Israeli spyware

How to stop a product that threatens our rights ?

THE PEGASUS EFFECT

THE GLOBAL IMPACT OF ISRAELI SURVEILLANCE TECHNOLOGY

The Israeli military functions as an incubator for the country's private surveillance sector. This makes the NSO Group, the maker of Pegasus spyware, a case study in how repressive technologies piloted on Palestinians are deployed globally. Pegasus infections have been detected in at least 45 countries and counting.

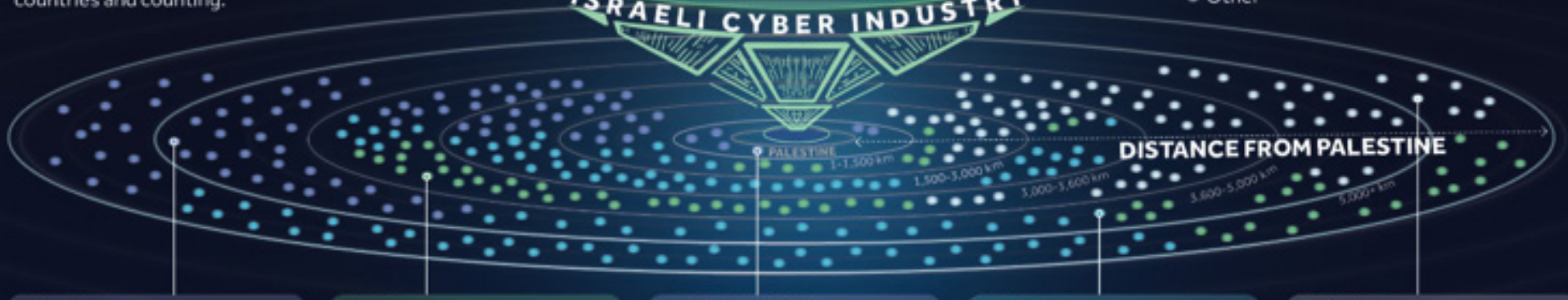
This visual shows a sample of

336 CASES OF PEOPLE IN 25 COUNTRIES

TARGETED BY PEGASUS SPYWARE EXPORTED BY THE ISRAELI GOVERNMENT

= 1 PERSON INFECTED BY PEGASUS

- Human Rights Defender
- Journalist
- Politician
- Other



TOGO
HUMAN RIGHTS DEFENDER
Targeted an anti-corruption activist fighting for constitutional and electoral reform

SPAIN
POLITICIAN
Targeted dozens of Catalan independence leaders. The Spanish Prime Minister & Defense Minister were also hacked

PALESTINE
HUMAN RIGHTS DEFENDER
Targeted human rights researchers at prominent organizations documenting Israeli war crimes

INDIA
JOURNALIST
Targeted human rights defenders and opponents of the Modi regime, including by planting false evidence on their devices

MEXICO
OTHER
Targeted the parent of one of 43 students kidnapped by police. Journalists & human rights defenders were the most frequent targets

VISUALIZINGPALESTINE

MIND THE GAP

SOURCES https://bit.ly/vp-pegasus
WWW.VISUALIZINGPALESTINE.ORG

@visualizingpal
/visualizing_palestine
fb.me/visualizingpalestine

AUG 2022

What is Spyware

Spyware is a new technology of espionage. By exploiting design flaws in phones and in computers (known as “zero-day loopholes” – security flaws unknown to developers), private companies have adapted military intelligence technology to spy on civilians. They are selling this technology to governments, police forces, intelligence units and possibly to non-government organizations such as corporations.

Spyware leaves no trace on hacked devices. This allows the customer to turn any smartphone into a bugging device by activating the microphone and camera remotely, to read materials on the phone (including entire messaging history, emails, social media), and even to write text and create files which appear to have been created by the phone’s owner.

In recent years, spyware has been used against human rights activists, journalists and lawyers, among others, to silence critical voices, destroy opposition parties and even to orchestrate the kidnapping, torture and assassinations of individuals. Evidence of spyware was found in the attempt to sabotage the investigation into the disappearance of 43 students in Mexico[1] and the killing of the journalist Jamal Khashoggi[2].

After Amnesty International exposed that over 50’000 phone numbers[3] were submitted to the Israeli spyware company NSO Group for hacking, computer analyst whistleblower Edward Snowden among many technology experts warned that until this technology is banned[4], it will easily spread and be used to target hundreds of millions of victims.

Why is Israel in the center of it all?

Israel is headquarters to more spyware companies than any other country in the world[5] including NICE (the spyware division of NICE was bought by Elbit Systems, Israel’s largest arms company), Verint, NSO Group, Black Cube, Candiru, Cytrox, Cellebrite and Intellexa.

These companies all boast that their technology has been taken directly from the Israeli military, and that the founders of these companies are graduates of Israeli intelligence units “8200”[6], “81”[7], and the Mossad[8].

This spyware technology was designed and tested as part of the Israeli occupation and apartheid regime in Palestine. It has been used to blackmail Palestinians into becoming collaborators. It has been used to sabotage the work of Palestinian civil society organizations who protect Palestinian human rights, and to silence attempts to hold Israeli security forces accountable for war crimes and crimes against humanity committed against Palestinians.[9]

Once the technology was successfully tested, Israeli spyware companies were authorized by the Israeli Ministry of Defense to sell the technology for profit. No less than 45 countries, including authoritarian regimes and leaders in Belarus, Brazil, Honduras, Hong Kong, Hungary, Russia, UAE, Uganda and more have bought it. Many countries around the world have access to spyware technology, but the State of Israel is actively selling it for profit.[10]

Why is spyware so dangerous?

Unlike police intelligence methods, spyware gives unrestricted power to anyone who uses it. There is no way to conduct a forensic analysis of the infected phone or computer in order to learn in what way it was tampered with. One can only learn that it was infected at some point in time. This allows individuals in law enforcement who have access to this technology to fabricate evidence, gathering information far beyond what a warrant allows and thus avoiding accountability.

Spyware companies argue that their technology is intended to fight terrorism and crime, but there is no evidence of any crime being prevented with the use of spyware.
In fact, once spyware has been used against a crime suspect, the very fact that the suspect’s devices have been hacked could serve as a defense that no evidence brought against the suspect can be trusted. Spyware does not help prevent terrorism and crime, but quite the opposite.

What must be done?

Spyware can affect any of us. The organizations which protect us from tyranny in civil society, in legal representation, in the media – are all vulnerable to spyware attacks. As customers of technology (when we buy phones and computers), we become vulnerable when spyware companies turn our devices against us and violate our privacy.

It is the job of our governments, legislative and judicial institutions to protect our safety and privacy and to ban the use of spyware. Phone manufacturers must be made accountable for the zero-day loopholes rather than be allowed to profit by selling them to spyware companies and then selling us, the customers, protective mechanisms or new phones to protect us from the security oversights which they themselves created.

In order to ban spyware we must:

- Build an intersectional movement. We must work together with those who have been attacked, activists, journalists, lawyers, civil rights defenders, those who are fighting for climate justice, gender equality, and migrant rights and those who are worried about the shrinking space of democracy and the violation of privacy.
- Inform the public about the dangers of spyware and demand action.[11]
- A simple ban is not enough. Steps must be taken to ensure that spyware cannot be profitable and that companies which produce and sell it, as well as the owners, management and employees of these companies, will be held accountable for the harm which they cause.

Together we will build campaigns on social media, shame the spyware companies and the tech companies which refuse to take responsibility for the zero-day vulnerabilities in their devices. Eventually, we will achieve a global ban on this harmful technology.

We demand:

- A global ban on the sale and use of spyware
- Phone manufacturers to be held accountable on the national and international levels for zero-day loopholes
- Spyware manufacturers to be held accountable for the use of their products

We will:

- Build a global, intersectional movement
- Run information campaigns to educate the public about the dangers of spyware
- Target spyware and tech companies which refuse to take responsibility
- Advocate to states, regional and global organisations to take action to ban spyware

For regular updates please visit: **https://bdsmovement.net/israeli-spyware-facilitates-human-rights-violations**

1 https://www.amnesty.org/en/latest/news/2022/08/disappearance-of-43-ayotzinapa-students/

2 https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/

3 https://forbiddenstories.org/about-the-pegasus-project/

4 https://www.inputmag.com/tech/snowden-calls-for-ban-on-spyware-following-nso-group-revelation

5 https://visualizingpalestine.medium.com/fact-sheet-the-israeli-cyber-industry-d2a64b43094

6 https://restofworld.org/2021/inside-israels-lucrative-and-secretive-cybersurveillance-talent-pipeline/

7 https://www.haaretz.com/israel-news/tech-news/2021-06-29/ty-article/idf-vs-nso-8200-battle-israel-cyber-talent-getting-dark/0000017f-da7d-d432-a77f-df7f77900000

8 https://www.timesofisrael.com/german-firm-acquires-ex-mossad-chiefs-cybersecurity-startup-for-700m/

9 https://visualizingpalestine.medium.com/fact-sheet-the-israeli-cyber-industry-d2a64b43094

10 Ibid.

11 https://www.amnesty.org/en/documents/doc10/4516/2021/en/

VISUALIZING**PALESTINE**

חרם! מבפנים
BOYCOTT!
From Within