Coalition against Stalkerware

In November 2019, ten organizations (5 IT Security industry and 5 advocacy/non-profit organizations) launched the Coalition Against Stalkerware, a global initiative to provide support to survivors of domestic violence, to combat the use of stalkerware, and to work towards increasing public awareness about this issue. The Coalition's Founding partners include: Avira, Electronic Frontier Foundation, European Network for the Work with Perpetrators of Domestic Violence, G DATA, Kaspersky, Malwarebytes, National Network to End Domestic Violence, NortonLifeLock, Operation Safe Escape, and Weisser Ring. In its first year, the Coalition has more than doubled its membership to 26 partners, including other domestic violence advocacy and direct service organizations, additional IT security vendors, mobile security companies, privacy solutions providers, an association of technology journalists, and organizations focused on cyber safety.

What is stalkerware?

Stalkerware is commercially available software that enables a remote operator to monitor the activities on another user's device without their consent. It allows the operator to collect keystrokes, monitor messages, call information and GPS locations – all without the user's knowledge. It can often be used to abuse the privacy of current or former partners.

Stalkerware can be installed on both Android and iOS devices. There are also desktop versions of commercial spyware, but these are not particularly popular.

How pervasive is stalkerware?

The Coalition sees stalkerware as an increasing problem.

In 2019, **Kaspersky** detected a 67% increase of stalkerware on its users' mobile devices on a global level – compared to 2018. In 2020, the number of stalkerware installations worldwide during the first 10 months (from January to October) amounted to more than 48,500, which is close to the total of almost 52,000 the company observed over the same period in 2019.

According to **Malwarebytes** from January to end of June in 2020, monitor detections rose 780%, and spyware detections rose 1,677%.

There is no indication that stalkerware will be disappearing. Cybersecurity experts see incidents every day around the globe. In addition, recent UK survey ran by **Certo Software** shows that only 31% of people surveyed thought that spying on someone else's phone was illegal.

Findings of the Second National Survey on technology abuse and domestic violence in Australia ran in 2020 by **WESNET**, are that 99.3% of domestic violence practitioners have clients experiencing technology-facilitated abuse.

European Institute for Gender Equality research states that "seven in ten women (70%) who have experienced cyber stalking, have also experienced at least one form of physical or/and sexual violence from an intimate partner".

Coalition partners reported increases in domestic violence in Spring 2020, due to the COVID-19 lockdowns. In France, the **Centre Hubertine Auclert** said there was a 50% increase of calls to the main helpline for domestic violence victims. For India, the **Cyber Peace Foundation** states that 89% of the total number of cases registered to legal services authorities across the country were of domestic violence.

COALITION AGAINST STALKERWARE

The Coalition Against Stalkerware's Values and Objectives

The Coalition formed to facilitate bidirectional dialogue among those committed to protecting individuals from stalkerware and other forms of tech-enabled abuse. The Coalition's partners work to drive real outcomes through their collaboration, including:

- improving technical mitigation of stalkerware via creating consensus-based definition and detection criteria, developing a stalkerware sample and metadata information sharing mechanism for IT security vendors, other tech firms, academics, independent security researchers, etc.;
- providing technical assistance to organizations that support survivors of domestic violence;
- raising public awareness via hosting a number of events.

Our future plans

The Coalition's plans for its second year include:

Step #1	**Samples exchange:** Outreach to individuals and organizations that can contribute to the stalkerware sample/metadata information sharing mechanism
Step #2	**Technical capacity of NPOs:** Series of informational and technical assistance seminars to assist support organizations working with survivors of domestic violence and other individuals targeted by stalkerware
Step #3	**Policymakers:** Additional data collection to inform evidence-based policymaking to respond to threats posed by stalkerware
Step #4	**New partners**: Further expansion of the Coalition to include additional organizations globally to assist in the mission of combating stalkerware and protecting individuals

Links:
https://stopstalkerware.org

Interested in Becoming a Partner?

To become a new partner, please use the web form at the Coalition's web site: **stopstalkerware.org**/partners/become-partner/