesia is of special concern, where civic space has shrunk in past years due to the ongoing assault on the rights to freedom of expression, peaceful assembly and association, personal security and freedom of arbitrary detention.

In 2022, Amnesty International published "Silencing voices, suppressing criticism", a documenting the decline of civil liberties and the shrinking civic space in Indonesia. Between January 2019 and May 2022, Amnesty International recorded at least 90 cases of digital harassment and other forms of digital attacks directed against civil society, resulting in at least 148 victims, which include civil society actors like human rights defenders, activists, journalists, environmental defenders, students, and protestors. The intimidation took many forms, including password theft of their social media accounts, spam calls from unidentified international numbers and digital harassment such as intrusions during online discussions. These attacks were carried out by unidentified parties pushing to spread fear and silence civil society voices.

Given this existing precedent of attacks in the digital sphere, also documented by SAFENet, Lokataru Foundation and Privacy International, the sale and transfer of highly invasive spyware and surveillance technologies to Indonesia are concerning for human rights.

3.2ABSENCE OF A REGULATORY FRAMEWORK TO CURB THE MISUSE OF SPYWARE AND SURVEILLANCE TECHNOLOGY

Governments are obliged under international law not only to respect and fulfil human rights, but also to protect people from abuses by third parties such as private companies. Indonesia's legal framework recognizes the rights to freedom of expression, peaceful assembly and association, personal security,

and freedom of arbitrary detention, having ratified numerous international human rights treaties including the International Covenant on Civil and Political Rights (ICCPR).

Indonesia does not have laws specifically governing the lawful use of spyware and surveillance technologies. The most relevant regulatory framework concerns the use of wiretapping for law enforcement purposes, including Law No. 11/2008, as amended by Law No. 19/2016 and by Law No. 1/2024 on the Electronic Information and Transactions Law (EIT Law). According to the EIT Law, wiretapping is the activity of listening to, recording, diverting, altering, obstructing and/or logging the transmission of electronic information and/or electronic documents that are not public in nature, whether through wired communication networks or wireless networks, such as electromagnetic radiation or radio frequency transmission.

The EIT Law explicitly stipulates that wiretapping can only be carried out in the context of law enforcement at the request of the police, prosecutor's office or other institutions (Article 31). Interception in general requires a warrant from a judge as it is a form of forceful measures for obtaining access to and recording information (Law 36/1999 on Telecommunication). The Law on State Intelligence passed in October 2011 broadly authorises the Indonesian State Intelligence Agency (BIN) to engage in activities "to prevent and/or to fight any activity, work, intelligence activity, and/or opponent that may be harmful to national interests and national security" (article 6), which may include communications surveillance.

However, there are no specific mechanisms to request transparency or disclose the use of interception methods in such instances of 'national security' or law enforcement concern, including spyware and other surveillance deployments, to challenge alleged abuses, or to claim redress to victims, leaving the public in the dark and posing a significant risk to civil society in Indonesia.

OBJ

4. HIGHLY INVASIVE SPYWARE AND DUAL-USE TECHNOLOGIES

States can only engage in lawful targeted digital surveillance if it's accompanied by robust human rights protections to prevent abuse. According to international human rights standards, such surveillance should be based on individualised reasonable suspicion, conducted within the bounds of the law, strictly necessary to achieve a legitimate aim, and executed in a proportionate and non-discriminatory manner.

However, even with a regulatory framework compliant with the highest human rights standards, certain highly invasive spyware poses a significant risk of rights violations. This type of spyware grants unrestricted access to devices and cannot be independently audited, making it incompatible with human rights standards.

The European Data Protection Supervisor emphasises that such invasive tools severely compromise privacy rights to the extent that individuals are effectively deprived of them, rendering their use disproportionate and unacceptable. Similarly, the UN Special Rapporteur on Counterterrorism argues for a ban on spyware that lacks meaningful limitations on functionality and cannot be audited independently.

Highly invasive spyware like Cyrus, Pegasus and Predator (and any of their rebranded versions) fall into this category, as they inherently access vast amounts of data on devices and cannot currently be audited independently. Consequently, Amnesty International concludes that the deployment of highly invasive spyware cannot be considered compliant with human rights standards.

DUAL-USE AND NON DUAL-USE EQUIPMENT

Enforcing regulations on dual-use technologies (which have both civilian and military applications) is particularly crucial in addressing the proliferation of highly invasive spyware and other surveillance technology, which poses a severe threat to human rights worldwide. Such highly invasive spyware can be covertly deployed to conduct very intrusive surveillance against civil society, and suppress freedom of expression which can have a chilling effect. Without effective enforcement mechanisms, this technology can be readily exported and exploited leading to egregious violations and abuses of human rights, including the right to privacy. The unchecked spread of highly invasive spyware underscores the urgent need for robust oversight and enforcement of dual-use regulations to prevent its misuse and protect individuals' rights to privacy and free expression.

Many dual-use technologies rely on components and infrastructure that may not themselves be subject to dual-use regulations but are integral to the functioning of systems with potential military applications. Moreover, the reliance on countries that export non-dual-use technologies essential for the operation of dual-use systems further underscores the significance of enforcement efforts in upholding human rights. By ensuring strict enforcement of regulations governing the export and transfer of these non-dual-use items, governments can prevent the proliferation of dual-use systems that pose a threat to human rights. Collaborative efforts among exporting and importing countries are essential to establish comprehensive controls that address the full spectrum of technologies involved in dual-use systems, thereby promoting accountability and safeguarding against their misuse.

5. SPYWARE AND OTHER SURVEILLANCE PRODUCTS IN INDONESIA

This section outlines the evidence that Amnesty International has identified that relates to the sale, export and deployment of spyware and surveillance technologies by a number of different companies and governments. Cumulatively, these findings demonstrate how extensive the sales and deployments of spyware and surveillance technologies have been to just one country, Indonesia, as well the failure of exporting countries to provide any sort of transparency on how such sales are regulated.

5.1 FINFISHER

BACKGROUND

FinFisher was one of the earliest groups of companies selling highly invasive spyware to governments around the world. While they had corporate entities in a number of countries, their headquarters was in Germany. Since 2011, FinFisher's FinSpy spyware has been reportedly used to target activists in Bahrain, political opposition in Turkey and others around the world. Their FinSpy spyware supports the targeting and infection of Windows, Mac, and Linux operating systems, as well as Android and iOS mobile devices. In May 2023, a German Public Prosecutor's Office filed criminal charges against FinFisher in Germany, following a criminal investigation on suspicion of illegally exporting spyware products to Turkish authorities without the legally required export licence. The investigation was started after several German civil society organisations filed a criminal complaint with German prosecutors following the alleged discovery of FinSpy spyware samples targeting a Turkish opposition political group in 2017.

German corporate records show that the FinFisher group of companies including FinFisher GmbH, FinFisher Holdings GmbH,FinFisher Labs GmbH and Raedarius m8 GmbH, . FinFisher Holdings is now known as Vilicius Holdings GmbH according to the German company registry.

FinFisher's FinSpy spyware has previously been linked to Indonesia. In March 2013, Citizen Lab published a report based-on internet scanning measurements which identified FinSpy customer servers hosted in Indonesia. A 2015 follow-up publication based on internet scanning by Citizen Lab attributed FinFisher servers to Indonesia's National Encryption Body ("Lembaga Sandi Negara") which in 2017 was renamed to the National Cyber and Crypto Agency ("Badan Siber dan Sandi Negara").

A German Division of the Federal Ministry for Economy and climate protection answered to questions send by a German politician, that the group of FinFisher companies only received one export license in 2015, the customer remains unknown.

FINFISHER SUMMARY

Amnesty International linked Raedarius M8 Sdn Bhd ("Raedarius M8") to Finfisher by reviewing extracts of corporate records from company registers in Malaysia and Germany. Raedarius M8 in Malaysia is wholly owned by German Raedarius M8 GmbH. German Raedarius M8 is wholly-owned by FinFisher Holding GmbH, which is the holding company of FinFisher GmbH and FinFisher Labs GmbH according to the German company registry.

RAEDARIUS M8 SDN BHD SHIPMENTS

Amnesty International has identified shipment records in commercial trade databases which show a hardware shipment from Raedarius M8 to the Indonesian company PT. Digital Solusi Prima in August 2021. (PT is a designation for companies based in Indonesia.)

The shipment records do not state the exact nature of the hardware sent from the FinFisher entity in Malaysia to Indonesia, nor do they detail the end-user of this product. It is unclear if the exported computer hardware is related to FinFisher's FinSpy spyware, another surveillance product or another

technology sold by the company. Some hardware components in the shipment appear to be off-the-shelf computer accessories which may form part of a larger system.

Date	Sender	Receiver	Goods	Declared value in U.S. Dollars
7 August 2021	Raedarius M8 Sdn Bhd	PT. Digital Solusi Prima	POWER SUPPLY FOR SINGLE BOARD COMPUTER RASPBERRY PI	72.61
7 August 2021	Raedarius M8 Sdn Bhd	PT. Digital Solusi Prima	FANLESS COMPUTER ACCESSORIES	24.2
7 August 2021	Raedarius M8 Sdn Bhd	PT. Digital Solusi Prima	CHARGER FOR MAX	96.81
7 August 2021	Raedarius M8 Sdn Bhd	PT. Digital Solusi Prima	PLASTIC CASE	363.05
7 August 2021	Raedarius M8 Sdn Bhd	PT. Digital Solusi Prima	FANLESS COMPUTER	726.11
7 August 2021	Raedarius M8 Sdn Bhd	PT. Digital Solusi Prima	FANLESS COMPUTER ACCESSORIES	96.81
7 August 2021	Raedarius M8 Sdn Bhd	PT. Digital Solusi Prima	PLASTIC CASE	363.05
7 August 2021	Raedarius M8 Sdn Bhd	PT. Digital Solusi Prima	FANLESS COMPUTER ACCESSORIES	48.4
7 August 2021	Raedarius M8 Sdn Bhd	PT. Digital Solusi Prima	SINGLE BOARD COMPUTER RASPBERRY PI	217.84
7 August 2021	Raedarius M8 Sdn Bhd	PT. Digital Solusi Prima	FANLESS COMPUTER ACCESSORIES	12.11
7 August 2021	Raedarius M8 Sdn Bhd	PT. Digital Solusi Prima	POWER SUPPLY FOR FANLESS COMPUTER	96.81
7 August 2021	Raedarius M8 Sdn Bhd	PT. Digital Solusi Prima	FANLESS COMPUTER SPARE PART	84.72
7 August 2021	Raedarius M8 Sdn Bhd	PT. Digital Solusi Prima	BATTERY UNIT	193.64

Table 1: Raedarius M8 Sdn Bhd shipments to Digital Solusi Prima

The shipment records in the above table are obtained from commercial companies selling their import/export records. Amnesty International bought these shipment records. Amnesty International has not been able to determine where Raedarius M8 originally imported this hardware from.

A 2018 report by Access Now documented an Indonesian Android application from 2016 which contained an embedded FinSpy spyware sample. The 2016 Android FinSpy spyware sample used the domain satgas[.]net as an API endpoint. This domain has pointed at various Indonesian IP addresses over several years. Passive DNS records show that when this domain was first registered it briefly pointed at the Indonesia IP address 27.50.30[.]56, which is located in an IP range hosting multiple services linked to the Indonesian National Counter Terrorism Agency ("Badan Nasional Penanggulangan Terorisme" – BNPT). There is insufficient evidence to confirm if BNPT is a customer of FinFisher based on this technical information alone.

Amnesty International wrote to Vilicius Holdings GmbH, formerly known as FinFisher Holding GmbH, and PT. Digital Solusi Prima for confirmation and clarification on the above-mentioned evidence,

including questions on the identified sale and any other potential spyware and surveillance technology transfers since 2017, the respective export licenses and any human rights due diligence assessments carried out in accordance with the UN Guiding Principles on Business and Human Rights. Neither Vilicius Holdings GmbH nor PT. Digital Solusi Prima had responded to Amnesty International's questions at the time of publication.

5.2WINTEGO SYSTEMS LTD

BACKGROUND

Wintego Systems Ltd ("Wintego") is an Israeli cyber-surveillance company that markets spyware tools for smartphones and a range of tactical network interception technologies under the WINT brand. While some of Wintego's products have been documented through the years, there has been a large gap in public understanding of what Wintego offers.

Forbes published an article in September 2016 detailing Wintego Systems' CatchApp, which allows, through Wintego tactical WINT product, to intercept WhatsApp messages. In August 2022, Google's Project Zero published an analysis of an exploit targeting the Linux kernel which Wintego combined with a Chrome browser or Samsung browser exploit to remotely compromise an Android phone. No customers of Wintego Systems have been publicly named.

WINTEGO **5 B 020**

1 Ha-tsmikha St.
PO Box 241
2069204 Yokneam Ilit
ISRAEL
contact@wintego.com
www.wintego.com

Classification thématique / Classification by theme

Lutte anti-terrorisme - Forces Spéciales • Maintien de l'ordre
Anti-terrorism - Special forces • Law enforcement

Activités - produits / Activities - Products

Ecoute / contre-écoute • Logiciel de traitement et d'analyse des données • Téléphonie mobile
Audio surveillance / Counter surveillance • Data processing and analysis software • Mobile telephony

Profil / Profile

Wintego: Your Long-Term Cyber Intelligence Partner

Wintego's core expertise is in developing cyber intelligence solutions for government, law enforcement, military, and intelligence agencies.
The Wintego platform consists of a variety of advanced solutions for injecting cyber agent (Trojans) providing remote data-extraction capabilities, and supports cyber intelligence operations on many types of mobile phones and operating systems.
The extracted data includes messages from instant messaging apps, private messages, social-network profiles, photos and videos, email messages, and more.
Wintego's solutions have been deployed by numerous government agencies around the globe.

Wintego Cyber Agents

Wintego Helios

WINTEGO SUMMARY

Amnesty International identified network infrastructure associated with Wintego's Helios spyware, as well as malicious domains, used in Indonesia and in other countries. Through open-source information from trade databases and the website of the company, Amnesty International also identified a Wintego reseller in Singapore: Ataka Enterprises PTE Ltd ("Ataka"). Amnesty International subsequently found a blog post by a self-identified employee of Ataka from 9 April 2019. The blog post claims Ataka is a partner of the Indonesian National Police to whom they supply "the Helios Android and Tactical Web Intelligence". Amnesty International identified an additional Wintego shipment to the Indonesian National Police from ESW Systems PTE Ltd ("ESW Systems"), another Singapore-based company. Amnesty International classifies Wintego's 'Helios' as a form of highly invasive spyware.

WINTEGO NETWORK INFRASTRUCTURE

Network analysis shows that in August 2018 the website tribunnews.org, which mimics the legitimate TribunNews.com, was loading an external webpage using an embedded iFrame, as captured by the URLScan.io service, from the domain coolbrandlabs.com. The landing page also included metadata spoofing the legitimate news website.

Such spyware infection domains are normally chosen to look legitimate and interesting to the potential targets of the spyware customer. In a one-click attack, the target will typically be tricked into opening a link that appears relevant to their interests but then infects their device.

Amnesty International attributes the domains tribunnews.org and coolbrandlabs[.]com to Wintego. When the coolbrandlabs[.]com domain was first registered, it pointed to the Israeli IP 31.168.34[.]139. This same IP range includes multiple Ips hosting a Fortinet VPN appliance. One of these VPN IP addresses was listed in a publicly indexed system administration document confirming that the VPN server belongs to Wintego.

Internet scan data shows that multiple IP addresses in the same IP range have in the past returned self-signed TLS certificates for the VPN appliance. One of these IP addresses, 31.168.34.138, has also served a self-signed certificate with the certificate common name "Helios". Helios is listed in public marketing material as the name of Wintego's spyware or "cyber agent" product. Other domains in the same IP range also imitated mobile device manufactures such as the domain "galaxyupdate[.]network", which impersonates Samsung's Galaxy brand.

IP	Common Name	Cert Issuer	Issued	First Seen	Last Seen
31.168.34.138	helios	helios	14 August 2017	2 September 2019	22 March 2019
31.168.34.138	galaxyupdate[.]network	COMODO RSA Domain Validation Secure Server CA	November 2018	3 October 2019	5 October 2019
31.168.34.138	FG100E4Q17021631	Fortigate Certificate Authority	13 November 2017	25 September 2019	16 December 2020

Table 2: TLS certificates on Wintego IP range

Neighbouring IP hosted domains include coolbrandlabs[.]com and other domains imitating device firmware updates or hosting the Wintego corporate VPN.

IP Address	Domain	Cert Issued	First Seen	Last Seen
31.168.34.138	galaxyupdate[.]network	2018-11-12	3 October 2019	5 October 2019
31.168.34.138	FG100E4Q17021631 (VPN)	2017-11-13	25 September 2019	Currently active
31.168.34.139	coolbrandlabs[.]com	22 July 2018	7 July 2018	23 October 2018
31.168.34.139	neuropathynews[.]net	2019-05-04	21 May 2019	26 May 2021
31.168.34.140	neuropathynews[.]net	2019-05-04	24 January 2021	4 May 2021
31.168.34.140	lidarfirmwareupdate.network	2021-05-03	9 May 2021	9 May 2021
31.168.34.141	FG100E4Q17021631 (VPN)	2017-11-13	25 September 2019	16 December 2020
31.168.34.142	FG100E4Q17021631 (VPN)	2017-11-13	21 November 2020	16 December 2020

Table 3: Domains on Wintego IP range

It is unclear if the coolbrandlabs[.]com domain was only used for testing purposes or if it was also used to target individuals. Passive DNS and internet scan data shows that from late October 2018 the coolbrandlabs[.]com was pointing to a server in Indonesia hosted on IP 182.23.27.149. This same IP continued to serve a valid TLS certificate for the coolbrandlabs[.]com domain until at least January 2020.

Amnesty International identified additional network infrastructure which appears linked to Wintego's Helios spyware product. In addition to domains linked to Indonesia, other suspect domains cloned media websites from Europe and multiple news websites based in Senegal or other sub-Saharan African based websites. Amnesty International has published these domains to support further civil society research.

Wintego Domain	Imitated domain
dakaractu.news	dakaractu.com
afrinews.eu	afrinews.co.za
expressotelecom.eu	expressotelecom.com
jeuneafrique.eu	jeuneafrique.com
jeuneafrique.news	jeuneafrique.com
jotnanews.co	jotnanews.com
jotnanews.fr	jotnanews.com
jotnanews.live	jotnanews.com
senedroid.net	senedroid.com
senego.fr	senego.com
senego.info	senego.com
seneweb.eu	seneweb.com
seneweb.news	seneweb.com

Table 4: Wintego domains with a focus on Senegal and Sub-Saharan Africa

WINTEGO SHIPMENTS AND POTENTIAL CUSTOMERS

Using shipment data from commercial databases and information posted on websites and blog posts, Amnesty International has found information indicating that Wintego's cyber-surveillance products were sold to the Indonesian National Police ("Kepolisian Negara Republik Indonesia") via two Singapore-based companies, Ataka and ESW Systems. (Please refer to Section 5.6 Broker companies in Indonesia and Singapore for more information on Ataka and ESW Systems). Amnesty International has not been able to confirm whether these were sold in one or multiple deals.

ATAKA

On a 2021 archived version of their website, Ataka listed a range of cyber-intelligence products they offer to "law enforcement and security agency customers", including a cyber intelligence platform from Wintego Systems (see Figure 1). A "cyber intelligence system" with an identical description was advertised on an earlier version of their website in 2018, but without the Wintego company name.

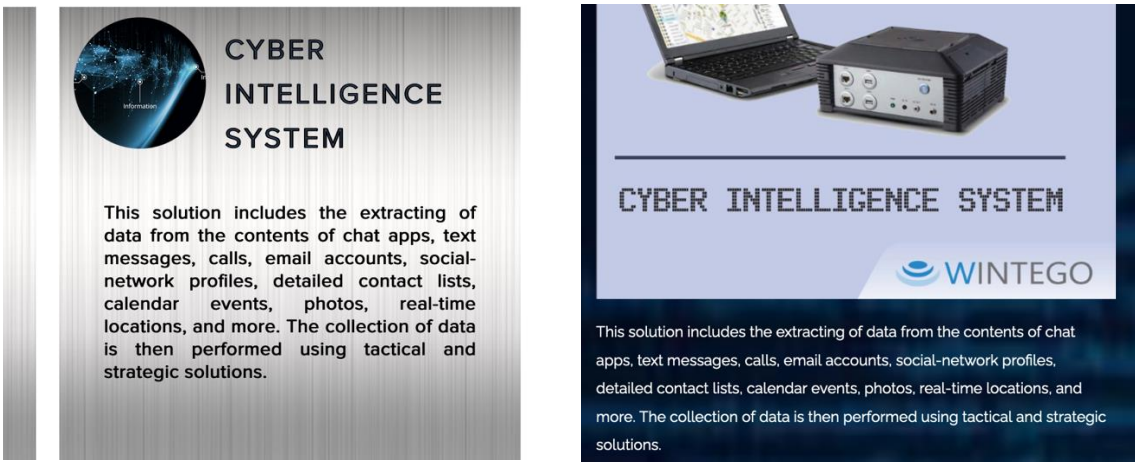


Figure 1: Images from archived versions of the Ataka website

Amnesty International also identified a blog post by an individual self-identifying as an employee of Ataka published on 9 April 2019. The blog post identifies the Indonesian National Police as a partner to whom Ataka supplies "the Helios Android and Tactical Web Intelligence" system. (Wintego's Helios spyware product is unrelated to Intellexa's "Helios" spyware).

ESW SYSTEMS

Analysis of commercial trade databases revealed a shipment titled "WINT SYSTEM" from Singaporean-firm ESW Systems to the Indonesian National Police ("Slog Polri" on trade records, but also known as "Kepolisian Negara Republik Indonesia") in September 2019. This appears to refer to WINT, a tactical cyber-surveillance product sold by Wintego. (For more information on ESW Systems, please refer to the section 5.6. Broker companies in Indonesia and Singapore).

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

Table 5: ESW Systems shipment

In addition, a project was mentioned for the "public sector" on the archived website of PT. Royal Cemerlang Teknologi, a corporate entity linked to Radika, which closely resembles a Wintego product. The project was listed as "Android-based Investigation System and Web Information Collection System". Amnesty International was unable to verify whether that refers to the Helios agent or the WINT product from Wintego .

Amnesty International contacted Wintego, Ataka, ESW Systems and PT. Royal Cemerlang Teknologi (Radika) for confirmation and clarification on the above-mentioned evidence, including questions on the identified sales, shipments and any other potential spyware and surveillance technology transfers since 2017; the respective government tenders; any human rights due diligence assessments carried out in accordance with the UN Guiding Principles on Business and Human Rights; and the relationship between the four different companies. None of the companies responded to Amnesty International's questions at the time of publication.

Amnesty International also contacted the Indonesian National Police to inquire about existing or past tenders for spyware and surveillance purchases; spyware and surveillance imports from several companies; and the use of spyware and surveillance technologies in compliance with human rights

law. The Indonesian National Police declined to respond to the allegations contained in the research findings.

Amnesty International contacted the Israeli Defense Export Controls Agency (DECA), for comments and clarifications on any received export licenses for spyware and surveillance technology imports to Indonesia and/or to Singapore, on any human rights assessments carried out, and on the commitment of the Israeli Government to implement an export control system that curbs human rights abuses. DECA responded:

> *"Israel controls export of cyber surveillance systems in accordance with the Israeli Defence Export Control legislation. Israel authorizes export of cyber surveillance systems to Government entities only, for anti-terror and law enforcement purposes, subject to receipt of EUCs and additional limitations as required.*
>
> *"While establishing our export control policies and reviewing licences applications human rights' considerations constitute an integral part of the process.*
>
> *"Furthermore and as a routine Israel reviews its own export control regulation, including cyber surveillance systems related aspects, in order to reduce the risk of misusing such systems.*
>
> *"As per specific questions relating to the country mentioned in your letter, I wish to clarify that Israel does not make public its defence export control policy, including information regarding licences."*

5.3INTELLEXA CONSORTIUM

BACKGROUND

The Intellexa consortium is a linked group of companies in various jurisdictions, which have at times included entities in North Macedonia, Hungary, Ireland, Switzerland, British Virgin Islands, Cyprus, and Greece. (Intellexa's activities, as part of the wide 'Intellexa Alliance', a technological and commercial alliance concluded with other Europe-based companies, is covered in Amnesty International's Predator Files report). The Intellexa consortium's most notable product is the highly invasive spyware platform Predator designed to compromise targeted iOS and Android devices. Research by Amnesty International, Citizen Lab and other partners has found that Intellexa's Predator spyware has been used to target civil society and political figures around the world including senior European and US legislators, a journalist and a former META manager in Greece, and Egyptian journalists and political opposition, among others. In July 2023, it was announced that an investigation by Greece's data protection authority into the use of Predator spyware traced more than 350 SMS messages relating to attempts to install surveillance software and that 92 phone users were notified that their mobile phones had been targeted.

On 18 July 2023, the United States Department of Commerce added the Intellexa consortium to their Entity List "for trafficking in cyber exploits used to gain access to information systems, threatening the privacy and security of individuals and organizations worldwide. Recognizing the increasingly key role that surveillance technology plays in enabling campaigns of repression and other human rights abuses, the Commerce Department's action today targets these entities' ability to access commodities, software, and technology that could contribute to the development of surveillance tools that pose a risk of misuse in violations or abuses of human rights." The U.S. Entity List is a trade control list maintained by the U.S. Department of Commerce, identifying foreign entities restricted from accessing American technology and goods due to national security or foreign policy concerns. Inclusion in the Entity List is intended to limit or prevent companies or individuals from sourcing hardware and

services from the United States and should block any procurement of services of those companies by the United States government.

On 5 March 2024, the United States Department of the Treasury implemented sanctions to corporate entities and members of the Intellexa consortium. The reasoning given was for "developing, operating, and distributing commercial spyware technology used to target Americans, including U.S. government officials, journalists, and policy experts".

INTELLEXA NETWORK INFRASTRUCTURE AND MALICIOUS DOMAINS

Using internet scanning techniques, Amnesty International's Security Lab has identified multiple Predator one-click infection domains that imitate legitimate Indonesian news websites and politically critical voices including Predator domain Suaraoposisi[.]net. The website is named Suara Oposisi (English: "Opposition voice"), which may suggest an attempt to attract users interested in political opposition issues. Other Predator domains imitated Papuan news website Suara Papua, referring to Papua and West Papua provinces, indicating likely targets in a region where human rights violations against activists and civil society are rampant. Another Intellexa Predator infection domain geloraku[.]id, registered in 2023, may refer to either the Gelora News website or the Gelora political party.

Through analysis of internet scanning data, Amnesty International identified an Indonesian IP address which hosted a server matching a fingerprint for Intellexa Predator backend servers. The backend server was hosted on IP address 103.106.174.99 and first appeared in internet scans in December 2021. This internet scan data confirms that a Predator customer system was deployed in Indonesia in late 2021. Amnesty International believes that the same Intellexa Predator customer continued to be active in Indonesia as of December 2023.

The earliest Indonesia-linked Predator infection domains identified by Amnesty International were registered in March 2022, including ewestpapua[.]org and nindonesia[.]news.

Previous research from Amnesty International has shown that Intellexa and other surveillance vendors frequently use international and domestic brokers and agents when negotiating spyware deals. In the case of Indonesia, this investigation has not identified any shipment or export records which we can associate with the sale of Predator to Indonesia.

Amnesty International contacted the Intellexa consortium for confirmation on the above-mentioned evidence, including questions on any spyware and surveillance technology exports to Indonesia and Singapore; the relevant export licenses; and any human rights due diligence assessments carried out in accordance with the UN Guiding Principles on Business and Human Rights. The Intellexa consortium did not respond substantively prior to publication.

Amnesty International also contacted the General Secretariat for International Economic Affairs and Openness in Greece to inquire about spyware and surveillance technology export license requests received and reviewed by the Secretariat; and the findings from the internal monitoring exercise conducted by the Secretariat on exports of cyber-surveillance items to Madagascar and Sudan. The General Secretariat for International Economic Affairs and Openness did not respond to Amnesty International's questions prior to publication.

5.4CANDIRU (SAITO TECH)

BACKGROUND

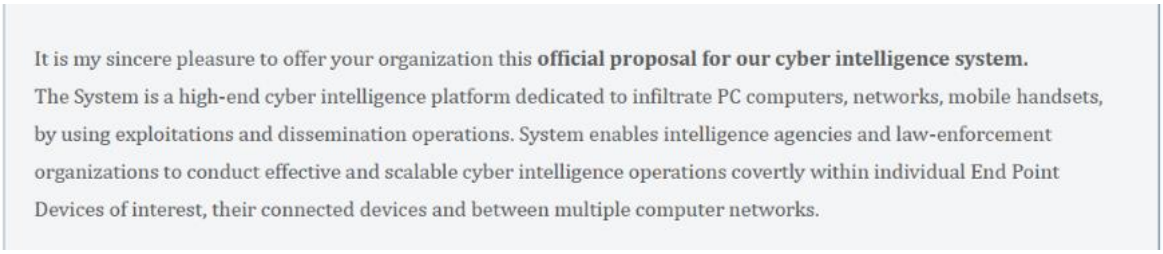
Saito Tech, also known as Candiru, is an Israeli cyber-surveillance vendor which offers a "cyber infiltration system", marketed as "Cyrus", designed to "infiltrate PC computers, networks, mobile handsets, by using exploitations and dissemination operations" according to a leaked Candiru

commercial proposal from 2020, published by The Marker, which outlines some of Candiru's capabilities for compromising Windows PC as well as Android and iOS mobile devices. The company has been renamed numerous times, most recently to Saito Tech. For the purposes of this briefing, the company is referred to as Candiru.

In November 2021, the United States Department of Commerce added several Candiru corporate entities to the Entity List based on "evidence that these entities developed and supplied spyware to foreign governments that used these tools to maliciously target government officials, journalists, businesspeople, activists, academics, and embassy workers. These tools have also enabled foreign governments to conduct transnational repression, which is the practice of authoritarian governments targeting dissidents, journalists and activists outside of their sovereign borders to silence dissent. Such practices threaten the rules-based international order."

Amnesty International found through network measurements both network infrastructure and malicious domains it associates with Saito Tech ("Candiru"). Amnesty International also found a hardware shipment, which Amnesty International associates with the Candiru system, to the Indonesian National Police as the end-user through Singapore-based Heha PTE Ltd ("Heha").

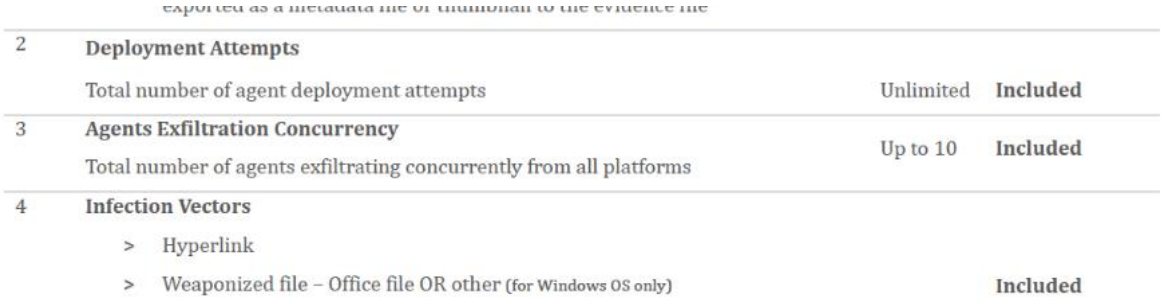
CANDIRU NETWORK INFRASTRUCTURE AND PROPOSAL



It is my sincere pleasure to offer your organization this **official proposal for our cyber intelligence system.** The System is a high-end cyber intelligence platform dedicated to infiltrate PC computers, networks, mobile handsets, by using exploitations and dissemination operations. System enables intelligence agencies and law-enforcement organizations to conduct effective and scalable cyber intelligence operations covertly within individual End Point Devices of interest, their connected devices and between multiple computer networks.

Figure 2: Screenshot from leaked Candiru proposal (Source: The Marker)

The leaked 2020 Candiru commercial proposal described in detail the range of features supported by the Cyrus spyware system, as well as optional add-ons which enable the expansion of the system to target individuals located in other countries. The proposal included a limit of "Agents Exfiltration Concurrency" as 10, which signifies the number of simultaneous infections that can be active at any one given time. The potential customer is provided with an offer to purchase additional "concurrent Infiltration Agents", which can expand the number of individuals the system can target during the same time.



2	**Deployment Attempts**		
	Total number of agent deployment attempts	Unlimited	**Included**
3	**Agents Exfiltration Concurrency**		
	Total number of agents exfiltrating concurrently from all platforms	Up to 10	**Included**
4	**Infection Vectors**		
	> Hyperlink		
	> Weaponized file – Office file OR other (for Windows OS only)		**Included**

Figure 3: Second screenshot from leaked Candiru proposal (Source: The Marker)

In a July 2021 report, researchers at Citizen Lab identified a suspected Candiru customer system 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.

An analysis by the Amnesty International Security Lab of the network infrastructure uncovered additional domain names which most likely have been registered on behalf of the same Candiru

customer. These domains mimic other Indonesian news websites including TribunNews, Tirto, MediaIndonesia and ANTARA News. The Candiru domain indoprogress[.]co and the other related domains were registered in November 2020. These domains are all related to the indoprogress[.]co Candiru domain. However, the Security Lab has not confirmed if these additional domains have all hosted Candiru spyware infection servers.

The Security Lab has continued to observe additional malicious Candiru spyware domains with a focus on Indonesia into 2022. These include domains promising digital security tips, a purported message from the Gelora political party about a controversial political project, and a website imitating an Islamic charity.

Candiru Domain	Website Title
aqaf.net	10 tips untuk penjelajahan web yang lebih aman dan terjamin
	10 tips for safer and more secure web browsing
gelora.org	Pemindahan IKN Perlu Penjelasan dan Narasi Komprehensif, Jika Tidak Akan Terhambat – Partai Gelora Indonesia
	The transfer of IKN needs a comprehensive explanation and narrative, otherwise it will be hampered - Gelora Indonesia Party
nusantaraqurban.com	QURBAN NUSANTARA – Cara Qurban Online|Tebar Qurban Ke Pelosok Nusantara | LAZNAS Sahabat Yatim Indonesia
	QURBAN NUSANTARA – How to Qurban Online | Spread Qurban to remote areas of the archipelago | LAZNAS Friends of Indonesian Orphans

Table 6: Candiru domains in Indonesia in 2022

CANDIRU SHIPMENTS

Trade records obtained by Amnesty International indicate that Singaporean firm Heha sent three shipments related to a cyber-surveillance system from Singapore to the Indonesian National Police in 2020 and 2021. All three shipments from Heha appear linked to a spyware product as the items are described as components for a "CYBER INTELLIGENCE INFILTRATION; EXFILTRATION SYSTEM". The shipments are listed as sent to the Indonesian National Police on 20 May 2020, 3 July 2020 and 27 January 2021 with a combined declared value of 33,169,153.27 USD.

While the shipments from Heha to the Indonesian National Police do not include an identifiable product or company name, we cross-referenced sources and found that there are significant correlations in the description and timing of the shipments which suggest Candiru as the likely original supplier of this cyber-surveillance system.

4. BOM (BILL OF MATERAIL)

HARDWARE COMPONENTS			
#	Item	Qty.	Description spec.
1	Management Server	1	Intel Xeon 8 core processor 32GB RAM 1GB NICs 2 PSU's Rack mount kit
2	Virtualization Servers	3	2 x Intel Xeon 8core processors 192GB RAM 1GB NICs 2 PSU's Rack mount kit
3	Central Storage	1	2 controllers 2 PSU's 15TB usable storage space Rack mount kit
4	Backup Server	1	Intel Xeon 8core processor 32GB RAM 1GB NICs 2 PSU's Rack mount kit
5	Switches	2	48 Port x 1GB switch
6	UPS	1	At least 5KVA Rack mounted
7	Firewall	2	Appliance supporting system traffic
8	KVM + Screen	1	Rack mounted KVM + Screen
9	Server Rack	1	42U 19" server rack

Figure 4: Bill of material from the leaked Candiru system proposal as published by the Marker.

The first of these sources was the previously referenced leaked proposal which included an itemised list of the key hardware components of the system, which align closely with the hardware included in the shipments to Indonesia. The description of "AGENTS CONCURRENCY", "CYBER INTELLIGENCE INFILTRATION" and "EXFILTRATION" also align between the trade records and the proposal, albeit these are relatively common terms used to by the industry.

Amnesty International cross-referenced the hardware components from the Candiru proposal with the shipments to Indonesia. The following component names and descriptions are as detailed in the export manifest.

Shipment Date	Component	Detailed Description
20 May 2020	MANAGEMENT SERVER	DELL EMC POWEREDGE R640
20 May 2020	VIRTUALIZATION SERVER	DELL EMC POWEREDGE R640
20 May 2020	BACKUP SERVER	DELL EMC POWEREDGE E740XD
20 May 2020	SWITCH	DELL EMC NETWORKING N3000E-ON
20 May 2020	UPS	SMART-UPS SRT5000VA RM 230V
20 May 2020	FIREWALL	FORTIGATE-101E-FG-101E-BDL
20 May 2020	KVM+SCREEN	DAV 2108 8-PORT ANALOG DMPU CONSOLE PE KVMS, VM, CAC & USB 2.0
20 May 2020	SERVER RACK	NETSHELTER SX 42U 600MMX1070MM DIP ENCLOSURE WITH SIDES BLACK

3 July 2020	MANAGEMENT SERVER	DELL EMC POWEREDGE R640
3 July 2020	VIRTUALIZATION SERVER	DELL EMC POWEREDGE
3 July 2020	BACKUP SERVER	DELL EMC POWEREDGE 740XD
3 July 2020	SWITCH	DELL EMC NETWORKING N3000E-ON
3 July 2020	UPS	SMART-UPS SRT5000VA RM 23
3 July 2020	FIREWALL	FORTIGATE -101E-FG-101E-B
3 July 2020	KVM+SCREEN	KVM+SCREEN DAV 2108 8 PORT ANALOG DMPU CON
3 July 2020	SERVER RACK	NETSHELTER SX 42U 600MMX1070MM

Table 7: Shipments

These shipments are declared with a total worth of 79,303.31 USD for the shipments in May 2020 and 75,815.00 USD for the shipments in July 2020 for a total of 155,188.31 USD.

All of the above listed items were described in the import record as a "HARDWARE SYSTEM" and "CYBER INTELLIGENCE INFILTRATION". A separate set of imports on 27 January 2021 appear to be related to the software components and licences for the system.

Shipment Date	**Detailed Description**	**Weight (KG)**	**Value (USD)**
27 January 2021	CYBER INTELLIGENCE INFILTRATION SYSTEM SOFTWARE SYSTEM **MAIN SYSTEM**	0.52	11,754,077.42
27 January 2021	CYBER INTELLIGENCE INFILTRATION SYSTEM SOFTWARE SYSTEM **AGENTS CONCURRENCY**	0.48	11,065,043.56
27 January 2021	CYBER INTELLIGENCE INFILTRATION AND EXFILTRATION SYSTEM SOFTWARE SYSTEM **AGENTS CONCURRENCY**	1.00 KG	10,194,913.98

Table 8: Shipments

The stated value on the import records described the "MAIN SYSTEM" software component license as 11,754,077.42 USD, with two additional "AGENTS CONCURRENCY" imports valued at 11,065,043.56 USD and 10,194,913.98 USD respectively. With the added 155,188.31 USD of hardware, the total value of these three shipments is 33 089 849,96 USD.

Drawing on the technical evidence and trade data outlined above, Amnesty International assesses with high confidence that the Candiru spyware system was supplied to Indonesian authorities around 2020. Internet scans and other technical measurements show that Candiru spyware domains with a focus on Indonesia, as well as additional Candiru server infrastructure were deployed in the country around that time. The identified trade records, which closely match the hardware specifications in a published Candiru proposal, additionally support Amnesty International's findings that the Candiru spyware platform was supplied to the country. The trade data also indicates the Indonesian National Police as the likely end-user of the Candiru spyware. The earliest Indonesia-related Candiru domains were first registered in the months following the suspected Candiru shipments.

Amnesty International contacted Saito Tech (Candiru) and Heha PTE LTD for clarification on the above-mentioned evidence, in particular questions about spyware and surveillance transfers to Indonesia and Singapore, specifically to the Indonesian National Police; about any human rights due diligence assessments carried out in accordance with the UN Guiding Principles on Business and

Human Rights; about the malicious domain names identified; and about the relationship between the two companies.

Candiru responded to Amnesty International to state:

> *"The company operates under the regulation of Israeli Ministry of Defense Export Control Agency (DECA) – Export Control Law, 5766-2007.*
>
> *"As such - the company is legally prohibited from providing any information regarding its licenses, nor can confirm or deny any of the detailed questions presented by you.*
>
> *"Please refer to the extent of the licensing and legal procedures publicly stated by the Israeli Ministry of defense, Defense Export Controls Agency (DECA), which will shed some light and help you further understand some of the due diligence related actions conducted by the company and navigating its legal actions."*

Amnesty International contacted the Indonesian National Police to inquire about existing or past tenders for spyware and surveillance purchases; spyware and surveillance imports from several companies; and the use of spyware and surveillance technologies in compliance with human rights law. The Indonesian National Police declined to respond to the allegations contained in the research.

Amnesty International contacted the Israeli Defense Export Controls Agency (DECA), for comments and clarifications on any received export licenses for spyware and surveillance technology imports to Indonesia and/or to Singapore, on any human rights assessments carried out, and on the commitment of the Israeli Government to implement an export control system that curbs human rights abuses. DECA's response is included at the end of Section 5.2.

5.5NSO GROUP, CIRCLES AND Q CYBER TECHNOLOGIES

BACKGROUND

NSO Group is a company based in Israel that develops and sells the Pegasus spyware platform designed to covertly compromise mobile devices such as iPhones and Android devices, as well as Blackberry in the past. NSO Group's Pegasus spyware has been forensically confirmed in at least 12 countries according to evidence uncovered by Amnesty International, Citizen Lab, Access Now, Reporters Without Borders and other researchers.

In November 2021, the United States Department of Commerce added NSO Group to the Entity List based on "evidence that these entities developed and supplied spyware to foreign governments that used these tools to maliciously target government officials, journalists, businesspeople, activists, academics, and embassy workers. These tools have also enabled foreign governments to conduct transnational repression, which is the practice of authoritarian governments targeting dissidents, journalists and activists outside of their sovereign borders to silence dissent. Such practices threaten the rules-based international order."

CIRCLES SUMMARY

Circles is a Bulgaria-based subsidiary of the NSO Group. Amnesty International confirmed the presence of Circles network infrastructure found in Indonesia, which Amnesty International associates with Indonesia-based Radika, as highlighted previously by CitizenLab in their "Running in Circles" publication. Amnesty International also confirmed a shipment of Luxembourg-based Q Cyber Technologies to an Indonesian company.

PRIOR FINDINGS BY INDONESIALEAKS

The investigative collective IndonesiaLeaks and their media partners, among them Tempo, published an investigation in June 2023 identifying Indonesia as a potential customer of NSO

Group's Pegasus spyware, which has been used to unlawfully target civil society members worldwide.

The IndonesiaLeaks findings were based on an analysis of import records and statements from multiple anonymous sources who indicated that Pegasus was sold to, and deployed in, Indonesia. In addition, IndonesiaLeaks also reported that sources stated that both the Indonesian National Police (Kepolisian Negara Republik Indonesia) and the State Intelligence Agency (Badan Intelijen Negara - BIN) had acquired access to Pegasus. Amnesty International has not independently confirmed these findings.

The IndonesiaLeaks investigation also reported that an Indonesian company, Radika won government tenders in Indonesia in 2017 for a "zero click intrusion [sic] system" and 2018 for a "zero click intrusion system (IOS)". A zero-click intrusion system is a spyware platform that is capable of infecting devices without requiring any action from the targeted individual. At the time, NSO Group's Pegasus spyware was one of the few commercially available spyware systems promising such a zero-click capability.

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
57	PENGADAAN ALMATSUS PENGEMBANGAN ZERO CLICK INSTRUSION SYSTEM (IOS) APBN TA. 2018	PT. RADIKA KARYA UTAMA	LPSE Kepolisian Republik Indonesia	14 February 2018	Rp 149.831.000.000,00

Figure 5: Tender document (Source: OpenTender.net)

Earlier research by Citizen Lab has also identified evidence that mobile network interception and geo-location systems developed and sold by Circles were deployed on IP addresses in Indonesia from September 2018 until at least December 2020.

Amnesty International attributed a surveillance system to Circles, a Bulgaria-based company affiliated with NSO Group, deployed in Indonesia as well as confirmed surveillance hardware shipments by Q Cyber Technologies SARL, a Luxembourg-based company also affiliated with NSO Group, to Indonesia.

CIRCLES NETWORK INFRASTRUCTURE

Amnesty International confirmed that Circles' surveillance systems were deployed on IP ranges 203.142.69.82–84 and 117.102.125.50–52. Both IP-blocks were registered to "RADIKA KARTA UTAMA" during the period these surveillance systems were operational. Amnesty International did not find a company with the name "Radika Karta Utama", however the name is similar to PT. Radika Karya Utama, which has a history of procuring surveillance systems on behalf of Indonesian authorities.

LUXEMBOURG-BASED Q CYBER TECHNOLOGIES SHIPMENTS

Amnesty International also confirmed that Q Cyber Technologies SARL based in Luxembourg, a corporate entity tied to NSO Group, is listed in commercial trade databases as responsible for shipping hardware components to an Indonesian company on 15 December 2020. Q Cyber Technologies has previously been reported in the Washington Post on for alleged sales of NSO Group's Pegasus spyware in 2018 to Saudi Arabia, and by Direkt36 in 2022 for a to Hungary. The outlined evidence

indicates that Radika has procured cyber-surveillance systems from NSO Group companies, but the technical evidence does not necessarily indicate involvement in procurement or deployment of Pegasus specifically. The only evidence of deployment by Radika is of a Circles system.

Amnesty International contacted Circles and Q Cyber Technologies SARL, both affiliated with the Israeli-based NSO Group, and PT. Radika Karya Utama for clarification on the above-mentioned evidence, including questions on the identified exports to Indonesia and any other spyware and surveillance technology sales to the country; on the required export licenses; on any human rights due diligence assessments carried out in accordance with the UN Guiding Principles on Business and Human Rights; on the identified IP-blocks; and on the relationship between NSO Group affiliates and PT. Radika Karya Utama. NSO Group responded to our questions:

> *As the NSO Group has previously responded to Amnesty, NSO Group is fully committed to upholding the UN Guiding Principles on Business and Human Rights (UNGPs). In the first half of 2020, NSO Group has adopted its Human Rights Due Diligence Procedure to implement the company's Human Rights Policy and help the company comply with applicable local laws as well as international human rights standards and in accordance with the UNGPs and the US Department of State Guidance on Implementing the UNGP for Transactions Linked to Foreign Government End-Users for Products or Services with Surveillance Capabilities. The multi-step due diligence procedure requires the assessment of the potential human rights impact of a proposed business opportunity prior to the sale of the company's product to a customer, paying particular attention to the state of rule of law, human rights, and safeguards, processes and institutional norms in the customer's country. Consistent with the Human Rights Due Diligence Procedure, we perform extensive due diligence on potential business opportunities. These steps are designed to help identify, prevent, and mitigate the risks of adverse human rights impacts associated with potential misuse of our products.*
>
> *As part of the review required by the Human Rights Due Diligence Procedure, when a new sales or marketing opportunity is identified, the designated compliance team conducts a risk assessment to evaluate human rights-related risks associated with the proposed opportunity considering the country and the specific end-user. The country review incorporates nine external, widely recognized governance and human rights indices to evaluate the relative strength of the proposed customer country's protection of human rights. Following the risk assessment and classification, the compliance team conducts a due diligence review. The steps required during this phase correspond to the proposed opportunity's assigned risk category and rely on information gathered from a number of sources, including open-source research, discussions with NSO Group employees, interviews with potential customers, and background materials prepared by external consultants or investigative firms. Finally, all proposed engagements must be reviewed and approved by designated committees within the company.*
>
> *I encourage you to review our 2021 and 2023 Transparency and Responsibility Reports, which outline our human rights policies, practices, and strict adherence to the UNGPs. We have made respect for human rights a core tenet across our operations and decision-making processes.*
>
> *Many of the issues raised in your letter are recycled information that has appeared in previous reports. We will not readdress these old issues.*
>
> *With respect to your specific inquiries, there have been no active Geo-location or Mobile End Point Intelligence systems provided by the NSO Group to Indonesia under our current Human Rights Due Diligence Procedure. As we have stated in the past, we cannot comment on specific existing or past customers. As we have also stated, all sales of our systems are to vetted government end-users. If there is any involvement of any private entity, it is solely as a commercial intermediary and they never receive any access to the operational systems. This is true even prior to the implementation of our current Human Rights Due Diligence*

Procedure. The previous vetting process was different from our current process but also included an in-depth review of the sales opportunity, including receipt of specific reports from independent outside sources.

In its response to questions about Q Cyber Technologies SARL, NSO Group stated that:

> *"Q Cyber Technologies SARL has never received any export license from Luxembourg as this was never required under law, since no export-controlled items have been exported from Luxembourg. NSO Group is closely regulated by export control authorities in the countries from which we export our products. The countries from which our systems have been exported have been included in our Transparency and Responsibility Report in the past, as well as publically stated in our appearance before the EU PEGA Committee. There have been no revisions to the export control framework affecting the company."*

and confirmed that all sales are made to vetted government end-users and, if any private entities are involved, it is as commercial intermediaries who do not receive access to the operational systems. On export controls, NSO Group confirmed that the company is closely regulated by export control authorities in the countries from which they export their products. The company pointed to their Transparency and Responsibility Report for more information on countries from which their systems have been exported. NSO Group claimed that Q Cyber Technologies SARL never received any export license from Luxembourg as it was not required under law, since no export-controlled items have been exported from Luxembourg.

Amnesty International contacted the Israeli Defense Export Controls Agency (DECA), for comments and clarifications on any received export licenses for spyware and surveillance technology imports to Indonesia and/or to Singapore, on any human rights assessments carried out, and on the commitment of the Israeli Government to implement an export control system that curbs human rights abuses. DECA's response is included at the end of Section 5.2.

Finally, Amnesty International contacted the Indonesian National Police and the National Cyber and Crypto Agency in Indonesia for clarification on the above-mentioned findings, including questions about existing or past tenders for spyware and surveillance purchases; spyware and surveillance technology purchases by the Agency; and on the use of spyware and surveillance technology in compliance with human rights law. The National Crypto and Cyber Agency have not responded to Amnesty International's questions at the time of publication. The Indonesian National Police declined to respond to the allegations contained in the research.

5.6BROKER COMPANIES IN INDONESIA AND SINGAPORE

According to Amnesty International's evidence, Indonesia appears to rely on a murky ecosystem of surveillance suppliers, brokers and resellers that obscure the sale and transfers of spyware surveillance technology. The majority of sales and transfers took place via broker companies based in Indonesia and Singapore, including Indonesian Radika and related "Royal Group" companies, Singapore-based Heha PTE Ltd, and Singapore based ESW Systems PTE Ltd, 3L PTE Ltd and White Global Holdings PTE Ltd.

RADIKA AND RELATED "ROYAL GROUP" COMPANIES

Radika is a company based in Indonesia with a history of procuring surveillance technologies on behalf of Indonesian government agencies among a wider range of commercial activities unrelated to surveillance systems. Radika is also known under other corporate entities, including PT. Royal Cemerlang Teknologi and PT. Royal Arta Jayamanggala. The wider constellation of companies has at times described themselves as part of the Royal Group holding company.

As previously outlined (see Section 5.5 NSO Group, Circles and Q Cyber Technologies), public tender documents show that Radika has won government tenders for a zero-click intrusion system and has

had telecom surveillance and geolocation systems from the NSO Group affiliate company Circles deployed on IP networks registered to their company.

WHITE GLOBAL HOLDINGS, 3L AND ESW SYSTEMS

White Global Holdings PTE Ltd ("White Global Holdings") is a company located in Singapore, which alongside 3L PTE Ltd ("3L") and ESW Systems, also located in Singapore, make up a group of "associated and/or affiliated" companies, as described in the former's website, active in the sale of surveillance and other military and policing technologies.

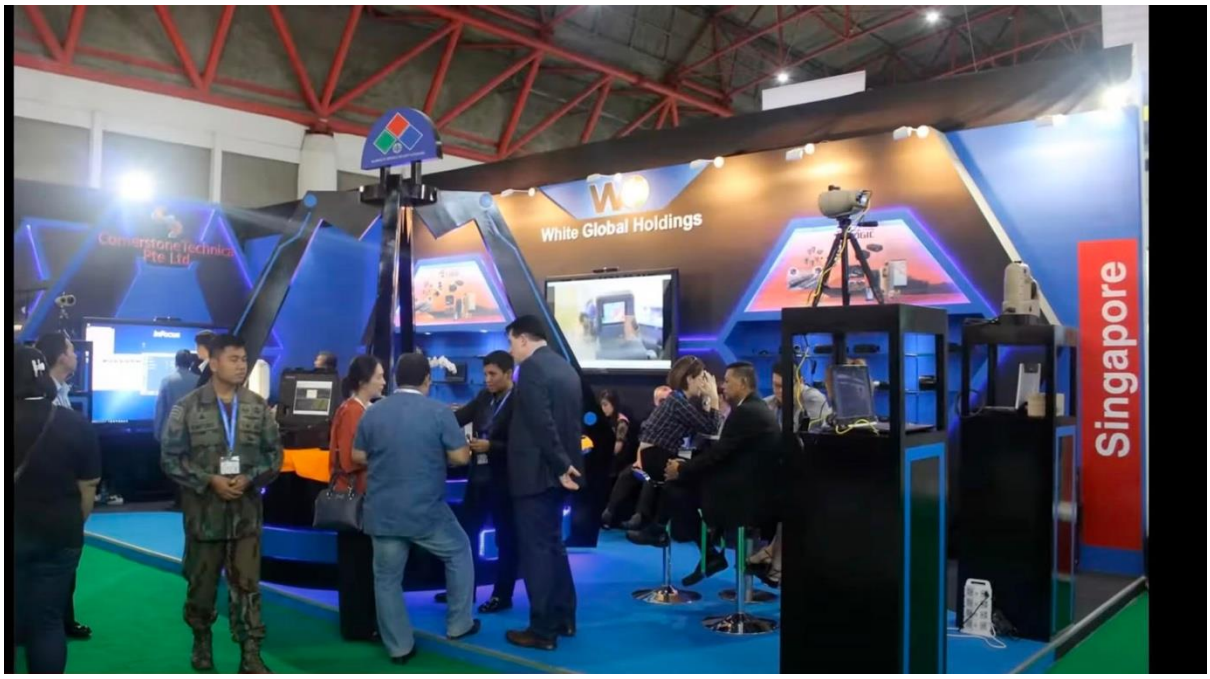


Figure 6: White Global Holdings has been active for over a decade and has participated in multiple regional industry trade fairs, including INDODEFENSE 2014 and INDODEFENSE 2016 where it had a stand. Stand of White Global Holdings at Indodefense 2016 as recorded by "KUKU PRODUCTION Rental Multimedia Audio Visual"

Both White Global Holdings and 3L are set up by a nominal company secretary and their beneficial owner is unknown. ESW Systems was also established with a nominal company secretary and its beneficial owner is also unknown. Corporate records show three Indonesian citizens had shares in the company and ceased as members on 21 August 2018. Two of the individuals also own Indonesian companies: Sastrawan Kamto, co-founder of PT. Royal Cemerlang Teknologi, which is active on the same address as PT. Radika Karya Utama; and Stanley Thirtabrata, who owns Softnet Indonesia.

Trade records show that White Global Holdings shipped an "Android one click installation module" on 19 March 2019 to the Indonesian "Treasurer of the National Cyber and Crypto Agency". This product description suggests the sale of a one-click spyware solution which can infect targeted Android devices. Amnesty International was unable to determine if this product is related to one of the spyware manufactures previously discussed, or to another manufacturer.

Trade records obtained by Amnesty International show that on 15 July 2021, Singapore-based ESW Systems exported amongst other components a "BASIC GRAPHICAL DETECTION AND IDENTIFICATION LICENSE (30.000 WATCH LIST)" to the Indonesian National Police valued at 11,061,033.66 USD. Amnesty International was unable to determine the original manufacturer or exact nature of this product. Other items included in this shipment to the Indonesia National Police are described as "BASIC REAL TIME GEOLOCATION TRACKING LICENSE" and "BASIC REAL TIME GEOLOCATION TRACKING". These other items suggest the system may be some form of mobile network traffic analysis or geolocation system which are used for surveillance purposes and would be covered by dual-use regulation.

As previously described in Section 5.2 Wintego Systems, trade records also show that ESW Systems has exported a product titled "WINT SYSTEM" to the Indonesian National Police, which we interpret as a surveillance product from Wintego Systems (who, as noted above, market spyware tools and a range of tactical network interception technologies under the WINT brand).

Amnesty International contacted White Global Holdings, ESW Systems and 3L for clarification on the above-mentioned findings, including questions on the identified spyware and surveillance technology transfers to Indonesia; on the existence of tenders for spyware and surveillance technology purchases in Indonesia; on the necessary human rights due diligence assessments carried out in accordance with the UN Guiding Principles on Business and Human Rights and on the relationship between the three companies and with Radika. None of the companies responded to Amnesty International's questions prior to publication.

Amnesty International also contacted the Indonesian National Police and the National Cyber and Crypto Agency in Indonesia for clarification on the above-mentioned findings, including questions about existing or past tenders for spyware and surveillance purchases; about spyware and surveillance technology purchases by the Agency; and about the use of spyware and surveillance technology in compliance with human rights law. The National Crypto and Cyber Agency has not responded to Amnesty International's questions in time for publication. The Indonesian National Police declined to respond to the allegations contained in the research.

Finally, Amnesty International contacted PT. Radika Karya Utama (and its director Andy Utama) and the "Royal Group" entities, PT. Royal Cemerlang Teknologi (and its director Sastrawan Kamto) and PT. Royal Arta Jayamanggala. Amnesty International inquired about the above-mentioned evidence, including questions on spyware and surveillance technology purchases; on any human rights due diligence assessments carried out in accordance with the UN Guiding Principles on Business and Human Rights; and on the relationship between PT. Radika Karya Utama, 3L PTE Ltd, White Global Holdings PTE Ltd and ESW Systems PTE Ltd. The company did not respond to Amnesty International's questions prior to publication.

HEHA

Heha is a company based in Singapore, that, among other things, is involved in the procurement of spyware and surveillance products to Indonesia. Trade records obtained from commercial trade platforms show three separate exports of computer hardware from Heha to the Indonesian National Police in 2020 and 2021 of a "CYBER INTELLIGENCE INFILTRATION; EXFILTRATION SYSTEM", with a declared combined value of approximately 33 million USD. (This shipment is described in more detail in the previous Section, 5.4 Candiru).

Amnesty International contacted Heha for clarification on the above-mentioned sale, including questions about the manufacturer of the sold technology; about any existing tender for the procurement of the sold technology; and about the necessary human rights due diligence assessments carried out in accordance with the UN Guiding Principles on Business and Human Rights. Heha has not responded to Amnesty International's questions in time for publication.

Amnesty International also contacted the Indonesian National Police inquiring about existing or past tenders for spyware and surveillance purchases; about spyware and surveillance technology purchases by the Agency; and about the use of spyware and surveillance technology in compliance with human rights law. The Indonesian National Police declined to respond to the allegations contained in the research.

6. CONCLUSION: AN INDUSTRY OUT OF CONTROL

Amnesty International has identified an extensive range of highly invasive spyware and surveillance products that have been supplied to various companies and state agencies in Indonesia including the Indonesian National Police and the National Cyber and Crypto Agency. Amnesty International has also documented an additional set of suspected surveillance imports to Indonesia where it has not been possible to conclusively identify the source or the exact nature of the products transferred.

While Amnesty International has uncovered significant evidence about the spyware and surveillance systems supplied, Amnesty International has little visibility into who these tools may have been used against. Highly invasive spyware tools are designed to be covert and to leave as few traces as possible. This built-in secrecy can make it exceedingly difficult to detect cases of unlawful misuse of these tools against civil society, and risks creating impunity-by-design for rights violations. In Indonesia, where civil society has faced an ongoing assault on the rights to freedom of expression, peaceful assembly and association, personal security and freedom from arbitrary detention, this is of particular concern.

This research also provides a case-study of how a murky web of suppliers, brokers and resellers are used locally and internationally to procure spyware and surveillance products. Intentional or otherwise, these non-transparent networks of companies can hide the nature of surveillance exports, while making independent oversight more difficult for judicial authorities, regulators, and civil society organisations.

Where export regulations exist, they are often limited in their ability to protect rights. This is because they fail to account for all relevant types of surveillance technologies and for all the potential threats posed to human rights, or, they risk suffering from weak enforcement and reduced transparency. Sensitive surveillance purchases may side-step or be exempt from normal transparent public procurement processes. Surveillance vendors may perform jurisdictional arbitrage and side-step regulatory oversight by exporting from an entity based in a lax export control regulatory environment. It becomes exceedingly difficult to identify where such invasive tools are being sold and to control if the suppliers have followed legally mandated rules for export licencing or performed their human rights due diligence assessments. Overall, inadequate regulation enforcement can lead to a culture of non-compliance, encourage risk-taking behaviour, and allow for a long-term deterioration of compliance culture.

For effective enforcement, governments need to invest in monitoring and compliance mechanisms, to ensure that the penalties for violations are substantial enough to deter non-compliance, and to demonstrate a consistent commitment to upholding export control laws. This involves a combination of technology, resources and international cooperation to track and regulate exports effectively.

Amnesty International calls on all countries to ban the sale, transfer, export and use of highly invasive spyware, which cannot be independently audited or limited in its functionality and so is fundamentally incompatible with human rights. Amnesty International also calls on all countries to implement a global moratorium – a halt on the sale, transfer, and use of surveillance technology – until there is a proper human rights regulatory framework in place that protests people from the misuse of these tools.

The Security Lab provides support to civil society members around the world who may be concerned about spyware attacks and unlawful digital surveillance. If you are a human rights defender, activist or journalist, and think you may have been a victim of a spyware attack, contact us for digital forensics support.

7. RECOMMENDATIONS

7.1 KEY RECOMMENDATIONS TO THE CYBER-SURVEILLANCE INDUSTRY

Companies operating in the cyber-surveillance industry including Intellexa consortium, Wintego Systems, Candiru and NSO Group, and affiliated entities, should:

- Immediately cease the production, sale, export and transfer of highly invasive spyware and/or exploits that does not include technical safeguards allowing for its lawful use under a human right respecting regulatory framework.
- Conduct human rights due diligence to ensure their activities do not cause or contribute to human rights abuses, and that such abuses are not directly linked to their operations, products or services by their business relationships such as with companies beyond the first tier in their value chain, including any end user that is able to target members of civil society in Indonesia, in accordance with international human rights standards. Identified safeguards that ensure the company's operations, products or services are rights-respecting must immediately be put in place.
- Urgently take the necessary steps to cease any activity found to be causing or contributing to adverse human rights impacts and prevent and mitigate further harm from unlawful surveillance, in particular of human rights defenders, journalists, and other members of civil society. This includes immediately terminating the use, support and sale of its technologies in states where state authorities have a history of digitally and/or physically targeting members of civil society or in which adequate legal safeguards against abuses are not present.
- Provide remediation, including adequate compensation and other forms of effective redress, to victims of unlawful surveillance who were targeted due to their operations.
- Ensure transparency regarding the volume, nature, value, destination, and end users of their surveillance technology transfers.

7.2 KEY RECOMMENDATIONS TO ALL STATES

- Enforce a ban on the sale, transfer, export or use of highly invasive spyware. Such spyware cannot, at present, be independently audited or limited in its functionality to only those functions that are necessary and proportionate to a specific use and target.
- Audit any relevant export licences granted to Wintego Systems, Candiru ("Saito Tech"), Intellexa and NSO Group ("Q Cyber Technologies") and conduct an independent, impartial, transparent investigation to determine the extent of any unlawful targeting or surveillance transfers, and offer remedy, to culminate in a public statement on the results of efforts and steps to prevent future harm.
- Ensure strong enforcement of export control regulations for non-highly invasive spyware and other dual-use surveillance technologies.
- Implement a human rights regulatory framework that governs surveillance in line with international human rights standards. Until such a framework is implemented, a moratorium on the purchase, sale, transfer, export and use of all spyware should be enforced.
- Implement domestic legislation that imposes safeguards against human rights violations and abuses through digital surveillance and establish accountability mechanisms designed to provide victims of surveillance abuses a pathway to remedy.

- Ensure that surveillance companies conduct human rights due diligence in relation to their operations, including on the use of their products and services by other companies beyond the first tier in their value chain.
- Take meaningful steps to ensure transparency and accountability regarding human rights due diligence regulation and practices, including by granting public access to beneficial ownership information of companies registered in their jurisdiction.

7.3KEY RECOMMENDATIONS TO THE EUROPEAN UNION AND ITS MEMBER STATES

- European Union (EU) member states and the European Commission should ensure the robust implementation of the 2021 EU Export Control Rules and ensure that exports that threaten human rights are prohibited.
- EU member states must adopt and enforce legislation that requires all corporate actors to respect human rights and implement human rights due diligence measures in line with the UN Guiding Principles. As part of the Corporate Sustainability Due Diligence Directive (CSDDD), the EU should ensure proper transposition of the CSDDD into the law of EU Member States and its strong implementation. EU Member States should require companies to conduct human rights due diligence with respect to the full value chain including the purchase, sale, transfer, export, and use of products. Companies operating in all sectors, including those producing spyware, as well as financial institutions, should implement the requirements on the CSDDD.

7.4KEY RECOMMENDATIONS TO THE STATE OF INDONESIA

- The Government of Indonesia should conduct an independent, impartial, and transparent investigation into the purchase of the spyware and surveillance technologies mentioned in this report, including whether there have been instances of human rights violations due to use of such technologies.
- The Government of Indonesia and relevant agencies including the Indonesian National Police, the National Cyber and Crypto Agency and the State Intelligence Agency should refrain from purchasing or using highly invasive spyware and other surveillance technology whose use is not governed by safeguards adequate to prevent abuse.
- The Government of Indonesia should enforce a ban on the purchase, sale, transfer and use of highly invasive spyware. Such spyware cannot, at present, be independently audited or limited in its functionality to only those functions that are necessary and proportionate to a specific use and target.
- The Indonesian House of Representatives should implement a human rights regulatory framework that governs surveillance and that is in line with international human rights standards. In particular, the Indonesian House of Representatives should formulate a specific law that imposes safeguards against human rights violations and abuses through digital surveillance, including a) establishing accountability mechanisms designed to provide victims of surveillance abuses a pathway to remedy, b) providing transparency about the volume and purpose of such surveillance deployments, and c) establishing oversight institutions to oversee the implementation of the said law and mechanisms.

- Until a human rights regulatory framework that governs surveillance is implemented, the Government of Indonesia should enforce a moratorium on the purchase, sale, transfer, and use of all spyware and rights-threatening surveillance technology.

8. APPENDIX 1: SURVEILLANCE INDUSTRY GLOSSARY

TERM	DEFINITION
BASEBAND	A mobile *baseband* is the hardware and software components in a mobile phone that are responsible for communicating over a radio interface with a mobile cell phone tower or base station.
COMMERCIAL SPYWARE	*Commercial or mercenary spyware* are surveillance products developed and sold by corporate actors to governments to conduct surveillance operations. So called "end-to-end" commercial spyware systems provide a full system for device infection and data collection. Components of these systems include the exploits used to install the spyware, a spyware agent that runs on the target device after infection and backend systems to gather and analyse the collected surveillance data.
EXPLOIT	An *exploit* is a piece of software or code that takes advantage of (or exploits) one or more software vulnerabilities to gain access to a device. On modern mobile devices exploits must bypass numerous layered security defences and can be highly complex. A full exploit chain targeting latest device versions can sell for millions of euros.
SOFTWARE VULNERABILITY	A *software vulnerability* is a technical flaw or weakness in a software component or piece of code which can be exploited by an attacker to bypass security defences.
SPYWARE (HIGHLY INVASIVE SPYWARE)	*Spyware* is software that enables an operator to gain covert access to information from a target's computer system or device. *Highly invasive spyware* is spyware that by default gains total access to data stored or transmitted from the target's device and that is designed to leave no traces on the device. As such, highly invasive spyware cannot be independently audited, and its deployment is incompatible with human rights.
SPYWARE AGENT	A *spyware agent* (or implant) is the final software code installed on a computer or phone after it has been successfully infected. The agent is responsible for collecting data from the device, activating sensors such as microphones and cameras, and uploading this data to the spyware operator.
ONE-CLICK	A *one-click* attack (sometimes referred to as 1-click attack) requires action from the target to enable the infection of their device, typically by opening a malicious link. Various social engineering techniques are used to trick the target into opening the link, including spoofing legitimate websites or news articles. If clicked on, the attack link loads an exploit chain to first compromise the web browser and ultimately install the spyware agent on the target device.
TACTICAL INFECTION	A tactical infection vector allows an attacker to attack devices in close physical proximity. Malicious Wi-Fi networks and mobile base stations can be used to silently redirect a nearby target to an exploit link. Attackers can also exploit vulnerabilities in cellular baseband software and Wi-Fi interfaces to infect nearby devices using radio packets sent over the air.
VECTOR	*Vector* is a surveillance industry term for the different pathways or techniques that can be used to deliver an exploit to a target device. These include so called *one-click* and *zero-click* vectors.
ZERO-CLICK	A *zero-click* attack (sometimes referred to as 0-click attack) is a surveillance industry marketing term for any vector that can infect a device without requiring a user action, such as clicking on a link.

TERM	DEFINITION
	Fully remote zero-click attacks allow infection over the internet, often by exploiting flaws in popular messaging apps such as iMessage or WhatsApp. Non-remote or *tactical* zero-click attacks can silently infect devices where the attacker has privileged network access or is in physical proximity to the target.
ZERO-DAY	A *zero-day vulnerability* is a software flaw that is not known to the original software developer and for which a software fix is not available. A zero-day exploit taking advantage of this flaw can successfully target even fully patched and updated devices.

Amnesty International is a movement of 10 million people which mobilizes the humanity in everyone and campaigns for change so we can all enjoy our human rights. Our vision is of a world where those in power keep their promises, respect international law and are held to account. We are independent of any government, political ideology, economic interest or religion and are funded mainly by our membership and individual donations. We believe that acting in solidarity and compassion with people everywhere can change our societies for the better.

Contact

info@amnesty.org

amnesty.org

facebook.com/
AmnestyGlobal

@Amnesty

Amnesty International
Peter Benenson House
1 Easton Street
London WC1X 0DW, UK

Index: **ASA 21/7974/2024**
Publication: **May 2024**
Original language: **English**