They protect the law while breaking it: inside Europol's malware IT system

Europol's secret IT system was used to spy on journalists, lawyers and politicians across Europe, a Forbidden Stories investigation with Access Now and Citizen Lab has found.

Forbidden Stories, Access Now, Citizen Lab, Tech Policy Press, Mr Robot, Amnesty International

Europol, the European Union's law enforcement agency, has been secretly using its own internal IT system to spy on journalists, lawyers and politicians across Europe, a Forbidden Stories investigation with Access Now and Citizen Lab has found.

Europol's system, known as the Secure Information Exchange Network Application (SIENA), was used to deploy spyware against at least 11 people in 6 countries, including Germany, Spain, Poland, Romania, Slovenia and Lithuania. The spyware was deployed through Europol's own infrastructure, using its own servers, and was used to target people who had been in contact with Europol's Most Wanted Fugitives.

Europol's system was used to deploy spyware against at least 11 people in 6 countries, including Germany, Spain, Poland, Romania, Slovenia and Lithuania. The spyware was deployed through Europol's own infrastructure, using its own servers, and was used to target people who had been in contact with Europol's Most Wanted Fugitives.

The spyware was deployed through Europol's own infrastructure, using its own servers, and was used to target people who had been in contact with Europol's Most Wanted Fugitives.

The spyware was deployed through Europol's own infrastructure, using its own servers, and was used to target people who had been in contact with Europol's Most Wanted Fugitives.

The spyware was deployed through Europol's own infrastructure, using its own servers, and was used to target people who had been in contact with Europol's Most Wanted Fugitives.

A shadow IT environment

Europol's SIENA system was built to be a secure, encrypted messaging system for law enforcement officers across the EU. It was never designed to be a surveillance tool. But Europol's own internal documents show that it was used to deploy spyware against at least 11 people in 6 countries, including Germany, Spain, Poland, Romania, Slovenia and Lithuania. The spyware was deployed through Europol's own infrastructure, using its own servers, and was used to target people who had been in contact with Europol's Most Wanted Fugitives.

> Europol's SIENA system was built to be a secure, encrypted messaging system for law enforcement officers across the EU. It was never designed to be a surveillance tool. But Europol's own internal documents show that it was used to deploy spyware against at least 11 people in 6 countries, including Germany, Spain, Poland, Romania, Slovenia and Lithuania. The spyware was deployed through Europol's own infrastructure, using its own servers, and was used to target people who had been in contact with Europol's Most Wanted Fugitives.

The spyware was deployed through Europol's own infrastructure, using its own servers, and was used to target people who had been in contact with Europol's Most Wanted Fugitives.

The spyware was deployed through Europol's own infrastructure, using its own servers, and was used to target people who had been in contact with Europol's Most Wanted Fugitives.

The spyware was deployed through Europol's own infrastructure, using its own servers, and was used to target people who had been in contact with Europol's Most Wanted Fugitives.

Pressure to deliver

The spyware was deployed through Europol's own infrastructure, using its own servers, and was used to target people who had been in contact with Europol's Most Wanted Fugitives.