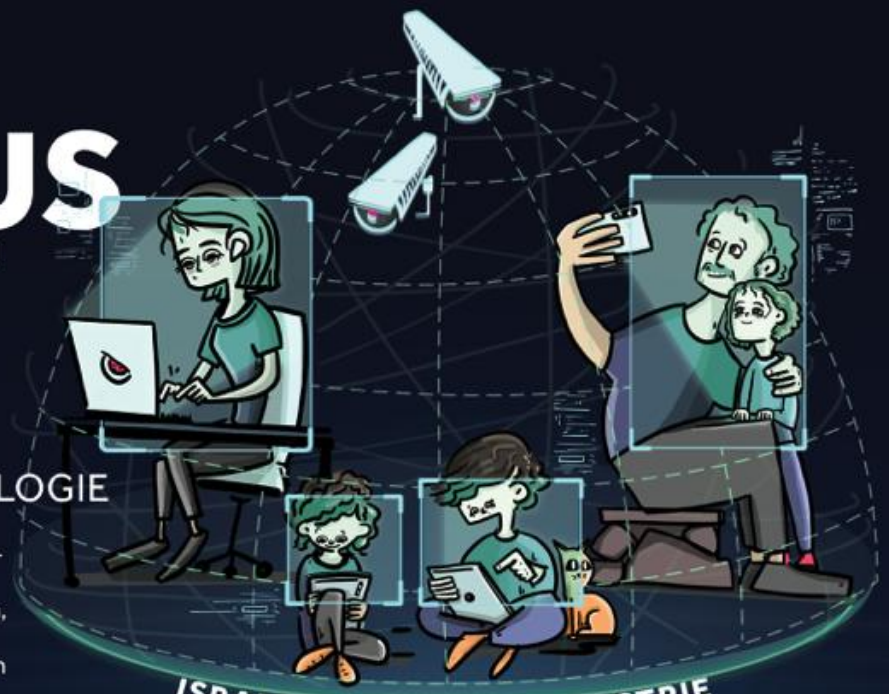
Israelische Spyware

Wie kann ein Produkt gestoppt werden, das unsere Rechte bedroht?

DER PEGASUS EFFEKT

DIE GLOBALEN AUSWIRKUNGEN DER ISRAELISCHEN ÜBERWACHUNGSTECHNOLOGIE

Das israelische Militär wirkt wie ein Brutkasten für den privaten Überwachungssektor. Die NSO-Gruppe, Produzent von Pegasus, dient hier als Fallstudie, die zeigt, wie repressive Technologien, erst an Palästinensern getestet, dann global eingesetzt werden. Pegasus-Infektionen wurden bis jetzt in mindestens 45 Ländern entdeckt.



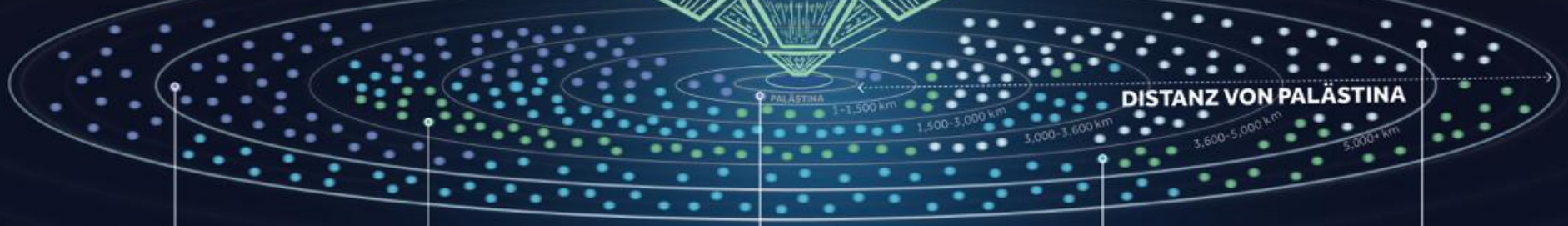
Der Clip zeigt einige der

336 FÄLLE VON MENSCHEN IN 25 LÄNDERN

DIE DAS ZIEL DER SPIONAGEWAFFE PEGASUS WURDEN. PEGASUS WIRD VON DER ISRAELISCHEN REGIERUNG EXPORTIERT

= 1 PERSON, VON PEGASUS BETROFFEN

- Menschenrechtsverteidiger
- Journalist
- Politiker/Regierungsvertreter
- Andere



TOGO
MENSCHENRECHTSVERTEIDIGER

Ziel war ein Antikorruptions-Aktivist, der sich für Verfassungs-und Wahlreformen einsetzt.

SPANIEN
POLITIKER

Dutzende Katalanen, Vertreter der Unabhängigkeitsbewegung, waren Ziel. Auch der spanische Premierminister und Verteidigungsminister wurden gehackt.

PALÄSTINA
MENSCHENRECHTSVERTEIDIGER

Ziel waren Menschenrechtsforscher bekannter Organisationen, die israelische Kriegsverbrechen dokumentieren.

INDIEN
JOURNALISTEN

Ziel waren Menschenrechtsverteidiger und Opponenten der Modi-Regierung, denen dabei auch fälschliche Informationen auf ihre Geräte gespielt worden sind.

MEXICO
ANDERE

Zielte auf Eltern von einem der 43 Studenten, die von der Polizei gekidnapped worden waren. Journalisten und Menschenrechtsverteidiger waren die häufigsten Ziele.

VISUALIZINGPALESTINE AL-HAQ MIND THE GAP

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

@visualizingpal
/visualizing_palestine
fb.me/visualizingpalestine

AUG 2022

Was ist Spyware?

Spyware ist eine neue Spionage-Technologie. Unter Ausnutzung von Konstruktionsfehlern in Telefonen und Computern (bekannt als «Zero-Day-Schlupflöcher» – Sicherheitslücken, die den Entwickler*innen nicht bekannt sind) haben private Unternehmen militärische Geheimdiensttechnologie angepasst, um Zivilistpersonen auszuspionieren. Sie verkaufen diese Technologie an Regierungen, Polizeikräfte, Nachrichtendienste und möglicherweise auch an nichtstaatliche Organisationen wie Unternehmen.

Spyware hinterlässt auf gehackten Geräten keine Spuren. Damit können die Kund*innen jedes Smartphone in ein Abhörgerät verwandeln, indem sie das Mikrofon und die Kamera aus der Ferne aktivieren, Einträge auf dem Telefon lesen (einschließlich des gesamten Nachrichtenverlaufs, der E-Mails und der Posts in sozialen Medien). Sie können sogar Texte schreiben und Dateien erstellen, die so aussehen, als seien sie von den Besitzer*innen des Telefons erstellt worden.

In den letzten Jahren wurde Spyware unter anderem gegen Menschenrechtsaktist*innen, Journalist*innen und Anwält*innen eingesetzt, um kritische Stimmen zum Schweigen zu bringen, Oppositionsparteien zu zerstören und sogar, um Entführung, Folter und Ermordung von Personen zu koordinieren. Beweise für Spyware wurden bei dem Versuch gefunden, die Recherchen im Zusammenhang mit dem Verschwinden von 43 Student*innen in Mexiko[1] und der Ermordung des Journalisten Jamal Khashoggi zu sabotieren[2].

Nachdem Amnesty International aufgedeckt hatte, dass über 50 000 Telefonnummern[3] an das israelische Softwareunternehmen NSO Group zum Hacken weitergegeben wurden, warnte neben vielen anderen Technologieexpert*innen der Computeranalytiker und Whistleblower Edward Snowden davor, dass sich diese Technologie, solange sie nicht verboten ist[4], leicht verbreiten und gegen Hunderte Millionen von Opfern eingesetzt werden wird.

Warum steht Israel im Zentrum des Geschehens?

In Israel haben mehr Spyware-Unternehmen ihren Firmensitz als in jedem anderen Land der Welt[5], darunter NICE (die Spyware-Abteilung von NICE wurde von Elbit Systems, Israels größtem Rüstungsunternehmen, aufgekauft), Verint, NSO Group, Black Cube, Candiru, Cytrox, Cellebrite und Intellexa.

Alle diese Unternehmen rühmen sich damit, dass sie ihre Technologie direkt vom israelischen Militär übernommen haben. Die Gründer*innen dieser Unternehmen sind Abgänger*innen der israelischen Geheimdiensteinheiten «8200»[6], «81»[7] und des Mossad[8].

Diese Spionagetechnologie wurde im Rahmen des israelischen Besatzungs- und Apartheidregimes in Palästina entwickelt und getestet. Sie wurde eingesetzt, um Palästinenser*innen zur Kollaboration zu erpressen. Sie wurde eingesetzt, um die Arbeit palästinensischer zivilgesellschaftlicher Organisationen zu untergraben, die die palästinensischen Menschenrechte schützen, und um Versuche zu unterbinden, israelische Sicherheitskräfte für Kriegsverbrechen und Verbrechen gegen die Menschlichkeit, die an Palästinenser*innen[9] begangen werden, zur Verantwortung zu ziehen.

Nach der erfolgreichen Testung der Technologie erteilt das israelische Verteidigungsministerium israelischen Spyware-Unternehmen die Genehmigung, die Technologie gewinnbringend zu verkaufen. Nicht weniger als 45 Länder, darunter autoritäre Regime und Staatsoberhäupter in Belarus, Brasilien, Honduras, Hongkong, Ungarn, Russland, den Vereinigten Arabischen Emiraten, Uganda und anderen Ländern, haben sie gekauft. Viele Länder auf der Welt haben Zugang zu Spionagetechnologie, aber der Staat Israel verkauft sie aktiv und gewinnbringend[10].

Warum ist Spyware so gefährlich?

Im Gegensatz zu den Methoden des polizeilichen Nachrichtendienstes gibt Spyware allen, die sie einsetzen, uneingeschränkte Macht. Es gibt keine

Möglichkeit, eine forensische Analyse eines infizierten Telefons oder Computers durchzuführen, um herauszufinden, auf welche Weise das Gerät manipuliert wurde. Man kann nur feststellen, dass das Gerät irgendwann infiziert wurde. Dies ermöglicht es Einzelnen in den Strafverfolgungsbehörden, die Zugang zu dieser Technologie haben, Beweise zu fälschen und Informationen zu sammeln, die weit über das hinausgehen, was ein Haftbefehl erlaubt, und sich damit der Verantwortung zu entziehen.

Die Spyware-Unternehmen argumentieren, dass ihre Technologie der Bekämpfung von Terrorismus und Kriminalität dient, aber es gibt keine Beweise dafür, dass durch den Einsatz von Spyware Verbrechen verhindert wurden.

Sobald Spyware gegen eine*n Verdächtige*n eingesetzt wurde, könnte die Tatsache, dass die Geräte der Verdächtigen gehackt wurden, als Argument dafür herhalten, dass den Beweisen, die gegen die Verdächtigen vorgelegt werden, nicht vertraut werden kann. Spionageprogramme tragen nicht zur Verhinderung von Terrorismus und Kriminalität bei, sondern bewirken genau das Gegenteil.

Was muss getan werden?

Spyware kann jede*n von uns treffen. Die Organisationen, die uns vor Tyrannei schützen – in der Zivilgesellschaft, als Rechtsbeistand, in den Medien – sind alle mögliche Ziele für Spyware-Angriffe. Als Kund*innen von Technologie (z.B. Telefon- und Computerkäufe) werden wir angreifbar, wenn Spyware-Unternehmen unsere Geräte gegen uns einsetzen und unsere Privatsphäre verletzen.

Es ist die Aufgabe unserer Regierungen, Parlamente und Justizorgane, unsere Sicherheit und Privatsphäre zu schützen und die Verwendung von Spyware zu verbieten. Telefonhersteller*innen müssen für die Zero-Day-Schlupflöcher verantwortlich gemacht werden, anstatt sie an Spyware-Unternehmen verkaufen zu dürfen, um uns als Kund*innen dann Schutzmechanismen oder neue Telefone zu verkaufen, die uns vor den Sicherheitslücken schützen sollen, die sie selbst geschaffen haben.

Um Spyware zu verbieten, müssen wir:

- eine intersektionelle Bewegung aufbauen. Wir müssen mit all jenen zusammenarbeiten, die angegriffen wurden, mit Aktivist*innen, Journa list*innen, Anwält*innen, Bürgerrechtler*innen, mit Menschen, die sich für Klimagerechtigkeit, Gleichstellung der Geschlechter und die Rechte von Migrant*innen einsetzen oder sich Sorgen über das Schrumpfen demokratischer Räume und die Verletzung der Privatsphäre machen;
- die Öffentlichkeit über die Gefahren von Spyware informieren und Maßnahmen fordern ;[11]
- über ein einfaches Verbot hinaus Schritte unternehmen, um sicherzustellen, dass mit Spyware keine Profite gemacht werden können und Hersteller, Verkäufer sowie die Eigentümer*innen, das Management und die Mitarbeiter*innen solcher Unternehmen für den Schaden, den sie verursachen, zur Verantwortung gezogen werden.

Gemeinsam werden wir Kampagnen in den sozialen Medien durchführen und Spyware- sowie Technologieunternehmen, die sich weigern, die Verantwortung für die Zero-Day-Schlupflöcher in ihren Geräten zu übernehmen, bloßstellen. Das letztliche Ziel ist die Durchsetzung eines weltweiten Verbots dieser schädlichen Technologie.

Wir fordern:

- ein weltweites Verbot des Verkaufs und der Verwendung von Spyware;
- dass Telefonhersteller*innen auf nationaler und internationaler Ebene für Zero-Day-Schlupflöcher zur Rechenschaft gezogen werden;
- dass Spyware-Hersteller*innen für die Verwendung ihrer Produkte zur Rechenschaft gezogen werden

Wir werden:

- eine globale, intersektionelle Bewegung aufbauen;
- Informationskampagnen durchführen, um die Öffentlichkeit über die Gefahren von Spyware aufzuklären;

- Spyware- und Technologieunternehmen, die sich weigern, Verantwortung zu übernehmen, ins Visier nehmen;
- uns dafür einsetzen, dass Staaten, regionale und globale Organisationen Maßnahmen zum Verbot von Spyware ergreifen.

Regelmäßige Updates finden sich auf: **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.haaretz.com/israel-news/tech-news/2021-06-29/ty-article/idf-vs-nso-8200-battle-is-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/